Microsoft

PRODUIT OFFICIEL DE FORMATION MICROSOFT

22414B

Implémentation d'une infrastructure Server avancée

Les informations contenues dans ce document, y compris les références à des adresses URL et à d'autres sites Web Internet, pourront faire l'objet de modifications sans préavis. Sauf mention contraire, les sociétés, produits, noms de domaines, adresses de messagerie, logos, personnes, lieux et événements utilisés dans les exemples sont fictifs et toute ressemblance avec des sociétés, produits, noms de domaines, adresses de messagerie, logos, personnes, lieux et événements réels est purement fortuite et involontaire. L'utilisateur est tenu d'observer la réglementation relative aux droits d'auteur applicable dans son pays. Aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système de restitution, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre) sans l'autorisation expresse et écrite de Microsoft Corporation.

Microsoft peut détenir des brevets, avoir déposé des demandes d'enregistrement de brevets ou être titulaire de marques, droits d'auteur ou autres droits de propriété intellectuelle portant sur tout ou partie des éléments qui font l'objet du présent document. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, la fourniture de ce document n'a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

Les noms de fabricants, de produits ou les URL sont fournis uniquement à titre indicatif et Microsoft ne fait aucune déclaration et exclut toute garantie légale, expresse ou implicite, concernant ces fabricants ou l'utilisation des produits avec toutes les technologies Microsoft. L'inclusion d'un fabricant ou produit n'implique pas l'approbation par Microsoft du fabricant ou du produit. Des liens vers des sites Web tiers peuvent être fournis. Ces sites ne sont pas sous le contrôle de Microsoft et Microsoft n'est pas responsable de leur contenu ni des liens qu'ils sont susceptibles de contenir, ni des modifications ou mises à jour de ces sites. Microsoft n'est pas responsable de la diffusion Web ou de toute autre forme de transmission reçue d'un site connexe. Microsoft fournit ces liens pour votre commodité, et l'insertion de n'importe quel lien n'implique pas l'approbation du site en question ou des produits qu'il contient par Microsoft.

© 2013 Microsoft Corporation. Tous droits réservés.

Microsoft et les marques commerciales figurant dans la page http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx sont des marques commerciales du groupe de sociétés Microsoft. Toutes les autres marques sont la propriété de leurs propriétaires respectifs.

Numéro de produit : 22414B

Numéro de référence : X18-86880

Date de publication : 8/2013

TERMES DU CONTRAT DE LICENCE MICROSOFT
COURS MICROSOFT AVEC FORMATEUR

Les présents termes du contrat de licence constituent un contrat entre Microsoft Corporation (ou en fonction du lieu où vous vivez, l'un de ses affiliés) et vous. Lisez-les attentivement. Ils portent sur votre utilisation du contenu qui accompagne le présent contrat, y compris le support sur lequel vous l'avez reçu, le cas échéant. Les présents termes de licence s'appliquent également au Contenu du Formateur et aux mises à jour et suppléments pour le Contenu Concédé sous Licence, à moins que d'autres termes n'accompagnent ces produits. ces derniers prévalent.

EN ACCÉDANT AU CONTENU CONCÉDÉ SOUS LICENCE, EN LE TÉLÉCHARGEANT OU EN L'UTILISANT, VOUS ACCEPTEZ CES TERMES. SI VOUS NE LES ACCEPTEZ PAS, N'ACCÉDEZ PAS AU CONTENU CONCÉDÉ SOUS LICENCE, NE LE TÉLÉCHARGEZ PAS ET NE L'UTILISEZ PAS.

Si vous vous conformez aux présents termes du contrat de licence, vous disposez des droits stipulés ci-dessous pour chaque licence acquise.

1. DÉFINITIONS.

a. « Centre de Formation Agréé » désigne un Membre du Programme Microsoft IT Academy ou un Membre Microsoft Learning Competency, ou toute autre entité que Microsoft peut occasionnellement désigner.

b. « Session de Formation Agréée » désigne le cours avec formateur utilisant le Cours Microsoft avec Formateur et mené par un Formateur ou un Centre de Formation Agréé.

c. « Dispositif de la Classe » désigne un (1) ordinateur dédié et sécurisé qu'un Centre de Formation Agréé possède ou contrôle, qui se trouve dans les installations de formation d'un Centre de Formation Agréé et qui répond ou est supérieur au niveau matériel spécifié pour le Cours Microsoft avec Formateur concerné.

d. « Utilisateur Final » désigne une personne qui est (i) dûment inscrite et participe à une Session de Formation Agréée ou à une Session de Formation Privée, (ii) un employé d'un membre MPN, ou (iii) un employé à temps plein de Microsoft.

e. « Contenu Concédé sous Licence » désigne le contenu qui accompagne le présent contrat et qui peut inclure le Cours Microsoft avec Formateur ou le Contenu du Formateur.

f. « Formateur Agréé Microsoft » ou « MCT » désigne une personne qui est (i) engagée pour donner une session de formation à des Utilisateurs Finaux au nom d'un Centre de Formation Agréé ou d'un Membre MPN, et (ii) actuellement Formateur Agréé Microsoft dans le cadre du Programme de Certification Microsoft.

g. « Cours Microsoft avec Formateur » désigne le cours avec formateur Microsoft qui forme des professionnels de l'informatique et des développeurs aux technologies Microsoft. Un Cours Microsoft avec Formateur peut être labellisé cours MOC, Microsoft Dynamics ou Microsoft Business Group.

h. « Membre du Programme Microsoft IT Academy » désigne un membre actif du Programme Microsoft IT Academy.

i. « Membre Microsoft Learning Competency » désigne un membre actif du programme Microsoft Partner Network qui a actuellement le statut Learning Competency.

j. « MOC » désigne le cours avec formateur « Produit de Formation Officiel Microsoft » appelé Cours Officiel Microsoft qui forme des professionnels de l'informatique et des développeurs aux technologies Microsoft.

k. « Membre MPN » désigne un membre actif Silver ou Gold du programme Microsoft Partner Network.

l. « Dispositif Personnel » désigne un (1) ordinateur, un dispositif, une station de travail ou un autre dispositif électronique numérique qui vous appartient ou que vous contrôlez et qui répond ou est supérieur au niveau matériel spécifié pour le Cours Microsoft avec Formateur concerné.

m. « Session de Formation Privée » désigne les cours avec formateur fournis par des Membres MPN pour des clients d'entreprise en vue d'enseigner un objectif de formation prédéfini à l'aide d'un Cours Microsoft avec Formateur. Ces cours ne font l'objet d'aucune publicité ni promotion auprès du grand public et la participation aux cours est limitée aux employés ou sous-traitants du client d'entreprise.

n. « Formateur » désigne (i) un formateur accrédité sur le plan académique et engagé par un Membre du Programme Microsoft IT Academy pour donner une Session de Formation Agréée et/ou (ii) un MCT.

o. « Contenu du Formateur » désigne la version du formateur du Cours Microsoft avec Formateur et tout contenu supplémentaire uniquement conçu à l'usage du Formateur pour donner une session de formation en utilisant le Cours Microsoft avec Formateur. Le Contenu du Formateur peut inclure des présentations Microsoft PowerPoint, un guide de préparation du formateur, des documents de formation du formateur, des packs Microsoft One Note, un guide de préparation de la classe et un formulaire préliminaire de commentaires sur le cours. À des fins de clarification, le Contenu du Formateur ne contient aucun logiciel, disque dur virtuel ni machine virtuelle.

2. DROITS D'UTILISATION. Le Contenu Concédé sous Licence n'est pas vendu. Le Contenu Concédé sous Licence est concédé sous licence sur la ***base d'une copie par utilisateur***, de sorte que vous devez acheter une licence pour chaque personne qui accède au Contenu Concédé sous Licence ou l'utilise.

2.1 Vous trouverez ci-dessous cinq sections de droits d'utilisation. Une seule vous est applicable.

a. **Si vous êtes un Membre du Programme Microsoft IT Academy :**

i. Chaque licence achetée en votre nom ne peut être utilisée que pour consulter une (1) copie du cours Microsoft avec Formateur sous la forme sous laquelle il vous a été fourni. Si le Cours Microsoft avec Formateur est en format numérique, vous êtes autorisé à installer une (1) copie sur un maximum de trois (3) Dispositifs Personnels. Vous n'êtes pas autorisé à installer le Cours Microsoft avec Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas.

ii. Pour chaque licence que vous achetez au nom d'un Utilisateur Final ou Formateur, vous êtes autorisé à :

1. distribuer une (1) version papier du Cours Microsoft avec Formateur à un (1) Utilisateur Final qui est inscrit à la Session de Formation Agréée et uniquement immédiatement avant le début de la Session de Formation Agréée qui est l'objet du Cours Microsoft avec Formateur fourni, **ou**
2. fournir à un (1) Utilisateur Final le code d'accès unique et les instructions permettant d'accéder à une (1) version numérique du Cours Microsoft avec Formateur, **ou**
3. fournir à un (1) Formateur le code d'accès unique et les instructions permettant d'accéder à un (1) Contenu Formateur,

pour autant que vous vous conformiez à ce qui suit :

iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,

iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,

v. vous veillerez à ce que chaque Utilisateur Final ayant reçu la version papier du Cours Microsoft avec Formateur reçoive une copie du présent contrat et reconnaisse que son utilisation du Cours Microsoft avec Formateur sera soumises aux termes du présent accord, et ce avant de lui fournir ledit Cours Microsoft avec Formateur. Chacun devra confirmer son acceptation du présent contrat d'une manière opposable aux termes de la réglementation locale avant d'accéder au Cours Microsoft avec Formateur,

vi. vous veillerez à ce que chaque Formateur donnant une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,

vii. vous n'utiliserez que des Formateurs qualifiés qui ont une connaissance et une expérience approfondies de la technologie Microsoft qui est l'objet du Cours Microsoft avec Formateur donné pour toutes vos Sessions de Formation Agréées.

viii. vous ne donnerez qu'un maximum de 15 heures de formation par semaine pour chaque Session de Formation Agréée qui utilise un cours MOC, et

ix. vous reconnaissez que les Formateurs qui ne sont pas MCT n'auront pas accès à l'ensemble des ressources destinées au formateur du Cours Microsoft avec Formateur.

b. **Si vous êtes un Membre du Microsoft Learning Competency :**

i. Chaque licence achetée en votre nom ne peut être utilisée que pour consulter une (1) copie du cours Microsoft avec Formateur sous la forme sous laquelle il vous a été fourni. Si le Cours Microsoft avec Formateur est en format numérique, vous êtes autorisé à installer une (1) copie sur un maximum de trois (3) Dispositifs Personnels. Vous n'êtes pas autorisé à installer le Cours Microsoft avec Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas.

ii. Pour chaque licence que vous achetez au nom d'un Utilisateur Final ou Formateur, vous êtes autorisé à :

1. distribuer une (1) version papier du Cours Microsoft avec Formateur à un (1) Utilisateur Final participant à la Session de Formation Agréée et uniquement immédiatement avant le début de la Session de Formation Agréée qui est l'objet du Cours Microsoft avec Formateur fourni, **ou**
2. fournir à un (1) Utilisateur Final participant à la Session de Formation Agréée le code d'accès unique et les instructions permettant d'accéder à une (1) version numérique du Cours Microsoft avec Formateur, **ou**
3. fournir à un (1) Formateur le code d'accès unique et les instructions permettant d'accéder à un (1) Contenu Formateur,

pour autant que vous vous conformiez à ce qui suit :

iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,

iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,

v. vous veillerez à ce que chaque Utilisateur Final ayant reçu une version papier du Cours Microsoft avec Formateur reçoive une copie du présent contrat et reconnaisse que son utilisation du Cours Microsoft avec Formateur sera soumise aux termes du présent accord, et ce avant de lui fournir ledit Cours Microsoft avec Formateur. Chacun devra confirmer son acceptation du présent contrat d'une manière opposable aux termes de la réglementation locale avant d'accéder au Cours Microsoft avec Formateur,
vi. vous veillerez à ce que chaque Formateur donnant une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,
vii. vous n'utiliserez que des Formateurs qualifiés qui possèdent la Certification Microsoft applicable qui est l'objet du Cours Microsoft avec Formateur donné pour vos Sessions de Formation Agréées,
viii. vous n'utiliserez que des MCT qualifiés qui possèdent également la Certification Microsoft applicable qui est l'objet du cours MOC donné pour toutes vos Sessions de Formation Agréées utilisant MOC,
ix. vous ne donnerez accès au Cours Microsoft avec Formateur qu'aux Utilisateurs Finaux, et
x. vous ne donnerez accès au Contenu du Formateur qu'aux Formateurs.

c. **Si vous êtes un Membre MPN :**

i. Chaque licence achetée en votre nom ne peut être utilisée que pour consulter une (1) copie du cours Microsoft avec Formateur sous la forme sous laquelle il vous a été fourni. Si le Cours Microsoft avec Formateur est en format numérique, vous êtes autorisé à installer une (1) copie sur un maximum de trois (3) Dispositifs Personnels. Vous n'êtes pas autorisé à installer le Cours Microsoft avec Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas.
ii. Pour chaque licence que vous achetez au nom d'un Utilisateur Final ou Formateur, vous êtes autorisé à :
    1. distribuer une (1) version papier du Cours Microsoft avec Formateur à un (1) Utilisateur Final participant à la Session de Formation Privée et uniquement immédiatement avant le début de la Session de Formation Privée qui est l'objet du Cours Microsoft avec Formateur fourni, **ou**
    2. fournir à un (1) Utilisateur Final qui participe à la Session de Formation Privée le code d'accès unique et les instructions permettant d'accéder à une (1) version numérique du Cours Microsoft avec Formateur, **ou**
    3. fournir à un (1) Formateur qui donne la Session de Formation Privée le code d'accès unique et les instructions permettant d'accéder à un (1) Contenu Formateur,

    pour autant que vous vous conformiez à ce qui suit :
iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,
iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Privée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Privée,
v. vous veillerez à ce que chaque Utilisateur Final ayant reçu une version papier du Cours Microsoft avec Formateur reçoive une copie du présent contrat et reconnaisse que son utilisation du Cours Microsoft avec Formateur sera soumise aux termes du présent accord, et ce avant de lui fournir ledit Cours Microsoft avec Formateur. Chacun devra confirmer son acceptation du présent contrat d'une manière opposable aux termes de la réglementation locale avant d'accéder au Cours Microsoft avec Formateur,

vi. vous veillerez à ce que chaque Formateur donnant une Session de Formation Privée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Privée,
vii. vous n'utiliserez que des Formateurs qualifiés qui possèdent la Certification Microsoft applicable qui est l'objet du Cours Microsoft avec Formateur donné pour toutes vos Sessions de Formation Privées,
viii. vous n'utiliserez que des MCT qualifiés qui possèdent la Certification Microsoft applicable qui est l'objet du cours MOC donné pour toutes vos Sessions de Formation Privées utilisant MOC,
ix. vous ne donnerez accès au Cours Microsoft avec Formateur qu'aux Utilisateurs Finaux, et
x. vous ne donnerez accès au Contenu du Formateur qu'aux Formateurs.

d. **Si vous êtes un Utilisateur Final :**
Pour chaque licence que vous achetez, vous êtes autorisé à utiliser le Cours Microsoft avec Formateur exclusivement pour votre formation personnelle. Si le Cours Microsoft avec Formateur est en format numérique, vous pouvez y accéder en ligne à l'aide du code d'accès unique que vous a fourni le prestataire de formation et installer et utiliser une (1) copie du Cours Microsoft avec Formateur sur un maximum de trois (3) Dispositifs Personnels. Vous êtes également autorisé à imprimer une (1) copie du Cours Microsoft avec Formateur. Vous n'êtes pas autorisé à installer le Cours Microsoft avec Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas.

e. **Si vous êtes un Formateur :**
i. Pour chaque licence que vous achetez, vous êtes autorisé à installer et utiliser une (1) copie du Contenu du Formateur sous la forme dans laquelle il vous a été fourni sur un (1) Dispositif Personnel exclusivement pour préparer et donner une Session de Formation Agréée ou une Session de Formation Privée, et à installer une (1) copie supplémentaire sur un autre Dispositif Personnel comme copie de sauvegarde, utilisable uniquement pour réinstaller le Contenu du Formateur. Vous n'êtes pas autorisé à installer ou utiliser une copie du Contenu du Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas. Vous êtes également autorisé à imprimer une (1) copie du Contenu du Formateur uniquement pour préparer et assurer une Session de Formation Agréée ou une Session de Formation Privée.
ii. Vous pouvez personnaliser les parties écrites du Contenu du Formateur qui sont logiquement associées à la présentation d'une session de formation conformément à la version la plus récente du contrat MCT. Si vous choisissez d'exercer les droits qui précèdent, vous acceptez de vous conformer à ce qui suit : (i) les personnalisations ne peuvent être utilisées que pour donner des Sessions de Formation Agréées et des Sessions de Formation Privées, et (ii) toutes les personnalisations seront conformes au présent contrat. À des fins de clarté, toute utilisation de « *personnaliser* » ne fait référence qu'à la modification de l'ordre des diapositives et du contenu, et/ou à la non-utilisation de l'ensemble du contenu ou des diapositives, et ne signifie pas le changement ou la modification d'aucune diapositive ni d'aucun contenu.

2.2 **Dissociation de composants.** Le Contenu Concédé sous Licence est concédé sous licence en tant qu'unité unique et vous n'êtes pas autorisé à dissocier les composants ni à les installer sur différents dispositifs.

2.3 **Redistribution du Contenu Concédé sous Licence.** Sauf stipulation contraire expresse dans les droits d'utilisation ci-dessus, vous n'êtes pas autorisé à distribuer le Contenu Concédé sous Licence ni aucune partie de celui-ci (y compris les éventuelles modifications autorisées) à des tiers sans l'autorisation expresse et écrite de Microsoft.

2.4 **Programmes et Services Tiers.** Le Contenu Concédé sous Licence peut contenir des programmes ou services tiers. Les présents termes du contrat de licence s'appliqueront à votre utilisation de ces programmes ou services tiers, excepté si d'autres termes accompagnent ces programmes et services.

2.5 **Conditions supplémentaires.** Le Contenu Concédé sous Licence est susceptible de contenir des composants auxquels s'appliquent des termes, conditions et licences supplémentaires en termes d'utilisation. Les termes non contradictoires desdites conditions et licences s'appliquent également à votre utilisation du composant correspondant et complètent les termes décrits dans le présent contrat.

3. CONTENU CONCÉDÉ SOUS LICENCE BASÉ SUR UNE TECHNOLOGIE PRÉCOMMERCIALE. Si l'objet du Contenu Concédé sous Licence est basé sur une version précommerciale d'une technologie Microsoft (« **version précommerciale** »), les présents termes s'appliquent en plus des termes de ce contrat :

a. **Contenu sous licence en version précommerciale**. L'objet du présent Contenu Concédé sous Licence est basé sur la version précommerciale de la technologie Microsoft. La technologie peut ne pas fonctionner comme une version finale de la technologie et nous sommes susceptibles de modifier cette technologie pour la version finale. Nous sommes également autorisés à ne pas éditer de version finale. Le Contenu Concédé sous Licence basé sur la version finale de la technologie est susceptible de ne pas contenir les mêmes informations que le Contenu Concédé sous Licence basé sur la version précommerciale. Microsoft n'a aucune obligation de vous fournir quelque autre contenu, y compris du Contenu Concédé sous Licence basé sur la version finale de la technologie.

b. **Commentaires**. Si vous acceptez de faire part à Microsoft de vos commentaires concernant le Contenu Concédé sous Licence, directement ou par l'intermédiaire de son représentant tiers, vous concédez à Microsoft, gratuitement, le droit d'utiliser, de partager et de commercialiser vos commentaires de quelque manière et à quelque fin que ce soit. Vous concédez également à des tiers, à titre gratuit, tout droit de propriété sur leurs produits, technologies et services, nécessaires pour utiliser ou interfacer des parties spécifiques d'un logiciel, produit ou service Microsoft qui inclut les commentaires. Vous ne donnerez pas d'informations faisant l'objet d'une licence qui impose à Microsoft de concéder sous licence son logiciel, ses technologies ou produits à des tiers parce que nous y incluons vos commentaires. Ces droits survivent au présent contrat.

c. **Durée de la Version Précommerciale**. Si vous êtes un Membre du Programme Microsoft IT Academy, un Membre Microsoft Learning Competency, un Membre MPN ou un Formateur, vous cesserez d'utiliser toutes les copies du Contenu Concédé sous Licence basé sur la technologie précommerciale (i) à la date que Microsoft vous indique comme date de fin d'utilisation du Contenu Concédé sous Licence basé sur la technologie précommerciale, ou (ii) soixante (60) jours après la mise sur le marché de la technologie qui fait l'objet du Contenu Concédé sous Licence, selon la date la plus proche (« **Durée de la Version Précommerciale** »). Dès l'expiration ou la résiliation de la durée de la version précommerciale, vous supprimerez définitivement et détruirez toutes les copies du Contenu Concédé sous Licence en votre possession ou sous votre contrôle.

4. **CHAMP D'APPLICATION DE LA LICENCE.** Le Contenu Concédé sous Licence n'est pas vendu. Le présent contrat ne fait que vous conférer certains droits d'utilisation du Contenu Concédé sous Licence. Microsoft se réserve tous les autres droits. Sauf si la réglementation applicable vous confère d'autres droits, nonobstant la présente limitation, vous n'êtes autorisé à utiliser le Contenu Concédé sous Licence qu'en conformité avec les termes du présent contrat. Ce faisant, vous devez vous conformer aux restrictions techniques contenues dans le Contenu Concédé sous Licence qui ne vous permettent de l'utiliser que d'une certaine façon. Sauf stipulation expresse dans le présent contrat, vous n'êtes pas autorisé à :
   - accéder au Contenu Concédé sous Licence ou à y autoriser l'accès à quiconque qui n'a pas acheté une licence valide du Contenu Concédé sous Licence,
   - modifier, supprimer ou masquer les mentions de droits d'auteur ou autres notifications de protection (y compris les filigranes), marques ou identifications contenue dans le Contenu Concédé sous Licence,
   - modifier ou créer une œuvre dérivée d'un Contenu Concédé sous Licence,
   - présenter en public ou mettre à disposition de tiers le Contenu Concédé sous Licence à des fins d'accès ou d'utilisation,
   - copier, imprimer, installer, vendre, publier, transmettre, prêter, adapter, réutiliser, lier ou publier, mettre à disposition ou distribuer le Contenu Concédé sous Licence à un tiers,
   - contourner les restrictions techniques contenues dans Contenu Concédé sous Licence, ou
   - reconstituer la logique, décompiler, supprimer ou contrecarrer des protections, ou désassembler le Contenu Concédé sous Licence, sauf dans la mesure où ces opérations seraient expressément permises par les termes du contrat de licence ou la réglementation applicable nonobstant la présente limitation.

5. **DROITS RÉSERVÉS ET PROPRIÉTÉ.** Microsoft se réserve tous les droits qui ne vous sont pas expressément concédés dans le présent contrat. Le Contenu Concédé sous Licence est protégé par les lois et les traités internationaux en matière de droits d'auteur et de propriété intellectuelle. Les droits de propriété, droits d'auteur et autres droits de propriété intellectuelle sur le Contenu Concédé sous Licence appartiennent à Microsoft ou à ses fournisseurs.

6. **RESTRICTIONS À L'EXPORTATION.** Le Contenu Concédé sous Licence est soumis aux lois et réglementations américaines en matière d'exportation. Vous devez vous conformer à toutes les lois et réglementations nationales et internationales en matière d'exportation applicables au Contenu Concédé sous Licence. Ces lois comportent des restrictions sur les utilisateurs finals et les utilisations finales. Des informations supplémentaires sont disponibles sur le site www.microsoft.com/exporting.

7. **SERVICES D'ASSISTANCE TECHNIQUE.** Dans la mesure où le Contenu Concédé sous Licence est fourni « en l'état », nous ne fournissons pas de services d'assistance technique.

8. **RÉSILIATION.** Sans préjudice de tous autres droits, Microsoft pourra résilier le présent contrat si vous n'en respectez pas les conditions générales. Dès la résiliation du présent contrat pour quelque raison que ce soit, vous arrêterez immédiatement toute utilisation et détruirez toutes les copies du Contenu Concédé sous Licence en votre possession ou sous votre contrôle.

9. **LIENS VERS DES SITES TIERS.** Vous êtes autorisé à utiliser le Contenu Concédé sous Licence pour accéder à des sites tiers. Les sites tiers ne sont pas sous le contrôle de Microsoft et Microsoft n'est pas responsable du contenu de ces sites, des liens qu'ils contiennent ni des modifications ou mises à jour qui leur sont apportées. Microsoft n'est pas responsable du Webcasting ou de toute autre forme de transmission reçue d'un site tiers. Microsoft fournit ces liens vers des sites tiers pour votre commodité uniquement et l'insertion de tout lien n'implique pas l'approbation du site en question par Microsoft.

10. **INTÉGRALITÉ DES ACCORDS.** Le présent contrat et les éventuelles conditions supplémentaires pour le Contenu du Formateur, les mises à jour et les suppléments constituent l'intégralité des accords en ce qui concerne le Contenu Concédé sous Licence, les mises à jour et les suppléments.

11. **RÉGLEMENTATION APPLICABLE.**

    a. États-Unis. Si vous avez acquis le Contenu Concédé sous Licence aux États-Unis, les lois de l'État de Washington, États-Unis d'Amérique, régissent l'interprétation de ce contrat et s'appliquent en cas de réclamation ou d'actions en justice pour rupture dudit contrat, sans donner d'effet aux dispositions régissant les conflits de lois. Les lois du pays dans lequel vous vivez régissent toutes les autres réclamations, notamment les réclamations fondées sur les lois fédérales en matière de protection des consommateurs, de concurrence déloyale et de délits.

    b. En dehors des États-Unis. Si vous avez acquis le Contenu Concédé sous Licence dans un autre pays, les lois de ce pays s'appliquent.

12. **EFFET JURIDIQUE.** Le présent contrat décrit certains droits légaux. Vous pouvez bénéficier d'autres droits prévus par les lois de votre État ou pays. Vous pouvez également bénéficier de certains droits à l'égard de la partie auprès de laquelle vous avez acquis le Contenu Concédé sous Licence. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre État ou pays si celles-ci ne le permettent pas.

13. **EXCLUSIONS DE GARANTIE. LE CONTENU CONCÉDÉ SOUS LICENCE EST FOURNI « EN L'ÉTAT » ET « TEL QUE DISPONIBLE ». VOUS ASSUMEZ TOUS LES RISQUES LIÉS À SON UTILISATION. MICROSOFT ET SES AFFILIÉS RESPECTIFS N'ACCORDENT AUCUNE GARANTIE OU CONDITION EXPRESSE. VOUS POUVEZ BÉNÉFICIER DE DROITS SUPPLÉMENTAIRES RELATIFS AUX CONSOMMATEURS EN VERTU DU DROIT DE VOTRE PAYS, QUE CE CONTRAT NE PEUT MODIFIER. LORSQUE CELA EST AUTORISÉ PAR LE DROIT LOCAL, MICROSOFT ET SES AFFILIÉS RESPECTIFS EXCLUENT TOUTES GARANTIES IMPLICITES DE QUALITÉ, D'ADÉQUATION À UN USAGE PARTICULIER ET D'ABSENCE DE VIOLATION.**

14. **LIMITATION ET EXCLUSION DE RECOURS ET DE DOMMAGES. VOUS POUVEZ OBTENIR DE MICROSOFT, DE SES AFFILIÉS RESPECTIFS ET DE SES FOURNISSEURS UNE INDEMNISATION EN CAS DE DOMMAGES DIRECTS LIMITÉE À U.S. $5.00. VOUS NE POUVEZ PRÉTENDRE À AUCUNE INDEMNISATION POUR LES AUTRES DOMMAGES, Y COMPRIS LES DOMMAGES SPÉCIAUX, INDIRECTS, INCIDENTS OU ACCESSOIRES ET LES PERTES DE BÉNÉFICES.**

    Cette limitation concerne :
    - toute affaire liée au Contenu Concédé sous Licence, au logiciel, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers ; et
    - les réclamations pour rupture de contrat ou violation de garantie, les réclamations en cas de responsabilité sans faute, de négligence ou autre délit dans la limite autorisée par la loi en vigueur.

    Elle s'applique également même si Microsoft connaissait l'éventualité d'un tel dommage. La limitation ou l'exclusion ci-dessus peut également ne pas vous être applicable si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages incidents, indirects ou de quelque nature que ce soit.

Dernière mise à jour : septembre 2012.

Bienvenue !

Merci de suivre notre formation. En collaboration avec nos sites Microsoft Certified Partners for Learning Solutions et nos centres Microsoft IT Academy, nous avons élaboré des formations de premier plan aussi bien destinées aux informaticiens souhaitant approfondir leurs connaissances qu'aux étudiants se destinant à une carrière informatique.

- **Formateurs et instructeurs Microsoft Certified**—Votre instructeur possède des compétences techniques et pédagogiques. Il répond aux exigences actuelles en matière de certification. En outre, si les instructeurs dispensent des formations sur l'un de nos sites Certified Partners for Learning Solutions, ils sont également évalués tout au long de l'année par les stagiaires et par Microsoft.
- **Avantages des examens de certification**—À l'issue d'une formation, pensez aux examens de certification Microsoft. Les certifications Microsoft valident vos compétences en matière de technologies Microsoft et peuvent faire la différence lors d'une recherche d'emploi ou pour faire progresser votre carrière. Une étude IDC indépendante a conclu que pour 75 % des responsables, les certifications sont importantes pour les performances des équipes1. Renseignez-vous auprès de votre instructeur pour connaître les promotions et remises auxquels vous pourriez avoir droit sur les examens de certification Microsoft.
- **Garantie de satisfaction du client**—Nos Certified Partners for Learning Solutions offrent une garantie de satisfaction et engagent leur responsabilité à ce sujet. À la fin du cours, nous vous demandons de bien vouloir remplir un formulaire d'évaluation sur votre expérience du jour. Vos commentaires sont les bienvenus !

Nous vous souhaitons une agréable formation et une carrière couronnée de succès.

Cordialement,

Microsoft Learning
www.microsoft.com/france/formation

Microsoft | Learning

[1] *IDC*, Value of Certification: Team Certification and Organizational Performance, *novembre 2006*

Remerciements

Formation Microsoft souhaite reconnaître la contribution apportée par les personnes citées ci-dessous à l'élaboration de ce titre et les en remercier. Elles ont en effet déployé des efforts aux différents stades de ce processus pour vous proposer une expérience de qualité en classe.

Stan Reimer : expert technique

Stan Reimer est président de S. R. Technical Services Inc et travaille comme consultant, instructeur et auteur. Stan bénéficie d'une expérience approfondie en matière de conseil sur les déploiements Active Directory® et Exchange Server pour certaines des plus grandes entreprises du Canada. Stan est le principal auteur de deux ouvrages Active Directory pour Microsoft Press® Press®. Au cours des neuf dernières années, Stan a écrit des cours pour la Formation Microsoft, en se spécialisant dans les cours Active Directory et Exchange Server. Stan est instructeur certifié par Microsoft (MCT) depuis plus de 12 ans.

Conan Kezema : expert technique

Conan Kezema, titulaire d'une licence d'enseignement, certifié MCSA (Microsoft Certified Solutions Associate) et instructeur certifié par Microsoft (MCT), est un éducateur, consultant, architecte de systèmes de réseau et auteur spécialiste en technologies Microsoft. En tant qu'associé de S.R. Technical Services, Conan est un expert technique, concepteur pédagogique et auteur de nombreux projets de développement de cours Microsoft.

Andy Schan : expert technique

Andy Schan est consultant en infrastructure informatique et auteur, et a 15 années d'expérience dans le domaine de l'architecture et du déploiement des technologies Microsoft pour les utilisateurs professionnels, principalement avec Microsoft Exchange (à commencer par Exchange 4.0 et MS Mail), Windows Server® (à commencer par Windows NT 3.51), et est expert en technologies de gestion d'identité et d'accès, notamment avec les services de domaine Active Directory (AD DS), les services Active Directory Rights Management Services (AD RMS), les services Active Directory Federation Services (AD FS) et le Gestionnaire d'identités Microsoft Forefront®. Il est co-auteur du livre Microsoft Exchange Server 2010 Best Practices publié par Microsoft Press, ainsi qu'un guide d'étude Exchange Server 2007 publié par Sybex. Andy a conçu et mis en œuvre certains des plus vastes déploiements de services RMS dans le monde, et a participé à une étude de cas AD RMS publiée par Microsoft. Il a également participé à la conférence NetPro Directory Experts ainsi qu'à la conférence The Experts de Quest sur les déploiements AD RMS à grande échelle et la personnalisation d'AD RMS. Il a également conçu et déployé des services AD FS pour d'importants clients des secteurs privé et public, notamment dans le cadre du Technology Adoption Program pour Windows Server 2008 de Microsoft. Andy est actuellement employé par Microsoft Consulting Services en tant que consultant en matière d'infrastructure.

Vladimir Meloski : expert technique

Vladimir est MCT, membre du programme Microsoft MVP (Most Valuable Professional) sur Exchange Server et consultant en solutions d'infrastructures et communications unifiées basées sur Microsoft Exchange Server, Microsoft Lync® Server et Microsoft System Center. Vladimir a 16 ans d'expérience professionnelle en informatique et a participé à des conférences Microsoft en Europe et aux États-Unis en tant que présentateur, modérateur, surveillant d'ateliers pratiques et expert technique. Il a également travaillé en tant qu'expert technique et réviseur technique pour plusieurs cours MOC (Microsoft Official Curriculum).

Dave Franklyn : expert technique

Dave Franklyn, MCT, certifié MCSE (Microsoft Certified Solutions Expert), MCITP (Microsoft Certified IT Professional) et MVP Windows Expert-It Pro Microsoft, est formateur et consultant expérimenté en technologies de l'information à l'université d'Auburn à Montgomery en Alabama. Il enseigne depuis 15 ans. Il travaille avec des ordinateurs depuis 1976, à l'époque où il a commencé sa carrière dans les systèmes mainframe. Il est passé très tôt dans le domaine des réseaux. Avant de rejoindre l'université d'Auburn, il a passé 22 ans dans l'US Air Force en tant qu'expert en communications électroniques et systèmes informatiques et a pris sa retraite en 1998. Il est président du groupe Windows des professionnels de l'informatique de Montgomery.

Ronnie Isherwood : expert technique

Ronnie Isherwood, MCITP, MCT, membre de la British Computer Society (MBCS), travaille dans le secteur de l'informatique depuis plus de 15 ans. Il a 13 ans d'expérience professionnelle en tant qu'ingénieur système et consultant en solutions basées sur serveur. En outre, il a huit ans d'expérience professionnelle dans les technologies de virtualisation. Il a contribué à plusieurs programmes éducatifs de la communauté System Center, a participé aux événements de la communauté Microsoft Private Cloud, aux phases bêta du programme de formation Microsoft et a été orateur à la conférence E2E sur la virtualisation. Il a pour passion technologique la virtualisation et sa gestion. Ronnie est co-fondateur d'un groupe d'utilisateurs local de Windows et membre du comité de l'institut agréé d'informatique. Avant de devenir ingénieur système, il a appris la programmation en Basic et en Microsoft Visual Basic®, et a offert des solutions pour le secteur des services financiers.

Telmo Sampaio : expert technique

Telmo Sampaio est Geek en chef à MCTrainer.NET à Miami, Floride. Il est spécialiste de System Center, Microsoft SharePoint®, Microsoft SQL, et .NET. Telmo a écrit sa première application en 1984, avec l'idée de démontrer des principes physiques à ses camarades de classe. Sa passion pour la technologie et l'enseignement a fait de lui un développeur autodidacte depuis l'enfance. En 1989, il a déménagé à Wellesley au Massachussetts, lorsque son père a été transféré pour un an à Boston dans le cadre de son travail. Il a continué de développer des applications pour démontrer des concepts physiques et mathématiques, et a décidé de demeurer aux États-Unis après le départ de sa famille. En 1991, il est rentré au Brésil a étudié l'analyse des systèmes à l'université Pontif'cia Universidade Católica de Rio de Janeiro. Lorsque Microsoft étendit son programme MCP au Brésil, Telmo fut l'une des premières personnes certifiées dans son pays. Il a commencé à assurer des cours Microsoft en 1994. Il en est venu rapidement à diriger le plus important centre de formation d'Amérique latine. Jusqu'à présent, il a été certifié dans plus de 20 produits Microsoft différents au terme de plus de 80 examens. Après être retourné aux États-Unis en 2003, Telmo est devenu contributeur à plusieurs examens de certification Microsoft, auteur pour les cours et manuels officiels, et orateur lors d'événements tels que TechEd, PASS et MMS. Telmo habite à Miami en Floride avec son épouse Joanne et passe ses week-ends avec ses trois garçons : Marco, Rafael et Enzo. Du moins quand il n'est pas en voyage autour du monde pour assurer des formations.

Damir Dizdarevic : expert technique et développeur de contenu

Damir Dizdarevic est MCT, MCSE, MCTS, et MCITP (Microsoft Certified Information Technology Professional). Il est l'un des responsables et instructeurs du centre de formation de Logosoft d.o.o. (Sarajevo, Bosnie-Herzégovine). Damir a plus de 17 années d'expérience en matière de plateformes Microsoft et il est spécialiste de Windows Server, d'Exchange Server, de la sécurité et de la virtualisation. Il a travaillé en tant qu'expert technique et réviseur technique sur de nombreux cours MOC et a publié plus de 400 articles dans différents magazines informatiques tels que Windows ITPro et INFO Magazine. Il intervient aussi fréquemment et avec brio dans la plupart des conférences Microsoft en Europe de l'Est. En outre, il est membre du programme Microsoft MVP pour la gestion de l'infrastructure de Windows Server.

Christian Booth : réviseur technique

Christian Booth est MCSE : Cloud privé, MCTS dans de nombreux produits et MCITP : EA ; il est directeur et architecte en chef à Denali Advanced Integration à Redmond dans l'État de Washington. Christian a plus de 16 années d'expérience en matière de plateformes Microsoft et il est spécialiste de System Center, de Windows Server et de virtualisation. Christian a travaillé en tant qu'expert technique, auteur d'éléments d'examen, concepteur de formation et réviseur technique sur de nombreux cours Microsoft MOC. Il intervient aussi fréquemment et avec brio dans la plupart des conférences Microsoft et partenaires dans l'Ouest des États-Unis, où il partage ses connaissances dans le domaine de System Center et de la virtualisation. Christian facilite à ses clients l'accès en profondeur aux technologies de Microsoft, développe des formations, dirige le Groupe d'utilisateur du cloud privé et tient un blog sur des sujets liés à System Center. Il est également MVP en System Center Cloud et Gestion de centres de données.

Sommaire

Module 1 : Vue d'ensemble de la gestion dans un centre de données d'entreprise

Leçon 1: Vue d'ensemble du centre de données d'entreprise 1-2
Leçon 2: Vue d'ensemble des composants de Microsoft System Center 2012 1-14
Atelier pratique : Éléments à prendre en compte pour implémenter un centre de données d'entreprise 1-29

Module 2 : Planification et implémentation d'une stratégie de virtualisation de serveur

Leçon 1 : Planification d'un déploiement VMM 2-2
Leçon 2 : Planification et implémentation d'un environnement hôte de virtualisation de serveur 2-11
Atelier pratique : Planification et implémentation d'une stratégie de virtualisation de serveur 2-23

Module 3 : Planification et implémentation des réseaux et du stockage pour la virtualisation

Leçon 1 : Planification d'une infrastructure de stockage pour la virtualisation 3-2
Leçon 2 : Implémentation d'une infrastructure de stockage pour la virtualisation 3-12
Leçon 3 : Planification et implémentation d'une infrastructure réseau pour la virtualisation 3-19
Atelier pratique : Planification et implémentation des réseaux et du stockage de virtualisation 3-33

Module 4 : Planification et déploiement d'ordinateurs virtuels

Leçon 1 : Planification de la configuration des ordinateurs virtuels 4-2
Leçon 2 : Préparation aux déploiements d'ordinateurs virtuels avec VMM 4-18
Leçon 3 : Déploiement d'ordinateurs virtuels 4-31
Atelier pratique : Planification et implémentation d'une stratégie de déploiement et de gestion d'ordinateurs virtuels 4-42

Module 5 : Planification et implémentation d'une solution d'administration de la virtualisation

Leçon 1 : Planification et implémentation de l'automatisation de System Center 2012 5-2
Leçon 2 : Planification et implémentation de l'administration de System Center 2012 5-10
Leçon 3 : Planification et implémentation des options de libre-service dans System Center 2012 5-17
Atelier pratique : Planification et implémentation d'une solution d'administration pour la virtualisation 5-24

Module 6 : Planification et implémentation d'une stratégie d'analyse des serveurs

Leçon 1 : Planification de l'analyse dans Windows Server 2012 **6-2**
Leçon 2 : Vue d'ensemble de System Center Operations Manager **6-11**
Leçon 3 : Planification et configuration de packs d'administration **6-27**
Leçon 4 : Planification et configuration des notifications et de la création de rapports **6-34**
Leçon 5 : Configuration de l'intégration à VMM **6-40**
Atelier pratique : Implémentation d'une stratégie d'analyse des serveurs **6-47**

Module 7 : Planification et implémentation d'une haute disponibilité pour des services et des applications de fichiers

Leçon 1 : Planification et implémentation d'espaces de stockage **7-2**
Leçon 2 : Planification et implémentation du système de fichiers DFS **7-8**
Leçon 3 : Planification et implémentation du système de fichiers NLB **7-16**
Atelier pratique : Planification et implémentation d'une haute disponibilité pour des services et des applications de fichiers **7-21**

Module 8 : Planification et implémentation d'une infrastructure haute disponibilité à l'aide du clustering avec basculement

Leçon 1 : Planification d'une infrastructure pour le clustering avec basculement **8-2**
Leçon 2 : Implémentation du clustering avec basculement **8-13**
Leçon 3 : Intégration du clustering avec basculement avec la virtualisation de serveur **8-21**
Leçon 4 : Planification d'un cluster de basculement multisite **8-34**
Atelier pratique : Planification et implémentation d'une infrastructure hautement disponible à l'aide du clustering avec basculement **8-39**

Module 9 : Planification et implémentation d'une infrastructure de mise à jour de serveur

Leçon 1 : Planification et implémentation d'un déploiement WSUS **9-2**
Leçon 2 : Planification des mises à jour logicielles avec System Center 2012 Configuration Manager **9-12**
Leçon 3 : Planification et implémentation des mises à jour dans une infrastructure de virtualisation de serveur **9-25**
Atelier pratique : Planification et implémentation d'une infrastructure de correction de serveur **9-33**

Module 10 : Planification et implémentation d'une stratégie de continuité des activités de l'entreprise

Leçon 1 : Vue d'ensemble de la planification de la continuité des activités de l'entreprise **10-2**
Leçon 2 : Planification et implémentation des stratégies de sauvegarde **10-13**
Leçon 3 : Planification et implémentation de la récupération **10-22**
Leçon 4 : Planification et implémentation de la sauvegarde et de la récupération des ordinateurs virtuels **10-32**
Atelier pratique : Implémentation d'une stratégie de sauvegarde d'ordinateurs virtuels avec DPM **10-40**

Module 11 : Planification et implémentation d'une infrastructure à clé publique

Leçon 1 : Planification et implémentation d'un déploiement d'autorité de certification **11-2**
Leçon 2 : Planification et implémentation de modèles de certificats **11-17**
Leçon 3 : Planification et implémentation la distribution et la révocation de certificats **11-24**
Leçon 4 : Planification et implémentation de l'archivage et de la récupération de clé **11-34**
Atelier pratique : Planification et implémentation d'une infrastructure AD CS **11-39**

Module 12 : Planification et implémentation d'une infrastructure de fédération d'identités

Leçon 1 : Planification et implémentation d'une infrastructure de serveur AD FS **12-2**
Leçon 2 : Planification et implémentation des fournisseurs de revendications et parties de confiance AD FS **12-17**
Leçon 3 : Planification et implémentation des revendications et des règles de revendication AD FS **12-24**
Atelier pratique : Planification et implémentation d'une infrastructure AD FS **12-32**

Module 13 : Planification et implémentation d'une infrastructure de gestion des droits relatifs à l'information (IRM)

Leçon 1 : Planification et implémentation d'un cluster AD RMS **13-3**
Leçon 2 : Planification et implémentation de modèles et stratégies AD RMS **13-22**
Leçon 3 : Planification et implémentation de l'accès externe aux services AD RMS **13-33**
Leçon 4 : Planification et implémentation de l'intégration d'AD RMS au contrôle d'accès dynamique **13-46**
Atelier pratique : Planification et implémentation d'une infrastructure AD RMS **13-54**

Corrigés des ateliers pratiques

Atelier pratique du module 1 : Éléments à prendre en compte pour implémenter un centre de données d'entreprise **L1-1**
Atelier pratique du module 2 : Planification et implémentation d'une stratégie de virtualisation de serveur **L2-3**
Atelier pratique du module 3 : Planification et implémentation des réseaux et du stockage de virtualisation **L3-9**
Atelier pratique du module 4 : Planification et implémentation d'une stratégie de déploiement et de gestion d'ordinateurs virtuels **L4-21**
Atelier pratique du module 5 : Planification et implémentation d'une solution d'administration pour la virtualisation **L5-29**
Atelier pratique du module 6 : Implémentation d'une stratégie d'analyse des serveurs **L6-41**
Atelier pratique du module 7 : Planification et implémentation d'une haute disponibilité pour des services et des applications de fichiers **L7-51**
Atelier pratique du module 8 : Planification et implémentation d'une infrastructure hautement disponible à l'aide du clustering avec basculement **L8-63**
Atelier pratique du module 9 : Planification et implémentation d'une infrastructure de correction de serveur **L9-79**
Atelier pratique du module 10 : Implémentation d'une stratégie de sauvegarde d'ordinateurs virtuels avec DPM **L10-93**
Atelier pratique du module 11 : Planification et implémentation d'une infrastructure AD CS **L11-99**
Atelier pratique du module 12 : Planification et implémentation d'une infrastructure AD FS **L12-111**
Atelier pratique du module 13 : Planification et implémentation d'une infrastructure AD RMS **L13-125**

À propos de ce cours

Cette section décrit brièvement le cours 22414B : Implémentation d'une infrastructure Server avancée, et apporte un complément d'informations relatif au public visé, aux connaissances préalables souhaitées et aux objectifs du cours.

Description du cours

Public visé

Ce cours s'adresse aux professionnels de l'informatique qui sont chargés de la planification, de la conception et du déploiement d'une infrastructure Windows Server® 2012 physique et logique avec les services de domaine Active Directory® en entreprise, y compris les services réseau. Les candidats disposent généralement de connaissances des systèmes d'exploitation Windows Server précédents et de la certification MCSA (Microsoft Certified Solutions Associate) Windows Server 2012 ou des compétences équivalentes.

Le public secondaire visé par cette formation se compose de candidats professionnels de l'informatique qui souhaitent passer l'examen 70-414 : Implémentation d'une infrastructure de serveur d'entreprise avancée, en tant qu'examen autonome ou dans le cadre de la condition requise à l'obtention de la certification MCSE (Microsoft Certified Solutions Expert).

Connaissances préalables des stagiaires

Outre une expérience professionnelle, les stagiaires qui assistent à cette formation doivent posséder les connaissances techniques suivantes :

- les protocoles TCP/IP et les concepts de mise en réseau ;
- Windows Server 2012 et AD DS, y compris la planification, la conception et le déploiement d'AD DS et d'une infrastructure de réseau ;
- l'utilisation de scripts et de fichiers de commandes ;
- les concepts de sécurité tels que l'authentification et l'autorisation ;
- les outils de déploiement, d'empaquetage et de création d'images ;
- le travail en équipe, ou en tant qu'équipe virtuelle ;
- la création de propositions et l'émission de recommandations en matière de budget.
- Les stagiaires doivent avoir obtenu la certification Windows Server 2012 MCSA et terminé le cours 22413B : Conception et implémentation d'une infrastructure Windows Server, ou avoir des connaissances équivalentes.

Les stagiaires qui assistent à cette formation peuvent satisfaire aux conditions préalables en suivant les cours suivants, ou en obtenant les connaissances et compétences équivalentes :

- 22410B : Installation et configuration de Windows Server 2012
- 22411B : Administration de Windows Server 2012
- 22412B : Configuration des services avancés de Windows Server 2012
- 22413B : Conception et implémentation d'une infrastructure Windows Server

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Objectifs du cours

À la fin de ce cours, les stagiaires seront à même d'effectuer les tâches suivantes :

- décrire les éléments à prendre en compte pour la gestion d'un centre de données d'entreprise ;
- planifier et implémenter une stratégie de virtualisation de serveur à l'aide de System Center 2012 ;
- planifier et implémenter les réseaux et le stockage pour la virtualisation ;
- gérer et déployer des ordinateurs virtuels ;
- gérer un déploiement d'ordinateur virtuel ;
- planifier et implémenter une stratégie d'analyse des serveurs ;
- planifier et implémenter la haute disponibilité pour des services et des applications de fichiers ;
- planifier et implémenter une infrastructure hautement disponible à l'aide du clustering avec basculement ;
- planifier et implémenter une infrastructure de mises à jour de serveurs ;
- planifier et implémenter une stratégie de continuité des activités de l'entreprise ;
- planifier et implémenter une infrastructure à clé publique (PKI) ;
- planifier et implémenter une infrastructure de fédération d'identités ;
- planifier et implémenter une infrastructure de gestion des droits relatifs à l'information (IRM).

Plan du cours

Le plan du cours est le suivant :

Module 1, Vue d'ensemble de la gestion dans un centre de données d'entreprise

Module 2, Planification et implémentation d'une stratégie de virtualisation de serveur

Module 3, Planification et implémentation des réseaux et du stockage pour la virtualisation

Module 4, Planification et déploiement d'ordinateurs virtuels

Module 5, Planification et implémentation d'une solution d'administration de la virtualisation

Module 6, Planification et implémentation d'une stratégie d'analyse des serveurs

Module 7, Planification et implémentation d'une haute disponibilité pour des services et des applications de fichiers

Module 8, Planification et implémentation d'une infrastructure haute disponibilité à l'aide du clustering avec basculement

Module 9, Planification et implémentation d'une infrastructure de mise à jour de serveur

Module 10, Planification et implémentation d'une stratégie de continuité des activités de l'entreprise

Module 11, Planification et implémentation d'une infrastructure à clé publique

Module 12, Planification et implémentation d'une infrastructure de fédération d'identités

Module 13, Planification et implémentation d'une infrastructure de gestion des droits relatifs à l'information (IRM)

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Documents de cours

Votre kit de cours contient les documents suivants :

- **Manuel du cours** : un guide de formation succinct qui fournit toutes les informations techniques importantes dans un format concis et très ciblé, parfaitement adapté à l'apprentissage en classe.
- **Leçons** : ces sections guident les stagiaires au travers des objectifs de formation et leur fournissent les points clés essentiels pour un apprentissage en classe réussi.
- **Ateliers pratiques** : ils fournissent aux stagiaires une plateforme réaliste de mise en application des connaissances et compétences acquises dans le module.
- **Contrôles des acquis et éléments à retenir** : ils fournissent une documentation de référence pratique qui favorise la mémorisation des connaissances et compétences.
- **Corrigés des ateliers pratiques** : ils fournissent des instructions pas à pas pour la résolution des ateliers pratiques.



Contenu d'accompagnement du cours à l'adresse **http://www.microsoft.com/learning/companionmoc** (*Certains de ces sites adressées dans ce cours sont en anglais.*) **:** il offre un contenu numérique facile à parcourir, dans lequel il est possible d'effectuer des recherches et qui comprend de précieuses ressources en ligne intégrées proposées en complément du manuel du cours.

- **Modules** : les modules incluent l'accompagnement du cours, tel que les questions et les réponses, les étapes détaillées de la démonstration et les liens de la rubrique Documentation supplémentaire, pour chaque leçon. De plus, les modules incluent les questions et réponses de contrôles des acquis de l'atelier pratique, ainsi que des sections sur les contrôles des acquis et éléments à retenir, qui contiennent les questions et réponses de contrôle des acquis, les meilleures pratiques, des astuces et réponses sur les problèmes courants et la résolution des problèmes, des scénarios et problèmes concrets avec les réponses.
- **Ressources** : elles incluent des ressources supplémentaires présentées par catégories qui vous donnent un accès immédiat à du contenu utile et à jour disponible sur TechNet, MSDN® ou Microsoft Press®.
- **Évaluation du cours** : À la fin du cours, les stagiaires auront l'occasion de remplir une fiche d'évaluation en ligne pour faire part de leurs commentaires sur le cours, le centre de formation et l'instructeur.
- Pour adresser d'autres commentaires ou remarques sur le cours, les stagiaires peuvent envoyer un message électronique à l'adresse support@mscourseware.com. Pour obtenir des informations sur le programme MCP (Microsoft Certification Program), envoyez un message électronique à l'adresse mcphelp@microsoft.com.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Environnement d'ordinateur virtuel

Cette section fournit des informations pour configurer l'environnement de la classe afin de prendre en charge le scénario d'entreprise du cours.

Configuration de l'ordinateur virtuel

Dans ce cours, vous allez utiliser Microsoft Hyper-V® pour effectuer les ateliers pratiques.

Important : à la fin de chaque atelier pratique, vous devez fermer l'ordinateur virtuel *sans* enregistrer les modifications. Pour fermer un ordinateur virtuel sans enregistrer les modifications, procédez comme suit :

1. Sur l'ordinateur virtuel, dans le menu **Action**, cliquez sur **Fermer**.
2. Dans la boîte de dialogue **Fermer**, dans la liste **Que doit faire l'ordinateur virtuel ?**, cliquez sur **Éteindre** et supprimer les modifications, puis cliquez sur **OK**.

Le tableau suivant illustre le rôle de chaque ordinateur virtuel utilisé dans ce cours :

Ordinateur virtuel	Rôle
22414B-LON-Host1, LON-Host2	Ordinateurs hôtes Windows Server 2012 (démarrage à partir d'un fichier vhd)
22414B-LON-DC1	Contrôleur de domaine dans le domaine Adatum.com
22414B-LON-SVR1, LON-SVR2, LON-SVR3	Serveurs membres dans le domaine Adatum.com
22414B-LON-VMM1	Serveur System Center Virtual Machine Manager (VMM) 2012
22414B-TOR-SVR1	Serveur membre dans le domaine Adatum.com, dans une filiale
22414B-TOR-SS1	Windows Server 2012 avec cibles iSCSI préconfigurées
22414B-LON-OM1	Serveur System Center Operations Manager 2012 (Operations Manager)
22414B-LON-OR1	Serveur System Center Orchestrator (Orchestrator)
22414B-LON-DM1	Serveur System Center Data Protection Manager 2012 (Data Protection Manager)
22414B-LON-WSUS	Serveur Windows Server Update Services
22414B-LON-CA1	Serveur autonome
22414B-LON-CL1	Ordinateur client avec Microsoft® Office 2010 dans le domaine Adatum.com
22414B-LON-CORE	Serveur autonome exécutant l'installation minimale de Windows Server 2012.
22414B-PRS-DC1	Contrôleur du domaine TreyResearch.net
22414B-PRS-CL1	Ordinateur client avec Microsoft® Office 2010 dans le domaine TreyResearch.net

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration logicielle

Les logiciels suivants sont installés sur chaque ordinateur virtuel :

- Windows Server 2012
- Microsoft Windows 8
- Microsoft System Center 2012 SP1
- Microsoft SQL Server® 2008 R2

Configuration de la classe

L'ordinateur virtuel sera configuré de la même façon sur tous les ordinateurs de la classe.

Niveau des éléments matériels du cours

Pour garantir une utilisation satisfaisante, les formations Microsoft requièrent une configuration matérielle minimale pour les ordinateurs de l'instructeur et des stagiaires dans toutes les classes Microsoft CPLS (Certified Partner for Learning Solutions) dans lesquelles les produits officiels de formation Microsoft sont utilisés.

Ces cours requièrent le niveau matériel 7. Les ressources supplémentaires sont nécessaires en raison de l'inclusion de Windows System Center 2012. Tous les ordinateurs virtuels seront créés et exécutés sous Hyper-V dans Windows Server 2012. L'ordinateur hôte pour ce cours est mis à disposition en configuration de démarrage à partir d'un disque dur virtuel (démarrage natif).

Le niveau matériel 7 est spécifié comme suit :

- Processeur Intel VT (Intel Virtualization Technology) ou AMD-V (AMD Virtualization) 64 bits (double cœur 2,8 GHz ou supérieur recommandé).
- Doubles disques durs de 500 Go à 7 200 tr/mn SATA ou supérieurs (agrégés).
- 16 Go de mémoire vive (RAM).
- DVD : double couche recommandée.
- Carte réseau.
- Carte audio.
- Carte vidéo : prend en charge la résolution 1440X900.
- Moniteur : moniteurs doubles SVGA 17 pouces ou plus grand avec prise en charge de la résolution minimum 1440 X 900

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 1

Vue d'ensemble de la gestion dans un centre de données d'entreprise

Table des matières :

Vue d'ensemble du module **1-1**

Leçon 1: Vue d'ensemble du centre de données d'entreprise **1-2**

Leçon 2: Vue d'ensemble des composants de Microsoft System Center 2012 **1-14**

Atelier pratique : Éléments à prendre en compte pour implémenter un centre de données d'entreprise **1-29**

Contrôle des acquis et éléments à retenir **1-31**

Vue d'ensemble du module

Dans beaucoup de grandes entreprises, le centre de données d'entreprise qui héberge la plupart des services informatiques a énormément changé au cours des dernières années. L'une des plus grandes évolutions importantes est l'introduction de la virtualisation. Dans de nombreux cas, le déploiement par défaut des nouveaux serveurs est effectué sur un ordinateur virtuel plutôt que sur un ordinateur physique. Les centres de données ont connu d'autres modifications car les organisations doivent gérer l'évolution des exigences métier.

Ces modifications impliquent que le centre de données d'entreprise est désormais plus complexe qu'auparavant et qu'il doit être bien plus réactif aux changements. La gestion du centre de données est devenue plus complexe car les organisations cherchent à optimiser les performances et à fournir des fonctionnalités telles que le libre-service. Ces exigences ont provoqué le besoin d'un nouvel ensemble d'outils de gestion pour gérer le centre de données.

Ce module décrit certaines des modifications et des nouvelles exigences que les organisations rencontrent dans leurs centres de données. Il explique ensuite comment vous pouvez utiliser Microsoft® System Center 2012 pour gérer cet environnement.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- décrire le centre de données d'entreprise ;
- expliquer comment utiliser System Center 2012 pour gérer le centre de données d'entreprise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble du centre de données d'entreprise

Beaucoup de grandes organisations ont déployé un ou plusieurs centres de données centraux pour fournir la plupart de leurs services informatiques. Ces centres de données ont dû s'adapter pour gérer l'évolution des exigences métier. Cette leçon décrit certaines des modifications que les organisations ont apportées à leur centre de données et comment les nouvelles exigences en matière d'outils et de processus informatiques ont évolué suite à ces modifications.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire un centre de données d'entreprise ;
- décrire l'importance de la virtualisation dans le centre de données ;
- décrire les outils nécessaires pour gérer et surveiller le centre de données ;
- décrire la configuration requise et les options permettant d'assurer la sécurité du centre de données ;
- décrire l'importance de fournir des fonctionnalités de surveillance et de création de rapport dans le centre de données ;
- décrire les options permettant d'implémenter la haute disponibilité et la continuité des activités dans le centre de données ;
- décrire les options d'automatisation du centre de données.

Qu'est-ce qu'un centre de données d'entreprise ?

La définition la plus simple d'un centre de données d'entreprise est qu'il s'agit d'un emplacement centralisé à partir duquel les organisations fournissent les services informatiques requis pour répondre à leurs exigences et atteindre leurs objectifs. La plupart des centres de données d'entreprise fournissent un ensemble semblable de services principaux, notamment :



- Services d'infrastructure. Les centres de données d'entreprise fournissent un ensemble principal de services requis pour permettre le fonctionnement de tous les autres services. Ceux-ci comprennent l'infrastructure réseau principale et les services réseau tels que le protocole DHCP (Dynamic Host Configuration Protocol) et DNS (Domain Name System).
- Services d'authentification et de sécurité. La plupart des organisations utilisent les services de domaine Active Directory® (AD DS) pour fournir une base de données de sécurité centrale pour l'authentification et l'autorisation utilisateur. Il est possible que certaines organisations doivent également fournir des services de sécurité supplémentaires pour authentifier les utilisateurs dans les applications qui ne sont pas intégrées à AD DS ou pour l'authentification des utilisateurs ne disposant pas d'un compte AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Stockage central des données. Quasiment tous les centres de données d'entreprise assurent le stockage centralisé des données. Ces données peuvent être stockées dans des dossiers partagés sur des serveurs de fichiers, dans des bases de données ou sur des sites Web. Les utilisateurs de toute l'organisation ont besoin d'un accès sécurisé à ces données.
- Services de collaboration et messagerie. Dans de nombreuses organisations, le courrier électronique est une partie essentielle des processus métier. Dans certaines organisations, d'autres outils de collaboration, tels que la messagerie instantanée, la conférence de bureau et d'autres outils interactifs basés sur le Web, deviennent plus importants. Le centre de données d'entreprise permet d'accéder à ces services.
- Applications serveur. Le centre de données d'entreprise permet d'accéder à une grande variété d'applications serveur. Ces applications peuvent comprendre des applications Web, des applications de base de données, des applications de bureau à distance ou même des ordinateurs virtuels auxquels les utilisateurs peuvent accéder.

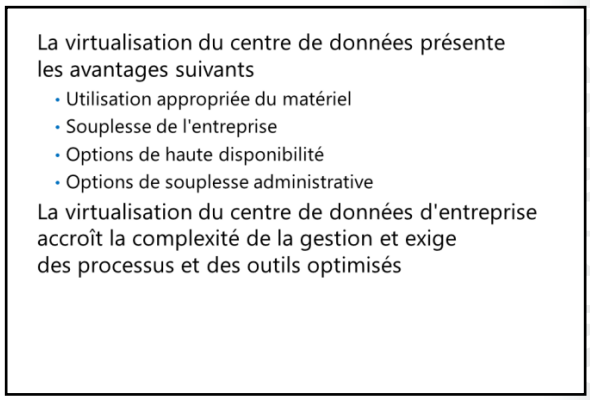
Il n'y a pas eu de modifications importantes de l'ensemble principal de services fourni par les centres de données d'entreprise, mais la manière dont les organisations informatiques fournissent ces services a radicalement changé. En général, les services que les centres de données d'entreprise fournissent et les clients qui consomment ces services ont été faciles à prévoir et à gérer. Initialement, la plupart des centres de données de services étaient destinés aux utilisateurs internes, qui se connectaient aux services en utilisant les ordinateurs de bureau connectés à un réseau câblé. Les organisations déployaient les services sur des serveurs physiques et les services informatiques comprenaient généralement comment déployer et gérer les nouveaux services requis. La limite du centre de données et les clients qu'il prenait en charge étaient facilement définissables et plutôt statiques.

Cependant, au cours des 10 dernières années, le mode de fonctionnement d'un centre de données d'entreprise et la manière dont il fournit ses services ont considérablement modifié les centres de données. Les centres de données doivent désormais fournir des services à une grande variété de clients, y compris à des appareils mobiles, qui se connectent toujours au centre de données à partir des réseaux internes de l'organisation, mais également depuis des emplacements et des réseaux externes à l'organisation. Cela signifie que les organisations doivent désormais fournir l'accès aux services internes depuis Internet, tout en fournissant des niveaux de sécurité beaucoup plus élevés. Les organisations sont devenues beaucoup plus conscientes du coût et de l'impact environnemental de l'exécution de grands centres de données, par conséquent les services informatiques sont invités à optimiser les performances et l'utilisation de tous les composants de centre de données. Les organisations florissantes peuvent généralement s'adapter rapidement à l'évolution des exigences métier et les services informatiques doivent être en mesure de déployer rapidement et efficacement les nouveaux services que ces changements d'exigences métier nécessitent. Au fur et à mesure que les organisations se diversifient et repoussent leurs limites en ce qui concerne les personnes qui peuvent accéder aux services informatiques, il devient de plus en plus important que ces services soient toujours disponibles et que l'organisation ait un plan de continuité des activités extrêmement efficace.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Virtualisation d'un centre de données d'entreprise

La virtualisation est l'une des fonctionnalités centrales d'un centre de données d'entreprise, en particulier la virtualisation de serveur. Dans la plupart des organisations, à l'exception des plus petites, presque tous les nouveaux serveurs sont déployés sous forme d'ordinateurs virtuels. La gestion d'un environnement qui est presque totalement virtualisé fournit de nombreux avantages.



- Utilisation appropriée du matériel. Le principal avantage que la plupart des organisations retirent de la virtualisation, c'est qu'elles peuvent utiliser totalement le matériel de serveur. Les organisations peuvent en effet déployer un plus petit nombre d'hôtes de virtualisation sous forme d'ordinateurs physiques, puis déployer plusieurs ordinateurs virtuels sur chaque hôte. Cela leur permet d'utiliser entièrement les ressources matérielles au lieu d'avoir plusieurs ordinateurs physiques déployées avec une utilisation très faible. Étant donné qu'elles déploient moins d'ordinateurs physiques, les organisations peuvent constater une forte diminution des exigences d'alimentation et de refroidissement des centres de données.
- Souplesse de l'entreprise. Le deuxième avantage important que les organisations retirent de la virtualisation, c'est la possibilité de répondre très rapidement aux changements d'exigences métier. Dans un environnement virtuel, une demande de déploiement d'un nouveau serveur, d'un nouvel ensemble de serveurs ou d'une nouvelle application émise par un groupe de l'entreprise peut être traitée en quelques heures au lieu de plusieurs jours ou semaines. Si un serveur doit être déplacé vers un autre emplacement, il suffit de copier des fichiers sur un réseau.
- Options de haute disponibilité. La virtualisation de serveur fournit également de nouvelles options importantes pour l'implémentation de la haute disponibilité. Vous pouvez utiliser les mêmes options de haute disponibilité dans un environnement virtuel que dans un environnement physique. Par exemple, vous pouvez déployer des ordinateurs virtuels qui utilisent l'équilibrage de la charge réseau (NLB), le clustering avec basculement ou la haute disponibilité des applications. La virtualisation offre également la possibilité de rendre l'ordinateur virtuel hautement disponible afin de vous permettre de fournir la haute disponibilité pour les services et applications qui ne la prennent pas en charge en mode natif. Vous pouvez ainsi proposer des options supplémentaires de haute disponibilité pour toutes les applications.
- Options de délégation administrative, de libre-service et d'automatisation. Les environnements virtuels fournissent beaucoup d'autres options pour améliorer les processus de gestion dans un centre de données. Dans un environnement virtuel, vous pouvez facilement donner aux utilisateurs de l'entreprise l'accès à un ou deux ordinateurs virtuels seulement. Avec les outils de gestion et les processus appropriés, vous pouvez créer des processus qui permettront à ces utilisateurs de gérer leur petite partie du centre de données, y compris des options de création de serveurs ou de services supplémentaires.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

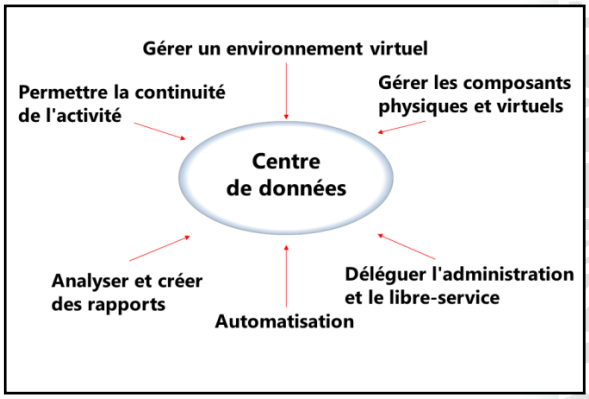
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Alors que le déploiement d'un environnement virtuel peut fournir des avantages très importants, il ajoute également un niveau de complexité aux processus de gestion. Pour gérer un environnement virtuel, vous devez gérer la couche physique ou hôte ainsi que la couche virtuelle. Ces couches peuvent être gérées séparément dans une grande mesure, mais il y a toujours une forte dépendance entre elles. Si vous gérez mal la couche physique et qu'un hôte physique s'arrête accidentellement, cela risque d'affecter de nombreux groupes de l'entreprise dont les ordinateurs virtuels s'exécutaient sur cet hôte. Si vous gérez mal les ordinateurs virtuels et qu'un ordinateur virtuel commence à consommer trop de ressources hôte, d'autres ordinateurs virtuels peuvent être affectés.

La virtualisation fournit des avantages très importants pour presque toutes les organisations. Pour gérer correctement l'environnement virtuel, vous devez implémenter les processus et les outils qui peuvent optimiser les avantages de la virtualisation tout en réduisant la complexité de gestion.

Outils de gestion et de surveillance du centre de données

En même temps que le centre de données d'entreprise, les exigences en matière d'outils pour gérer le centre de données ont changé. Dans le centre de données traditionnel, vous pouvez gérer la plupart des composants à l'aide d'outils spécialisés pour chaque composant particulier, sans avoir à réellement vous soucier de la façon dont cet outil de gestion interagit avec les autres composants du centre de données.



Lorsque les centres de données sont devenus plus complexes, le besoin d'outils de gestion plus intégrés a augmenté. Voici quelques exemples de la manière dont les exigences en matière d'outils ont changé :

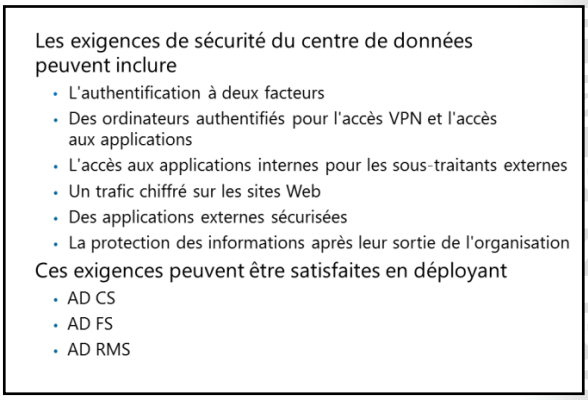
- Les outils doivent être optimisés pour la gestion des environnements virtuels. Dans les centres de données actuels, presque tous les nouveaux serveurs sont déployés en tant qu'ordinateurs virtuels ; de nombreuses applications sont déployées en tant qu'applications virtuelles à l'aide de la virtualisation de présentation, la virtualisation d'application ou la virtualisation de bureau. Tout outil que vous utilisez pour gérer un centre de données doit pouvoir gérer tous les composants du centre de données virtualisé.
- Les outils doivent gérer les composants aussi bien virtuels que physiques du centre de données. Bien que la plupart des nouveaux serveurs et applications soient virtualisés, tous les centres de données nécessitent toujours une couche informatique physique. Cela peut inclure des serveurs et des applications s'exécutant toujours sur un matériel physique, mais cela inclura sans aucun doute la couche hôte de l'environnement virtualisé. Les outils de gestion doivent être en mesure de gérer à la fois la couche physique et la couche virtuelle en utilisant les mêmes consoles d'administration et processus de gestion.

Remarque : Le choix du bon système d'exploitation à exécuter sur les ordinateurs virtuels et sur les hôtes physiques est une partie importante du processus de planification. Windows Server® 2012 est conçu pour optimiser l'intégration aux solutions de gestion telles que Microsoft System Center 2012 Service Pack 1 (SP1).

- Les outils doivent fournir des options de délégation des fonctions administratives, y compris le libre-service. L'une des fonctionnalités clés d'un centre de données est la capacité de répondre rapidement et efficacement aux changements de situations et d'exigences métier. Dans cet environnement, la gestion de tous les composants par un seul groupe d'administrateurs d'entreprise risque d'être inefficace. Pour permettre une réponse rapide à un changement de situation, les outils de gestion doivent autoriser la délégation efficace et sécurisée des tâches à d'autres administrateurs, ou autoriser la délégation du libre-service aux divisions qui peuvent traiter les changements d'exigences sans aucune interaction avec les administrateurs d'entreprise qui ont configuré les outils.
- Les outils doivent fournir les moyens d'automatiser les processus. Afin d'activer des fonctionnalités telles que le libre-service et de permettre une gestion efficace et exempte d'erreurs des composants de centre de données, les outils de gestion doivent fournir un moyen d'automatiser un bon nombre des tâches de gestion. Les outils doivent permettre à ces tâches de s'exécuter automatiquement selon une planification, lorsqu'une action d'un utilisateur les initialise ou en réponse à une alerte de surveillance. Les tâches déclenchées par un processus automatisé peuvent interagir avec un ou plusieurs composants de centre de données.
- Les outils doivent permettre la surveillance et la création de rapports pour tous les composants du centre de données. À mesure que la complexité du centre de données augmente, l'importance de surveiller tous les composants du centre de données et de fournir des rapports intelligents sur l'état actuel de tous les composants augmente également. Les administrateurs ne peuvent pas surveiller tous les composants individuellement ; ils ont besoin d'outils capables de capturer les informations de surveillance de tous les composants, mais qui signalent uniquement les informations pertinentes sur chaque composant. Étant donné que de nombreux composants dépendent d'autres composants, les outils de surveillance doivent comprendre les relations entre les composants.
- Les outils doivent fournir les moyens d'assurer la continuité de l'activité. Dans le centre de données d'entreprise, certains services et composants doivent être disponibles en permanence. Tout temps mort non planifié de ces composants peut avoir un impact très important sur l'activité. Les outils de gestion doivent fournir les moyens d'appliquer des mises à jour aux services et aux composants sans aucune incidence sur la disponibilité des services. Ils doivent également fournir les moyens de récupérer un service en cas de défaillance de celui-ci.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fourniture de services sécurisés dans le centre de données



Dans un centre de données traditionnel, AD DS fournit la majeure partie de la fonctionnalité qui est nécessaire pour que les utilisateurs internes se connectent au réseau et pour activer l'accès sécurisé aux services et applications réseau. Si tous les utilisateurs disposent de comptes AD DS et se connectent uniquement au réseau en utilisant les ordinateurs internes qui sont membres du même environnement AD DS, il est facile de fournir un accès sécurisé aux services et applications du centre de données. Cependant, de nombreuses organisations exigent maintenant que de nombreux types d'utilisateurs différents accèdent aux ressources du centre de données, et ces utilisateurs utiliseront une grande variété de périphériques pour accéder à ces ressources. Les utilisateurs qui ont besoin d'accéder aux ressources du centre de données peuvent inclure les employés en déplacement et ceux qui travaillent à domicile. Ils peuvent également inclure des utilisateurs qui ne sont pas des employés, mais des clients ou des personnes travaillant pour des organisations partenaires. Les utilisateurs peuvent utiliser un ordinateur portable géré pour accéder aux ressources, mais aussi des ordinateurs non gérés ou des appareils mobiles. Voici certaines des exigences de sécurité que les organisations peuvent avoir :

- Le groupe de sécurité de l'organisation peut exiger que les administrateurs qui effectuent les tâches d'administrateur de domaine ou d'administrateur d'entreprise sur le réseau fournissent deux facteurs d'authentification. Cela signifie qu'il est possible que le fait de fournir uniquement un nom d'utilisateur et un mot de passe ne constitue pas un niveau de sécurité adéquat.
- L'organisation peut exiger que les utilisateurs utilisent les ordinateurs portables qui sont membres du domaine Active Directory interne s'ils souhaitent se connecter à certains sites Web hautement sécurisés ou se connecter au réseau interne via un réseau privé virtuel (VPN).
- Les exigences de sécurité de l'organisation peuvent stipuler que seuls les employés sont autorisés à avoir des comptes d'utilisateur dans le domaine AD DS. Cependant, l'organisation doit fournir l'accès aux sites Web et aux applications afin que les sous-traitants puissent travailler aussi bien en interne qu'à l'extérieur.
- L'organisation peut avoir besoin d'assurer le chiffrement de tout le trafic d'authentification et d'accès Web vers des sites accessibles sur Internet.
- L'organisation peut avoir déployé une application de commande de produits pour les clients externes. Cette application doit être sécurisée afin que seuls les utilisateurs autorisés puissent accéder à l'application et passer des commandes.
- L'organisation peut avoir implémenté des règles de sécurité sur la façon de partager des types d'informations spécifiques avec des utilisateurs à l'intérieur et à l'extérieur la société. L'organisation a besoin d'une méthode pour appliquer ces exigences de sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans ces scénarios, il peut être difficile de répondre à toutes les exigences de sécurité uniquement avec AD DS. Il est possible qu'AD DS ne fournisse pas la fonctionnalité requise, et même s'il le faisait, la plupart des organisations n'exposent pas leurs contrôleurs de domaine AD DS internes directement à Internet en raison des problèmes de sécurité.

Microsoft a donc développé des services Active Directory supplémentaires pour traiter les exigences métier et de sécurité que vous ne pouvez pas traiter entièrement à l'aide d'AD DS uniquement, notamment :

- Les services de certificats Active Directory (AD CS), qui fournissent une infrastructure à clé publique (PKI) pouvant être utilisée pour publier et gérer les certificats qui fournissent des niveaux de sécurité supplémentaires au sein de l'organisation.
- Les services fédérés Active Directory (AD FS), qui permettent aux organisations partenaires d'établir des approbations fédérées. Cela permet à ces organisations de gérer leurs propres identités numériques et d'accéder à des applications hébergées par une autre organisation.
- Les services AD RMS (Active Directory Rights Management Services), qui fournissent la protection et le contrôle d'accès aux informations confidentielles, comme des documents et des messages électroniques. Vous pouvez appliquer cette protection même une fois que le contenu est sorti de l'organisation.
- Les services AD LDS (Active Directory Lightweight Directory Services), qui sont un annuaire LDAP qui fournit aux organisations une prise en charge flexible des applications compatibles avec Active Directory si elles souhaitent éviter la surcharge de gestion induite par un déploiement complet d'AD DS.

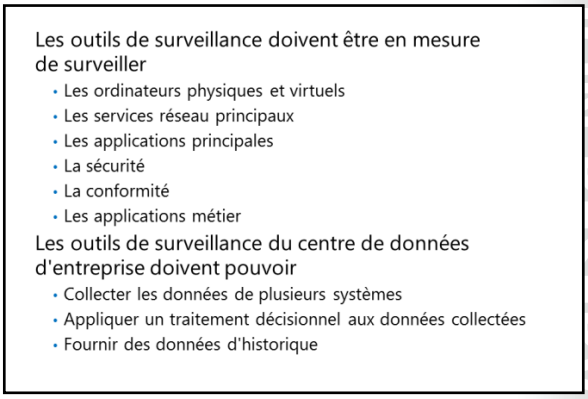
Documentation supplémentaire : Tous ces services Active Directory supplémentaires sont étudiés dans ce cours, à l'exception d'AD LDS. Pour plus d'informations sur AD LDS, voir la page Vue d'ensemble des services AD LDS (Active Directory Lightweight Directory Services) à l'adresse http://go.microsoft.com/fwlink/?LinkID=286067.

Ces services Active Directory supplémentaires étendent les fonctions et fonctionnalités d'AD DS, mais peuvent également être étroitement intégrés à AD DS. Par exemple, vous pouvez configurer AD CS pour qu'il émette automatiquement des certificats d'ordinateur pour tous les ordinateurs membres d'un domaine AD DS. Vous pouvez configurer AD LDS pour synchroniser certaines informations avec AD DS. Les utilisateurs ne peuvent tirer parti des services AD FS et AD RMS qu'après s'être connectés à leurs comptes AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Surveillance et création de rapports sur les services de centre de données

Un outil de surveillance et de création de rapports efficace est essentiel dans un centre de données d'entreprise. De nombreux services et applications différents seront déployés dans le centre de données et les services peuvent changer fréquemment. Dans cet environnement, il est impératif de bien comprendre ce qui doit être surveillé et de fournir les outils appropriés pour effectuer la surveillance. Les zones clés du centre de données d'entreprise qui doivent être surveillées sont les suivantes :



- Ordinateurs physiques et virtuels.
  Presque tous les services et applications du centre de données s'exécutent sur des ordinateurs physiques ou virtuels. Il est donc primordial que les administrateurs d'entreprise disposent d'informations sur les performances de tous les ordinateurs du centre de données. Les performances et la disponibilité du matériel physique des hôtes et du matériel virtuel des invités doivent être surveillées. Cela inclut le sous-système de disque, les périphériques connectés au réseau SAN ou au périphérique de stockage NAS, et d'autres périphériques matériels.
- Services réseau principaux. Presque tous les services du centre de données ont besoin d'un ensemble de services principaux pour fonctionner. Ces services principaux comprennent l'infrastructure réseau, DNS et AD DS. Si ces services ne sont pas fonctionnels ou s'ils sont surchargés, les autres services ne fonctionneront pas comme prévu. Le système de surveillance de l'entreprise doit être en mesure de surveiller les performances et la disponibilité de ces services principaux et de fournir des alertes en cas de problème.
- Applications principales. De nombreuses applications du centre de données dépendent d'un ensemble d'applications principales fournies. Ces applications, y compris les serveurs de messagerie, les serveurs de base de données et les serveurs Web, peuvent être déployées par une équipe centrale d'administrateurs. Ces applications sont accessibles à tous les utilisateurs et à l'infrastructure peut-être partagée par toutes les applications métier. Étant donné que les processus et les applications métier dépendent de la disponibilité de ces applications principales et de la fourniture des services adéquats par celles-ci, ces applications doivent être surveillées.
- Sécurité. Au fur et à mesure que les limites du centre de données et des clients qui y accèdent sont devenues plus floues, le rôle de la surveillance de la sécurité a considérablement augmenté. De nombreux types de clients différents, y compris des clients non gérés, peuvent se connecter au centre de données. Le centre de données est maintenant conçu pour fournir des services aux utilisateurs où qu'ils soient et pas seulement aux utilisateurs situés dans le bâtiment physique de l'organisation. En conséquence, il est primordial que des outils soient disponibles pour surveiller les risques de violation de sécurité et garantir le déclenchement instantané d'une alerte en cas de violation de la sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Conformité aux contrats de niveau de service (SLA) ou aux normes. De nombreuses organisations ont défini des contrats SLA qui définissent les exigences en matière de disponibilité et de performances des composants du centre de données. Les outils de gestion du centre de données doivent être capables de surveiller et de générer des rapports sur la conformité à ces contrats SLA et éventuellement à d'autres normes de l'organisation et du secteur.
- Applications métier. Outre la surveillance de l'infrastructure partagée et des applications principales, il est également important de surveiller les applications métier individuellement. C'est nécessaire pour s'assurer que l'application métier fournit les services requis et également pour vérifier qu'une application métier unique ne consomme pas plus que son partage des composants partagés. La surveillance d'une application métier unique peut impliquer de surveiller plusieurs applications. Par exemple, une application unique peut utiliser un programme d'équilibrage de la charge matérielle, plusieurs serveurs Web, un serveur de base de données en cluster et des serveurs de fichiers. La surveillance de cette application exige un outil capable de surveiller chaque composant et de comprendre les dépendances entre chaque composant.

De nombreux fabricants de matériel fournissent des outils de surveillance pour surveiller les composants du système d'exploitation et les composants matériels physiques. Windows Server fournit des outils de surveillance tels que l'Analyseur de performances, qui peut rassembler des informations détaillées sur les performances de tout système d'exploitation et des nombreux composants d'application s'exécutant sur le serveur. Le problème avec ces outils, c'est qu'ils peuvent généralement seulement surveiller les serveurs uniques, et seulement collecter les informations, mais pas les analyser intelligemment.

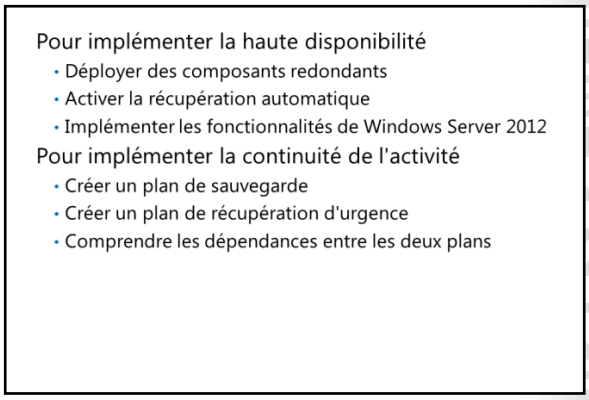
Le centre de données d'entreprise a besoin d'outils capables d'effectuer les opérations suivantes :

- Collecter les informations de surveillance détaillées de plusieurs systèmes et applications. Les outils de surveillance doivent être capables de collecter des informations sur l'ensemble des différents composants, services et applications qui sont déployés dans le centre de données. Cela peut inclure le matériel fourni par de nombreux fabricants différents, différents types de système d'exploitation et de nombreux types d'application variés.
- Appliquer un traitement décisionnel aux informations collectées. Il ne suffit pas de collecter les informations, car les données brutes ne sont généralement pas explicites. Vous devez analyser les données et mettre en corrélation les données de différentes sources afin d'en extraire la signification. Les outils de surveillance doivent assurer ce traitement décisionnel et être configurables pour garantir que les informations sont explicites pour chaque application.
- Fournir des données d'historique. Les outils de surveillance doivent fournir le moyen de stocker les informations sur les performances antérieures et de générer des rapports sur celles-ci. C'est nécessaire pour comprendre comment les caractéristiques de performances d'une application peuvent avoir changé au fil du temps et pour fournir des informations utiles pour une planification future.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Haute disponibilité et continuité de l'activité

Le centre de données d'entreprise fournit des services à une grande variété de clients potentiels, y compris aux employés internes et externes de l'organisation, à ses clients et à ses partenaires commerciaux. Ces clients peuvent accéder aux services du centre de données à tout moment à partir de n'importe où. De ce fait, il est primordial que les services soient extrêmement disponibles et réactifs. En cas de panne d'un service, il est essentiel qu'il soit restauré aussi rapidement que possible.



Implémentation de la haute disponibilité

Afin de garantir la haute disponibilité, un système doit pouvoir survivre à la défaillance d'un ou plusieurs composants sans provoquer aucune interruption d'un service ou d'une application. Afin de garantir la haute disponibilité, vous devez :

- Déployer des composants redondants. Si un système doit survivre à la défaillance de composants individuels, vous devez déployer plusieurs composants qui fournissent la même fonction. Certains composants peuvent fournir la redondance au niveau du serveur individuel. Par exemple, vous pouvez déployer des serveurs avec plusieurs cartes réseau et plusieurs alimentations. D'autres composants, tels que les commutateurs réseau, les connexions Internet ou au réseau étendu (WAN), et les sources d'alimentation, peuvent être déployés au niveau du centre de données. Dans certains cas, vous pouvez fournir la redondance en déployant plusieurs serveurs physiques ou virtuels qui fournissent la même fonctionnalité. Dans certains cas, un niveau de redondance unique peut être suffisant, tandis que dans d'autres, vous pouvez souhaiter une protection contre plusieurs défaillances du même composant.
- Implémenter le basculement automatique ou la récupération. Pour fournir une solution hautement disponible, il est important que le système puisse effectuer un basculement ou une récupération suite à la perte d'un composant unique. Le système doit pouvoir détecter une défaillance d'un composant et être en mesure d'effectuer une récupération automatique suite à cette défaillance. En général, pour ce faire, les services fournis par le composant défectueux sont déplacés vers un composant redondant. Il est important que ce basculement se produise automatiquement et qu'il ne nécessite pas l'attention ni l'intervention de l'administrateur.

Dans de nombreux cas, une solution hautement disponible fournira également l'équilibrage de charge. Cela signifie que, si tous les composants redondants sont fonctionnels, les demandes de service des clients seront réparties entre tous les composants. Par exemple, si tous les serveurs Web d'un déploiement hautement disponible sont fonctionnels, les demandes client d'un site Web sur les serveurs Web seront réparties entre tous les serveurs disponibles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Il existe de nombreuses manières différentes d'assurer la haute disponibilité. Dans un centre de données d'entreprise, il est très courant de voir des sources d'alimentation redondantes, des systèmes de refroidissement redondants, des connexions réseau redondantes et une infrastructure de stockage redondante.

Windows Server 2012 fournit plusieurs options pour implémenter la haute disponibilité, notamment :

- L'association de cartes réseau, qui peut être utilisée pour gérer les connexions réseau redondantes.
- Les espaces de stockage, qui peuvent être utilisés pour assurer la redondance et le basculement automatique des périphériques de stockage connectés au serveur.
- L'équilibrage de charge Windows, qui fournit la haute disponibilité et l'équilibrage de charge pour les services basés sur le Web.
- Le clustering avec basculement, qui fournit la haute disponibilité pour de nombreux services, y compris les ordinateurs virtuels Windows Server 2012 Hyper-V®.
- Le système de fichiers DFS, que vous pouvez utiliser pour créer plusieurs copies des dossiers et fichiers partagés afin d'optimiser les performances et d'améliorer la disponibilité.

Implémentation de la continuité d'activité

Idéalement, toute interruption potentielle des services sera réduite en implémentant la haute disponibilité dans le centre de données d'entreprise. Toutefois, il est également crucial que les organisations disposent de moyens de récupération suite à une défaillance sortant du cadre de la solution de haute disponibilité. Par exemple, plusieurs composants peuvent être défaillants ou un centre de données entier peut échouer.

Il existe de nombreuses manières différentes d'assurer la continuité de l'activité, selon le type d'incident contre lequel l'organisation est protégée. Beaucoup de grandes organisations ont déployé des centres de données de récupération d'urgence et ont implémenté des plans de basculement de centre de données complet en cas de défaillance d'un centre de données. Presque toutes les organisations effectuent des sauvegardes régulières de leurs centres de données et stockent ces sauvegardes hors site pour s'assurer de pouvoir effectuer une récupération suite à la perte du centre de données.

Lorsque vous créez un plan de continuité de l'activité, vous devez inclure les éléments suivants :

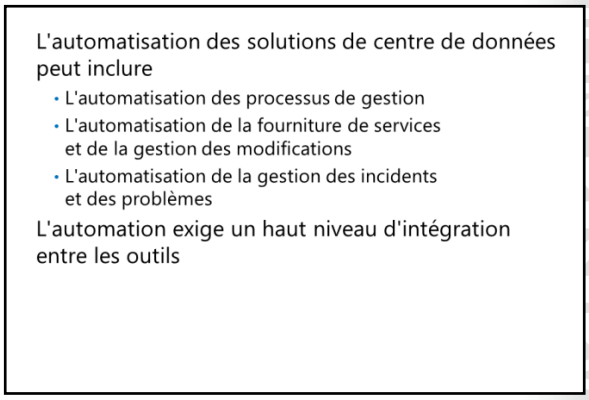
- Un plan de sauvegarde. Toutes les données importantes pour l'organisation doivent être sauvegardées. En outre, toutes les informations de configuration des ordinateurs qui sont importantes pour la restauration des services du centre de données d'entreprise doivent être sauvegardées. Par exemple, il est primordial que les contrôleurs de domaine AD DS soient sauvegardés, en particulier si tous les contrôleurs de domaine se trouvent dans le même centre de données.
- Un plan de récupération d'urgence. Le plan de récupération d'urgence décrit en détails comment vous allez récupérer les données ou les services en cas de perte de données ou de défaillance de service. Il doit fournir des informations détaillées sur les éléments requis pour effectuer la récupération et la manière d'effectuer la récupération.

Le plan de sauvegarde et récupération doit être créé en tenant compte des dépendances entre ces deux plans. Les plans de continuité de l'activité comprennent fréquemment des contrats SLA pour les objectifs de point de récupération (RPO) et les objectifs de temps de récupération (RTO). Les RPO définissent la quantité de perte de données accessible en cas de défaillance majeure. Par exemple, le RPO peut stipuler que jamais plus de quatre heures de données ne doivent être perdues en cas de défaillance d'un serveur de fichiers hébergeant des partages de fichiers. Avec ce RPO, vous devez veiller à sauvegarder les données au moins toutes les 4 heures. Les RTO définissent le délai nécessaire pour récupérer les données ou un service. Si vous avez un RTO d'une heure pour les serveurs de fichiers, vous devrez peut-être effectuer la sauvegarde sur disque plutôt que sur bande afin de restaurer les données assez rapidement pour respecter le RTO.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Automatisation des solutions de centre de données

Lorsque le centre de données d'entreprise se développe et devient plus complexe, la gestion manuelle de tous les composants de centre de données peut devenir inefficace. Pour rendre la gestion plus efficace, il est important que vous exploriez les options d'automatisation d'autant de tâches répétitives que possible. Voici certaines options d'automatisation :



- Automatisation des processus de gestion. Bon nombre des tâches les plus courantes effectuées par les administrateurs réseau peuvent être automatisées. L'un des types les plus courants de tâches pouvant être automatisées sont les tâches où vous mettez en service de nouveaux objets ou composants. Par exemple, dans une grande organisation, le processus de création de comptes d'utilisateurs peut être long et complexe car il peut être nécessaire d'affecter l'utilisateur à plusieurs groupes, de configurer plusieurs attributs et de créer le compte sur plusieurs systèmes. Vous pouvez facilement automatiser ces tâches en déployant un outil tel que Forefront® Identity Manager, que vous pouvez configurer pour effectuer toutes ces tâches suite à une unique demande. La mise en service de nouveaux ordinateurs virtuels est une autre tâche qui est souvent automatisée. En créant des modèles à l'avance et en utilisant des fonctionnalités telles que le placement intelligent dans Microsoft System Center 2012 - Virtual Machine Manager (VMM), vous pouvez déclencher la création de nouveaux ordinateurs virtuels avec un minimum d'effort.
- Automatisation de la fourniture de services et de la gestion des modifications. De nombreuses organisations développent le processus d'automatisation des processus de gestion pour fournir une autre manière de démarrer le processus. Au lieu d'avoir un administrateur qui lance le processus, vous pouvez fournir aux utilisateurs finaux ou aux groupes de l'entreprise des outils leur permettant de lancer des demandes de service, qui lanceront alors automatiquement les processus de gestion automatisés. Par exemple, vous pourriez donner aux groupes professionnels l'accès à un outil tel que Microsoft System Center 2012 Orchestrator ou Microsoft System Center 2012 App Controller, et autoriser les administrateurs des groupes de l'entreprise à lancer la création d'un nouvel ensemble d'ordinateurs virtuels dont ils ont besoin pour déployer une nouvelle application.
- Automatisation de la gestion des incidents et des problèmes. Une autre option d'automatisation des tâches du centre de données consiste à automatiser la résolution des problèmes, ce qui peut nécessiter l'intégration de plusieurs composants de centre de données différents au centre de données. Par exemple, un système de surveillance peut détecter qu'un ordinateur virtuel ou une application consomme davantage de ressources que la normale. Ce système de surveillance peut déclencher une alerte, que le système de gestion des ordinateurs virtuels recevra. Le système de gestion des ordinateurs virtuels peut ensuite déplacer cet ordinateur virtuel vers un autre hôte disposant de davantage de ressources disponibles. Si une application consomme davantage de ressources que d'habitude ou si l'application ne répond plus, l'alerte ne peut inviter à un redémarrage de l'application. Microsoft System Center 2012 Service Manager fournit ce type de fonctionnalité.

L'automatisation des processus métier requiert presque toujours l'intégration de plusieurs composants et outils au centre de données. L'une des fonctionnalités clés de System Center 2012 est justement l'intégration entre les différents composants.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Vue d'ensemble des composants de Microsoft System Center 2012

L'évolution du centre de données d'entreprise implique que les processus et les outils de gestion ont également dû changer. En raison du niveau très élevé d'interdépendance entre les différents composants du centre de données, il est primordial que les outils utilisés pour gérer le centre de données soient également intégrés et puissent être utilisés pour gérer tous les composants et fournir tous les services requis.

System Center 2012 est conçu pour être une suite de gestion complète pour le centre de données d'entreprise. Avec System Center 2012, Microsoft a regroupé tous les composants de System Center dans un produit unique avec une meilleure intégration entre les produits. Cette leçon présente les divers composants de System Center 2012 et décrit comment ces outils peuvent être utilisés pour gérer le centre de données d'entreprise.

Objectifs de la leçon

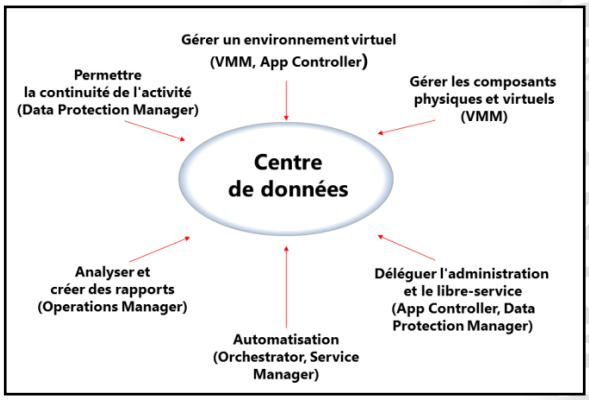
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire comment Microsoft System Center 2012 peut être utilisé pour gérer le centre de données d'entreprise ;
- décrire Microsoft System Center 2012 Configuration Manager ;
- décrire VMM ;
- décrire App Controller ;
- décrire Service Manager ;
- décrire Microsoft System Center 2012 Orchestrator ;
- décrire Microsoft System Center 2012 Operations Manager ;
- décrire Microsoft System Center 2012 Data Protection Manager ;
- décrire les autres outils de System Center.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Utilisation de Microsoft System Center 2012 pour gérer le centre de données d'entreprise

System Center 2012 fournit les outils permettant de déployer, gérer, faire fonctionner, automatiser et surveiller les centres de données.



Voici la liste des composants de Microsoft System Center 2012 :

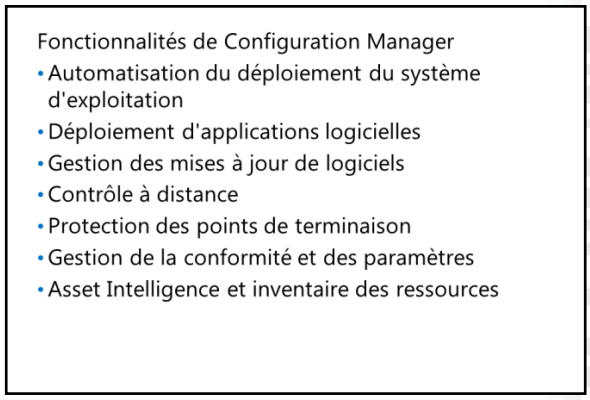
- Configuration Manager.
  Configuration Manager assure la gestion des logiciels, le déploiement du système d'exploitation, ainsi que la gestion des appareils mobiles. Vous pouvez utiliser Configuration Manager pour la gestion des mises à jour avancées et des mises à jour de fournisseurs tiers, et il inclut également Microsoft Endpoint Protection. Endpoint Protection est la solution anti-programmes malveillants d'entreprise pour les périphériques clients. Il permet aux administrateurs de gérer la sécurité des clients à partir d'une console unique.
- VMM. VMM fournit aux administrateurs un outil d'administration unique pour déployer et gérer une infrastructure de virtualisation, y compris des composants tels que des hôtes, du stockage, des réseaux, des bibliothèques et des serveurs de mise à jour. Cette infrastructure fournit la base de la gestion de la configuration et du déploiement des ordinateurs virtuels.
- App Controller. App Controller fournit un portail libre-service pour les administrateurs qui déploient et gèrent des applications et des services sur un ou plusieurs sites. App Controller vous permet d'accéder aux ressources d'un ou plusieurs serveurs VMM et de plusieurs abonnements Windows Azure™ et de les gérer.
- Service Manager. Service Manager offre la gestion des services, l'automatisation des processus, le suivi des biens et un portail libre-service pour accéder aux ressources définies dans un catalogue de services. Service Manager offre un moyen facile de créer une base de données de gestion de la configuration, qui extrait des données d'AD DS et des composants de System Center. Cela permet aux sociétés d'établir et d'utiliser des contrôles et des opérations conformément aux instructions d'ITIL (Information Technology Infrastructure Library) ou de Microsoft Operations Framework.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Orchestrator. Orchestrator est un composant d'automatisation de Runbook qui permet aux administrateurs d'intégrer et d'automatiser leurs centres de données. Orchestrator utilise des packs d'intégration, y compris de nombreux packs prêts à l'emploi qui permettent aux administrateurs de connecter différents systèmes.
- Operations Manager. Operations Manager est le composant de gestion destiné à la surveillance des applications et des performances. Vous pouvez intégrer Operations Manager à VMM, Service Manager, Orchestrator et Data Protection Manager. Operations Manager utilise des packs d'administration fournisseur qui fournissent des informations détaillées sur les applications et assurent la surveillance de leur état d'intégrité.
- Data Protection Manager. Data Protection Manager est un composant de sauvegarde d'entreprise qui exécute des sauvegardes de niveau bloc des applications. Il utilise les enregistreurs du service VSS pour aider à protéger et récupérer des applications telles que Microsoft SQL Server®, Microsoft Exchange Server®, Microsoft SharePoint Server® 2012 et les services de domaine Active Directory® (AD DS). En outre, il fournit des enregistreurs VSS spécifiques pour les composants de System Center 2012.

Vue d'ensemble de Configuration Manager

Configuration Manager assure la gestion des stocks et des logiciels, le déploiement du système d'exploitation, ainsi que la gestion des appareils mobiles. Configuration Manager fournit plusieurs fonctionnalités et avantages clés, notamment :



- Automatisation du déploiement du système d'exploitation. Cela implique de fournir aux administrateurs les outils nécessaires pour créer et déployer des images de système d'exploitation sur les ordinateurs en utilisant un environnement PXE (Preboot Execution Environment) ou des supports portables, tels que des lecteurs flash USB ou des DVD.
- Déploiement d'applications logicielles. Cela permet aux administrateurs de gérer le déploiement d'applications vers les utilisateurs sur des périphériques tels que des ordinateurs de bureau, des serveurs, des portables et des appareils mobiles. En outre, les administrateurs peuvent créer un catalogue d'applications et le publier sur un site Web en libre-service.
- Gestion des mises à jour de logiciels. Cela inclut la gestion avancée, la surveillance et le déploiement des mises à jour logicielles.
- Regroupement avancé des ressources et outils de contrôle à distance. Cela permet aux administrateurs de contrôler les clients à distance à partir de la console Configuration Manager.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Protection des points de terminaison. La protection des points de terminaison de Configuration Manager active la gestion de la sécurité des appareils, le Pare-feu Windows, et la détection et la suppression des logiciels malveillants.
- Gestion de la conformité et des paramètres. La fonctionnalité de paramètres de conformité vous permet de suivre, d'évaluer et de corriger la conformité de la configuration des périphériques tels que les serveurs, les stations de travail, les ordinateurs portables et les appareils mobiles.
- Dans Configuration Manager, Asset Intelligence et l'inventaire des ressources offrent la possibilité de collecter des informations sur le matériel et les logiciels de l'organisation. Vous pouvez également surveiller l'utilisation des licences de logiciel.

Configuration Manager comprend les autres fonctionnalités suivantes :

- Administration des fonctionnalités et des plans d'alimentation.
- Gestion de la surveillance et de l'intégrité des clients.
- Gestion des bureaux virtuels.
- Gestion des appareils mobiles Active Sync.

Microsoft System Center 2012 Configuration Manager Service Pack 1 (SP1) inclut de nouvelles fonctions et fonctionnalités, y compris la prise en charge des éléments suivants :

- Windows® 8.
- Déploiement des applications Windows 8.
- Administration en temps réel des tâches associées à Microsoft System Center 2012 Endpoint Protection.

Liens de référence : Pour plus d'informations sur les fonctionnalités de System Center 2012 Configuration Manager, accédez à la page http://go.microsoft.com/fwlink/?LinkID=286070.

Vue d'ensemble de Virtual Machine Manager

VMM fournit aux administrateurs un outil d'administration unique pour déployer et gérer une infrastructure de virtualisation, y compris des composants tels que des hôtes, du stockage, des réseaux, des bibliothèques et des serveurs de mise à jour. Cette infrastructure fournit la base de la gestion de la configuration et du déploiement des ordinateurs virtuels. Vous pouvez utiliser VMM pour gérer un seul ordinateur hôte d'un ordinateur virtuel ou jusqu'à 400 hôtes et 8 000 invités.

Fonctionnalités de VMM
- Déploiement complet des hôtes
- Création d'hôtes et de clusters
- Groupes d'hôtes
- Gestion interplateforme
- Configuration du stockage/Configuration réseau
- Placement intelligent/Optimisation dynamique
- Optimisation de l'alimentation
- PRO
- P2V

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

VMM est constitué d'un serveur VMM, d'une base de données VMM et de la console Virtual Machine Manager. Il s'agit des composants principaux exigés par un déploiement et vous pouvez les déployer sur un seul serveur ou sur plusieurs serveurs. Une section ultérieure de ce module détaille les conditions requises pour le déploiement.

Voici quelques fonctionnalités clés de VMM :

- Déploiement complet des hôtes. Vous pouvez automatiser le déploiement des ordinateurs hôtes Windows Server où le rôle serveur Hyper-V est installé sur les serveurs physiques dotés d'un contrôleur BMC (Baseboard Management Controller) et qui répondent aux conditions préalables de découverte et de déploiement. System Center 2012 SP1 permet aux administrateurs de découvrir plus d'informations sur les ressources d'un hôte cible et de configurer plus de paramètres réseau, tels que des commutateurs logiques.
- Création d'hôtes et de clusters. Vous pouvez créer facilement des hôtes et des clusters Hyper-V à l'aide de la console Virtual Machine Manager qui simplifie le déploiement manuel et réduit la possibilité d'erreurs de configuration.
- Groupes d'hôtes. Vous pouvez regrouper des hôtes en fonction d'une séparation logique, telle que l'utilisation métier, les performances ou l'emplacement géographique, et vous pouvez également appliquer des modifications à plusieurs hôtes.
- Gestion interplateforme. VMM prend en charge la gestion des hôtes et des pools XenServer de Citrix et prend en charge les hôtes VMware ESX via l'intégration à VMware vSphere.

 **Remarque :** VMM SP1 peut gérer uniquement les hôtes Windows Server 2008 R2 ou Windows Server 2012. Vous ne pouvez pas gérer les ordinateurs hôtes Windows Server 2008 à l'aide de VMM SP1. Vous pouvez également gérer XenServer versions 6.0 et 6.1 à l'aide de VMM SP1. Cependant, vous devez d'abord installer le pack d'intégration System Center sur les hôtes XenServer, puis ajouter les hôtes dans VMM.

- Configuration du stockage. VMM prend en charge la découverte, la classification et l'approvisionnement du stockage pour vos hôtes Hyper-V, y compris les capacités d'allocation dynamique. La détection du stockage VMM fonctionne avec les fournisseurs de stockage SMI-S (Storage Management Initiative Specification), CIM-XML (Common Information Model-Extensible Markup Language) et SMP. En outre, VMM 2012 SP1 prend également en charge le nouveau service Gestion du stockage Windows basé sur des normes et le protocole SMB 3.0.
- Configuration réseau. La configuration réseau permet la création de réseaux logiques, de pools d'adresses MAC (Media Access Control) et des équilibrages de charge pris en charge. En outre, VMM prend en charge les nouvelles fonctionnalités de virtualisation réseau de Windows Server 2012, notamment la possibilité d'exécuter des adresses se chevauchant sur le même réseau physique.
- Placement intelligent. Cette fonctionnalité vous aide à sélectionner un hôte approprié, en fonction de l'ordinateur virtuel que vous déployez, et inclut des évaluations des hôtes selon les seuils d'utilisation prévus, tels que le pourcentage d'unité centrale (UC), d'E/S et de débit du réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

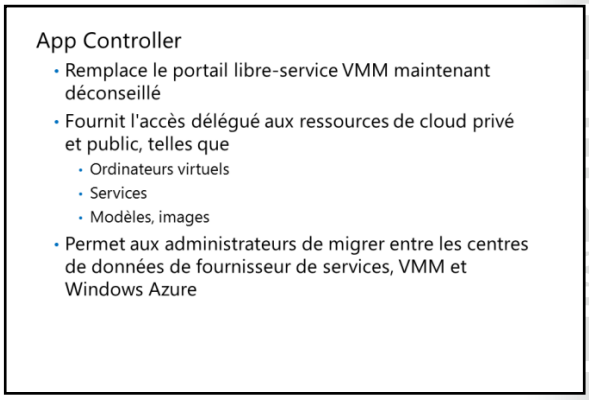
- Optimisation dynamique. VMM peut équilibrer automatiquement les charges de travail en fonction de seuils configurables pour les principales ressources, telles que l'utilisation de l'UC, de la mémoire, du disque et du réseau.
- Optimisation de l'alimentation. Vous pouvez configurer VMM pour qu'il utilise les seuils que vous spécifiez. Cela permet l'évacuation des hôtes sous-exploités appartenant à un cluster. Vous pouvez ensuite arrêter ces hôtes afin d'économiser l'énergie. Lorsque la demande augmente, vous pouvez redémarrer ces hôtes.
- Optimisation des ressources et des performances (PRO). Les conseils PRO peuvent offrir une correction prédéfinie selon les alertes. Par exemple, vous pouvez utiliser les conseils PRO pour lancer la migration dynamique d'un ordinateur virtuel depuis un ordinateur hôte largement utilisé vers un ordinateur hôte disposant de davantage de capacité.
- Microsoft Server Application Virtualization (Server App-V). Server App-V permet la virtualisation des applications serveur. VMM comporte un concepteur de modèles et de services intégré qui peut vous aider à construire des applications à un ou plusieurs niveaux. Vous pouvez ensuite déployer ces applications comme des services, que vous pouvez monter en charge via l'automatisation.
- Migration P2V (physique vers virtuel). VMM comporte une fonctionnalité intégrée qui vous permet d'effectuer des migrations P2V et V2V (virtuel vers virtuel).

Liens de référence : Pour plus d'informations sur les nouvelles fonctionnalités de VMM 2012 et VMM 2012 SP1, accédez à la page suivante : Nouveautés de System Center 2012 - Virtual Machine Manager, à l'adresse http://go.microsoft.com/fwlink/?LinkId=253224.

Vue d'ensemble d'App Controller

App Controller est un portail libre-service qui permet aux administrateurs et aux utilisateurs finaux de contrôler, déployer et configurer des applications et des ordinateurs virtuels entre des déploiements VMM et des clouds publics.

App Controller remplace le portail libre-service VMM, qui n'est plus fourni dans System Center 2012 SP1.



Gestion des instances VMM

Vous pouvez configurer App Controller pour utiliser jusqu'à cinq serveurs VMM et leurs ressources. App Controller fournit l'accès Web via lequel vous pouvez contrôler les applications et les ordinateurs virtuels ainsi que leurs ressources, y compris les bibliothèques et les partages.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion des ressources de cloud public

App Controller peut également contrôler jusqu'à 20 abonnements Windows Azure™. Il vous permet de télécharger des disques durs virtuels et des images sur Windows Azure à partir d'une bibliothèque ou de partages réseau, et d'ajouter des ordinateurs virtuels aux services déployés dans Windows Azure. En outre, vous pouvez manipuler les ordinateurs virtuels et les faire migrer vers et depuis Windows Azure.

Dans System Center 2012 SP1, App Controller vous permet désormais d'ajouter une connexion à un fournisseur d'hébergement d'infrastructure de fournisseur de services, via laquelle vous pouvez connecter votre instance d'App Controller à un service configuré par un fournisseur d'hébergement qui utilise Service Provider Foundation. Service Provider Foundation permet aux fournisseurs de services d'offrir l'infrastructure en tant que service (IaaS) à leurs clients.

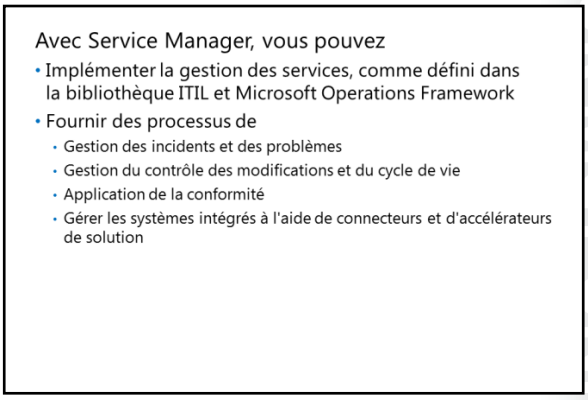
App Controller vous permet d'effectuer les opérations suivantes :

- Utiliser l'accès basé sur un rôle aux ressources VMM.
- Utiliser l'accès basé sur un rôle aux ressources d'abonnement Windows Azure.
- Télécharger des fichiers VHD et des images sur Windows Azure à partir d'une bibliothèque VMM.
- Migrer un ordinateur virtuel de VMM vers Windows Azure.

Lorsque vous concevez un environnement de virtualisation, vous ne souhaitez probablement pas donner à toutes les personnes du service informatique l'accès à vos serveurs hôtes de virtualisation et de gestion des systèmes. En outre, vous ne souhaitez probablement pas déployer et gérer des consoles de gestion pour chaque fournisseur ou employé informatique susceptible de ne nécessiter qu'occasionnellement une interaction avec un ordinateur virtuel. Si un employé n'accède régulièrement qu'à un sous-ensemble d'un déploiement d'ordinateurs virtuels, vous devez lui accorder des autorisations uniquement pour les tâches qu'il doit effectuer, et rendre visibles uniquement les systèmes dont il a besoin. App Controller est un portail Web qui fournit cet accès et des capacités de libre-service permettant aux administrateurs de déployer et d'administrer des ressources sur plusieurs serveurs VMM, ainsi que des ressources de centre de données de fournisseur de services et Window Azure.

Vue d'ensemble de Service Manager

Service Manager est un composant destiné à l'automatisation des processus métier et à l'implémentation de la gestion des services comme défini dans la bibliothèque ITIL (Information Technology Infrastructure Library) et Microsoft Operations Framework. Il existe de nombreux processus prêts à l'emploi pour la gestion des incidents et des problèmes, ainsi que pour la gestion des modifications, des versions et du cycle de vie.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les environnements de virtualisation sont dynamiques par nature. Par conséquent, vous devez idéalement les régir à l'aide de processus et de procédures documentés qui sont basés sur la bibliothèque ITIL ou Microsoft Operations Framework. Service Manager peut vous aider à régir l'informatique de virtualisation ou de cloud privé avec les fonctionnalités suivantes :

- Gestion des incidents, des problèmes, des modifications et des versions. Service Manager offre aux propriétaires d'application et d'infrastructure, aux administrateurs, aux analystes de service et aux utilisateurs finaux un emplacement unique à partir duquel ils peuvent régir et gérer les modifications de déploiement et administrer un environnement de virtualisation complexe. Il fournit un portail basé sur Microsoft SharePoint® que vous pouvez personnaliser et configurer facilement avec un catalogue de logiciels ou de services que vous pouvez lier à des offres de demande de libre-service. Vous pouvez configurer des offres de demande pour déclencher les processus système et les processus d'approbation qui fournissent la demande. Cela fournit un niveau d'automatisation qui augmente notablement l'efficacité.
- Conformité. Service Manager comporte un pack d'administration téléchargeable, qui peut vous aider à gérer et automatiser la gouvernance informatique et les responsabilités en matière de risques et de conformité, ce qui vous permet de lier efficacement les objectifs complexes de l'entreprise à l'infrastructure Microsoft.

 **Remarque :** Les packs d'administration étendent les fonctionnalités de System Center 2012 et permettent l'intégration entre ses composants. Vous pouvez télécharger et installer une grande variété de packs d'administration pour la plupart des composants de System Center.

- Une plateforme intégrée. Service Manager a plusieurs connecteurs disponibles qui permettent d'exploiter ses fonctionnalités d'intégration complète. Vous pouvez utiliser ces connecteurs pour importer des données dans la base de données de gestion de la configuration du Gestionnaire de serveur à partir d'AD DS, de fichiers de valeurs séparées par des virgules (CSV) et d'autres composants de System Center.

Voici quelques-uns des connecteurs disponibles :

- AD DS. AD DS ajoute des informations sur les utilisateurs, les groupes, les imprimantes et les ordinateurs.
- Operations Manager. Il existe deux connecteurs pour Operations Manager. Le premier importe les éléments de configuration qui sont détectés. Le second est un connecteur d'alerte qui peut créer des incidents en fonction d'alertes. Si Operations Manager utilise le pack d'administration Windows Azure, les alertes de Windows Azure sont également disponibles.
- Orchestrator. Orchestrator offre la possibilité d'appeler des Runbooks et vous pouvez ensuite remplir des demandes de catalogue de services automatiquement quand vous utilisez les Runbooks avec le portail libre-service.
- Configuration Manager. Configuration Manager vous permet d'importer les éléments de configuration matérielle et logicielle gérables.
- VMM. VMM importe des objets de modèle et des classifications de stockage que vous pouvez utiliser pour créer des offres de services.

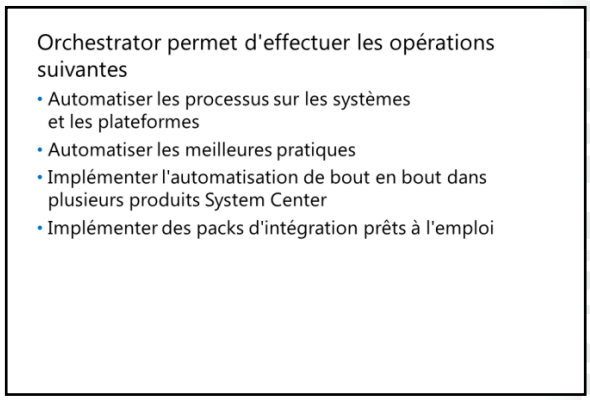
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Microsoft fournit également un accélérateur de solution, Cloud Services Process Pack. Il vous permet d'utiliser des formulaires prédéfinis et une fonctionnalité d'automatisation qui exploite Service Manager, Orchestrator et VMM pour fournir une offre IaaS complète avec une fonctionnalité de libre-service. Ce pack permet aux administrateurs de remplir le catalogue de services avec une offre de demande qui peut être automatisée pour fournir des ressources de cloud et d'ordinateur virtuel aux utilisateurs finaux, tout en garantissant que les processus d'approbation de l'entreprise sont suivis.

Documentation supplémentaire : Pour plus d'informations, accédez à la page suivante : System Center 2012 - Composants de Service Manager, à l'adresse http://go.microsoft.com/fwlink/?LinkId=253994.

Vue d'ensemble d'Orchestrator

Orchestrator est une solution d'automatisation des processus informatiques que vous pouvez utiliser pour automatiser la création, la surveillance et le déploiement des ressources principales de votre environnement. Les administrateurs de centre de données effectuent de nombreuses tâches quotidiennes critiques pour vérifier que leur infrastructure est hautement disponible et fiable. Ils doivent également être en mesure de réduire le temps nécessaire pour mettre une nouvelle infrastructure en service tout en fournissant des capacités de libre-service aux utilisateurs finaux. En outre, les administrateurs doivent préserver les normes de qualité et l'efficacité du système.



À l'aide d'Orchestrator, vous pouvez effectuer les opérations suivantes :

- Automatiser les processus de votre centre de données, indépendamment du matériel ou de la plateforme.
- Automatiser vos opérations de centre de données et normaliser les meilleures pratiques afin d'améliorer l'efficacité opérationnelle.
- Connecter les différents systèmes de différents fournisseurs.

Orchestrator utilise des Runbooks pour automatiser les tâches fréquentes qui doivent être effectuées dans un centre de données. Vous pouvez créer des Runbooks à l'aide de Runbook Designer dans Orchestrator. Runbook Designer est une interface de glisser-déplacer simple qui facilite la conception de processus permettant d'effectuer des tâches complexes.

Voici quelques exemples de Runbooks :

- Création d'utilisateurs Active Directory.
- Déploiement d'ordinateurs virtuels.
- Ajout d'utilisateurs à des groupes.
- Déploiement d'agents de sauvegarde ou de surveillance.
- Envoi de messages de notification pour indiquer l'état ou l'achèvement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Intégration d'Orchestrator à d'autres composants de System Center

Orchestrator comporte un certain nombre d'activités de Runbook intégrées qui remplissent un large éventail de fonctions pouvant être étendues avec des packs d'intégration. Les packs d'intégration contiennent les activités et les objets de Runbook qui donnent à Orchestrator la possibilité d'étendre ses fonctionnalités à d'autres composants Microsoft et tiers. Le pack d'intégration pour Service Manager comprend les activités qui permettent à Orchestrator d'obtenir le détail des incidents et des problèmes qui ont été générés dans l'environnement Service Manager. Cette intégration fournit un mécanisme utile pour l'automatisation de tâches avec Service Manager. Par exemple, vous pouvez créer dans Orchestrator un Runbook qui crée un enregistrement de problème dans Service Manager lorsque le nombre d'incidents liés à celui-ci atteint un nombre spécifique.

Le pack d'intégration pour Data Protection Manager comprend les activités qui vous permettent d'automatiser des tâches dans l'environnement Data Protection Manager. Par exemple, vous pouvez créer un Runbook qui automatise la protection d'une source de données, telle qu'un serveur SQL Server, en fonction d'un nouveau service configuré dans VMM.

La génération de Runbooks à partir des activités des packs d'intégration peut garantir que les tâches répétitives sont effectuées rapidement et avec une exactitude accrue. En outre, vous pouvez concevoir vos propres packs d'intégration pour créer les flux de travail et les processus nécessaires.

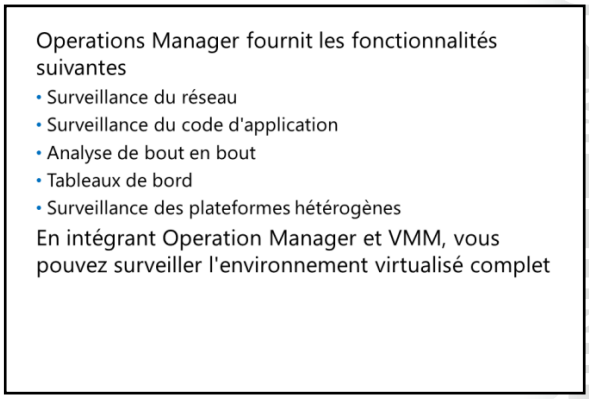
Les packs d'intégration mis à jour pour System Center 2012 sont disponibles dans le centre de téléchargement Microsoft.

Orchestrator est doté de plusieurs nouvelles fonctionnalités dans System Center 2012 SP1, notamment :

- Nouveaux packs d'intégration, y compris certains packs d'intégration tiers.
- Fonctionnalités de gestion pour les rôles d'utilisateur libre-service de VMM.
- Fonctionnalités de gestion pour plusieurs tampons VMM (unités d'échelle). En outre, vous pouvez agréger les résultats de plusieurs tampons.
- Intégration à App Controller pour gérer les environnements hébergés.

Vue d'ensemble d'Operations Manager

Operations Manager est une solution de surveillance et d'alerte interplateforme qui assure la surveillance de l'infrastructure et des applications. Vous pouvez intégrer Operations Manager à VMM, Service Manager et Orchestrator pour fournir une correction automatisée en réponse aux erreurs, aux problèmes de performances et aux pannes. Operations Manager fournit également des packs d'administration pour surveiller d'autres systèmes, y compris de nombreux composants matériels et logiciels tiers.



Operations Manager comprend les fonctionnalités suivantes :

- Surveillance du réseau. Operations Manager prend en charge la découverte des routeurs et des commutateurs réseau. Il fournit une plateforme avec laquelle vous pouvez surveiller les réseaux, du Bureau aux serveurs.
- Surveillance du code d'application. Operations Manager fournit des informations de surveillance détaillées sur les applications, y compris les applications .NET et Java Enterprise Edition, et permet d'identifier et de repérer précisément les problèmes liés aux applications.
- Analyse de bout en bout. Operations Manager peut surveiller les applications de bout en bout. Cela signifie qu'il peut surveiller l'application, le système d'exploitation sur lequel elle s'exécute, le matériel sur lequel repose le système d'exploitation et les périphériques réseau qui sont utilisés pour fournir l'accès à cette application. Si l'application est distribuée sur plusieurs systèmes, vous pouvez configurer Operations Manager pour montrer la topologie de l'application dans un volet unique afin que les opérateurs puissent voir immédiatement où se situe le problème dans cette topologie.
- Tableaux de bord. Operations Manager offre des tableaux de bord prédéfinis et facilement personnalisables pour surveiller les statistiques clés, les alertes et les problèmes à partir d'une console de gestion unique.
- Surveillance des plateformes hétérogènes. Operations Manager surveille non seulement les serveurs et les applications Windows, mais il gère également les systèmes Linux et UNIX pour détecter les problèmes d'intégrité et de performances.

Operations Manager utilise les packs d'administration qui contiennent les informations sur les objets que vous surveillez. Ceux-ci sont généralement développés par les fournisseurs des applications, par exemple, Microsoft crée des packs d'administration pour chaque version de ses systèmes d'exploitation et applications serveur tels que Microsoft SQL Server et Microsoft Exchange Server.

 **Liens de référence :** Pour rechercher et télécharger des packs d'administration pour System Center, accédez à la page suivante : http://go.microsoft.com/fwlink/?LinkID=286068.

Intégration d'Operations Manager et VMM

VMM et Operations Manager peuvent être intégrés pour fournir la surveillance complète des ordinateurs hôtes physiques et des ordinateurs virtuels. L'intégration de VMM à Operations Manager présente plusieurs avantages, notamment les possibilités suivantes :

- Surveiller l'intégrité et la disponibilité des ordinateurs virtuels, des hôtes, du serveur de gestion VMM, du serveur de base de données VMM et des serveurs de bibliothèque. Vous pouvez également surveiller un environnement virtuel basé sur VMWare.
- Voir les vues de diagramme de votre environnement virtualisé à partir de la console Operations Manager.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Implémenter les conseils PRO, qui collectent les données de performances des ordinateurs hôtes, des ordinateurs virtuels et des applications. Les conseils PRO vous permettent d'automatiser les modifications apportées à VMM et à l'environnement hôte, en fonction des informations de performances fournies par Operations Manager. Par exemple, si un disque dur physique est défaillant, une alerte dans Operations Manager peut déclencher l'évacuation de l'hôte dont le sous-système de disque est dégradé. Un autre exemple pourrait être l'utilisation des informations de performances pour monter automatiquement en charge une batterie de serveurs Web en réponse à une augmentation des transactions dans VMM. Les rapports sont disponibles dans la console Virtual Machine Manager, mais les données d'affichage sont récupérées à partir d'Operations Manager.
- Activer l'intégration du mode maintenance. Lorsque vous placez des hôtes en mode de maintenance, VMM tente de les mettre en mode de maintenance dans Operations Manager.
- Intégrer SQL Server Analysis Services (SSAS), qui vous permet d'exécuter des rapports de prévisions qui peuvent prévoir l'activité hôte selon l'historique de l'espace disque, de la mémoire, des E/S réseaux, des E/S de disque et de l'utilisation de l'UC. Il prend également en charge l'utilisation d'un réseau SAN pour les prévisions d'utilisation.

Liens de référence : Pour plus d'informations, accédez à la page Connexion de VMM à Operations Manager - http://go.microsoft.com/fwlink/?LinkID=286069.

Vue d'ensemble de Data Protection Manager

Data Protection Manager est une solution de sauvegarde et récupération des données qui fonctionne pour les sauvegardes disque-à-disque et disque-à-bande. Elle vous permet de sauvegarder et restaurer des serveurs Microsoft Windows et des serveurs d'applications tels que SQL Server, Exchange Server, Hyper-V, les serveurs de fichiers, AD DS et SharePoint Server. Data Protection Manager inclut également la prise en charge de la récupération de l'état du système et de la récupération complète, offre une protection pour les clients de Bureau Windows, et fournit quelques éléments libre-service.

Data Protection Manager fournit les fonctionnalités suivantes
- Sauvegardes VSS
- Sauvegarde et récupération de niveau élément Hyper-V
- Prise en charge des hôtes et des invités Hyper-V
- Intégration à Operations Manager
- Intégration à d'autres composants de System Center 2012
- Fonctionnalité de libre-service

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous planifiez un environnement de virtualisation, vous devez implémenter un système de sauvegarde capable de sauvegarder les éléments suivants :

- Ordinateurs virtuels. Parfois appelées sauvegardes traditionnelles, au niveau invité ou d'ordinateur virtuel, les sauvegardes n'ont généralement pas conscience de la virtualisation et sont conçues avec une application à l'esprit. Par exemple, les sauvegardes Microsoft Exchange doivent protéger les composants Exchange, tels que les magasins et les boîtes aux lettres. En outre, si vous souhaitez protéger l'intégralité de la structure de serveur, vous devez effectuer une sauvegarde de l'état du système et inclure les pilotes de données. Si vous devez récupérer tout le serveur, vous devez effectuer la récupération à partir d'une sauvegarde complète de tous les composants.
- Serveurs hôtes. Une sauvegarde au niveau de l'hôte, à ne pas confondre avec la sauvegarde de l'hôte lui-même, est une sauvegarde compatible avec Hyper-V conçue pour protéger les fichiers de virtualisation qui comportent un ordinateur virtuel, tels que les fichiers de configuration d'ordinateurs virtuels, les disques durs virtuels et les instantanés. Data Protection Manager utilise le service VSS pour sauvegarder des fichiers alors qu'ils s'exécutent. Vous pouvez utiliser cette forme de sauvegarde pour récupérer un ordinateur virtuel complet ou l'un de ses disques, en place, sur le même serveur hôte de virtualisation ou sur un autre serveur hôte de virtualisation.

Data Protection Manager fournit certaines fonctionnalités importantes en tant que système de sauvegarde de centre de données :

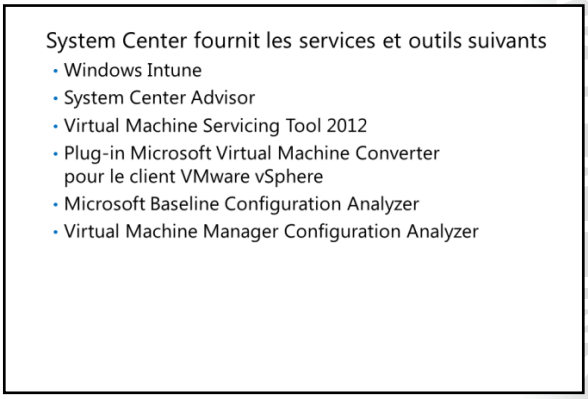
- Sauvegardes VSS. Data Protection Manager utilise VSS pour assurer la protection des sources de données lorsque la source de données continue de s'exécuter. Cela signifie que les applications et les serveurs n'ont pas besoin d'être mis hors connexion pendant que Data Protection Manager leur fournit la protection. Après l'exécution d'une sauvegarde complète initiale, Data Protection Manager peut sauvegarder uniquement les modifications de bloc, de façon incrémentielle, ce qui permet une sauvegarde et une restauration rapides et efficaces.
- Prise en charge de la récupération de niveau élément Hyper-V. Data Protection Manager peut récupérer des fichiers, des dossiers, des volumes et des disques durs virtuels spécifiques à partir d'une sauvegarde de niveau hôte des ordinateurs virtuels Hyper-V.
- Prise en charge des hôtes et des invités Hyper-V. Data Protection Manager prend en charge la protection basée sur l'hôte, où l'agent est installé sur l'ordinateur hôte, et la protection basée sur l'invité, où l'agent est installé sur l'ordinateur virtuel. Pour les invités exécutant Windows Server 2003 et versions plus récentes, Data Protection Manager fournit des sauvegardes en ligne qui garantissent que Data Protection Manager n'interrompt pas l'ordinateur virtuel protégé en assurant la protection.
- Intégration à Operations Manager, qui fournit la surveillance de l'environnement Data Protection Manager à l'aide du pack d'administration Data Protection Manager. La console centrale de Data Protection Manager qui est intégrée à Operations Manager vous permet de surveiller tous les serveurs Data Protection Manager à partir d'un ordinateur central. Vous pouvez utiliser la console centrale pour ouvrir une console d'administration Data Protection Manager afin de gérer Data Protection Manager à distance.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Intégration à d'autres composants de System Center 2012. Grâce à l'intégration de Data Protection Manager à Orchestrator, il est possible d'automatiser des fonctions telles que la protection et la récupération de données. En utilisant Service Manager et le portail libre-service conjointement avec Data Protection Manager et Orchestrator, vous pouvez également offrir ces fonctions en tant que services dans le cloud privé.
- Fonctionnalité de libre-service. Data Protection Manager comporte également une fonction de libre-service qui permet aux administrateurs de configurer et déléguer la fonctionnalité de restauration aux utilisateurs libre-service. Vous pouvez accorder l'autorisation d'effectuer la restauration sur le même serveur ou sur un autre serveur, et contrôler les autres serveurs.

Autres services et outils de System Center

System Center fournit plusieurs services et outils qui ne font pas partie de ses composants principaux, notamment deux services System Center basés sur le cloud (Windows Intune™ et Microsoft System Center Advisor) et plusieurs outils téléchargeables qui sont détaillés dans les sections suivantes.



Windows Intune

Windows Intune est une solution de gestion et sécurité des ordinateurs basée sur le cloud. Vous pouvez l'utiliser pour déployer des logiciels, prendre en charge des clients via le contrôle à distance, créer des stratégies de gestion des mises à jour et vérifier que votre version de System Center 2012 Endpoint Protection est à jour. Windows Intune offre un grand nombre des fonctionnalités disponibles avec System Center 2012 Configuration Manager, mais sans qu'il soit nécessaire d'avoir un déploiement sur site. La version actuelle de Windows Intune s'intègre à System Center 2012 Configuration Manager SP1 pour permettre aux administrateurs de gérer les périphériques enregistrés avec les deux produits à partir d'une seule console.

System Center Advisor

System Center Advisor est un service d'optimisation basé sur le cloud qui analyse proactivement vos serveurs en utilisant les meilleures pratiques. Il utilise un agent qui peut communiquer avec une passerelle unique pour réduire la bande passante. Le service vérifie les problèmes connus avec Windows Server, AD DS, SQL Server, Exchange Server, SharePoint Server et Hyper-V. System Center Advisor et Window Intune sont des services basés sur le cloud, tandis que les éléments suivants de cette liste sont des outils spécifiques aux tâches.

Virtual Machine Servicing Tool 2012

Virtual Machine Servicing Tool permet aux administrateurs de mettre à jour hors connexion les ordinateurs virtuels des bibliothèques VMM automatiquement. En outre, les administrateurs peuvent mettre à jour les ordinateurs virtuels arrêtés et les modèles d'ordinateur virtuel, et appliquer les mises à jour directes aux disques durs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Plug-in Virtual Machine Converter pour le client VMware vSphere

Les administrateurs qui souhaitent convertir des ordinateurs virtuels VMware en ordinateurs virtuels Hyper-V peuvent utiliser le plug-in Virtual Machine Converter pour le client VMware vSphere. Il étend le client vSphere pour permettre les conversions à partir du menu contextuel de l'ordinateur virtuel.

Microsoft Baseline Configuration Analyzer 2.0

Microsoft Baseline Configuration Analyzer 2.0 peut vous aider à maintenir la configuration optimale du système en analysant les configurations de vos ordinateurs par rapport à un ensemble prédéfini de recommandations et en créant des rapports sur les résultats. C'est un élément prérequis qui doit être installé pour Virtual Machine Manager Configuration Analyzer (VMMCA).

VMMCA

VMMCA est un outil de diagnostic que vous pouvez utiliser pour évaluer les paramètres de configuration des serveurs qui exécutent des rôles serveur VMM ou qui agissent en tant qu'hôtes d'ordinateur virtuel. L'outil VMMCA analyse les configurations matérielles et logicielles des systèmes spécifiés, puis les évalue par rapport à un ensemble de règles prédéfinies, en créant un rapport sur toutes les configurations qui ne sont pas optimales. Pour pouvoir exécuter VMMCA, vous devez d'abord installer Microsoft Baseline Configuration Analyzer.



Liens de référence : Pour plus d'informations, accédez à la page suivante :

- System Center 2012 – Modules complémentaires et extensions du composant Virtual Machine Manager - http://go.microsoft.com/fwlink/?LinkID=285266.
- Microsoft Baseline Configuration Analyzer 2.0 - http://go.microsoft.com/fwlink/?LinkID=286071.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Éléments à prendre en compte pour implémenter un centre de données d'entreprise

Scénario

A. Datum Corporation est une société d'ingénierie et de fabrication. Son siège social se trouve à Londres, en Angleterre, et elle a des filiales en Europe, en Australie et en Amérique du Nord. La société développe également son réseau de partenariats d'entreprise et fournit des services supplémentaires à ses clients. Elle est en pleine expansion et il devient évident que certaines de ses exigences métier évoluent également.

Face à ces changements, les responsables informatiques d'A. Datum lancent un projet pour évaluer l'infrastructure informatique actuelle. Il s'agit d'identifier les composants de l'infrastructure qui doivent être mis à niveau ou améliorés afin de fournir les services requis. Les responsables informatiques ont identifié les exigences suivantes comme principaux objectifs de la mise à niveau de l'infrastructure de serveur chez A. Datum :

- Autant que possible, tous les serveurs, services et applications doivent être déployés dans un environnement d'ordinateur virtuel. La gestion de l'environnement virtuel doit être optimisée pour la virtualisation, la surveillance et l'automatisation.
- Tous les services et applications doivent être disponibles pendant les heures d'ouverture normales, tandis que les services et les applications critiques doivent être disponibles 24 heures sur 24, 7 jours sur 7.
- Les exigences du service de sécurité doivent être satisfaites.
- Plusieurs groupes de l'entreprise ont identifié des exigences métier supplémentaires concernant les sites Web et les applications externes utilisés par les principaux partenaires commerciaux et clients.

Objectifs

À la fin de cet atelier pratique, vous serez à même de planifier l'implémentation des services dans un centre de données d'entreprise.

Durée approximative : 30 minutes

Aucun ordinateur virtuel n'est requis pour cet atelier pratique.

Exercice 1 : Planification de l'implémentation sécurisée de services dans un centre de données d'entreprise

Scénario

Les tâches principales de cet exercice sont les suivantes :

1. Examiner les exigences métier et du service informatique.
2. Déterminer comment répondre aux exigences métier et du service informatique.
3. Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur.

▶ Tâche 1 : Examiner les exigences métier et du service informatique

- Lire le scénario de l'atelier pratique

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Déterminer comment répondre aux exigences métier et du service informatique

Répondez aux questions suivantes :

1. Comment allez-vous répondre à la nécessité de fournir un outil unique pour gérer les hôtes de virtualisation et les ordinateurs virtuels ?
2. Comment allez-vous répondre à la nécessité pour les administrateurs de division de gérer leurs applications et leurs ordinateurs virtuels ?
3. Comment allez-vous répondre à la nécessité de fournir des informations détaillées sur les performances de tous les composants du centre de données ?
4. Comment allez-vous répondre à la nécessité d'automatiser les processus dans le centre de données ?
5. Comment allez-vous répondre à la nécessité de garantir la haute disponibilité des applications requises ?
6. Comment allez-vous répondre aux exigences du service de sécurité ?
7. Comment allez-vous répondre à la nécessité d'améliorer les performances du site Web de ventes ?
8. Comment allez-vous répondre à la nécessité de permettre l'intégration à Trey Research ?
9. Comment allez-vous répondre à la nécessité de fournir l'accès requis au site Web partenaire ?

▶ Tâche 3 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Se préparer à discuter des réponses avec la classe

Résultats : À la fin de cet exercice, vous aurez identifié les composants que vous devrez inclure dans la conception du centre de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question: Expliquez comment les composants de System Center sont intégrés et répertoriez les avantages de l'intégration.

Question: Quelle option de haute disponibilité supplémentaire, que vous n'avez pas avec les ordinateurs physiques, obtenez-vous en déployant des ordinateurs virtuels ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 2

Planification et implémentation d'une stratégie de virtualisation de serveur

Table des matières :

Vue d'ensemble du module **2-1**

Leçon 1 : Planification d'un déploiement VMM **2-2**

Leçon 2 : Planification et implémentation d'un environnement hôte de virtualisation de serveur **2-11**

Atelier pratique : Planification et implémentation d'une stratégie de virtualisation de serveur **2-23**

Contrôle des acquis et éléments à retenir **2-31**

Vue d'ensemble du module

Ce module présente les composants Microsoft® System Center 2012. Vous verrez comment ils peuvent s'intégrer pour vous permettre de configurer, déployer et gérer un environnement de virtualisation de serveur. Ultérieurement, vous examinerez la procédure de planification et les éléments à prendre en compte pour un déploiement Microsoft System Center 2012 - Virtual Machine Manager (VMM).

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- décrire comment utiliser System Center 2012 pour déployer et gérer un environnement de virtualisation ;
- planifier et implémenter une stratégie de virtualisation de serveur à l'aide de Windows® Server 2012 Hyper-V® et de VMM ;
- déployer des hôtes Hyper-V, configurer des groupes d'hôtes et implémenter des bibliothèques VMM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification d'un déploiement VMM

Cette leçon passe en revue la topologie de VMM et présente la configuration matérielle et logicielle requise pour ses composants principaux.

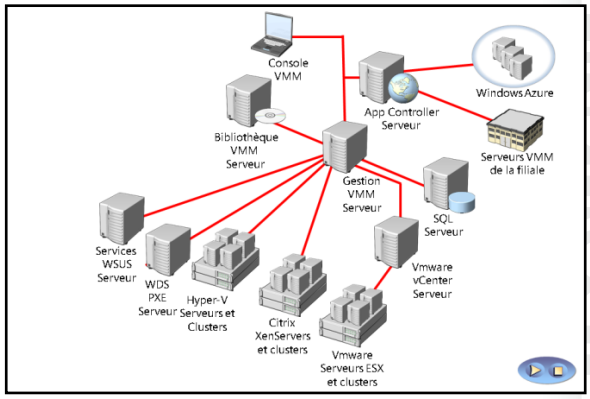
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- comprendre les options topologiques de base des composants principaux de VMM ;
- décrire la configuration requise pour le déploiement du serveur VMM ;
- décrire la configuration requise pour le déploiement de la base de données VMM ;
- décrire la configuration requise pour le déploiement de la bibliothèque VMM ;
- planifier le déploiement VMM de base.

Détermination de la topologie d'un déploiement VMM

La topologie d'un déploiement VMM varie selon les besoins de chaque client. Les facteurs de conception principaux comprennent la définition des limites d'administration et le placement des composants dans un segment réseau, un site ou une zone géographique avec la bande passante suffisante.



Lorsque vous planifiez un déploiement VMM, prenez en compte les éléments suivants :

- le nombre d'hôtes ;
- le nombre de sites de filiales disposant d'hôtes ;
- la sécurité, les groupes administratifs et les options de libre-service dont vous avez besoin ;
- la disponibilité et le temps de récupération que chacun des composants exige.

Le nombre d'hôtes détermine les ressources physiques et virtuelles que nécessite chaque serveur de composant présent dans le déploiement VMM. Le nombre d'hôtes maximum testé par serveur VMM est d'environ 4 000. Même s'il ne s'agit pas d'une limite physique, la demande sur un seul serveur de gestion impliquerait un fractionnement en plusieurs instances VMM. Il est possible d'utiliser App Controller avec cinq instances VMM. Par conséquent, en théorie, il est possible de gérer des ressources provenant de 20 000 à 500 000 ordinateurs virtuels, voire plus. Si votre déploiement présente des milliers d'hôtes, pensez à contacter le bureau régional de Microsoft Office pour obtenir de l'aide sur un déploiement personnalisé correspondant à votre environnement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le nombre de sites de filiales disposant d'hôtes et les fonctions de liaisons WAN (Wide Area Network) entre les filiales et le serveur de gestion VMM détermineront s'il faut envisager un déploiement VMM unique avec plusieurs serveurs de bibliothèques VMM ou un déploiement VMM pour chaque filiale.

VMM propose l'administration déléguée et le libre-service. Il est possible d'utiliser App Controller, le gestionnaire de service ou vos propres portails personnalisés pour que vos utilisateurs accèdent au libre-service. Quand vous déterminez le type de déploiement VMM approprié pour votre environnement, il est possible de planifier un déploiement en libre-service adapté à la conception. Par exemple, App Controller peut couvrir cinq déploiements VMM. Cependant, vos exigences de sécurité peuvent imposer le déploiement d'App Controller pour chaque déploiement VMM.

La disponibilité et le temps de récupération des composants constituent également des éléments importants pour déterminer la topologie d'un déploiement VMM. VMM est une application prenant en charge les clusters et qu'il est possible de rendre hautement disponible. Microsoft SQL Server® prend en charge les clusters. Il est possible d'installer le serveur de bibliothèque sur un cluster de serveurs de fichiers Microsoft, mais pas sur celui qui héberge une instance VMM en cluster. Microsoft Data Protection Manager peut sauvegarder vos composants VMM et, si nécessaire, peut se trouver sur un site distant et être utilisé pour restaurer un ou plusieurs composants hors site.

Pour consulter les toutes dernières informations sur les scénarios de déploiement, ainsi que sur les configurations requises pour chaque composant matériel et logiciel du Service Pack le plus récent, reportez-vous à TechNet.

- Si vous déployez VMM, prenez en compte que la base de données VMM ne prend plus en charge SQL Express. Par conséquent, il est nécessaire de déplacer votre base de données vers une version de SQL Server prise en charge.
- Un serveur de déploiement Windows est requis pour le déploiement sans système d'exploitation des hôtes Hyper-V. Le *déploiement sans système d'exploitation* fait référence au déploiement d'un hôte sur un ordinateur qui n'a pas de système d'exploitation.
- Au moins un serveur de bibliothèque est nécessaire, mais envisagez au moins une bibliothèque pour chaque site. Vous séparerez ces bibliothèques à l'aide d'une liaison WAN à débit réduit.
- Utilisez Windows Server Update Services (WSUS) ou Configuration Manager pour la gestion des mises à jour.
- App Controller a remplacé le portail libre-service. Il n'existe aucun chemin de mise à niveau à partir des portails existants en libre-service vers App Controller.
- Operations Manager est nécessaire pour utiliser la création de rapports VMM et pour tirer profit des astuces PRO (Ressource Performance Optimisation).
- La gestion des hôtes ESX et ESXI nécessite l'intégration de vSphere. Cela peut être intéressant si le nombre maximal d'hôtes ne vous suffit pas ou si, pour des raisons liées à l'entreprise ou au réseau, vous devez disposer de plusieurs serveurs VMM. Il est possible d'utiliser App Controller pour afficher des ressources de cinq serveurs VMM maximum.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans votre topologie, pensez aux services VMM que vous utiliserez et examinez les ports associés dont VMM se sert pour assurer la communication entre ses composants. Assurez-vous que les pare-feu ne bloquent pas de ports et déterminez si le composant coexiste avec une autre application que ces ports examinent. Si vous devez modifier un port par défaut, mettez à jour les règles du pare-feu qui y sont associées. Le tableau suivant répertorie certains des ports par défaut qu'il est possible de modifier pendant l'installation VMM.

Port	Description
8100	Permet la communication avec la console VMM.
5985	Permet la communication avec des agents sur des hôtes et des serveurs de bibliothèques.
443	Active les transferts de fichiers vers des agents sur des hôtes et des serveurs de bibliothèques.
8102	Permet la communication avec les services de déploiement Windows.
8101	Permet la communication avec des agents d'environnement de préinstallation Windows (Windows PE).
8103	Permet la communication avec l'agent Windows PE pour la synchronisation.

Remarque : Si vous prévoyez de déployer le contrôleur d'application sur le même serveur que le serveur de gestion VMM, vous devrez modifier le port utilisé par VMM pour les transferts de fichiers.

Planification de la base de données VMM

Avant l'apparition de VMM, l'édition Express de SQL Server était une option lors de l'installation. Cependant, seules les versions complètes de SQL Server sont actuellement prises en charge avec VMM.

La base de données VMM ne prend plus en charge SQL Express et exige que vous déplaciez votre base de données avant la mise à niveau

Jusqu'à 150 hôtes		Plus de 150 hôtes	
Ressource	**Recommandé**	**Ressource**	**Recommandé**
UC	Pentium 4, 2,8 GHz	UC	Double cœur, 2 GHz
RAM	4 Go	RAM	8 Go
Espace disque	150 Go	Espace disque	200 Go

Remarque : Si vous mettez à niveau une version antérieure de VMM et que vous utilisez une version non prise en charge de SQL Server, vous devez tout d'abord déplacer la base de données. Pour déplacer la base de données VMM, sauvegardez-la, copiez-la sur l'ordinateur qui exécute une version prise en charge de SQL Server, puis restaurez-la.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lors de la planification du placement de votre base de données VMM, pensez à la disponibilité au moment de la conception. S'il est nécessaire d'installer le serveur VMM en tant qu'application en cluster à haute disponibilité, planifiez également la disponibilité pour le serveur SQL qui héberge la base de données.

La base de données VMM peut se trouver sur un serveur SQL avec des bases de données d'autres applications. Par exemple, lors de petits déploiements, il est possible d'envisager l'hébergement de la base de données App Controller. App Controller est un composant distinct de System Center permettant de déléguer des droits et de proposer le libre-service pour votre environnement de virtualisation VMM. Lorsque vous planifiez l'hébergement des bases de données de plusieurs applications, examinez les configurations requises de chacune d'entre elles.

La base de données VMM doit être dans le même domaine que le serveur VMM. Dans le cas contraire, une approbation bidirectionnelle doit être mise en place. Le nom du serveur de base de données SQL ne doit pas dépasser 15 caractères et doit respecter la casse.

Configuration requise pour une base de données VMM

Le tableau suivant répertorie les versions de SQL Server qui sont prises en charge pour l'utilisation de VMM 2012 SP1.

Édition de SQL Server	Service Pack	Éditions
SQL Server 2008 R2 (64 bits)	Service Pack 1 (SP1) ou Service Pack 2 (SP2)	Standard, Enterprise et Datacenter
SQL Server 2012 Enterprise, Standard (64 bits)	Service Pack 1	Toutes

Planification d'un serveur de gestion VMM

Le serveur de gestion VMM exécute le service VMM, qui traite toutes les commandes et gère toutes les communications entre la base de données VMM, les serveurs de bibliothèques et les hôtes de l'ordinateur virtuel. Le serveur VMM prend en charge les clusters et vous pouvez le déployer comme hautement disponible si votre environnement de virtualisation est volumineux.

Lors du déploiement d'un serveur VMM, prenez en compte les éléments suivants

- Le serveur VMM est sans état et prend en charge les clusters
- Si votre serveur VMM est hautement disponible, il ne peut pas héberger de partage de bibliothèque et doit disposer d'un compte pour le service VMM

Configuration matérielle requise pour un serveur VMM

Jusqu'à 150 hôtes

Ressource	Recommandé
UC	Pentium 4, 2,8 GHz ou supérieur
RAM	4 Go
Espace disque	40 Go

Plus de 150 hôtes

Ressource	Recommandé
UC	Double cœur, 3,2 GHz ou supérieur
RAM	5 Go
Espace disque	50 Go

Lorsque vous planifiez un déploiement VMM, n'oubliez pas qu'App Controller peut se connecter à plusieurs serveurs de gestion VMM. Cela peut s'avérer utile lorsque vous déployez plusieurs serveurs de gestion, car cela permet de réduire le trafic entre les hôtes des filiales et un serveur de gestion centralisée.

Remarque : Si vous déployez un serveur de gestion (en cluster) hautement disponible, n'oubliez pas qu'il est impossible d'installer le partage de bibliothèques VMM comme partage en cluster sur le même serveur que celui sur lequel les serveurs de gestion se trouvent.

Remarque : Lorsque vous nommez le serveur de gestion, le nom de l'ordinateur ne peut pas contenir la chaîne de caractères SCVMM. Par exemple, il n'est pas possible de nommer le serveur *ADATUM-SCVMM-01*, mais *ADATUMSCVMMM01* peut être choisi.

Configuration requise pour un serveur de gestion VMM

Le tableau suivant décrit la configuration matérielle requise pour gérer jusqu'à 150 hôtes.

Composant matériel	Minimum	Recommandé
Processeur	Processeur 4, 2 gigahertz (GHz) (x64)	Biprocesseur, 2,8 GHz (x64) ou supérieur
Mémoire vive (RAM).	2 gigaoctets (Go)	4 Go
Espace disque (sans base de données VMM locale)	2 Go	40 Go
Espace disque (avec une version complète de Microsoft SQL Server installée localement)	80 Go	150 Go

Le tableau ci-dessous décrit la configuration matérielle requise pour gérer plus de 150 hôtes :

Composant matériel	Minimum	Recommandé
Processeur	Processeur Pentium 4, 2 GHz (x64)	Biprocesseur, 3,6 GHz (x64) ou supérieur
RAM	4 Go	8 Go
Espace disque dur	10 Go	50 Go

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si vous gérez plus de 150 hôtes, il est possible d'améliorer les performances en séparant les composants VMM. Par exemple, plutôt que d'utiliser le partage de bibliothèque par défaut sur le même serveur que le serveur VMM, il est possible de déployer un serveur de bibliothèques distinct. Inversement, il est possible d'utiliser une base de données VMM sur un serveur SQL dédié.

Le tableau suivant décrit la configuration logicielle requise pour l'installation d'un serveur de gestion VMM.

Configuration logicielle requise	Remarques
Un système d'exploitation pris en charge	Windows Server 2012 (installation complète), édition Standard ou Datacenter.
Service de gestion à distance de Windows (WinRM)	WinRM est inclus dans Windows Server 2012. Par défaut, le service de gestion à distance de Windows (gestion des services Web) est configuré pour démarrer automatiquement. Si le service de gestion à distance de Windows (gestion des services Web) n'est pas démarré, l'installation affiche une erreur pendant la vérification de la configuration requise. Pour que l'installation continue, redémarrez le service.
Microsoft .NET Framework 4 minimum	System Center 2012 SP1 requiert .NET Framework version 4 qui est intégrée à Windows Server 2012.
Kit d'évaluation et de déploiement de Windows (ADK) pour Windows 8	Windows ADK est disponible sur le Centre de téléchargement Microsoft à l'adresse http://www.microsoft.com/en-us/download/details.aspx?id=30652. Lorsque vous installez Windows ADK, sélectionnez les outils de déploiement et fonctionnalités d'environnement de préinstallation Windows.

Configuration requise pour les consoles VMM

Le tableau suivant décrit la configuration matérielle requise pour gérer jusqu'à 150 hôtes.

Composant matériel	Minimum	Recommandé
Processeur	Pentium 4, 550 mégahertz (MHz)	Pentium 4, 1 GHz ou supérieur
RAM	512 Mo	1 Go
Espace disque dur	512 Mo	2 Go

Le tableau suivant décrit la configuration matérielle requise pour gérer plus de 150 hôtes.

Composant matériel	Minimum	Recommandé
Processeur	Processeur 4, 1 GHz	Pentium 4, 2 GHz ou supérieur
RAM	1 Go	2 Go
Espace disque dur	512 Mo	4 Go

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le tableau suivant décrit la configuration logicielle requise pour l'installation de la console de Virtual Machine Manager.

Configuration logicielle requise	Remarques
Un système d'exploitation pris en charge	Répertoriés dans le tableau suivant
Windows PowerShell® 2.0 ou Windows PowerShell 3.0	Windows PowerShell 2.0 est inclus dans Windows Server 2008 R2 et Windows 7. Windows PowerShell 3.0 est inclus dans Windows Server 2012.
Microsoft .NET Framework 4 minimum	Sur un ordinateur qui exécute Windows 7, la version 3.5.1 de .NET Framework est installée par défaut. Sur un ordinateur qui exécute Windows Server 2008 R2, la version 3.5.1 de .NET Framework n'est pas installée par défaut. Cependant, il est possible d'utiliser l'Assistant d'installation de VMM pour installer la fonctionnalité. Sur un ordinateur qui exécute Windows 8 ou Windows Server 2012, .NET Framework 4 est inclus. .NET Framework 4.5 est disponible dans la page de téléchargement de Microsoft Visual Studio® 2012 page à l'adresse http://go.microsoft.com/fwlink/p/?linkId=285269.

Le tableau suivant répertorie les systèmes d'exploitation pris en charge sur lesquels vous pouvez installer la console Virtual Machine Manager.

Système d'exploitation	Édition	Architecture système
Windows Server 2008 R2 Service Pack 1 (installation complète)	Standard, Enterprise et Datacenter	x64
Windows 7 Service Pack 1	Professionnel, Enterprise ou Ultimate	x86 et x64
Windows Server 2012	Standard et Datacenter	x64
Client Windows 8	Standard, Pro et Enterprise	x86 et x64

Il est possible de déployer la console de Virtual Machine Manager sur le serveur de gestion de VMM ou sur un serveur ou une station de travail différent qui exécute un système d'exploitation pris en charge.

Pour activer l'intégration avec App Controller et Operations Manager, il est nécessaire d'installer la console de gestion VMM sur les autres serveurs de System Center. Il est possible d'intégrer Orchestrator et, éventuellement, d'installer la console sur le même serveur que Runbook Designer.

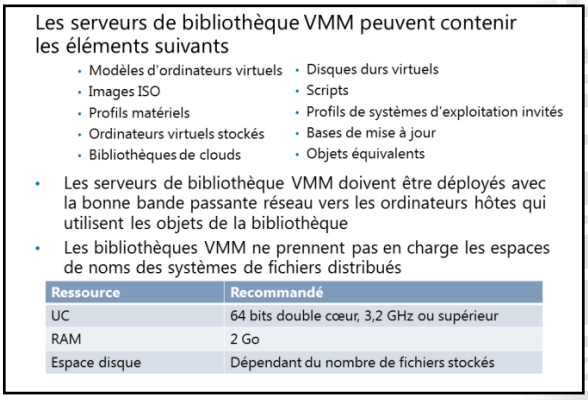
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Portail libre-service VMM

System Center SP1 n'inclut pas le portail libre-service VMM. Ce dernier est facultatif. App Controller est désormais le composant Web pour le libre-service. Un module ultérieur présente la planification et le déploiement d'App Controller.

Remarque : Il n'est pas possible de mettre à niveau le portail libre-service vers App Controller.

Création de l'architecture d'une bibliothèque VMM



Lorsque vous planifiez le matériel pour un serveur de bibliothèque, prenez en compte le nombre d'éléments qui nécessitent du stockage. En particulier, vous devez planifier des éléments tels que des modèles d'ordinateurs virtuels, des disques durs virtuels (VHD) et des images ISO (International Organization for Standardization), qui utilisent plus d'espace que des scripts et des profils.

Par exemple, un profil ne consomme pas beaucoup d'espace. Cependant, les modèles d'ordinateurs virtuels et les images ISO consommeront une quantité d'espace considérable. Il convient donc de planifier la croissance potentielle.

Par exemple, si vous souhaitez disposer d'une image pour Windows Server 2008 R2 et une image pour Windows Server 2012, chaque fichier ISO peut atteindre environ 4 Go. À titre de comparaison, les modèles d'ordinateurs virtuels peuvent atteindre 15 Go.

Prenez en compte les performances requises pour fournir efficacement ces fichiers. Plus votre déploiement sera volumineux, plus il est probable que vous transfèrerez simultanément plusieurs fichiers volumineux vers et à partir de la bibliothèque. Par conséquent, il convient d'en prendre la mesure au niveau de la bibliothèque afin de pouvoir répondre à la demande. Une autre solution consiste à disposer de plusieurs bibliothèques pour équilibrer la charge.

Configuration requise pour des serveurs de bibliothèque VMM

Le tableau suivant répertorie les configurations requises minimales et recommandées en matière de matériel pour l'installation d'un serveur de bibliothèque VMM :

Composant matériel	Minimum	Recommandé
Processeur	Pentium 4, 2.8 GHz	Double cœur, 3.2 GHz ou supérieur
RAM	2 Go	2 Go
Espace disque dur	Varie en fonction du nombre de fichiers stockés et de leur taille	Varie en fonction du nombre de fichiers stockés et de leur taille

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration logicielle requise pour des serveurs de bibliothèque VMM

Le tableau suivant répertorie les configurations requises minimales et recommandées en matière de logiciel pour l'installation et l'exécution d'un serveur de bibliothèque VMM :

Configuration logicielle requise	Notes
Un système d'exploitation pris en charge pour le serveur de bibliothèque VMM	Répertoriés dans le tableau suivant
WinRM	WinRM 2.0 est inclus dans Windows Server 2008 R2 et, par défaut, le service WinRM est configuré pour démarrer automatiquement (démarrage différé). WinRM est inclus dans Windows Server 2012. Par défaut, le service de gestion à distance de Windows est configuré pour démarrer automatiquement.

Le tableau suivant répertorie les systèmes d'exploitation pris en charge sur lesquels vous pouvez installer la bibliothèque VMM.

Système d'exploitation	Édition
Windows Server 2008 R2 Service Pack 1	Standard, Enterprise et Datacenter
Windows Server 2012 (installation complète ou minimale)	Standard et Datacenter

Question : Après avoir lu le scénario, répondez aux questions suivantes :

Comment pouvez-vous déterminer le nombre d'hôtes de virtualisation nécessaires au déploiement ? Quels facteurs devez-vous prendre en compte ?

Que pouvez-vous faire pour garantir que les développeurs peuvent créer des ressources sur site, puis les transférer vers Windows Azure™ ?

Que devez-vous prendre en compte lors de la planification pour déployer App Controller et le serveur de gestion VMM sur le même serveur ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2

Planification et implémentation d'un environnement hôte de virtualisation de serveur

La première étape de l'implémentation de la virtualisation de serveur consiste à planifier le déploiement des hôtes Hyper-V et à utiliser VMM pour gérer ces hôtes. Bien que vous puissiez gérer les hôtes Hyper-V individuellement, il est généralement plus efficace d'utiliser des groupes d'hôtes. Ainsi, vous pouvez configurer les paramètres qui s'appliquent à tous les hôtes des groupes. Cette leçon donne une vue d'ensemble de la planification et de l'implémentation d'hôtes et de groupes d'hôtes dans VMM.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- comprendre la console de gestion VMM ;
- ajouter des hôtes de virtualisation à VMM ;
- déployer les hôtes Hyper-V ;
- décrire les éléments à prendre en compte pour l'implémentation de groupes d'hôtes ;
- configurer les groupes d'hôtes ;
- gérer les bibliothèques VMM ;
- comprendre comment utiliser l'analyseur de configuration pour identifier les problèmes de serveur VMM.

Démonstration : Utilisation de la console de gestion VMM

Dans cette démonstration, vous allez apprendre à :

1. Utiliser des comptes RunAs.
2. Ajouter des hôtes.
3. Afficher les commandes Windows PowerShell sous-jacentes.
4. Afficher les travaux et leurs résultats.

 **Remarque :** Lors de l'ajout d'un hôte Hyper-V, VMM ajoute le rôle Hyper-V s'il n'existe pas. Veillez à ce que votre configuration BIOS prenne en charge un hôte de virtualisation Hyper-V.

 **Liens de référence :** Pour plus d'informations, consultez les conditions préalables à l'installation d'Hyper-V à l'adresse suivante : http://go.microsoft.com/fwlink/p/?linkId=203287.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

Présenter la console Virtual Machine Manager

1. Sur LON-VMM1, dans la barre de tâches, cliquez sur **Console Virtual Machine Manager**.
2. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session Microsoft Windows** est activée, puis cliquez sur **Connecter**. La console Microsoft System Center 2012 - Virtual Machine Manager s'ouvre.
3. Sélectionnez l'un des espaces de travail ci-après, puis passez en revue les différentes fonctionnalités qui apparaissent dans le volet de navigation et sur le ruban :
   - **Ordinateurs virtuels et services**
   - **Ensemble fibre optique**
   - **Bibliothèque**
   - **Travaux**
   - **Paramètres**

Ajouter un hôte Hyper-V

1. Dans la console Virtual Machine Manager, cliquez sur **Ensemble fibre optique**.
2. Sur le ruban, cliquez sur **Ajouter des ressources**, puis sur **Clusters et hôtes Hyper-V**. L'Assistant Ajout d'une ressource démarre.
3. Dans la page **Emplacement de la ressource**, cliquez sur **Ordinateurs Windows Server dans un domaine Active Directory approuvé**.
4. Dans la page **Informations d'identification**, cliquez sur **Entrer manuellement les informations d'identification**, puis entrez les informations d'identification ci-après.
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Dans la page **Étendue de la découverte**, cliquez sur **Spécifier les ordinateurs Windows Server par noms**, puis tapez **LON-HOST1**.
6. Dans la page **Ressources cibles**, sélectionnez **lon-host1.adatum.com**.
7. Dans la page **Paramètres de l'ordinateur hôte**, sélectionnez **Tous les ordinateurs hôtes**.
8. Dans la page **Résumé**, cliquez sur le bouton **Afficher le script**.
9. Cliquez sur **Fermer** pour fermer le script, puis sur **Terminer**.
10. Examinez l'état, puis fermez la fenêtre Travaux une fois la tâche terminée. Un message d'avertissement peut paraître et indiquer que MPIO (multipath I/O) n'est pas activé. Vous pouvez ignorer ce message pour cette tâche.
11. Fermez la console Virtual Machine Manager.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Ajout d'hôtes de virtualisation à VMM

Pour que VMM gère un hôte de virtualisation Microsoft Hyper-V, il est nécessaire de déployer le logiciel de l'agent VMM vers l'hôte à l'aide de la fonction Ajouter des hôtes dans la console VMM. Si l'hôte fait partie d'un réseau de périmètre, déployez manuellement le logiciel de l'agent, puis ajoutez l'hôte dans la console VMM.

Configuration requise pour la prise en charge d'hôtes hétérogènes

- VMWare vCenter Server 4.1 requis pour ESX
- Le serveur de Citrx Xen a besoin du paquet d'intégration de Citrix System Center

VMM 2008 R2 SP1	VMM 2012	VMM 2012 SP1
Virtual Server 2005 R2	Hyper-V	Hyper-V R2 SP1
Hyper-V	Hyper-V R2	Hyper-V R3
Hyper-V R2	Hyper-V R2 SP1	ESX 4.1 ESXi 4.1
Hyper-V R2 SP1	ESX 3.5 ESXi 3.5	ESX 5.0 ESX 5.1
ESX 3.x	ESX 4.1 ESXi 4.1	Citrix XenServer 6.0
ESX 4.0 (Limited)	Citrix XenServer 6.0	Citrix XenServer 6.1

Pour déployer un hôte Hyper-V dans un domaine approuvé :

1. Ouvrez la console VMM, cliquez sur l'espace de travail **Ensemble fibre optique**, cliquez sur le bouton **Ajouter des ressources** sur le ruban, puis cliquez sur Clusters et hôtes Hyper-V.
2. Dans la page **Emplacement de la ressource**, cliquez sur **Ordinateurs Windows Server dans un domaine Active Directory approuvé**, puis sur **Suivant**.
3. Dans la page **Informations d'identification**, choisissez entre Utiliser un compte RunAs (un compte déjà configuré avec des privilèges de domaine) et la saisie manuelle des informations d'identification d'un compte avec des privilèges pour installer l'agent sur le serveur hôte, puis cliquez sur **Suivant**.
4. Dans la page **Étendue de la découverte** il est possible de soit spécifier des noms d'ordinateurs en les saisissant sur des lignes distinctes dans le champ **Noms des ordinateurs**, soit cliquer sur **Spécifier une requête Active Directory pour rechercher les ordinateurs Windows Server**, taper une requête, puis cliquer sur **Suivant**.
5. Dans la page **Ressources cibles**, vous pouvez cliquer sur chaque hôte ou sur **Sélectionner tout**, puis sur **Suivant**. Une boîte de dialogue vous indiquera que vous êtes sur le point d'activer le rôle Hyper-V sur tous les serveurs dans le cadre du processus. Si vous choisissez d'activer le rôle, les serveurs redémarreront pendant le processus. Cliquez sur **OK** pour fermer la boîte de dialogue.
6. La page **Paramètres de l'ordinateur l'hôte** permet d'affecter l'hôte ou les hôtes à un groupe d'hôtes. Une section ultérieure de ce module détaille la notion de groupes d'hôtes. En outre, si vous disposez de plusieurs serveurs VMM, et qu'un autre environnement VMM gère actuellement votre hôte, il est possible d'associer de nouveau l'hôte à cet environnement en cliquant sur **Réassocier**. Il est également possible d'attribuer des chemins de placement par défaut. Ils correspondent aux emplacements dans lesquels Windows stockera les fichiers des nouveaux ordinateurs virtuels Hyper-V ou de ceux qui ont fait l'objet d'une migration. En outre, il est possible d'affecter ces chemins d'accès après avoir ajouté l'hôte, puis de cliquer sur **Suivant**,
7. Dans la page **Résumé**, confirmez les paramètres, puis cliquez sur **Terminer**. La fenêtre Travaux se lance pour vous permettre d'examiner la progression des déploiements d'agents.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Quand vous ajoutez un hôte dans un réseau de périmètre et que vous installez l'agent à partir d'un support d'installation VMM, vous êtes invité à générer un fichier de clé de chiffrement et à attribuer un mot de passe. N'oubliez pas le mot de passe et copiez le fichier généré quelque part sur le serveur VMM pour pouvoir y accéder. Suivez la procédure pour ajouter un hôte, et dans la page **Ressources cibles**, tapez le mot de passe dans le champ **Clé de chiffrement**, puis indiquez l'emplacement du fichier de clé de chiffrement. Le reste de la procédure est identique.

Remarque : Par défaut, le serveur de gestion VMM utilise le port 5986 pour la communication de l'agent avec des hôtes dans un réseau de périmètre et le port 443 pour les transferts de fichiers.

Il est également possible d'utiliser VMM pour gérer des hôtes VMware ESX, ESXi et Citrix XenServer. La procédure d'ajout d'hôtes de fournisseurs supplémentaires est similaire à celle utilisée pour les hôtes Hyper-V, à condition que votre environnement réponde aux conditions requises pour l'ajout de chaque type. Avant d'ajouter un hôte VMware à VMM, il est nécessaire de configurer un serveur vCenter et VMM pour s'y connecter. Avant d'ajouter un hôte Citrix XenServer, il est nécessaire d'ajouter le pack d'intégration Citrix System Center à l'hôte.

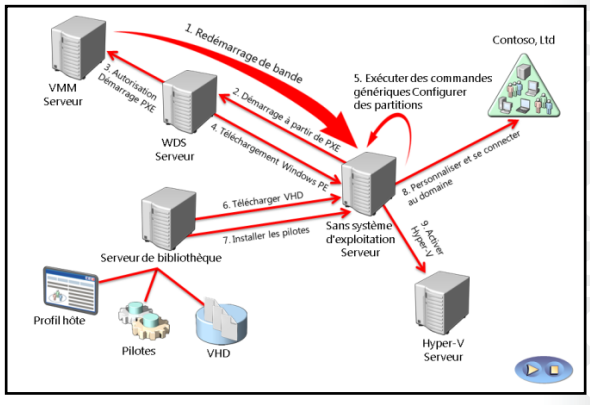
Méthode conseillée : Prenez en compte les exigences de sécurité avant d'ajouter d'autres hôtes de fournisseurs à votre réseau. Par exemple, il est nécessaire de décider du processus d'implémentation des certificats pour des hôtes de virtualisation, ainsi que du processus d'utilisation d'un compte RunAs.

Liens de référence : Pour plus d'informations, accédez à la page suivante :

- Configuration requise : hôtes VMware ESX à l'adresse http://go.microsoft.com/fwlink/p/?linkId=285337.
- Configuration requise : hôtes Citrix XenServer à l'adresse http://go.microsoft.com/fwlink/p/?linkId=285261.

Déploiement d'hôtes Hyper-V

Déploiement d'Hyper-V vers des serveurs sans système d'exploitation



Il est possible d'utiliser VMM et un serveur de services de déploiement Windows pour déployer des ordinateurs hôtes Windows Server 2008 R2 ou Windows Server 2012 sur des serveurs qui n'exécutent aucun système d'exploitation. Cette opération est connue sous l'appellation *déploiement sans système d'exploitation*. Pour ce faire, démarrez l'ordinateur hôte à l'aide de l'environnement PXE (Pre-Boot Execution Environment). Ensuite, les services de déploiement Windows déploient une image de disque VHD ou VHDX vers l'ordinateur hôte. Au redémarrage de l'ordinateur hôte, VMM active le rôle Hyper-V, puis ajoute le serveur au groupe d'hôtes choisi.

Hôtes d'ordinateurs virtuels

Le tableau suivant répertorie les configurations requises pour le déploiement sans système d'exploitation.

Logiciels	Notes
Ordinateur exécutant Windows Server 2008 R2 ou Windows Server 2012, avec le rôle Services de déploiement Windows installé.	Il servira de serveur PXE, qui lance l'installation du système d'exploitation de l'ordinateur physique. Seul le serveur Microsoft PXE est pris en charge.
Ordinateur physique avec contrôleur BMC (Baseboard Management Controller) qui prend en charge le protocole de gestion « hors plage ».	Intelligent Platform Management Interface versions 1.5 ou 2.0. Data Center Management Interface version 1.0. System Management Architecture for Server Hardware version 1.0 pour la gestion des services Web.
Image système Windows Server 2008 R2 ou Windows Server 2012.	L'image du système d'exploitation doit être Windows Server 2008 R2 ou une version plus récente, car elles prennent en charge le démarrage à partir d'un VHD. Il est possible de créer le fichier .vhd ou .vhdx en exécutant l'outil de préparation du système (Sysprep.exe).

Voici une liste d'étapes principales nécessaires à la préparation d'un déploiement sans système d'exploitation :

1. Vérifiez que les paramètres du BIOS peuvent prendre en charge Hyper-V.
2. Définissez l'ordre de démarrage du BIOS de sorte qu'il démarre à partir d'une carte réseau compatible PXE.
3. Ajoutez les fichiers du pilote dans la bibliothèque.
4. Réalisez une image du disque VHD ou VHDX approprié, disponible dans la bibliothèque.
5. Indiquez que vous disposez d'un profil hôte.
6. Vérifiez que le serveur VMM peut communiquer avec le contrôleur BMC, puis exécutez la découverte et le déploiement.

Voici une liste d'étapes principales qui surviennent pendant un déploiement sans système d'exploitation :

1. VMM offre le redémarrage « hors plage » vers le serveur hôte.
2. Le serveur hôte démarre à partir de Windows Deployment Services à l'aide de boot.wim.
3. Le serveur de Services de déploiement de Windows confirme l'autorisation de l'hôte à effectuer un démarrage PXE.
4. L'hôte télécharge l'image Windows PE de VMM.
5. L'hôte exécute l'exécution de la commande générique (GCE), puis configure des partitions telles qu'elles sont définies dans le profil hôte.
6. L'hôte télécharge le VHD ou le VHDX à partir du serveur de bibliothèque VMM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

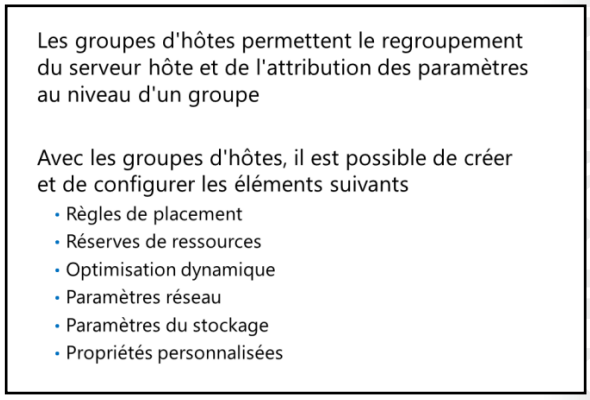
7. VMM installe des pilotes supplémentaires.
8. L'hôte redémarre. Il est ensuite possible de le personnaliser et de le connecter à un domaine.
9. VMM déploie l'agent.

Méthode conseillée : Éléments à prendre en compte pour le déploiement sans système d'exploitation :

- vérifiez que votre microprogramme BMC est à jour, et pensez à mettre à jour tout microprogramme avant le déploiement ;
- vérifiez que l'espace disponible sur la partition du serveur physique est suffisant pour le VHD, car VMM mettra des pilotes en cache pendant le déploiement ;
- lors de la création du fichier VHD ou VHDX, prenez en compte la taille du fichier d'échange de l'hôte. La RAM de l'hôte déterminera ce point. Une fois le serveur déployé, l'administration à distance ne sera pas activée. Pensez à créer une stratégie de groupe qui permette d'effectuer l'administration à distance.

Gestion des groupes d'hôtes

Les groupes d'hôtes vous permettent de planifier et gérer vos serveurs, ce qui facilite l'application de paramètres de gestion au niveau d'un groupe. Sauf indication contraire, le groupe d'hôtes par défaut (Tous les hôtes) correspond à l'emplacement sur lequel tous les serveurs résident.



Il est possible d'imbriquer des groupes d'hôtes. Par conséquent, à moins que vous désélectionniez les paramètres hérités du groupe d'hôtes parent, les paramètres du groupe parent s'appliqueront au groupe hébergé.

Pour créer des groupes d'hôtes, cliquez sur l'espace de travail **Ordinateurs virtuels et services**, puis dans le volet de navigation cliquez avec le bouton droit, puis cliquez sur **Créer un groupe d'hôte**. Le groupe d'hôtes par défaut est appelé **Tous les ordinateurs hôtes**. Pour modifier les propriétés du groupe d'hôtes, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Propriétés**. Dans la page des Propriétés **Général** du groupe d'hôtes, il est possible de modifier les paramètres suivants :

- nommer le groupe ;
- déplacer le groupe ;
- décrire le groupe ;
- autoriser les transferts de fichiers non chiffrés vers le groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Règles de placement

Par défaut, un groupe d'hôtes utilise le paramètre de placement du groupe d'hôtes parent. Si vous souhaitez configurer des règles de placement personnalisées au niveau du groupe individuel, bloquez l'héritage en modifiant le paramètre du groupe d'hôtes parent.

Dans la page **Règles de placement** des propriétés du groupe d'hôtes, il est possible d'affecter des règles de placement personnalisées. Par exemple, il est possible d'attribuer des valeurs personnalisées aux hôtes et aux ordinateurs virtuels. Ces valeurs détermineront le placement à condition que les critères suivants soient respectés :

- l'ordinateur virtuel *doit* correspondre à l'hôte ;
- l'ordinateur virtuel *devrait* correspondre à l'hôte ;
- l'ordinateur virtuel *ne doit pas* correspondre à l'hôte ;
- l'ordinateur virtuel *ne devrait pas* correspondre à l'hôte.

Réserves de ressources de l'ordinateur hôte

Les réserves de ressources sont des paramètres de placement qui permettent au système hôte de conserver les ressources pour sa propre utilisation. C'est utile lorsque des services supplémentaires s'exécutent sur un hôte Hyper-V. Cela peut être le cas dans une filiale disposant d'une bibliothèque VMM configurée.

Le tableau suivant présente, en détail, la procédure pour définir ou refuser les réserves de ressources suivantes au niveau de chaque hôte.

Ressource	Notes
UC	Il s'agit d'un pourcentage. La valeur par défaut est 10. Cependant, 10 % d'un seul processeur double cœur de 2 GHz n'est pas identique à 10 % de quatre processeurs à six cœurs de 2,8 GHz.
Mémoire	La valeur par défaut est 256 Mo, mais il est possible de la modifier ou de la définir en tant que pourcentage.
E/S de disque	La valeur par défaut est 0, mais il est possible de la définir en tant que pourcentage. Si vous utilisez un hôte en tant que bibliothèque VMM, il est possible de s'assurer qu'une quantité minimale est réservée.
Espace disque	Peut être une valeur numérique ou un pourcentage.
E/S réseau	La valeur par défaut est 0, mais il est possible de la définir en tant que pourcentage. Si vous utilisez un hôte en tant que bibliothèque VMM, il est possible de s'assurer qu'une quantité minimale est réservée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Optimisation dynamique

L'optimisation dynamique permet à VMM d'équilibrer automatiquement les charges de l'ordinateur virtuel dans un cluster hôte. En définissant les seuils de ressources minimales pour des hôtes, VMM migrera l'ordinateur virtuel vers d'autres hôtes si les ressources disponibles s'avèrent inférieures à ces seuils.

Le tableau suivant montre les seuils qu'il est possible de définir. Ces paramètres auront des conséquences sur tous les hôtes du groupe d'hôte.

Ressource	Notes
UC	La valeur par défaut est 30 %.
Mémoire	La valeur par défaut est 512 Mo.
E/S de disque	La valeur par défaut est 0.
Espace disque	Peut être une valeur numérique ou un pourcentage.
E/S réseau	La valeur par défaut est 0.

Outre l'équilibrage de la charge de travail, VMM peut également invoquer l'optimisation de l'alimentation. Pour faire, sélectionnez **Paramètres** sous la section **Optimisation de l'alimentation** de la page **Optimisation dynamique**.

Configuration requise pour l'optimisation de l'alimentation

Pour activer la gestion de l'alimentation, il est nécessaire de disposer d'un contrôleur BMC qui prenne en charge un de ces protocoles de gestion « hors plage » :

- Intelligent Platform Management Interface versions 1.5 ou 2.0 ;
- Data Center Management Interface version 1.0 ;
- System Management Architecture for Server Hardware version 1.0 pour la gestion des services Web.

Dans le coin droit de la page Vue d'ensemble de VMM, le nombre d'heures de fonctionnement de l'ordinateur enregistré pendant les 30 derniers jours apparaît. Si vous intégrez Operations Manager à VMM, alors les rapports d'optimisation d'alimentation sont disponibles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration de groupes d'hôtes

Dans cette démonstration, vous allez apprendre à créer des groupes d'hôtes, puis vous découvrirez les options qu'il est possible de configurer et de leur attribuer.

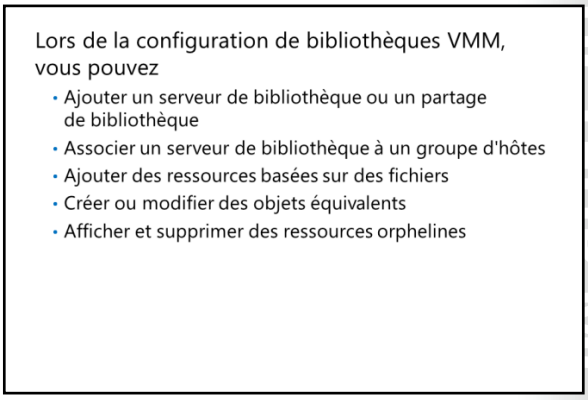
Procédure de démonstration

Examen des groupes d'hôtes de Virtual Machine Manager

1. Dans la barre de tâches, sur **LON-VMM1**, cliquez sur **Console Virtual Machine Manager**.
2. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session de Microsoft Windows** est sélectionnée, puis cliquez sur **Connecter**. La console Virtual Machine Manager s'ouvre.
3. Cliquez sur **Ordinateurs virtuels et services**, puis, dans le volet de navigation, sur **Tous les ordinateurs hôtes**.
4. Sur le ruban, cliquez sur **Créer un groupe hôte**.
5. Tapez **Classe** pour le nom du groupe d'hôtes.
6. Cliquez avec le bouton droit de la souris sur le groupe d'hôtes que vous avez créé, puis cliquez sur **Propriétés**.
7. Examinez les options et les paramètres sur chacune des pages.

Utilisation des bibliothèques VMM

Votre déploiement VMM peut inclure un ou plusieurs serveurs de bibliothèque. Il peut s'agit de n'importe quel serveur Windows qui correspond à la configuration requise. Quand vous ajouterez un serveur de bibliothèque à VMM, VMM déploiera un agent vers le serveur. Vous devez alors configurer un partage de fichiers pour stocker le contenu et ajouter un partage de bibliothèque dans VMM.



Quand vous ajoutez des fichiers sur le partage de bibliothèque VMM, VMM indexe les fichiers pour simplifier le processus de recherche. Par défaut, l'index s'actualise toutes les heures. Il est possible de désactiver l'actualisation ou de modifier la durée d'intervalle (exprimée en heures). L'actualisation des paramètres s'applique à l'ensemble de VMM et à toutes les bibliothèques.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le tableau suivant répertorie les fichiers que VMM indexera.

Ressource	Extension du nom de fichier
VHD	.vhd .vhdx .vmdk
Images ISO	.iso
Scripts Windows PowerShell	.ps1
Scripts SQL Server	.sql
Packages MSDeploy	.zip
Applications de la couche Données de SQL Server (DAC)	.dacpac
Packages de serveur App-V	.osd
Fichiers de pilote	.inf
Fichiers de réponses	.inf .xml
Ressources personnalisées	Dossiers avec extension .CR
Disquettes virtuelles	.vfd .flp

Documentation supplémentaire : Pour plus d'informations, consultez la vue d'ensemble Configuration de la bibliothèque à l'adresse http://go.microsoft.com/fwlink/p/?linkId=285262.

L'ajout et la suppression de serveurs de bibliothèque et de serveurs de bibliothèque de partage doivent répondre à la configuration requise du système d'exploitation et doivent appartenir au même domaine que le serveur VMM ou être effectués dans un domaine avec une approbation bidirectionnelle. Activez le partage de fichiers et d'impression sur les serveurs de bibliothèque. Tous les hôtes qui utilisent le serveur de bibliothèque doivent pouvoir utiliser le protocole SMB (Server Message Block) pour accéder au serveur de bibliothèque.

Remarque : Lorsque vous installez VMM, un partage de bibliothèque par défaut est créé. Par défaut, le partage de bibliothèque est nommé MSSCVMMLibrary et est placé sur le serveur de gestion VMM. Toutefois, si vous installez un serveur VMM (mis en cluster) hautement disponible, vous ne pouvez pas placer la bibliothèque dans le cluster où vous installez VMM.

Association des serveurs de bibliothèque à des groupes d'hôtes

Vous pouvez associer des serveurs de bibliothèque à des groupes d'hôtes spécifiques dans VMM. Cette opération est utile, car elle vous permet de déléguer des autorisations aux serveurs de bibliothèque lorsque vous déléguez des autorisations aux groupes d'hôtes. Lorsque vous utilisez des objets équivalents, cela permet au serveur VMM d'utiliser des ressources dans le même groupe d'hôtes. Cela empêche un serveur d'utiliser une ressource sur des liaisons WAN lentes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Ajouter des ressources basées sur des fichiers

Vous pouvez ajouter des ressources à la bibliothèque VMM de deux façons :

1. Vous pouvez utiliser un explorateur de fichiers tel que l'Explorateur Windows ou l'Explorateur de fichiers ou un autre utilitaire de copie de fichier pour copier ou déplacer des fichiers dans des partages de bibliothèque, tant que vous disposez des autorisations requises pour le dossier ou le partage.
2. Dans la console VMM, cliquez sur l'icône **Bibliothèque**, puis utilisez les options **d'importation et d'exportation de la ressource physique** situées sur le ruban.

Remarque : Pour afficher les ressources que vous avez ajoutées à une bibliothèque, actualisez le partage de bibliothèque manuellement. Pour afficher les ressources, cliquez avec le bouton droit sur le partage ou la bibliothèque, puis cliquez sur **Actualiser**.

Objets équivalents

Vous pouvez marquer les objets des bibliothèques VMM comme des objets équivalents, ce qui permet à VMM d'utiliser l'objet le plus proche. Par exemple, si vous disposez d'un fichier VHDX à Londres et d'une copie dans une bibliothèque VMM à New-York, vous pouvez les marquer comme des objets équivalents. Ensuite, lorsque vous déployez un ordinateur virtuel et qu'un modèle définit un objet correspondant à un objet équivalent, VMM détermine l'emplacement de cette ressource en fonction de l'emplacement de l'objet équivalent le plus proche.

Remarque : Pour éviter d'utiliser inutilement la bande passante réseau lorsque vous déployez des ressources de bibliothèque, associez une bibliothèque convenablement située à un groupe d'hôtes.

Ressources orphelines

Si un dossier, partage ou objet est supprimé d'une bibliothèque alors qu'un modèle pointe vers celui-ci, une représentation de l'objet reste visible dans la bibliothèque. Ceci est appelé un objet orphelin. Pour supprimer l'objet orphelin, vous devez supprimer les références de modèle qui s'y rapportent.

Remarque : Le rétablissement d'une ressource manquante dans la bibliothèque VMM n'entraîne pas sa réassociation automatique aux modèles qui l'ont déjà référencée. Pour résoudre ce problème, vous devez réimporter l'élément.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Après avoir ajouté un nouveau serveur de bibliothèque, il n'apparaît pas sous la zone Ensemble fibre optique.	
Une erreur se produit lorsque vous choisissez d'utiliser un lien vers un fichier ISO de la bibliothèque au lieu de télécharger le fichier sur l'ordinateur virtuel.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Gestion des bibliothèques VMM

Dans cette démonstration, vous allez apprendre à :

- ajouter un serveur de bibliothèque ou un partage de bibliothèque ;
- associer un serveur de bibliothèque à un groupe d'hôtes.

Procédure de démonstration

Configurer une bibliothèque et des partages de bibliothèques

1. Sur **TOR-SVR1,** sur le Tableau de bord du Gestionnaire de serveurs, cliquez sur **Services de fichiers et de stockage**, puis sur **Partages**.
2. Dans l'espace de travail RESSOURCES PARTAGÉES, cliquez sur **TÂCHES**, sur **Nouveau partage**, sur **Partage SMB – Rapide,** sur **Suivant**, sur **Suivant,** tapez **TORVMMLibrary**, cliquez sur **Suivant**, sur **Suivant**, sur **Suivant**, puis sur **Créer**.
3. Cliquez sur **Fermer**.
4. Sur **LON-VMM1,** ouvrez la console Virtual Machine Manager, cliquez sur **Bibliothèque** en bas à gauche de l'écran. Ajoutez **TOR-SVR1\TORVMMLibrary** en tant que nouveau serveur de bibliothèque à l'aide des informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : Pa$$w0rd
5. Examinez l'état du travail, puis fermez la fenêtre Travaux.

   Question : Pourquoi créer un objet équivalent ?

   Citez cinq types d'objets pouvant être stockés dans une bibliothèque.

   Comment empêcher deux serveurs Web de s'exécuter sur le même serveur hôte ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et implémentation d'une stratégie de virtualisation de serveur

Scénario

L'infrastructure informatique chez A. Datum se développe rapidement, mais la société cherche également à réduire les coûts liés à la croissance. Le centre de données de Londres est sur le point d'atteindre sa capacité maximale en matière d'espace et d'alimentation. La société souhaite éviter le coût de développement ou de création d'un nouveau centre de données.

En raison de ces contraintes, l'un des objectifs clés du projet de déploiement de Windows Server 2012 est de virtualiser autant de serveurs, de services et d'applications que possible. L'un des composants principaux de cette stratégie de virtualisation vise à optimiser la gestion de l'environnement virtuel.

La première étape du déploiement de l'environnement virtuel chez A. Datum consiste à planifier et à implémenter les couches d'hôte et de gestion pour la virtualisation. Vous êtes également responsable de la planification de la configuration de l'hôte pour le déploiement du serveur Hyper-V, ainsi que de la planification des composants de l'hôte, tels que les bibliothèques Virtual Machine Manager. Une fois la conception terminée, vous configurerez les composants de la couche de l'hôte requis dans VMM.

Objectifs

Dans cet atelier pratique, vous allez apprendre à :

- planifier le déploiement de l'hôte Hyper-V ;
- configurer des hôtes Hyper-V et des groupes d'hôtes dans VMM ;
- configurer la bibliothèque VMM.

Configuration de l’atelier pratique

Durée approximative : 60 minutes

Ordinateur(s) virtuel(s)	22414B-LON-DC1 22414B-LON-VMM1 22414B-TOR-SVR1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible. Avant de commencer cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22414B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Répétez l'étape 2 pour **22414B-LON-VMM1** et **22414B-TOR-SVR1**.
4. Cliquez sur **22414B-TOR-SVR1**, puis, dans le volet Actions, sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
5. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **Administrateur**
   - Mot de passe : **Pa$$w0rd**
   - Domaine : **ADATUM**
6. Répétez les étapes 4 et 5 pour **22414B-LON-VMM1**.

Exercice 1 : Planification du déploiement de l'hôte Hyper-V

Scénario

A. Datum envisage d'acheter environ 30 serveurs qu'il déploiera comme serveurs Hyper-V. A. Datum envisage de déployer la plupart des serveurs dans le centre de données de Londres, mais étudie également la possibilité de déployer certains des serveurs dans les centres de données de Toronto et de Sydney.

A. Datum achètera les serveurs des fournisseurs situés dans chaque pays, ce qui évitera aux spécifications matérielles pour les serveurs Hyper-V d'être identiques. Votre conception doit optimiser le placement d'ordinateur virtuel sur les serveurs Hyper-V et doit permettre des variations au niveau des configurations matérielles des serveurs.

A. Datum a déployé un serveur VMM unique au centre de données de Londres et prévoit de centraliser la gestion des serveurs Hyper-V à l'aide d'un serveur VMM. A. Datum compte créer plusieurs modèles d'ordinateur virtuel, ainsi que stocker les fichiers ISO d'installation dans l'environnement VMM. L'entreprise s'inquiète de la quantité de bande passante que cette configuration consommera d'une succursale à l'autre. Votre conception pour le déploiement d'Hyper-V et VMM doit réduire l'utilisation de la bande passante réseau entre Londres, Toronto et Sydney.

A. Datum souhaite tirer parti des options disponibles dans VMM pour gérer différemment les ordinateurs hôtes en fonction de l'emplacement du serveur hôte. Vous devez vérifier que les différents groupes d'administrateurs peuvent gérer les serveurs hôtes à Londres, Toronto et Sydney, et que les règles de distribution automatique des ordinateurs virtuels entre les hôtes sont différentes pour chaque emplacement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Documentation supplémentaire

Courrier électronique de Cristina Potra chez A. Datum

De : Cristina Porta
Envoyé : 24 août 2012 09:05
À : Thomas Anderson
Objet : Re : Éléments à prendre en compte pour le déploiement de VMM

Thomas,

Concernant le déploiement de VMM, nous avons discuté avec l'équipe réseau et il semblerait qu'il existe des contraintes au niveau de la bande passante. Nous espérons que votre topologie de déploiement permette d'éviter le déploiement de fichiers VHD et ISO sur le réseau WAN. Si vous souhaitiez procéder au déploiement à la fois sur les centres de données principal et secondaire de Londres, sachez qu'il n'y a aucun souci.

Je vous informe que tout le matériel est désormais présent ici. Les équipes de Sydney et de Toronto ont reçu leurs serveurs. Comme vous le savez, les filiales ne disposent pas de châssis de lame. Voici la liste du matériel dont ils disposent aux deux emplacements :

4 serveurs avec 96 Go de mémoire vive (RAM) et 2 processeurs à 6 cœurs, ainsi qu'1 serveur avec 64 Go de mémoire vive (RAM) et 2 processeurs à quatre cœurs. Les lames du châssis de Londres disposent de 128 Go de mémoire vive (RAM) et de 2 processeurs à 6 cœurs.

Suite à notre dernière réunion, je sais que les représentants de Toronto ont demandé que les serveurs ne soient pas alimentés pendant la journée de travail. Est-ce réalisable ?

Le responsable du développement à Sydney a suggéré que la batterie Web constituée de 4 serveurs ne puisse connaître de temps d'interruption que sur deux serveurs à la fois. Il arrive qu'un serveur sur quatre soit hors connexion et ce responsable s'inquiète de ce qui pourrait se produire, lors de la conversion des serveurs en serveurs virtuels, si 2 serveurs étaient sur le même hôte et que cet hôte tombait en panne tandis qu'un 3è était déjà hors connexion.

Je suis au courant que l'équipe Opérations a mis à niveau System Center Operations Manager et System Center Data Protection Manager vers la toute dernière version ; ils ont l'habitude de sauvegarder SQL et de surveiller un certain nombre de serveurs physiques et d'applications sur les deux sites.

Je pense que j'ai fait le tour de la question. Bonne chance pour votre conception.

Cordialement,

Cristina Porta

Chef de projet

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

----- Message d'origine -----
De : Thomas Anderson
Envoyé : 24 août 2012 08:45
À : Cristina Potra
Objet : Éléments à prendre en compte pour le déploiement de VMM

Cristina,

Avez-vous des informations sur le déploiement VMM, plus spécifiquement sur les nouvelles filiales ? Je travaille sur la proposition de conception finale et j'ai besoin de connaître toutes les exigences. En outre, disposez-vous d'autres informations dont je devrais avoir connaissance ?

Merci

Thomas

Stratégie de virtualisation de serveur chez A. Datum	
Numéro de référence du document : AD070405	
Auteur du document Date	Thomas Anderson 25 août

Présentation des exigences

- gestion centralisée de serveurs hôtes et d'ordinateurs virtuels ;
- délégation de l'administration aux filiales ;
- prendre en charge des variations au niveau matériel sur le serveur ;
- réduire l'utilisation de la bande passante ;
- empêcher les migrations d'ordinateurs virtuels de se produire pendant la journée (Toronto).

Informations supplémentaires

- configurer le déploiement sans système d'exploitation ;
- disposer d'un hôte de maintenance sur chaque site ;
- conserver une utilisation réduite de la bande passante ;
- fournir des rapports de gestion sur les économies d'énergie.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Stratégie de virtualisation de serveur chez A. Datum
Propositions 1. Est-il possible de disposer d'un seul serveur VMM capable de prendre en charge la configuration requise, ou devons-nous implémenter trois serveurs VMM avec App Controller pour afficher les ressources à partir de chacun d'entre eux ? 2. Combien de serveurs de bibliothèque doivent être déployés ? 3. Pouvons-nous empêcher un ordinateur virtuel de se mettre hors tension au cours de la journée ? 4. Comment pouvons-nous faire pour n'utiliser qu'un faible nombre de modèles pour le déploiement de serveurs ? 5. Quelles mesures seront prises pour éviter l'utilisation de la bande passante ? 6. Quels serveurs hôtes peuvent exiger des paramètres de réserve de ressources différents ? Où sont-ils installés ? 7. Quel est l'avantage du coût de maintenance ? Elle apparaît comme un gaspillage de ressources. Peut-elle apporter autre chose ? 8. Comment obtenir des rapports sur les économies d'énergie ?

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation fournie dans le manuel du stagiaire.

▶ Tâche 2 : Mettre à jour le document de proposition

- Répondez aux questions de la section Propositions du document Stratégie de virtualisation de serveur pour A. Datum.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions avec celles du corrigé de l'atelier pratique.

Exercice 2 : Configuration de groupes d'hôtes Hyper-V

Scénario

Maintenant que la conception du déploiement du serveur Hyper-V et de VMM est terminée, vous devez implémenter la configuration du groupe d'hôtes dans VMM. Vous ajouterez l'hôte Hyper-V à VMM, puis vous configurerez les groupes d'hôtes en fonction de la conception.

Les tâches principales de cet exercice sont les suivantes :

1. Ajouter un hôte Hyper-V à VMM.
2. Créer les groupes d'hôtes.
3. Configurer les groupes d'hôtes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Ajouter un hôte Hyper-V à VMM

Ajouter un hôte Hyper-V

1. Dans la barre de tâches, sur **LON-VMM1**, cliquez sur **Console Virtual Machine Manager**.
2. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session de Microsoft Windows** est sélectionnée, puis cliquez sur **Connecter**. La console Virtual Machine Manager s'ouvre.
3. Utilisez l'Assistant Ajout d'une ressource pour ajouter un nouvel hôte Hyper-V en utilisant les informations suivantes :
   - emplacement de l'ordinateur : **Ordinateurs Windows Server dans un domaine Active Directory approuvé**
   - informations d'identification : **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**
   - nom d'hôte : **LON-HOST1**
   - Groupe hôte : **Tous les ordinateurs hôtes**
4. Examinez l'état, puis fermez la fenêtre Travaux une fois la tâche terminée. Un message d'avertissement peut paraître et indiquer que MPIO (multipath I/O) n'est pas activé. Vous pouvez ignorer ce message pour cette tâche.

▶ Tâche 2 : Créer les groupes d'hôtes

Créer les groupes d'hôtes

1. Sur **LON-VMM1**, à partir de la console Virtual Machine Manager, cliquez sur **Ordinateurs virtuels et services**.
2. Sélectionnez le nœud **Tous les ordinateurs hôtes**, puis créez les groupes d'hôtes suivants :
   - **Hôtes de London**
   - **Hôtes de Toronto**
   - **Hôtes de Sydney**

▶ Tâche 3 : Configurer les groupes d'hôtes

Configurer les groupes d'hôtes

1. Sur **LON-VMM1**, à partir de la console Virtual Machine Manager, cliquez sur **Ordinateurs virtuels et services**.
2. Ouvrez la page **Propriétés** des **Hôtes de London**.
3. Définissez la mémoire réservée de l'hôte sur **1024 Mo**.
4. Au niveau du groupe d'hôtes parent, supprimez le caractère héréditaire de l'optimisation dynamique.
5. Configurez la migration automatique des ordinateurs virtuels et modifiez la fréquence des migrations de sorte qu'elles se produisent toutes les 60 minutes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Activez l'optimisation d'alimentation avec la planification par défaut.
7. Déplacez **LON-HOST1** vers le groupe d'hôtes **Hôtes de London**.
8. Ouvrez la page Propriétés des **Hôtes de Toronto**.
9. Au niveau du groupe d'hôtes parent, supprimez le caractère héréditaire de l'optimisation dynamique.
10. Configurez la migration automatique des ordinateurs virtuels et modifiez la fréquence des migrations de sorte qu'elles se produisent toutes les 60 minutes.
11. Activez les paramètres d'optimisation d'alimentation pour empêcher l'optimisation d'alimentation de fonctionner entre 7 am (du matin) et 19 pm du lundi au vendredi.

Exercice 3 : Configuration de bibliothèques VMM

Scénario

Vous avez décidé de déployer une bibliothèque VMM sur un serveur de fichiers situé au centre de données de Toronto afin de réduire l'utilisation du réseau lié au déploiement Hyper-V. Il est nécessaire de configurer la bibliothèque VMM sur le serveur, puis de répartir les composants VMM vers chaque bibliothèque. Vérifiez également que les administrateurs réseau qui créent des ordinateurs virtuels dans le centre de données de Toronto ont accès à tous les fichiers requis dans la bibliothèque.

▶ Tâche 1 : Configurer un serveur et un partage de bibliothèque

Configurer un serveur et un partage de bibliothèque

1. Sur **TOR-SVR1,** sur le Tableau de bord du Gestionnaire de serveurs, cliquez sur **Services de fichiers et de stockage**, puis sur **Partages**.
2. Dans l'espace de travail Partages, cliquez sur **TÂCHES**, puis créez un nouveau partage **Partage SMB – Rapide,** nommé **TORVMMLibrary**.
3. Sur **LON-VMM1**, dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Bibliothèque**.
4. Ajoutez **TOR-SVR1\TORVMMLibrary** en tant que nouveau serveur de bibliothèque avec les ressources par défaut. Utilisez les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Examinez l'état du travail, puis fermez la fenêtre Travaux une fois le travail terminé.

▶ Tâche 2 : Copier les fichiers requis vers le centre de données de la filiale

Copier manuellement des fichiers vers des partages de bibliothèques

1. Sur **LON-VMM1**, dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Bibliothèque**.
2. Développez **Serveurs de bibliothèque**, puis cliquez sur **LON-VMM1.Adatum.com**.
3. Dans le volet d'informations, cliquez avec le bouton droit de la souris sur **Disque vierge – Petit.vhdx**, puis cliquez sur **Ouvrir l'emplacement du fichier**.
4. Dans la fenêtre des disques durs virtuels, cliquez avec le bouton droit de la souris sur **Disque vierge – Petit.vhdx**, et cliquez sur **Copier**. Fermez la fenêtre VHDs, et dans le volet de navigation, développez **Serveurs de bibliothèque**, puis développez **tor-svr1.adatum.com**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Cliquez avec le bouton droit de la souris sur **TORVMMLibrary**, puis cliquez sur **Explorer**. Dans la fenêtre TORVMMLibrary, cliquez avec le bouton droit de la souris sur un espace vide, puis cliquez sur **Coller**.
6. Fermez la fenêtre TORVMMLibrary. Cliquez avec le bouton droit de la souris sur **tor-svr1.adatum.com**, puis cliquez sur **Actualiser**. Vérifiez que le fichier **Disque vierge – Petit.vhdx** apparaît dans la liste d'objets.

▶ Tâche 3 : Attribuer une bibliothèque à un groupe d'hôtes

Attribuer une bibliothèque à un groupe d'hôtes

1. Sur **LON-VMM1**, dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Bibliothèque**.
2. Développez **Serveurs de bibliothèque**, puis cliquez avec le bouton droit de la souris sur **tor-svr1.adatum.com**. Cliquez sur **Propriétés**.
3. Ajoutez **tor-svr1.adatum.com** au groupe d'hôtes **Hôtes de Toronto**.
4. Fermez la console Virtual Machine Manager.

▶ Pour préparer le module suivant

N'éteignez pas les ordinateurs virtuels, car vous en aurez besoin pendant le module suivant.

Question : Quel est le principal facteur pour les décisions de conception pour le déploiement VMM ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Impossibilité d'ajouter des hôtes ESX ou XenServer	

Problèmes réels et scénarios

Lors de la planification d'un projet de virtualisation, un certain nombre d'éléments physiques doivent être pris en compte en matière de centres de données et d'hôtes. La densité de serveur peut changer, ce qui entraînera des conséquences sur la consommation d'alimentation et sur le type de refroidissement requis. Par exemple, un châssis entièrement rempli de lames peut modifier les exigences en matière de refroidissement sur un centre de données utilisant une batterie de serveurs hôtes équipés de cartes graphiques (GPU) pour fournir Microsoft RemoteFX®. Cela peut entraîner une chaleur dégagée supérieure, augmentant de ce fait vos besoins en refroidissement.

Outils

Plug-in Microsoft Virtual Machine Converter pour le client VMware vSphere (version bêta à la connexion)

- Microsoft Virtual Machine Servicing Tool 2012 à l'adresse http://go.microsoft.com/fwlink/p/?linkId=285267.
- Microsoft Assessment and Planning Toolkit à l'adresse http://go.microsoft.com/fwlink/p/?linkId=285265.
- System Center 2012 Virtual Machine Manager Component Add-ons and Extensions à l'adresse http://go.microsoft.com/fwlink/p/?linkId=285266.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 3

Planification et implémentation des réseaux et du stockage pour la virtualisation

Table des matières :

Vue d'ensemble du module **3-1**

Leçon 1 : Planification d'une infrastructure de stockage pour la virtualisation **3-2**

Leçon 2 : Implémentation d'une infrastructure de stockage pour la virtualisation **3-12**

Leçon 3 : Planification et implémentation d'une infrastructure réseau pour la virtualisation **3-19**

Atelier pratique : Planification et implémentation des réseaux et du stockage de virtualisation **3-33**

Contrôle des acquis et éléments à retenir **3-44**

Vue d'ensemble du module

Après la conception et le déploiement des hôtes, l'étape suivante de l'implémentation d'une infrastructure de virtualisation de serveur consiste à planifier le stockage et les composants réseau. En particulier, la planification de l'infrastructure de stockage est cruciale car vous exécuterez de nombreux ordinateurs virtuels qui partageront tous le même stockage.

Ce module décrit les facteurs que vous devez prendre en compte lorsque vous planifiez le stockage et l'infrastructure réseau pour votre environnement virtuel, et les détails du déploiement de ces composants de Windows® Server 2012 Hyper-V® et Microsoft® System Center 2012 - Virtual Machine Manager (VMM).

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- planifier une infrastructure de stockage pour la virtualisation de serveur ;
- implémenter une infrastructure de stockage pour la virtualisation de serveur ;
- planifier et implémenter une infrastructure réseau pour la virtualisation de serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification d'une infrastructure de stockage pour la virtualisation

Avant de pouvoir déployer les ordinateurs virtuels, vous devez planifier et déployer l'infrastructure de stockage que les ordinateurs virtuels utiliseront. Dans cette leçon, vous allez explorer les options de stockage disponibles pour les ordinateurs virtuels.

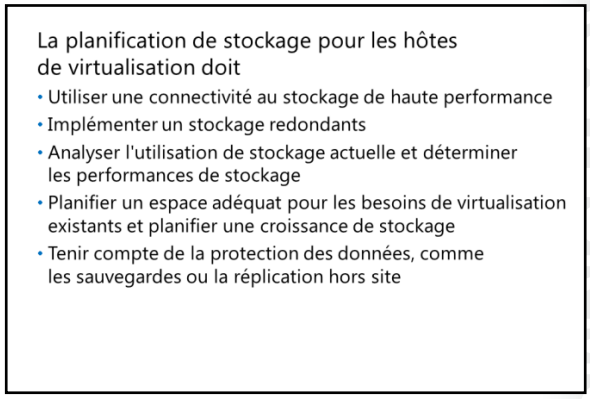
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options de stockage pour la virtualisation de serveur ;
- décrire les options de configuration du disque dur virtuel (VHD, Virtual Hard Disk) ;
- expliquer les éléments à prendre en compte lors de l'implémentation du stockage Fibre Channel ;
- expliquer les éléments à prendre en compte pour implémenter le stockage iSCSI (Internet SCSI) ;
- expliquer les éléments à prendre en compte pour l'implémentation du stockage NFS (Network File System) et SMB (Server Message Block) version 3.0 ;
- décrire les options disponibles pour rendre le stockage hautement disponible dans les scénarios de virtualisation de serveur.

Options de stockage pour la virtualisation de serveur

Un facteur important lors de la mise en service des ordinateurs virtuels est de s'assurer que l'infrastructure de stockage sous-jacente est fiable et peut offrir les performances adéquates. Cela inclut la copie aux heures d'utilisation les plus fortes, comme les sauvegardes, les analyses antivirus, et plusieurs démarrages d'ordinateur virtuel simultanés. Le stockage est l'une des ressources les plus compliquées et coûteuses à gérer dans les projets de virtualisation, et il est avantageux pour une organisation de concevoir des solutions de stockage qui offrent la flexibilité de mettre à l'échelle et d'atteindre une croissance future, mais pas la capacité de surapprovisionnement.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Windows Server 2012 repose sur, et présente, les nouvelles options de stockage pour la virtualisation, qui offrent des solutions de stockage hautement disponibles aux petites et moyennes entreprises. Ces solutions étaient auparavant disponibles uniquement en investissant dans les technologies de zone de stockage réseau (SAN) ou des logiciels tiers. Une section ultérieure de ce module détaille les nouvelles fonctionnalités de stockage qui sont importantes pour les déploiements de virtualisation.

Lorsque vous planifiez un environnement de virtualisation, les performances de disque dur virtuel peuvent affecter les performances de l'ordinateur virtuel. Les serveurs que vous mettez en service normalement avec la capacité de la mémoire vive (RAM) et du processeur peuvent encore rencontrer des performances insatisfaisantes si vous configurez mal le système de stockage ou si ce dernier est submergé par le trafic. Il est important de vérifier que la conception de stockage fournit les performances adéquates, et que votre conception comprend un plan d'analyse du stockage pour la disponibilité et les performances.

Tenez compte des facteurs suivants lors de la planification du stockage :

- Connexion hautes performances au stockage. Vous pouvez localiser des fichiers VHD ou VHDX sur le stockage local ou distant. Quand vous localisez ces fichiers sur un stockage distant, vous devez vérifier que la bande passante est adéquate et que la latence est minimale entre l'hôte et le stockage distant. Les connexions réseau au stockage qui sont lentes ou les celles présentant de la latence ont comme conséquence des performances diminuées au niveau de l'ordinateur virtuel.
- Stockage redondant. Le volume sur lequel les fichiers VHD sont stockés devrait être à tolérance de pannes. Ceci devrait s'appliquer si le disque VHD est enregistré sur un disque local ou sur un périphérique SAN distant. Les disques durs présentent une réelle défaillance. Par conséquent, l'ordinateur virtuel et l'hôte Hyper-V Windows Server 2012 devraient continuer de fonctionner après une défaillance de disque. Le remplacement des disques défectueux ne devrait pas avoir de conséquences sur le fonctionnement de l'hôte Hyper-V ou des ordinateurs virtuels.
- Stockage hautes performances. Le périphérique de stockage sur lequel vous stockez des fichiers VHD devrait présenter d'excellentes caractéristiques d'E/S. De nombreuses entreprises ont recours à des lecteurs hybrides SSD (Solid-State Drive) dans les baies RAID 1+0. Cela permet d'atteindre des performances et une redondance maximales, en particulier lorsque plusieurs ordinateurs virtuels s'exécutent simultanément sur le même stockage. Cela peut placer une charge d'E/S énorme sur un sous-système de disque, ainsi vous devez vérifier que vous choisissez un stockage de haute performance, ou les performances de vos ordinateurs virtuels pourraient en pâtir.
- Espace de croissance adéquat. Si vous configurez des disques VHD de telle sorte que leur capacité croisse automatiquement, il est important que l'espace soit suffisant pour que la taille des fichiers puisse augmenter. En outre, vous devez analyser soigneusement la croissance de sorte que vous ne rencontriez aucune interruption de service si un disque dur virtuel consomme tout l'espace disponible.
- Protection des données. Il est important de prendre en compte les performances de votre solution de sauvegarde et de son impact sur votre conception de stockage, ainsi que la quantité d'ordinateurs virtuels de données à héberger. Examinez les données existantes et vérifiez que vous pourrez sauvegarder les ordinateurs virtuels requis et son stockage dans un calendrier acceptable.

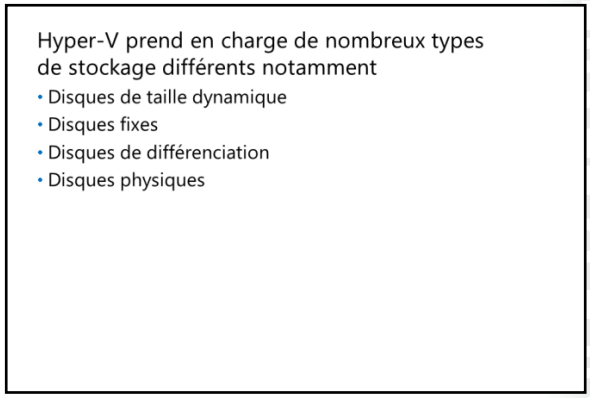
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Hyper-V propose des options de stockage flexibles comme la plupart des options prises en charge par Windows Server, par exemple, le stockage connecté localement comme un disque SATA (Serial Advanced Technology Attachment),

SCSI ou SSD. Hyper-V prend également en charge les réseaux SAN Fibre Channel et iSCSI connectés à distance. Hyper-V prend désormais en charge l'exécution de l'ordinateur virtuel dans les partages de fichiers avec le nouveau protocole SMB 3.0. Les leçons suivantes couvrent ces types de stockage de manière plus approfondie.

Options de configuration des disques virtuels

Hyper-V dans Windows 2012 présente un nouveau disque VHD, *VHDX*, avec une capacité de prise en charge de 64 To maximum. En outre, il assure une meilleure protection contre la corruption des données pendant les pannes d'alimentation et a amélioré l'alignement pour utiliser les grands disques physiques de secteur.



Hyper-V prend en charge un certain nombre de types de disques durs virtuels qui utilisent les disques VHD ou VHDX, notamment :

- Disques virtuels de taille dynamique.
  Ces disques durs virtuels sont très petits au départ et augmentent au fur et à mesure que vous y écrivez des données. À l'origine, les organisations utilisaient les disques de taille dynamique dans des environnements de test et de développement. Cependant, les améliorations des performances montrent que vous pouvez utiliser des disques dynamiques en production, et qu'ils offrent souvent des performances similaires à celles des disques fixes. Un disque de taille dynamique se développe uniquement dans la limite de l'espace que vous lui allouez lors de sa création. Vous pouvez développer le disque si nécessaire, de la taille du format de disque correspondant, qui est de 2 téraoctets pour le disque VHD et de 64 téraoctets pour le disque VHDX.

  Le problème potentiel avec l'utilisation des disques durs virtuels de taille dynamique est que vous devez gérer l'utilisation du stockage après déploiement. Si plusieurs disques durs virtuels à développement dynamique se trouvent dans un seul emplacement de stockage qui est inférieur à la taille maximale des disques VHD, vous devez surveiller l'emplacement de stockage pour vérifier que les disques durs virtuels ne se développent pas jusqu'à utiliser tout l'espace disponible.

  Un autre problème potentiel avec les disques VHD de taille dynamique est que la fragmentation du fichier VHD peut se produire sur le disque dur physique de l'ordinateur hôte. Cela peut affecter les performances du disque virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Disques VHD de taille fixe. Ces disques utilisent autant d'espace disque physique que vous en spécifiez lorsque vous créez le disque. Par exemple, si vous créez un disque VHD de taille fixe de 100 Go, il utilisera 100 Go d'espace disque physique. Le principal avantage à utiliser des disques de taille fixe est que tout le stockage que les disques requièrent est validée lorsque vous créez des disques. Ceci réduit tout risque de surestimation de vos ressources de stockage.

  La raison de choisir les disques durs virtuels de taille fixe est que les disques durs virtuels de taille dynamique peuvent ne pas prendre en charge certaines applications. Par exemple, Microsoft ne prend pas en charge Microsoft Exchange Server 2010 ou Exchange Server 2007 déployé sur des disques durs virtuels de taille dynamique.

  L'inconvénient des disques de taille fixe est que les disques peuvent prendre plus longtemps pour se déplacer d'un serveur à un autre.

- Disques de différenciation. Un disque VHD de différenciation est associé à un autre disque VHD dans une relation parent-enfant. Le disque de différenciation est l'enfant et le disque virtuel associé est le parent. Le disque parent peut être n'importe quel type de disque VHD. Le disque de différenciation (l'enfant) stocke un enregistrement de toutes les modifications apportées au disque parent et fournit une méthode d'enregistrement des modifications sans modifier le disque parent. En d'autres termes, vérifiez que les modifications sont apportées aux disques de différenciation et non au disque VHD d'origine. Vous pouvez fusionner les modifications du disque de différenciation vers le disque VHD d'origine, le cas échéant.

  Le disque dur de différenciation se développe dynamiquement lorsque les données prévues pour le disque parent sont écrites sur le disque de différenciation. Vous devez protéger en écriture ou verrouiller le disque parent. Si un autre processus modifie le disque parent et ne reconnaît pas la relation parent/enfant du disque de différenciation, alors tous les disques de différenciation liés au disque parent deviennent non valides. Par conséquent, toutes les données écrites sur ces disques seront perdues. En revanche, en verrouillant le disque parent, vous pouvez monter le disque sur plusieurs ordinateurs virtuels, de même qu'avec un disque en lecture seule ou un CD.

  Vous ne pouvez pas spécifier la taille d'un disque de différenciation. Les disques de différenciation peuvent devenir aussi grands que les disques parents auxquels vous les associez. Toutefois, contrairement aux disques de taille dynamique, vous ne pouvez pas compacter les disques de différenciation directement. Vous pouvez compacter les disques de différenciation uniquement après avoir fusionné le disque avec un disque parent de taille dynamique.

  Si vous utilisez des disques de différenciation, il est important d'avoir une convention d'affectation de noms standardisée pour les disques durs virtuels. L'examen du disque VHD dans le Gestionnaire Hyper-V ne met pas clairement en évidence s'il s'agit d'un lecteur de différenciation ou d'un disque parent.

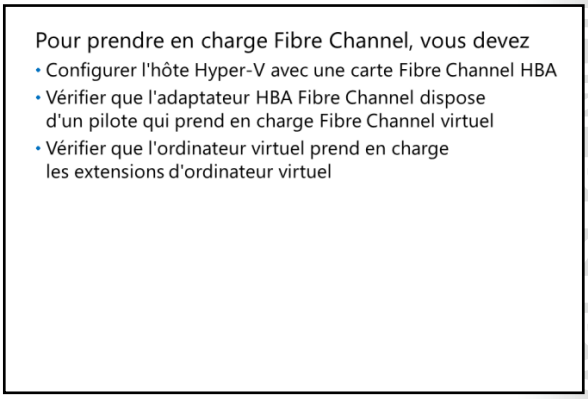
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Disques ou volumes physiques. Hyper-V permet également d'utiliser un disque de type physique (anciennement connu sous le nom de disque relais). Lorsque vous configurez un ordinateur virtuel pour qu'il utilise un disque physique, l'ordinateur virtuel utilise l'intégralité d'un disque ou volume physique sur l'ordinateur hôte. Si vous envisagez d'utiliser des disques physiques pour effectuer l'installation d'un système d'exploitation, vous devez stocker le fichier de configuration invité à un autre emplacement. Cela est dû au fait que l'installation du système d'exploitation consommera l'intégralité du disque physique. Par exemple, vous pouvez localiser le fichier de configuration sur un autre lecteur interne sur le serveur Hyper-V lui-même. Inversement, si l'ordinateur hôte fait partie d'un cluster de basculement, vous pouvez héberger le fichier de configuration sur un cluster distinct qui fournit des services de fichiers hautement disponibles. N'oubliez pas que vous ne pouvez pas développer dynamiquement les disques physiques. En outre, voici d'autres facteurs à prendre en compte :
    - Les disques physiques fournissent le stockage en vous permettant d'associer une source de données externe avec un ordinateur virtuel, puis permettent à l'ordinateur virtuel d'écrire directement sur la source de données sans encapsulation dans un disque VHD. Les lecteurs de stockage compatibles que vous pouvez utiliser pour les disques physiques pour les sources de données incluent les disques physiques, les partitions, les numéros d'unités logiques (LUN), les réseaux SAN et ceux à technologie iSCSI.
    - Les disques physiques n'ont aucun disque VHD. En revanche, ils utilisent un disque physique au lieu d'un disque VHD.
    - Les disques physiques transmettent directement toutes les requêtes de lecture et d'écriture au volume physique.
    - Les disques physiques ne prennent pas en charge les disques durs virtuels de taille dynamique, les disques de différenciation, ou les captures instantanées d'ordinateur virtuel.
    - Vous devez configurer le disque physique en tant que disque hors connexion pour que le serveur Hyper-V implémente les disques physiques.
    - Si vous voulez installer un système d'exploitation sur le disque physique, vous devez d'abord mettre le disque en ligne sur l'hôte et l'initialiser, puis le déconnecter. En tant que lecteur de démarrage, vous devez utiliser un canal IDE.
    - Si vous prévoyez d'utiliser le disque physique en tant que lecteur de stockage, vous devez le préparer dans le système d'exploitation avant de pouvoir placer des données dessus.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Implémentation du stockage Fibre Channel

Les cartes Fibre Channel virtuelles dans Hyper-V sont un composant matériel virtuel que vous pouvez ajouter à un ordinateur virtuel, ce qui lui permet d'accéder au stockage Fibre Channel sur des réseaux SAN. Pour déployer Fibre Channel virtuel :



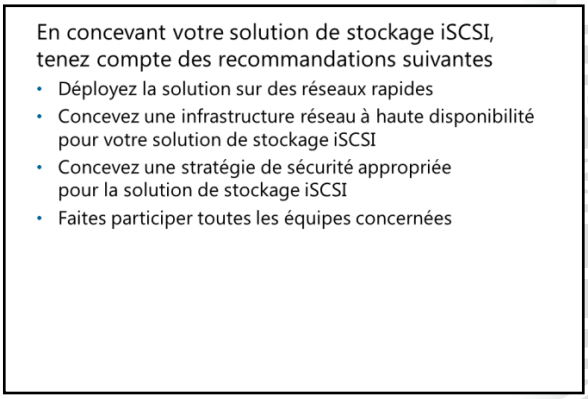
- Vous devez configurer l'hôte Hyper-V avec un adaptateur de bus hôte Fibre Channel (HBA).
- La carte Fibre Channel HBA doit disposer d'un pilote qui prend en charge Fibre Channel virtuel.
- L'ordinateur virtuel doit prendre en charge des extensions d'ordinateur virtuel.

Les cartes Fibre Channel virtuel prennent en charge la virtualisation de ports en exposant des ports HBA dans le système d'exploitation invité. Ceci permet à l'ordinateur virtuel d'accéder au réseau SAN à l'aide d'un nom WWN (World Wide Name) associé à l'ordinateur virtuel.

Hyper-V prend en charge MPIO (Multipath I/O) pour fournir un accès hautement disponible aux numéros d'unité logique (LUN) qui ont été exposés à l'hôte. Avec les cartes Fibre Channel virtuelles, vous pouvez fournir l'accès aux LUN directement à partir des ordinateurs virtuels qui peuvent également prendre en charge MPIO. Vous pouvez utiliser une combinaison de ces deux dans votre environnement de virtualisation.

Implémentation du stockage iSCSI

Le moyen simple et peu coûteux de configurer une connexion vers des disques distants consiste à utiliser le stockage iSCSI. Beaucoup de conditions requises par les applications nécessitent que les connexions de stockage distantes soient redondantes par nature pour obtenir une tolérance de panne ou une haute disponibilité. En outre, beaucoup de sociétés disposent déjà de réseaux à tolérance de pannes qui les rendent moins coûteux pour conserver la redondance par rapport aux réseaux SAN.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

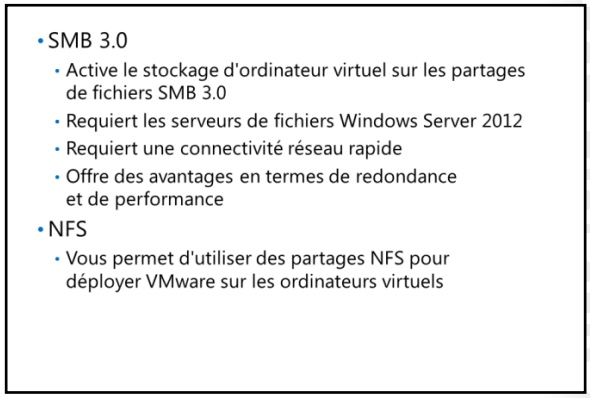
En concevant votre solution de stockage iSCSI, vous devez tenir compte des points suivants :

- Déployez la solution iSCSI sur un réseau d'au moins 1 Gigaoctet par seconde (Gbits/s). Examinez les fonctionnalités spécifiques que vous avez l'intention d'utiliser, et vérifiez que tout votre matériel peut prendre en charge ces fonctionnalités.
- Il est crucial que vous ayez une conception de haute disponibilité pour votre infrastructure réseau, parce que les périphériques et composants du réseau conduisent au transfert de données des serveurs au stockage iSCSI.
- Concevez une stratégie de sécurité appropriée pour votre solution de stockage iSCSI.
- Faites participer toutes les équipes appropriées dans l'implémentation de stockage, et confirmez si l'automatisation du déploiement de stockage sera possible pour les administrateurs de la virtualisation et de l'application.

Implémentation du stockage SMB 3.0 et NFS

SMB 3.0

Le partage de fichiers SMB fournit une alternative au stockage de fichiers d'ordinateur virtuel sur des périphériques SAN iSCSI ou Fibre Channel. Hyper-V prend en charge les données d'ordinateur virtuel de stockage, telles que les fichiers de configuration d'ordinateur virtuel, les captures instantanées et les fichiers VHD sur des partages de fichiers SMB 3. Si vous choisissez d'implémenter les partages de fichiers SMB, considérez les éléments suivants :



- Le partage de fichiers doit prendre en charge SMB 3.0, qui restreint le placement des disques VHD sur les partages de fichiers dont les serveurs de fichiers exécutent l'hôte Windows Server 2012. Les versions antérieures de Windows Server ne prennent pas en charge SMB 3.0.
- Vous devez vous assurer que la connectivité réseau au partage de fichiers est de 1 Go ou plus.
- Lors de la création d'un ordinateur virtuel dans Hyper-V sur Windows Server 2012, vous pouvez spécifier un partage réseau en sélectionnant l'emplacement de l'ordinateur virtuel et celui du disque VHD. Vous pouvez également attacher des disques stockés sur des partages de fichiers SMB 3.0. Avec les partages de fichiers SMB, il est possible d'utiliser à la fois des disques VHD et VHDX.

Remarque : Hyper-V sur SMB attribue les autorisations de compte d'ordinateur sur le partage, ainsi vous pouvez la configurer uniquement dans un environnement de service de domaine Active Directory (AD DS).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le nouveau protocole SMB dans Windows Server 2012 comprend les fonctionnalités suivantes :

- Basculement transparent SMB. Le protocole SMB a la capacité intégrée de gérer une défaillance de sorte que le client et le serveur puissent coordonner un déplacement transparent permettant un accès continu aux ressources avec un délai d'E/S minime. Il n'existe aucune défaillance pour les applications.
- SMB Scale-Out. La fonctionnalité SMB Scale-Out (montée en puissance parallèle SMB) vous permet d'accéder à des partages via plusieurs nœuds de cluster à l'aide des volumes partagés en cluster (CSV). Cela permet d'équilibrer des charges sur un cluster.
- SMB Direct (SMB ou RDMA). Autrefois rencontrée uniquement dans des scénarios de HPC (High Performance Computing), la fonctionnalité SMB Direct est maintenant disponible dans Window Server 2012. SMB Direct permet à une interface réseau RDMA (Remote Direct Memory Access) d'exécuter des transferts de fichiers à l'aide de la technologie présente sur l'interface réseau, sans intervention du système d'exploitation.
- SMB Multichannel. SMB Multichannel est automatiquement activé, et elle permet à SMB de détecter la configuration d'un réseau. Par exemple, s'il détecte que les deux interfaces réseau sont configurées et associées sur le client et le serveur, SMB peut se servir de toute la bande passante disponible.
- Chiffrement SMB. La fonctionnalité Chiffrement SMB permet le chiffrement sans recours au protocole de sécurité (IPsec), et vous pouvez la configurer par partage ou au niveau du serveur. Des clients SMB antérieurs ne peuvent pas se connecter aux serveurs ou partages chiffrés.
- VSS pour les partages de fichiers SMB. Les services VSS (Volume Shadow Copy Services) ont été améliorés pour effectuer des captures instantanées au niveau du partage. Les partages de fichiers distants agissent en tant que fournisseurs et intègrent une infrastructure de sauvegarde.
- SQL Server sur SMB. Vous pouvez enregistrer des bases de données de Microsoft SQL Server® sur des partages SMB 3.0, ce qui pourrait activer la consolidation d'infrastructure.

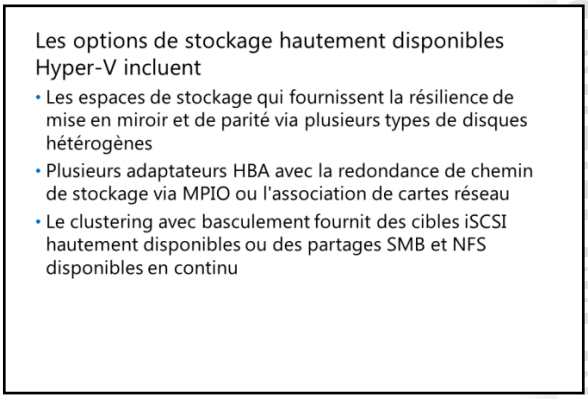
NFS

NFS est une solution de partage de fichiers qui utilise le protocole NFS, et qui vous permet de transférer des fichiers entre les ordinateurs qui exécutent Windows 2012 et les autres ordinateurs autres que Windows.

Windows Server 2012 comprend une pile NFS mise à jour, ce qui lui permet de fournir un basculement transparent aux clients NFS à l'aide des partages NFS disponibles en continu. Vous pouvez utiliser NFS en tant que stockage pour les ordinateurs virtuels VMware. Cependant, ce n'est pas une option pour le stockage Hyper-V.

Configuration des options de haute disponibilité pour le stockage Hyper-V

Les options de stockage hautement disponibles sont importantes pour vérifier que les ordinateurs virtuels s'exécutent de façon ininterrompue lorsqu'un composant matériel échoue. Avant de tenir compte des options spécifiques au stockage des ordinateurs virtuels Hyper-V, vous devriez tenir compte des composants typiques qui comportent le matériel de stockage, et envisagez comment utiliser ces derniers dans les solutions de stockage traditionnelles.



Vous pouvez utiliser les composants de base suivants en générant une solution de stockage hautement disponible :

- Matériel :
    - Alimentation. Dans la mesure du possible, utilisez les sources d'alimentation redondantes dans les solutions de stockage, et conservez éventuellement les disques d'échange sur le site. Les périphériques qui prennent en charge les alimentations secondaires sont les étagères, les serveurs et les commutateurs de disque.
    - Disques. Une solution de stockage hautement disponible doit pouvoir tolérer la défaillance de disque, et continuer à fournir un stockage sans interruption. Les contrôleurs fournisseurs de stockage traditionnels offrent divers niveaux RAID qui permettent la perte d'un ou de plusieurs disques.
    - Matériel réseau de stockage. La création d'une solution matérielle hautement disponible implique habituellement la suppression de tous les points de défaillance uniques, notamment les composants réseau de stockage, tels que les adaptateurs de bus hôte ou les cartes réseau. Cela peut nécessiter que vous ayez deux commutateurs de stockage et contrôleurs de stockage et que vous utilisiez MPIO, ou que l'association de cartes réseau est requise pour utiliser plusieurs chemins d'accès de stockage.

Il existe plusieurs options de stockage hautement disponibles dans Windows Server 2012, notamment :

- Espaces de stockage. Espaces de stockage est une nouvelle technologie dans Windows Server 2012 qui permet l'utilisation des disques liés USB, Fibre, iSCSI, SAS et SATA qui créent des disques virtuels qui les couvrent tous. Windows fournit un niveau de protection de disque en créant ces disques virtuels à l'aide de la protection de parité ou miroir. Ils permettent la défaillance de disque sans perte de données. Un module ultérieur de ce cours détaille leur fonctionnement. Cependant, il est important de comprendre que Windows Server peut créer des pools de stockage à travers les types de disques hétérogènes, et ce via plusieurs solutions qui peuvent toutes être hautement disponibles. Il s'agit des partages de fichiers NFS et SMB et des disques iSCSI.
- Clustering avec basculement. Les cibles iSCSI et les partages NFS et SMB, sont compatibles avec les ressources en cluster de basculement Windows. Par conséquent, vous pouvez éliminer un serveur Windows unique comme point de défaillance dans une solution de stockage. Cependant, pour présenter les espaces de stockage comme une ressource en cluster, vous pouvez utiliser le stockage liés aux disques SAS uniquement.
- MPIO. MPIO est une fonctionnalité de Windows qui permet le stockage Fibre ou iSCSI pour être accessible via plusieurs chemins d'accès. Cette étape est nécessaire sur un client, tel que l'hôte Hyper-V, de sorte qu'il soit connecté à la solution de stockage. Lors de l'utilisation de deux chemins d'accès, MPIO voit les deux emplacements de stockage, mais détermine qu'il représente en réalité un périphérique unique. MPIO gère le basculement des chemins d'accès, et utilise des algorithmes d'équilibrage de charge pour fournir l'accès accepté au stockage via le chemin d'accès moins saturé. Un module ultérieur dans ce cours propose plus de détails sur cette rubrique
- Association de cartes réseau et tolérance de pannes de réseau. Si vous souhaitez connecter des hôtes Hyper-V au stockage, nous vous recommandons d'avoir plusieurs cartes réseau et chemins d'accès. Vous devez fournir la redondance à l'aide de l'association de cartes réseau SMB ou NFS sur à la fois le serveur de fichiers et les hôtes Hyper-V. Si vous utilisez SMB, SMB Multichannel fournira automatiquement la meilleure bande passante disponible.

Liens de référence : Pour plus d'informations, consultez le blog de support Microsoft Storage Team Blog à l'adresse http://go.microsoft.com/fwlink/?LinkID=285270.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification d'une autre conception d'infrastructure

Vous êtes l'architecte de virtualisation de la société A. Datum et vous générez une solution de remplacement pour la plateforme d'e-commerce spécialisé vieillissante de la société. L'équipe d'e-commerce détient environ 1 000 lames physiques. En collaborant avec l'équipe d'application, vous avez exécuté un pilote et avez maintenant l'autorisation de passer à la virtualisation. Les propriétaires d'application ont insisté sur le fait que les défaillances de l'hôte physique ne doivent pas affecter trop de sessions actives. Globalement, vous pouvez effectuer la virtualisation, mais vous ne pouvez pas placer trop d'ordinateurs virtuels sur un hôte unique.

Comment planifieriez-vous une autre conception qui réduirait le niveau de l'infrastructure de commutation Fibre Channel et conserverait l'administration de stockage avec l'équipe SAN ?

A. Datum a un réseau SAN Fibre Channel existant qu'il reflète entre deux centres de données de l'entreprise basée à Londres. Vous envisagez de générer la batterie de serveurs Web e-commerce en utilisant 800 serveurs virtuels, et vous déterminez que le nombre maximal d'ordinateurs virtuels sera de 16 par hôte Hyper-V. Vous avez indiqué à l'administrateur SAN que vous achèteriez 54 serveurs hôtes physiques pour en placer 28 sur chaque site. Les adaptateurs HBA et commutateurs Fibre Channel sont très coûteux, et l'administrateur SAN n'a pas de suffisamment de ports disponibles sur les commutateurs Fibre Channel actuels. De plus, il ne dispose pas du budget pour en acquérir d'autres, donc il vous demande de revoir la conception et de proposer une alternative.

Question : Examinez le scénario ci-dessus. Comment planifieriez-vous une autre conception qui réduirait le niveau de l'infrastructure de commutation Fibre Channel et conserverait l'administration de stockage avec l'équipe SAN ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Implémentation d'une infrastructure de stockage pour la virtualisation

Maintenant que vous avez une vue d'ensemble des options de stockage disponibles avec Hyper-V, l'étape suivante consiste à implémenter et configurer ce stockage. Une des options disponibles pour implémenter le stockage Hyper-V est d'utiliser iSCSI.

Dans cette leçon, vous apprendrez comment configurer le stockage iSCSI sur le serveur Windows Server 2012 et comment gérer le stockage à partir de VMM.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- expliquer comment configurer le stockage iSCSI ;
- configurer une cible iSCSI ;
- expliquer comment gérer le stockage à l'aide de VMM ;
- configurer des disques virtuels et le stockage dans VMM.

Vue d'ensemble de la configuration iSCSI

iSCSI est un protocole qui prend en charge l'accès aux périphériques de stockage SCSI sur un réseau TCP/IP. iSCSI véhicule les commandes SCSI standard sur des réseaux IP pour faciliter les transferts de données sur les intranets et gérer le stockage sur de longues distances. Vous pouvez utiliser le protocole iSCSI pour transmettre des données sur des réseaux locaux (LAN), des réseaux étendus (WAN) ou même sur Internet.

iSCSI transmet les commandes SCSI sur les réseaux IP

Composant	Description
Réseau IP	Fournit la haute performance et la redondance
Cibles iSCSI	Est exécuté sur le périphérique de stockage et permet l'accès direct aux disques
Initiateurs iSCSI	Composant logiciel ou carte hôte qui, sur le serveur, fournit l'accès aux cibles iSCSI
IQN	Identificateur globalement unique servant à adresser les initiateurs et les cibles sur un réseau iSCSI



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

iSCSI s'appuie sur l'architecture de mise en réseau Ethernet standard, alors qu'il est facultatif, tout dépendant de votre choix d'utiliser ou non un matériel spécialisé tel qu'un adaptateur HBA ou des commutateurs réseau est facultative. iSCSI utilise TCP/IP (en général, le port TCP 3260). Cela signifie que iSCSI permet à deux hôtes de négocier des tâches, telles que l'établissement de session, le contrôle de flux ou la taille de paquet, puis d'échanger des commandes SCSI à l'aide d'un réseau Ethernet existant. Le protocole iSCSI utilise une architecture de sous-système de bus de stockage local très puissante et très répandue, qu'il émule sur des réseaux LAN et WAN, créant de ce fait un réseau SAN.

À la différence de certaines technologies SAN, le protocole iSCSI ne requiert aucun câblage spécialisé. Vous pouvez l'exécuter sur l'infrastructure existante de commutation et IP. Toutefois, comme meilleure pratique, vous pouvez améliorer les performances d'un déploiement SAN iSCSI en l'exécutant sur un réseau ou sous-réseau dédié.

 Remarque : Bien que vous puissiez utiliser une carte réseau Ethernet standard pour connecter le serveur au périphérique de stockage iSCSI, vous pouvez également utiliser des contrôleurs de bus hôte iSCSI dédiés.

Un déploiement de réseau SAN iSCSI comprend les éléments suivants :

- Réseau TCP/IP. Vous pouvez utiliser des cartes d'interface réseau standard et des commutateurs réseau Ethernet standard pour connecter les serveurs au périphérique de stockage. Pour offrir des performances suffisantes, le réseau doit fournir des vitesses d'au moins 1 Gbit/s et plusieurs chemins d'accès à la cible iSCSI. Une bonne pratique consiste à utiliser un réseau physique et logique dédié pour obtenir un débit rapide et fiable.
- Cibles iSCSI. Il s'agit d'une autre méthode pour accéder au stockage. Les cibles iSCSI présentent ou publient le stockage, comme des contrôleurs pour des lecteurs de disque dur de stockage local. Toutefois, vous pouvez accéder à ce stockage sur un réseau mais localement. Beaucoup de fournisseurs de stockage implémentent les cibles iSCSI au niveau matériel comme faisant partie du matériel de leur périphérique de stockage. D'autres périphériques ou appareils, tels que les périphériques de Windows Storage Server 2012, implémentent les cibles iSCSI à l'aide d'un pilote logiciel et d'au moins une carte Ethernet. Windows Server 2012 fournit le serveur cible iSCSI, qui est un service de rôle qui agit en tant que pilote du protocole iSCSI.
- Initiateurs iSCSI. La cible iSCSI affiche le stockage pour l'initiateur iSCSI ou *client*, qui agit en tant que contrôleur de disque local pour les disques distants. Windows Server 2008 et les dernières versions comprennent l'initiateur iSCSI et peuvent se connecter aux cibles iSCSI.
- Nom complet iSCSI. Les noms complets iSCSI sont des identificateurs uniques pour les initiateurs et cibles d'un réseau iSCSI. Lorsque vous configurez une cible iSCSI, vous devez configurer le nom complet iSCSI pour les initiateurs iSCSI qui s'y connecteront. Les initiateurs iSCSI utilisent également les noms complets iSCSI pour se connecter aux cibles iSCSI. Toutefois, si la résolution de noms sur le réseau iSCSI est un problème possible, vous pouvez identifier les points de terminaison iSCSI (à la fois cible et initiateur) par leurs adresses IP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration du stockage iSCSI pour la virtualisation

Dans cette démonstration, vous allez :

- ajouter le service de rôle du serveur cible iSCSI ;
- créer un pool de stockage ;
- créer un disque virtuel iSCSI ;
- créer une cible iSCSI ;
- vous connecter à une cible iSCSI.

Procédure de démonstration

Ajouter le service du rôle de serveur cible iSCSI

1. Sur **LON-SVR1**, ouvrez le Gestionnaire de serveur.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, installez les rôles et fonctionnalités suivantes sur le serveur local, puis acceptez les valeurs par défaut suivantes :
   - **Services de fichiers et de stockage (Installé)\Services de fichiers et iSCSI (Installé)\ Serveur cible iSCSI**

Créer un pool de stockage

1. Sur **LON-SVR1**, ouvrez l'outil **Gestion du disque**.
2. Dans la page **Gestion des disques**, cliquez sur **Action**, puis sur **Créer un disque dur virtuel**.
3. Créez et initialisez trois fichiers VHDX de 50 gigaoctets à la racine de **E:** :
   - **iSCSI1.vhdx**
   - **iSCSI2.vhdx**
   - **iSCSI3.vhdx**
4. Dans le Gestionnaire de serveur, dans le volet de navigation, cliquez sur **Services de fichiers et de stockage**, puis sur **Pools de stockage**.
5. Créez un pool de stockage appelé **VMPool**, puis créez un disque virtuel de 100 Go appelé **VMStorage**, et utilisez la parité pour assurer la protection de stockage. Créez et formatez un volume, nommez-le **VMStorage**, puis attribuez-lui la Lettre du lecteur **F**.

Se connecter à la cible iSCSI

1. Sur LON-HOST1, lancez l'Initiateur iSCSI, puis connectez-vous à la cible sur **LON-SVR1**.
2. Ouvrez la fenêtre de gestion des disques, mettez le nouveau disque en ligne, puis initialisez-le. Créez et nommez le volume **VMStorage**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion du stockage dans VMM

Gestion du stockage hôte

VMM peut voir le stockage lié aux hôtes Hyper-V, et lorsqu'il effectue des calculs de placement d'ordinateur virtuel, il peut calculer la quantité d'espace de stockage disponible sur les disques hôte associés.

La console VMM vous permet de découvrir, de classifier et de mettre en service le stockage à distance sur des baies de stockage prises en charge. Pour implémenter cette gestion du stockage, effectuez les étapes suivantes

1. Installez un fournisseur de stockage SMI-S
2. Connectez-vous au fournisseur de stockage SMI-S pour découvrir le stockage
3. Classez le stockage
4. Créez des unités logiques à partir du pool de stockage
5. Allouez les unités logiques ou les pools de stockage aux hôtes, groupes hôtes ou clusters hôtes

Remarque : Mise à jour des hôtes

Si vous ajoutez le stockage à un hôte de virtualisation, VMM ne le verra pas tant que vous n'actualisez pas l'hôte. Pour utiliser immédiatement le stockage récemment ajouté, vous pouvez effectuer une actualisation manuelle sur l'hôte.

Pour voir et travailler avec le stockage hôte, cliquez avec le bouton droit sur un hôte, puis dans la page Propriétés, cliquez sur Stockage. Dans la zone Stockage, vous verrez des zones pour chaque type de sous-système de disque. S'ils sont présents, vous pouvez les développer, les filtrer ou les configurer.

Gestion des baies de stockage

La console VMM vous permet de découvrir, de classifier et de mettre en service le stockage à distance sur des baies de stockage prises en charge. VMM automatise entièrement l'attribution de stockage sur un hôte Hyper-V ou un cluster hôte Hyper-V, puis fait le suivi du moindre stockage qu'il gère. Pour activer de nouvelles fonctionnalités de stockage, VMM utilise le service de gestion du stockage pour communiquer avec les baies externes via un fournisseur de stockage SMI-S (Storage Management Initiative Specification).

Par défaut, le service de gestion du stockage s'installe pendant l'installation VMM, mais pour gérer le stockage, vous devez installer un fournisseur de stockage SMI-S pris en charge sur un serveur disponible, puis ajouter le fournisseur à VMM.

Affichage de la vue d'ensemble du stockage

Dans l'espace de travail Ensemble fibre optique, sélectionnez **Stockage**, puis cliquez sur **Vue d'ensemble** dans le ruban pour afficher la vue d'ensemble du stockage. Comme votre centre de données virtuel se développe, la vue d'ensemble permet d'afficher ce que le centre de données met en service, et quelles ressources restent toujours disponibles.

Vous devez effectuer les étapes suivantes pour découvrir, classer et attribuer un stockage via VMM :

1. Pour une baie de stockage prise en charge, obtenez un fournisseur de stockage SMI-S à partir de votre fournisseur de baies de stockage, puis installez le fournisseur de stockage SMI-S sur un serveur disponible comme indiqué par votre fournisseur de stockage.
2. À partir de la console VMM, dans le nœud Stockage, connectez-vous au fournisseur de stockage SMI-S pour découvrir et classer le stockage. Connectez-vous au fournisseur avec soit l'adresse IPv4 (Internet Protocol version 4), soit le nom de domaine complet (FQDN).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. La classification du stockage consiste à attribuer une classification explicite aux pools de stockage. Par exemple, vous pouvez attribuer une classification de référence OR à un pool de stockage qui réside sur la baie de stockage la plus redondante et la plus rapide. Cela vous permet d'attribuer et d'utiliser la classification de stockage sans connaître réellement ses caractéristiques matérielles.
4. Dans le nœud de stockage, vous pouvez éventuellement créer des unités logiques à partir d'un pool de stockage géré.
5. Dans le nœud de stockage de la console VMM ou de la boîte de dialogue Propriétés du groupe hôte cible, vous devez allouer des unités logiques précréées ou des pools de stockage à des groupes hôtes spécifiques. Si vous allouez des pools de stockage, vous pouvez créer et attribuer des unités logiques directement à partir des hôtes gérés du groupe hôte ayant accès à la baie de stockage. En outre, si vous utilisez la mise en service rapide pour configurer les ordinateurs virtuels à l'aide des captures instantanées ou du clonage SAN, VMM pourra créer automatiquement des unités logiques à partir du pool de stockage.
6. Dans la console VMM, dans la boîte de dialogue Propriétés de l'hôte ou du cluster hôte, attribuez les unités logiques à partir du groupe hôte à des hôtes Hyper-V spécifiques ou aux clusters hôtes Hyper-V, en tant que CSV partagé ou stockage disponible. Si vous avez alloué un pool de stockage à un groupe hôte, vous pouvez créer et éventuellement attribuer des unités logiques directement à partir de la boîte de dialogue Propriétés de l'hôte ou du cluster hôte. Si la baie de stockage prend en charge la connectivité de l'hôte iSCSI, vous pouvez créer des sessions iSCSI sur la baie de stockage à partir de la boîte de dialogue Propriétés d'un hôte.

 **Liens de référence :** Pour obtenir la liste des baies de stockage prises en charge, accédez au site http://go.microsoft.com/fwlink/?LinkID=285283.

Attribution de stockage à des groupes hôtes

Les pools de stockage peuvent être attribués à des groupes hôtes. Grâce aux groupes hôtes, vous pouvez définir des groupes logiques de ressources informatiques physiques, ces groupes peuvent aider VMM et les administrateurs à déterminer le placement pour déployer de nouvelles charges de travail virtuelles. Par exemple, vous pouvez créer des groupes hôtes et attribuer des pools de stockage avec des classifications comme l'illustre le tableau.

Nom du groupe hôte	Classification du stockage	Type de stockage	UC du serveur hôte
Couche 1	Platine	Disques SSD (Solid State Drives)	3,6 Ghz
Couche 2	Or	SAS (Serial Attached SCSI) 15 000 rotations par minute (RPM)	3 Ghz
Couche 3	Argent	SAS (Serial Attached SCSI) 10 000 RPM	2,4 Ghz
Couche 4	Bronze	Série ATA 7200 RPM	2,0 GHz

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour ajouter un stockage à un groupe hôte, vous devez exécuter les étapes suivantes :

1. Cliquez avec le bouton droit sur le groupe hôte, puis cliquez sur **Propriétés**.
2. Cliquez sur **Stockage**, puis sur **Allouer les pools de stockage** ou **Allouer les unités logiques**.
3. Ajoutez le stockage au besoin.

Remarque : Le fournisseur de stockage SMI-S cible iSCSI pour Windows Server est disponible sur le CD d'installation System Center Virtual Machine Manager 2012 Service Pack 1 (SP1) sous : \amd64\Setup\msi\iSCSITargetSMISProvider.msi, ou sur le serveur VMM, sous \Program Files\Microsoft System Center 2012\Virtual Machine Manager\setup\msi\iSCSITargetProv\iSCSITargetSMISProvider.msi.

Démonstration : Configuration du stockage dans VMM

Dans cette démonstration, vous allez apprendre à utiliser VMM pour examiner et configurer le stockage pour des hôtes de virtualisation.

Vous étudierez également comment ajouter des classifications au stockage et comment ajouter des fournisseurs de stockage.

Procédure de démonstration

Actualisez le chemin d'accès à l'emplacement de l'ordinateur virtuel LON-HOST1 dans VMM

1. Ouvrez la console Virtual Machine Manager.
2. Cliquez sur l'espace de travail **Ensemble fibre optique**, développez **Serveurs**, cliquez avec le bouton droit sur **lon-host1**, puis sur **Actualiser**.
3. Dans le ruban, cliquez sur le bouton **Travaux**, attendez que le travail d'actualisation de l'hôte se termine, puis fermez la fenêtre Travaux.
4. Cliquez avec le bouton droit sur **lon-host1**, puis cliquez sur **Propriétés**.
5. Cliquez sur **Sélection élective**, **Ajouter**, **VMStorage**, puis cliquez sur **OK**. Cliquez encore une fois sur **OK** pour fermer la page **Propriétés**.

Créer des classifications de stockage

1. Dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Ensemble fibre optique**, puis sur **Stockage**.
2. Dans le ruban, cliquez sur **Créer une classification**, dans le champ **Nom**, tapez **Or**. Dans le champ **Description**, tapez **Lecteurs SAS 15K**, puis cliquez sur **Ajouter**.
3. Dans le ruban, cliquez sur **Créer une classification**, dans le champ Nom tapez **Argent**, dans le champ Description, tapez **Lecteurs SATA 7K**, puis cliquez sur **Ajouter**.
4. Cliquez sur le nœud **Classification et pools**, puis notez qu'il n'y a aucune capacité disponible.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Ajouter des fournisseurs de stockage

1. Sur **LON-VMM1**, dans la console Virtual Machine Manager, cliquez sur le bouton **Ensemble fibre optique**, cliquez avec le bouton droit sur **Stockage**, puis cliquez sur **Ajouter des périphériques de stockage**.
2. Dans la page **Sélectionner un type de fournisseur**, cliquez sur **Ajouter un serveur de fichiers Windows en tant que périphérique de stockage géré**, et cliquez sur **Suivant**.
3. Cliquez dans le champ **Adresse IP ou nom de domaine complet du fournisseur :** tapez **lon-svr1.adatum.com**, puis cliquez sur **Parcourir**.
4. Dans la page **Sélectionner un compte d'identification**, cliquez sur **Administrateur**, puis sur **OK**.
5. Dans la page **Spécifier l'étendue de la découverte**, cliquez sur **Suivant**.
6. Dans la page **Rechercher des informations**, examinez le résultat de la découverte, puis cliquez sur **Suivant**.
7. Dans la page **Sélectionner les périphériques de stockage**, cliquez sur **Suivant**.
8. Dans la page **Résumé**, cliquez sur **Terminer**, puis fermez la fenêtre Travaux.

Créer des partages de fichiers à partir de VMM

1. Sur **LON-VMM1**, cliquez sur **Ensemble fibre optique**, et dans le ruban, cliquez sur **Créer un partage de fichiers**.
2. Dans la page **Créer un partage de fichiers**, dans le champ **Nom**, tapez **GoldDisks**. Dans le champ **Chemin d'accès local**, tapez **F:**, puis cliquez sur **Ajouter**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Planification et implémentation d'une infrastructure réseau pour la virtualisation

Un autre composant important lorsque vous implémentez une solution de virtualisation de serveur est votre infrastructure réseau. Dans un déploiement de virtualisation de serveur, de nombreux ordinateurs virtuels doivent partager les cartes réseau fournies par l'ordinateur hôte.

Dans cette leçon, vous apprendrez comment planifier votre infrastructure réseau pour un environnement de virtualisation, notamment les aspects de la planification d'hôte et d'invité, la mise en réseau du stockage, le clustering et l'hébergement multiclient.

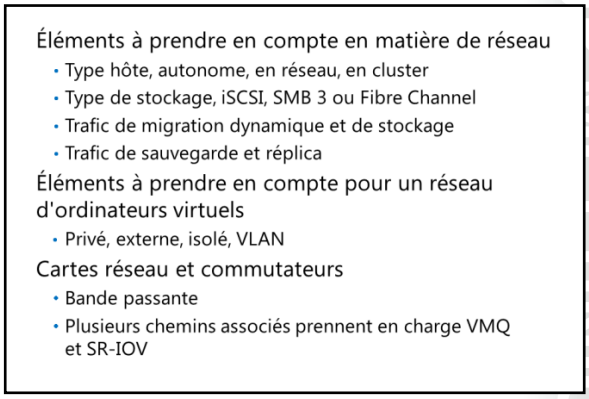
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire la configuration requise pour la mise en réseau Hyper-V ;
- expliquer les options pour la configuration du réseau virtuel ;
- configurer les réseaux virtuels ;
- expliquer les éléments à prendre en compte dans la planification du réseau pour un déploiement Hyper-V ;
- gérer les réseaux virtuels dans VMM ;
- expliquer comment gérer les paramètres des adresses IP et MAC (Media Access Control) dans VMM ;
- configurer les composants d'un réseau virtuel dans VMM ;
- décrire la virtualisation réseau ;
- configurer la virtualisation réseau.

Configuration requise pour un déploiement Hyper-V

La conception des centres de données et des infrastructures de communication modernes d'aujourd'hui repose sur l'expérience des professionnels de l'informatique acquise durant des décennies en matière d'hébergement et de réponse aux demandes d'applications, de serveurs et d'ordinateurs qui transmettent et reçoivent de vastes quantités de données différentes. La dernière décennie a connu une explosion des applications et technologies gourmandes en données, notamment :



- VoIP (Voice over IP). Le trafic au départ du bureau de l'utilisateur s'effectue autour d'une organisation souvent avec réenregistrement vocal dans le centre de données.
- Sauvegarde d'entreprise telle que la sauvegarde de disque-à-disque où de nombreux systèmes transmettent des données simultanément à un ou plusieurs serveurs de stockage via le réseau.

- Applications qui offrent leurs propres technologies de réplication telles que SQL Server et Microsoft Exchange Server. Celles-ci envoient de manière permanente des données quasiment en temps réel d'un site vers un autre.
- Les solutions de stockage iSCSI peuvent requérir leur propre réseau, bien que maintenant il redevient courant d'utiliser une mise en réseau convergée avec un débit élevé pour mettre plusieurs types de données en service.

D'autres technologies de réseau disponibles dans les centres de données modernes incluent :

- Les pare-feu, qui filtrent, sécurisent et publient des applications réseau en interne ou externe.
- Les périphériques d'équilibrage de charge, qui distribuent la charge ou rendent les applications hautement disponibles.
- Les périphériques de compression de données, qui gèrent et compressent des types de données spécifiques pour la transmission sur des liaisons plus lentes.

Quel est le rapport avec la configuration réseau Hyper-V ? Hyper-V est une autre couche du centre de données où la mise en réseau évolue rapidement. De nombreux périphériques réseau ont maintenant des équivalents virtuels ou des *appareils virtuels,* et Hyper-V fournit une prise en charge de nombreuses applications exigeantes qui n'étaient pas auparavant des candidats de virtualisation. Cela signifie que vous pouvez générer de très grands clusters Hyper-V capables d'héberger les résultats d'ordinateurs virtuels, chacun avec leurs propres exigences de mise en réseau. En outre, cela signifie que votre planification du réseau de virtualisation dépend entièrement des spécifications d'infrastructure ou de solutions.

Vous devez identifier la configuration de réseau requise pour un déploiement Hyper-V pendant le processus de planification de l'environnement hôte et invité. Vous devez définir les fonctionnalités que vous prévoyez d'utiliser pour déterminer à quelles exigences vous devez répondre.

Dans les versions Hyper-V antérieures, les conceptions optimales pour les clusters hôtes exigeaient que vous consacriez plusieurs cartes réseau à différents services. Windows Server 2012 introduit l'association de cartes réseau indépendantes des fournisseurs, qui vous permet d'agréger des cartes réseau d'hôte. Ceci fournit une redondance matérielle et une bande passante plus élevée. Vous pouvez également utiliser la Qualité de service (QoS) pour garantir la bande passante à plusieurs services qui s'exécutent sur les mêmes cartes réseau agrégées. Cela risque de réduire la complexité et le coût de l'infrastructure physique.

Voici quelques éléments à prendre en compte dans le cadre de la configuration de la planification :

- Hôtes Hyper-V autonomes. Il est possible d'exécuter un serveur Hyper-V en isolement, sans aucune carte réseau. Vous pouvez utiliser le Gestionnaire Hyper-V pour créer des réseaux privés internes qui permettront à plusieurs ordinateurs virtuels de communiquer. Cette configuration est utile uniquement dans les environnements de test et de développement, dans lesquels les ordinateurs virtuels n'ont besoin d'une connectivité à aucun autre ordinateur du réseau.
- Hôtes Hyper-V activés réseau. Si vous souhaitez gérer un serveur hôte Hyper-V à distance, ou faire en sorte que ses ordinateurs virtuels invités communiquent avec d'autres ordinateurs ou périphériques sur le réseau physique, vous devez avoir au moins une carte réseau physique sur l'ordinateur hôte. Vous pouvez configurer Hyper-V pour que l'hôte et ses ordinateurs virtuels partagent une seule et même carte réseau. Cela garantit que toute la connectivité réseau repose sur une carte réseau. Nous recommandons que, pour la résilience et les performances, vous configuriez plusieurs cartes réseau sur un hôte.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Clusters Hyper-V. Vous pouvez générer des clusters hôtes Hyper-V à l'aide d'un certain nombre de solutions. Chacun a ses propres exigences de mise en réseau spécifiques, telles que les partages de fichiers actifs SMB 3.0, ou l'utilisation de réseaux SAN iSCSI et Fibre Channel. Lors de l'utilisation de SMB 3.0 ou iSCSI, vous aurez besoin d'au moins une carte réseau physique. Nous recommandons vivement que vous déployez au moins deux cartes réseau physiques. L'une destinée à la connectivité de l'hôte et de l'ordinateur virtuel avec le reste du réseau, et l'autre carte réseau pour accéder au réseau de stockage. Les cartes réseau modernes prennent en charge les diverses fonctionnalités qui assistent spécifiquement la virtualisation et le stockage iSCSI, comme la file d'attente d'ordinateurs virtuels, la virtualisation SR-IOV et le déchargement des tâches IPsec. Lorsque vous tenez compte des fonctionnalités que vous souhaitez utiliser, il est important que vous vous souveniez que vous devez configurer les cartes réseau pour que vos hôtes prennent en charge ces fonctionnalités.
- Migration de stockage. Les migrations de stockage permettent de migrer le stockage de l'ordinateur virtuel d'un emplacement à un autre. Si vous utilisez des partages iSCSI ou SMB pour votre stockage, vous devez réfléchir à l'incidence que cette migration aura sur un autre trafic réseau. Vous pouvez définir le nombre de migrations simultanées. En outre, si vous utilisez cette fonctionnalité en production, vous devez effectuer un test pour voir l'impact à la fois sur le réseau et l'E/S du disque pour confirmer les paramètres optimaux.
- Migration en direct. Les hôtes Hyper-V peuvent envoyer et recevoir des migrations dynamiques des ordinateurs virtuels, mais le trafic de migration dynamique peut affecter un autre trafic. Par conséquent, vous devez le configurer pour utiliser n'importe quel réseau disponible ou un réseau dédié. Vous pouvez définir le nombre de migrations dynamiques simultanées adapté à la bande passante disponible. Cependant, vous devez effectuer le test de manière intensive lors de la conception du réseau pour les clusters hôtes Hyper-V, parce que cela déterminera le temps qui est nécessaire pour évacuer un hôte. En outre, vous pouvez déterminer l'incidence du mouvement des ordinateurs virtuels quand vous activez l'optimisation dynamique et quand les clusters sont déplacés entre les ordinateurs virtuels pour équilibrer l'utilisation des ressources.
- Réplica Hyper-V. Vous pouvez utiliser la fonction Réplica Hyper-V dans Windows Server 2012 pour répliquer des ordinateurs virtuels entre des serveurs hôtes Hyper-V. Vous devez tenir compte de la bande passante requise entre les hôtes, mais également de l'impact que cela pourrait avoir sur un autre trafic réseau :
    - Vous pouvez planifier la réplication Hyper-V initiale des ordinateurs virtuels et éventuellement envoyer la réplication initiale vers un lecteur de disque portable. Vous pouvez ensuite l'importer vers le serveur cible. Nous vous recommandons de tester la réplication dans un environnement de non-production et de calculer la densité du trafic de synchronisation entre les hôtes. Vous pouvez configurer le réplica Hyper-V pour effectuer la réplication sur des hôtes et clusters Hyper-V nommés spécifiques ou tous les hôtes Hyper-V.
    - Vous pouvez attribuer le port HTTP ou HTTPS que vous souhaitez utiliser pour la réplication. En outre, vous devez vérifier que vous configurez tous les pare-feu entre les hôtes Hyper-V pour permettre le trafic de réplication.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

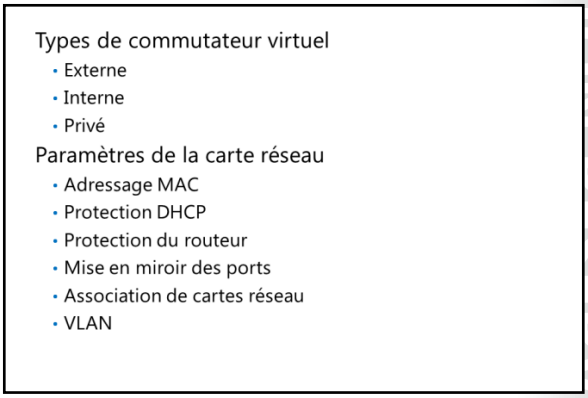
- Matériel de réseau. Vous devez déterminer quelles sont vos configurations matérielles réseau, et vérifier que le matériel de bout en bout prendra en charge votre ensemble de fonctionnalités choisies. Si vous souhaitez isoler des ordinateurs virtuels à l'aide de RÉSEAUX LOCAUX virtuels (VLAN), vous devez vérifier que vos cartes et commutateurs réseau entre chaque nœud de cluster les prennent en charge. Vous devez également tenir compte de certaines fonctionnalités réseau Hyper-V récentes, et déterminer si les cartes réseau que vous envisagez d'acheter les prendront en charge. Certaines fonctionnalités matérielles des cartes réseau permettent d'améliorer les performances réseau des ordinateurs virtuels, notamment :
  - VMQ (Virtual Machine Queue). VMQ est une fonctionnalité qui utilise le filtrage de paquet matériel pour fournir des données directement aux ordinateurs virtuels à partir d'un réseau externe. Cela réduit la charge de traitement des paquets de routage du système d'exploitation de gestion sur l'ordinateur virtuel.
  - SR-IOV. L'interface SR-IOV est une extension de la spécification PCI (Peripheral Component Interconnect) Express. SR-IOV permet à un périphérique, tel qu'une carte réseau, de différencier l'accès à ses ressources entre des fonctions matérielles PCI Express, notamment :
    - Une fonction physique PCI Express.
    - La fonction principale du périphérique et les fonctions SR-IOV publiées.
    - La fonction principale associée à la partition parente Hyper-V dans un environnement virtualisé.
- Déchargement des tâches IPsec. La version Hyper-V 3.0 active le déchargement des tâches IPsec au niveau de l'ordinateur, ce qui déplace certaines demandes sur l'unité centrale (CPU) de l'ordinateur virtuel vers un processeur dédié sur l'adaptateur réseau physique.

Les questions de planification de suivi peuvent vous aider à identifier les configurations requises en matière de mise en réseau pour un déploiement Hyper-V :

1. Quelle technologie de stockage est en place ou planifiée ? S'il s'agit de partages de fichiers iSCSI ou SMB 3.0, vous pouvez utiliser une infrastructure réseau physique distincte, ou bénéficier de la qualité de service et utiliser un réseau convergé.
2. Combien d'invités par hôte y-aura t-il ? Quel type de bande passante est nécessaire pour les invités et les hôtes ? Quelles statistiques d'analyse sont disponibles pour la migration des serveurs physiques existants ?
3. Allez-vous isoler le trafic de gestion pour les hôtes ?
4. Consacrerez-vous des réseaux au trafic de sauvegarde et de réplication ?
5. Lors du déploiement du clustering, utiliserez-vous une carte réseau dédiée ou partagée pour le trafic de migration dynamique ?
6. Comment sécuriserez-vous le trafic réseau ?
7. Exploiterez-vous un environnement de virtualisation multiclient ? Utiliserez-vous les réseaux VLAN ?
8. Votre équipe réseau gèrera t-elle l'attribution de tous les paramètres réseau et d'allocation d'adresses IP ? Fournira t-elle des plages d'adresses à attribuer aux pools VMM ?
9. Combien d'hôtes et combien de configurations de commutateurs différentes allez-vous utiliser ? La création dans VMM peut faire gagner un temps considérable.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des options des réseaux virtuels



Vous pouvez créer trois types de commutateurs virtuels sur vos serveurs hôtes Hyper-V, notamment :

- Externe. Vous pouvez créer un commutateur réseau virtuel que vous liez à une carte réseau physique dans le serveur hôte. Une fois que vous avez créé ce commutateur réseau virtuel, vous pouvez ensuite connecter une ou plusieurs cartes réseau d'ordinateur virtuel permettant l'accès des ordinateurs virtuels à un réseau physique. Vous pouvez créer un seul commutateur virtuel externe pour chaque carte réseau physique. Vous pouvez éventuellement permettre à l'hôte de partager la carte réseau avec le commutateur virtuel.
- Interne. La création d'un commutateur interne permet aux ordinateurs virtuels de communiquer entre eux et avec l'hôte Hyper-V. Cependant, les commutateurs internes ne permettent pas de communiquer avec le réseau physique.
- Privé. Un commutateur virtuel privé permet uniquement aux ordinateurs virtuels de communiquer entre eux. Vous pouvez créer plusieurs commutateurs virtuels privés sur un même hôte Hyper-V, pour isoler différents groupes d'ordinateurs virtuels.

Les paramètres VLAN, les commutateurs virtuels externes vous permettent de partager la carte réseau avec les ordinateurs invités virtuels. Dans ce cas, vous pouvez définir les ID VLAN pour le serveur hôte. Toutefois, ceci ne contrôle pas la configuration VLAN d'ordinateur virtuel.

Paramètres de la carte réseau

Vous pouvez également configurer les paramètres de carte réseau suivants :

- Adresse MAC. Au niveau du commutateur Hyper-V, vous pouvez définir la plage d'adresses que Hyper-V peut attribuer dynamiquement aux cartes réseau virtuelles. Au niveau de la carte réseau virtuelle, la configuration par défaut est « dynamique », bien que vous puissiez définir l'adresse manuellement, si nécessaire. Vous pouvez également activer l'usurpation d'adresse MAC. Par défaut, ce paramètre est désactivé ; le serveur ne peut utiliser que l'adresse MAC attribuée pour envoyer et recevoir des paquets.
- Protection DHCP. La protection DHCP (Dynamic Host Configuration Protocol) supprime les messages de serveur DHCP sur les ordinateurs virtuels non autorisés qui feignent d'être des serveurs DHCP. Vous pouvez définir ce paramètre au niveau de la carte réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Protection du routeur. Une protection de routeur, que vous pouvez définir au niveau de l'ordinateur virtuel, supprime la publication de routeur et le message de redirection des ordinateurs virtuels non autorisés qui feignent d'être des routeurs.
- Mise en miroir des ports. La mise en miroir des ports permet au trafic réseau de transiter au départ et à l'arrivée d'un ordinateur virtuel à des fins d'analyse. Cette opération s'effectue en copiant les paquets entrants et sortants, puis en transférant les copies vers un autre ordinateur virtuel configuré pour l'analyse.
- Association de cartes réseau. Vous pouvez configurer des ordinateurs virtuels pour utiliser l'association de cartes réseau.
- VLAN. Vous pouvez attribuer chaque invité à un réseau VLAN, si nécessaire.

Démonstration : Configuration des réseaux virtuels

Procédure de démonstration

Créer un réseau virtuel

1. Lancez le Gestionnaire de commutateur virtuel Hyper-V.
2. Vérifiez les options de commutateur.

Créer une carte réseau virtuelle

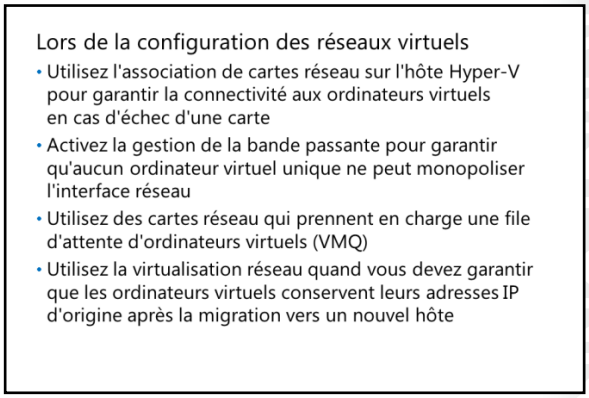
- Créez un nouvel ordinateur virtuel appelé **demo1**, puis connectez la carte réseau au nouveau commutateur réseau **Démo de classe**.

Vérifier les paramètres de la carte réseau virtuelle

1. Vérifiez les options de réseau pour l'ordinateur virtuel nouvellement créé demo1.
2. Supprimez l'ordinateur virtuel **demo1**, puis supprimez le nouveau commutateur **Démo de classe**.

Planification de réseaux pour un déploiement Hyper-V

Lorsque vous configurez des réseaux virtuels, les meilleures pratiques visent en général à garantir que vous mettez en service les ordinateurs virtuels avec la bande passante adéquate. Il s'agit d'éviter que les performances de tous les ordinateurs virtuels subissent les conséquences d'un fonctionnement gourmand en bande passante sur un ordinateur virtuel du même hôte, tel qu'une copie de fichier volumineux ou une pointe de trafic sur un site Web.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

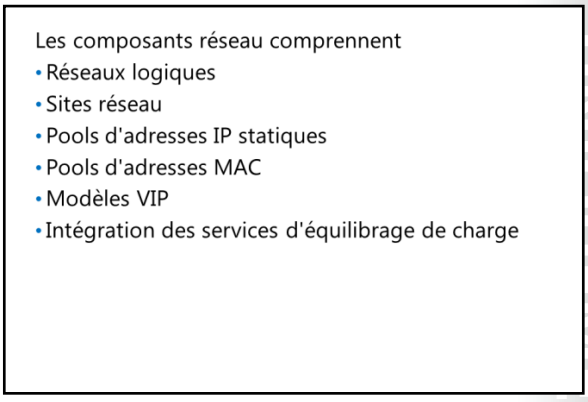
Les meilleures pratiques suivantes s'appliquent à la configuration de réseaux virtuels :

- Éléments à prendre en compte pour l'association de cartes réseau. Déployez plusieurs cartes réseau sur l'hôte Hyper-V, puis les configurez comme faisant partie d'une équipe. Cette démarche permet de s'assurer que la connectivité réseau sera conservée si les différentes cartes réseau échouent. Configurez plusieurs équipes qui se connectent à différents commutateurs pour vous assurer que la connectivité est maintenue si un commutateur matériel échoue.
- Éléments à prendre en compte pour la gestion de la bande passante. Vous pouvez utiliser la gestion de la bande passante pour allouer un minimum et un maximum de bande passante pour chaque carte réseau virtuelle. Configurez l'allocation de bande passante de manière à garantir que chaque ordinateur virtuel dispose d'une allocation de bande passante minimum. Cette démarche permet de s'assurer que si un autre ordinateur virtuel hébergé sur le même serveur Hyper-V rencontre une pointe de trafic, les autres ordinateurs virtuels peuvent communiquer normalement avec le réseau.
- Éléments à prendre en compte pour la file d'attente d'ordinateurs virtuels (VMQ). Mettez l'hôte Hyper-V en service avec une carte qui prend en charge la fonction VMQ, qui utilise le filtrage de paquet matériel pour fournir le trafic réseau directement à l'ordinateur virtuel. Cela améliore les performances, car l'hôte n'a pas besoin de copier le paquet du système d'exploitation hôte sur l'ordinateur virtuel. Quand vous ne configurez pas des ordinateurs virtuels de sorte qu'ils prennent en charge la fonction VMQ, le système d'exploitation hôte peut devenir un goulot d'étranglement quand il traite un trafic réseau volumineux.
- Éléments à prendre en compte pour la virtualisation réseau. La virtualisation réseau est compliquée à configurer, mais offre un avantage distinct par rapport aux réseaux VLAN, car il n'est pas nécessaire de configurer les réseaux VLAN sur tous les commutateurs qui se connectent à l'hôte Hyper-V. Vous pouvez effectuer toutes les configurations nécessaires quand vous avez besoin d'isoler des serveurs sur l'hôte Hyper-V sans impliquer l'équipe réseau. En revanche, si vous hébergez un grand nombre d'ordinateurs virtuels et devez les isoler, utilisez la virtualisation réseau plutôt que des réseaux VLAN.
- Éléments à prendre en compte pour la disponibilité, la protection et la récupération. Lors de la planification des clusters ou la réplication et les sauvegardes de site à site, tenez compte des emplacements où les goulots d'étranglement pourraient se produire. Vous pouvez utiliser les cartes Ethernet 10 Go dans certaines, ou toutes les sections d'infrastructure qui doivent mettre en service plusieurs hôtes simultanément, comme sur des serveurs de fichiers avec montée en puissance ou des hôtes de cible iSCSI et des serveurs de sauvegardes. Si possible, exécutez un pilote pour capturer des exemples de données, puis calculez le débit. Prévoyez d'analyser le trafic entre différentes sections du réseau virtuel, afin d'identifier les problèmes potentiels.

Gestion des réseaux virtuels dans VMM

La mise en réseau dans VMM comprend plusieurs améliorations qui permettent aux administrateurs de mettre efficacement les ressources réseau en service pour un environnement virtualisé. Vous pouvez maintenant tirer parti des fonctionnalités de mise en réseau suivantes :

- Créer et définir des réseaux logiques.
- Attribuer des adresses IP statiques et des adresses MAC statique.
- Intégrer les équilibrages de charge.



Réseaux logiques

Un réseau logique que vous combinez avec un ou plusieurs sites réseau associés est un regroupement nommé de sous-réseaux IP défini par l'utilisateur, des réseaux VLAN ou des paires sous-réseau IP/VLAN. Ceux-ci organisent et simplifient les attributions de réseau. Voici quelques exemples de réseau logiques possibles : BACKEND, FRONTEND, LAB, MANAGEMENT et BACKUP. Les réseaux logiques représentent une abstraction de l'infrastructure réseau physique sous-jacente, qui permet de modéliser le réseau selon des exigences opérationnelles et des propriétés de connectivité. Après avoir créé un réseau logique, vous pouvez l'utiliser pour spécifier le réseau sur lequel déployer un hôte ou un ordinateur virtuel (autonome ou partie d'un service). Les utilisateurs peuvent attribuer des réseaux logiques lorsqu'ils créent un ordinateur virtuel et un service, sans avoir à comprendre des détails du réseau.

Vous pouvez utiliser des réseaux logiques pour décrire des réseaux avec différentes fins, comme pour l'isolement du trafic et la mise en service des réseaux pour différents types de contrats de niveau de service (SLA). Par exemple, pour une application multiniveau, vous pouvez regrouper les sous-réseaux IP et les réseaux VLAN que vous utilisez pour la couche frontale Web en un réseau logique nommé FRONTEND. Vous pouvez choisir de regrouper les serveurs dans un réseau logique nommé BACKEND pour les sous-réseaux IP et les réseaux VLAN utilisés. Lorsqu'un utilisateur libre-service modèle l'application en tant que service, il peut choisir le réseau logique facilement pour les ordinateurs virtuels à chaque couche de service à laquelle il souhaite se connecter.

Au moins un réseau logique doit exister si vous souhaitez déployer des ordinateurs virtuels et des services. Par défaut, lorsque vous ajoutez un hôte Hyper-V à VMM, VMM crée automatiquement des réseaux logiques qui correspondent au premier nom de suffixe DNS (Domain Name System) du suffixe DNS spécifique à la connexion sur chaque carte réseau hôte. Pour rendre un réseau logique disponible à un hôte, vous devez associer le réseau logique à une carte réseau physique sur l'hôte, et la rendre disponible via un réseau virtuel externe ou un *commutateur virtuel externe*. Vous devez effectuer cette association pour chaque carte réseau.

Par défaut, lorsque vous ajoutez un hôte Hyper-V à VMM, si une carte réseau physique de l'hôte n'est associée à aucun réseau logique, VMM crée et associe automatiquement un réseau logique qui correspond au premier nom de suffixe DNS du suffixe DNS spécifique à la connexion. Par exemple, si le suffixe DNS de la carte réseau hôte est corp.contoso.com, VMM crée un réseau logique qui est nommé *corp.* Si vous n'associez aucun réseau virtuel à la carte réseau, si une tâche se connecte à un ordinateur virtuel via un réseau logique qui est associé à la carte réseau physique, VMM crée automatiquement un réseau virtuel externe. En outre, il l'associe au réseau logique. En revanche, aucun site réseau n'est créé automatiquement. Ces paramètres par défaut fournissent une solution pour vous aider à créer et déployer des ordinateurs virtuels sur votre réseau existant.

Sites réseau

Lorsque vous créez un réseau logique, vous pouvez créer un ou plusieurs sites réseau associés. Un site réseau associe un ou plusieurs sous-réseaux, réseaux VLAN, paires sous-réseau/VLAN à un réseau logique, et vous permet de définir des groupes hôtes auxquels le site réseau est disponible. Par exemple, si vous avez un groupe hôte à Seattle et un groupe hôte à New York, et que vous souhaitez rendre le réseau logique BACKEND disponible pour chaque groupe, vous pouvez créer deux sites réseau pour le réseau logique BACKEND. Vous pouvez limiter l'étendue d'un site réseau au groupe hôte de Seattle (et à tous les groupes hôtes enfants souhaités), et l'autre site réseau au groupe hôte de New York (et à tous les groupes hôtes enfants souhaités). En outre, vous devez ajouter les sous-réseaux et les réseaux VLAN appropriés pour chaque emplacement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pools d'adresses IP

Si vous associez un ou plusieurs sous-réseaux IP à un site réseau, vous pouvez créer un pool d'adresses IP. Un pool d'adresses IP *statique* permet à VMM d'attribuer des adresses IP statiques aux hôtes, comme lorsque vous utilisez VMM pour convertir un ordinateur nu en hôte Hyper-V ou pour les ordinateurs virtuels Windows qui s'exécutent sur n'importe quelle plateforme hyperviseur prise en charge. Les pools d'adresse IP statiques permettent à votre administrateur VMM de gérer les adresses IP de l'environnement virtuel. Cependant, la configuration des pools d'adresses IP statiques est facultative. Vous pouvez également attribuer des adresses automatiquement via le serveur DHCP s'il est disponible sur le réseau. Si vous utilisez le protocole DHCP, inutile de créer les pools d'adresses IP.

Pools d'adresses MAC

VMM peut attribuer des adresses MAC statiques automatiquement à de nouveaux périphériques réseau virtuel sur des ordinateurs virtuels Windows qui s'exécutent sur n'importe quel hôte Hyper-V, VMware ESX ou Citrix Xen-Server. VMM dispose de deux pools d'adresses MAC statiques par défaut : le pool d'adresses MAC par défaut (pour Hyper-V et Citrix Xen-Server) et le pool d'adresses MAC VMware par défaut (pour les hôtes VMware ESX). Vous devriez utiliser uniquement les pools d'adresses MAC statiques par défaut si vous définissez le type d'adresse MAC *Statique* pour un ordinateur virtuel. Si vous définissez l'ordinateur virtuel en sélectionnant le paramètre *Dynamique*, l'hyperviseur attribue l'adresse MAC. Vous pouvez utiliser les pools d'adresses MAC par défaut, ou vous pouvez configurer des pools d'adresses MAC personnalisés que vous limitez en étendue aux groupes hôtes spécifiques.

Modèles IP virtuels

Un modèle IP virtuel contient un équilibrage de charge, ainsi que les paramètres de configuration associés pour un type de trafic réseau spécifique. Par exemple, vous pouvez créer un modèle qui spécifie le comportement d'équilibrage de charge du trafic HTTPS en fonction d'un fabricant et modèle d'équilibrage de charge spécifique. Ces modèles représentent les meilleures pratiques en termes de configuration de l'équilibrage de charge. Après avoir créé un modèle IP virtuel, les utilisateurs (y compris les utilisateurs libre-service) peuvent spécifier le modèle IP virtuel à utiliser quand ils créent un service. Lorsque les utilisateurs modèlent un service, ils peuvent choisir un modèle disponible qui correspond le mieux à leurs équilibrages de charge et type d'application.

Intégration des services d'équilibrage de charge

En ajoutant un équilibrage de charge à VMM, vous pouvez équilibrer la charge des demandes sur les ordinateurs virtuels de la couche de service. Vous pouvez utiliser l'équilibrage de la charge réseau (NLB, Network Load Balancing), ou ajouter les équilibrages de charge matérielle pris en charge via la console VMM. VMM comprend NLB comme équilibrage de charge disponible et il utilise le tourniquet comme méthode d'équilibrage de charge. Pour ajouter des équilibrages de charge matérielle pris en charge, vous devez installer un fournisseur de configuration qui est disponible auprès du fournisseur d'équilibrage de charge. Le fournisseur de configuration est un plug-in VMM qui convertit les commandes Windows PowerShell® en appels d'interface de programmation d'applications (API, Application Programming Interface), propres à un fabricant et modèle d'équilibrage de charge. Les appareils d'équilibrage de la charge matérielle pris en charge sont F5 Big-IP, Brocade ServerIron et Citrix Netscaler. Vous devez obtenir le fournisseur d'équilibrage de charge auprès du fournisseur d'équilibrage de charge, et installer le fournisseur sur le serveur de gestion VMM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Commutateurs logiques

Les commutateurs logiques vous permettent d'appliquer une configuration unique à plusieurs hôtes. Vous pouvez les configurer en vue d'utiliser les profils de port natif, la classification de ports et les extensions de commutateur virtuel. Les types d'extensions de commutateur pris en charge sont les suivants :

- Analyse : Les extensions d'analyse permettent de surveiller et de générer des rapports sur le trafic, mais ne permettent pas de modifier des paquets.
- Capture. Les extensions de capture permettent d'inspecter et de tester le trafic, mais ne permettent pas de modifier les paquets.
- Filtrage. Les extensions de filtrage permettent de bloquer, modifier ou défragmenter des paquets. Elles permettent également de bloquer des ports.
- Transfert. Les extensions de transfert permettent de diriger le trafic en définissant des destinations ; elles permettent également de capturer et de filtrer le trafic. Pour éviter les conflits en ligne, une extension de transfert peut être active sur un commutateur logique.
- Gestionnaire d'extensions de commutateur virtuel. Un gestionnaire d'extensions de commutateur virtuel permet d'utiliser une console de gestion de fournisseurs réseau conjointement avec VMM. Pour cela, vous devez installer le logiciel du fournisseur sur le serveur VMM.

Profils de port natif

Vous pouvez utiliser des profils de port natif pour configurer les cartes de liaison montante qui doivent être disponibles sur les cartes réseau physiques auxquelles un commutateur se connecte. Vous pouvez attribuer ces derniers aux groupes hôtes, puis les activer pour la prise en charge de la virtualisation réseau Windows. Vous pouvez également utiliser les profils de port natif pour configurer les cartes virtuelles afin de vérifier des paramètres de déchargement, tels que VMQ, le déchargement des tâches IPsec et SR-IOV. Les profils de port des cartes réseau virtuelles vous permettent de réutiliser les mêmes paramètres sur plusieurs commutateurs, ce qui simplifie le déploiement de vos environnements virtuels.

En outre, vous pouvez spécifier des paramètres de bande passante minimum et maximum et l'épaisseur de bande passante pour définir la quantité de bande passante que la carte réseau virtuelle peut utiliser par rapport à d'autres cartes réseau virtuelles qui se connectent au même commutateur.

Les profils par défaut suivants ont déjà été créés dans VMM.

- Profil SR-IOV :
- Profil de carte réseau d'équilibrage de charge du réseau
- Cartes de bande passante à débit faible, moyen ou élevé
- Gestion des hôtes
- Migration en direct
- Cluster
- iSCSI
- Par défaut

Chacun de ces profils a été configuré avec des variantes de paramétrage en termes de déchargement, sécurité et bande passante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Classifications de ports

Vous pouvez créer des classifications de ports, puis les utilisez sur plusieurs commutateurs logiques pour aider à identifier et regrouper des ensembles de fonctionnalités.

Les classifications de ports par défaut suivantes ont déjà été créées dans VMM.

- SR-IOV
- Équilibrage de la charge réseau
- Charge de travail de migration dynamique
- Charge de travail du cluster hôte
- Bande passante à débit faible, moyen ou élevé
- Charge de travail iSCSI

Passerelles

Dans VMM, une passerelle autorise le trafic réseau dans et hors d'un réseau d'ordinateurs virtuels qui utilise la virtualisation réseau. Vous pouvez configurer ce paramètre pour le routage de réseau local, qui route le trafic entre le réseau d'ordinateur virtuel et le réseau physique. Vous pouvez également le configurer pour le routage de réseau distant, qui crée d'abord une connexion de réseau privé virtuel (VPN) avec un autre point de terminaison d'un site à site VPN. Le trafic s'effectue alors dans et hors du réseau d'ordinateur virtuel via le tunnel VPN.

Démonstration : Configuration des composants d'un réseau virtuel dans VMM

Dans cette démonstration, vous allez apprendre à utiliser VMM pour créer et configurer les composants réseau suivants :

- Réseaux logiques et pools d'adresses IP de réseau logique.
- Profils de port natif, liaisons montantes et cartes virtuelles.
- Commutateurs logiques.

Vous verrez également où attribuer des commutateurs logiques aux hôtes Hyper-V.

Procédure de démonstration

Créer un réseau logique

1. Sur **LON-VMM1**, lancez la console Virtual Machine Manager.
2. Cliquez sur l'espace de travail **Ensemble fibre optique** dans le ruban, cliquez sur **Créer**, puis sur **Réseau logique**.
3. Dans la page **Nom**, dans le champ **Nom**, tapez **Classe1**, puis cliquez sur **Autoriser les nouveaux réseaux d'ordinateurs virtuels créés sur ce réseau logique à utiliser la virtualisation de réseau**. Cliquez sur **Suivant**.
4. Dans la page **Site réseau**, cliquez sur **Ajouter**, puis dans la section **Groupes hôtes pouvant utiliser ce site réseau**, sélectionnez **Tous les ordinateurs hôtes**.

5. Dans la zone **VLAN et sous-réseaux IP associés**, cliquez sur **Insérer une ligne**, cliquez sur le champ **Réseau local virtuel**, puis tapez **3**. Cliquez sur le champ **Sous-réseau IP**, puis tapez **192.168.3.0/24**, cliquez sur **Suivant**, puis **Terminer**.
6. Fermez la fenêtre Travaux.

Créer un pool d'adresses IP de réseau logique

1. Cliquez sur l'espace de travail **Ensemble fibre optique**, puis dans le ruban, cliquez sur **Pool d'adresses IP**. Dans la page **Nom**, dans le champ **Nom**, tapez **Pool IP Classe1**, cliquez dans la zone de liste déroulante **Réseau logique**, puis cliquez sur **Classe1**, et **Suivant**.
2. Dans la page **Site réseau**, cliquez sur **Utiliser un site réseau existant**, puis vérifiez que **Classe1_0** est sélectionné. Cliquez dans la zone de liste déroulante **Sous-réseau IP**, sélectionnez **192.168.3.0/24**, puis cliquez sur **Suivant**.
3. Dans la page **Plage d'adresses IP**, vérifiez les options, puis cliquez sur **Suivant**.
4. Dans la page **Passerelle**, vérifiez les options, puis cliquez sur **Suivant**.
5. Dans la page **DNS**, vérifiez les options, puis cliquez sur **Suivant**. Dans la page **WINS**, vérifiez les options, cliquez sur **Suivant**, puis dans la page **Résumé**, cliquez sur **Terminer**, puis fermez la fenêtre Travaux.

Créer un profil de port natif de liaison montante

1. Dans le ruban, cliquez sur **Créer**, puis sur **Profil de port natif**.
2. Dans la page **Général**, cliquez dans le champ **Nom**, puis tapez **Liaison montante Classe1**. Cliquez sur **Profil de port de liaison montante**, puis cliquez sur **Suivant**.
3. Dans la page **Configuration réseau**, sous **Sites réseau**, cliquez sur **Classe 1_0**, sur l'option **Activer la virtualisation de réseau Windows**, puis cliquez sur **Suivant**.
4. Dans la page **Résumé**, cliquez sur **Terminer**, puis fermez la fenêtre Travaux.

Créer un commutateur logique

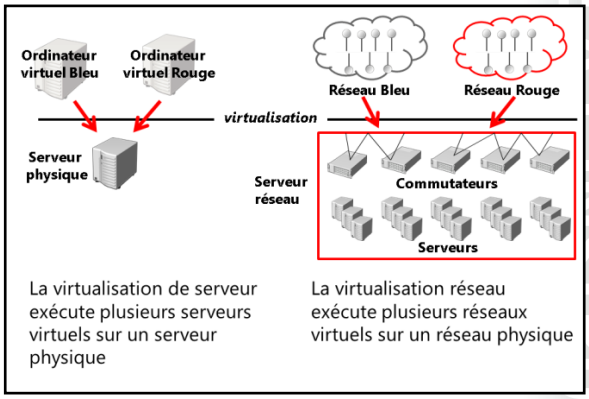
1. Dans le ruban, cliquez sur **Créer**, puis sur **Commutateur logique**.
2. Dans la page **Mise en route**, cliquez sur **Suivant** et dans la page **Général**, dans le champ **Nom**, tapez **Commutateur Classe1**, puis cliquez sur **Suivant**.
3. Dans la page **Extensions**, conservez les extensions par défaut puis cliquez sur **Suivant**.
4. Dans la page **Liaison montante**, cliquez sur **Ajouter**, cliquez dans la zone de liste déroulante **Profil de port**, sélectionnez **Liaison montante Classe1**, cliquez sur **OK**, puis sur **Suivant**.
5. Dans la page **Port virtuel**, cliquez sur **Ajouter**, puis dans la page **Ajouter un port virtuel**, cliquez sur **Parcourir**.
6. Dans la page **Sélectionner une classification de profil de port**, cliquez sur **Bande passante élevée**, puis sur **OK**. Cliquez sur l'option **Inclure un profil de port de carte réseau virtuelle dans ce port virtuel**, cliquez sur le **Profil de port de carte réseau virtuelle natif**, sélectionnez la **Carte à bande passante moyenne**, cliquez sur **OK**, puis sur **Suivant**.
7. Dans la page **Résumé**, cliquez sur **Terminer**.
8. Fermez la fenêtre Travaux.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Ajouter un commutateur logique à un serveur hôte

1. Depuis l'espace de travail Ensemble fibre optique, cliquez avec le bouton droit sur **lon-host1**, sur **Propriétés**, **Commutateurs virtuels**, **Nouveau commutateur virtuel**, puis sur **Nouveau commutateur logique**.
2. À ce stade, si vous avez une autre carte réseau, vous pouvez attribuer le commutateur logique à une carte physique.
3. Dans la page Propriétés, cliquez sur **Matériel**, puis faites défiler l'écran et développez **Cartes réseau**. Cliquez sur votre carte réseau physique, et notez que vous pouvez activer ou désactiver la carte pour le placement et la gestion des ordinateurs virtuels. Cliquez sur le réseau logique, et à droite sous **Connectivité de réseau logique**, attribuez les réseaux et les sous-réseaux IP logiques.
4. Cliquez sur **Annuler**.

Qu'est-ce que la virtualisation réseau ?



Vous pouvez utiliser la virtualisation réseau pour isoler des ordinateurs virtuels de différentes organisations, même s'ils partagent le même hôte Hyper-V. Par exemple, vous pourriez fournir une infrastructure en tant que service (IaaS) à différentes entreprises, ou vous pouvez simplement souhaiter évoquer une copie de certains ordinateurs virtuels sans créer un problème de réseau en créant des adresses IP en conflit. Vous pouvez utiliser la virtualisation réseau pour attribuer ces ordinateurs virtuels à des réseaux virtuels distincts qui s'exécutent sur même réseau physique/logique, mais qui sont isolés entre eux. La virtualisation réseau vous offre l'avantage de configurer toute l'isolation réseau sur l'hôte Hyper-V sans réseau VLAN. En outre, l'utilisation des passerelles ou des extensions VPN vous permet d'étendre les réseaux virtualisés pour la communication isolée entre les hôtes.

Vous pouvez continuer à exécuter des ordinateurs isolés avec les réseaux VLAN. En revanche, il est nécessaire de configurer les commutateurs physiques avec les ID VLAN appropriés.

Lorsque vous configurez la virtualisation réseau, chaque ordinateur virtuel invité a deux adresses IP qui incluent :

- Adresse IP du client. Le client attribue cette adresse IP à l'ordinateur virtuel. Vous pouvez configurer cette adresse IP de sorte que la communication avec le réseau interne du client soit possible même si l'ordinateur virtuel est hébergé sur un serveur Hyper-V qui est connecté à un réseau IP public distinct. L'utilisation de la commande **ipconfig** sur l'ordinateur virtuel permet d'afficher l'adresse IP du client.
- Adresse IP du fournisseur. Le fournisseur d'hébergement attribue cette adresse IP, visible par le fournisseur d'hébergement et par d'autres hôtes sur le réseau physique. Cette adresse IP n'est pas visible de l'ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez utiliser la virtualisation réseau pour héberger plusieurs ordinateurs physiques qui utilisent la même adresse de client, telle que 192.168.15.101, sur le même hôte Hyper-V. Dans pareille situation, le fournisseur d'hébergement attribue une adresse IP différente à chaque ordinateur virtuel. Toutefois, ces adresses ne sont pas visibles depuis ce dernier.

Vous pouvez gérer la virtualisation réseau à l'aide des applets de commande Windows PowerShell. Toutes les applets de commande de virtualisation réseau sont présentes dans le module Windows PowerShell NetWNV. Les clients accèdent aux ordinateurs virtuels qui tirent profit de la virtualisation réseau par l'intermédiaire du routage et de l'accès à distance. Ils établissent une connexion en tunnel à partir de leur réseau au réseau via le réseau virtualisé sur le serveur Hyper-V.

 **Liens de référence :** Pour une vue d'ensemble complète de la virtualisation réseau, accédez à http://go.microsoft.com/fwlink/?LinkID=285279.

Démonstration : Configuration de la virtualisation réseau

Dans cette démonstration, vous allez apprendre à activer et configurer la virtualisation réseau dans Windows Server 2012 et VMM. Pour les ordinateurs équipés uniquement d'une carte réseau, vous pouvez configurer plusieurs étapes, mais vous ne pourrez pas attribuer le commutateur logique à l'hôte ou déployer un ordinateur virtuel qui utilise la virtualisation réseau.

Procédure de démonstration

Activer le pilote du filtre de virtualisation réseau Windows

1. Dans la page **LON-HOST1**, ouvrez la page **Cartes réseau** puis sur la carte physique que les hôtes utilisent, activez **Pilote du filtre de virtualisation réseau Windows**, puis sélectionnez **OK**.

Actualiser LON-HOST1

1. Sur **LON-VMM1**, ouvrez la console Virtual Machine Manager, puis actualisez l'hôte.

Créer le réseau d'ordinateurs virtuels Rouge

1. Sur **LON-VMM1**, ouvrez la console Virtual Machine Manager, puis cliquez sur l'espace de travail **Ordinateurs virtuels et services**. Créez un réseau d'ordinateurs virtuels nommé **Classe1_Rouge**, puis sélectionnez l'isolation réseau, créez un sous-réseau nommé **Réseau Rouge**, et attribuez le sous-réseau **192.168.3.0/24**.

Créer le réseau d'ordinateurs virtuels Bleu

1. Dans l'espace de travail **Ordinateurs virtuels et services,** créez un autre réseau d'ordinateurs virtuels nommé **Classe1_Bleu**, puis sélectionnez l'isolation réseau, créez un sous-réseau nommé **Réseau Bleu**, et attribuez le sous-réseau **192.168.3.0/24**.

Créer des pools IP d'ordinateur virtuel

1. Créez un pool d'IP pour le réseau d'ordinateurs virtuels Bleu, nommé **Pool IP du réseau d'ordinateurs virtuels Bleu**, puis acceptez les valeurs par défaut et notez que la première adresse du pool est réservée.
2. Créez un pool d'IP du réseau d'ordinateurs virtuels Rouge, nommé **Pool IP du réseau d'ordinateurs virtuels Rouge**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et implémentation des réseaux et du stockage de virtualisation

Scénario

Après avoir terminé la conception et l'implémentation du serveur hôte et des couches de gestion de l'infrastructure de virtualisation, l'étape suivante consiste à planifier et implémenter le stockage et les couches du réseau.

Étant donné que de nombreux ordinateurs virtuels partageront la même infrastructure de stockage et réseau, il est primordial que ces couches soient hautement disponibles. En même temps, A. Datum ne dispose pas du budget nécessaire pour une mise en service excessive de son environnement virtuel, donc votre conception doit fournir suffisamment de capacité sans être trop excessive.

Les administrateurs de stockage à Londres conçoivent l'infrastructure de stockage à l'aide du réseau SAN Fibre Channel. Les administrateurs réseau de Londres sont responsables de concevoir la configuration réseau. Cependant, vous êtes chargé de créer la conception de stockage pour le déploiement Hyper-V à Toronto. Vous êtes également chargé de créer la conception de réseau à Toronto.

Objectifs

- planifier une infrastructure de stockage ;
- planifier une infrastructure réseau ;
- implémenter le stockage iSCSI pour les ordinateurs virtuels ;
- configurer les composants réseau pour le déploiement d'ordinateurs virtuels ;
- configurer la virtualisation réseau.

Configuration de l’atelier pratique

Durée approximative : 60 minutes

Ordinateur(s) virtuel(s)	22414B-LON-DC1 22414B-LON-VMM1 22414B-LON-SVR1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour effectuer cet atelier pratique, vous devez vérifier que vous avez terminé l'atelier pratique du module 2. Vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, ouvrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22414B-LON-DC1**, et dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **Administrateur**
   - Mot de passe : **Pa$$w0rd**
   - Domaine : **ADATUM**
4. Dans le Gestionnaire Hyper-V, cliquez sur **22414B-LON-SVR1**, et dans le volet Actions, cliquez sur **Démarrer**.
5. Répétez les étapes 2 à 3 pour **22414B-LON-SVR1**.

Exercice 1 : Planification d'une infrastructure de stockage pour la virtualisation

Scénario

À Toronto, A. Datum envisage d'utiliser une infrastructure de stockage iSCSI pour les ordinateurs virtuels. L'équipe chargée de l'exploitation du serveur a fourni les informations suivantes relatives aux déploiements de serveurs qu'elle planifie pour la filiale de Toronto. Ils déploieront deux contrôleurs de domaine, qui sont également des serveurs DNS, comme les ordinateurs virtuels du centre de données de Toronto. Les serveurs nécessitent uniquement une partition du système d'exploitation standard. L'équipe d'exploitation du serveur déploiera précisément :

- Quatre serveurs Web en tant qu'ordinateurs virtuels pour le centre de données de Toronto. Les serveurs Web ont besoin d'une partition du système d'exploitation standard et d'environ 30 Go de stockage par serveur.
- Deux serveurs de fichiers en tant qu'ordinateurs virtuels pour le centre de données de Toronto. Les serveurs de fichiers ont besoin d'une partition du système d'exploitation standard et d'environ 1 To de stockage par serveur.
- Trois serveurs de base de données en tant qu'ordinateurs virtuels pour le centre de données de Toronto. Les serveurs de base de données ont besoin d'une partition du système d'exploitation standard et d'environ 900 Go de stockage par serveur.
- Quatre serveurs Exchange Server 2012 en tant qu'ordinateurs virtuels pour le centre de données de Toronto. Les serveurs Exchange ont besoin d'une partition du système d'exploitation standard et d'environ 3,5 To de stockage par serveur.

Vous devez planifier l'infrastructure de stockage pour le déploiement du stockage iSCSI à Toronto. A. Datum envisage de déployer deux serveurs Windows Server 2012 avec des cibles iSCSI. Vous devez créer une conception de stockage qui fournit le stockage suffisant et la disponibilité selon les exigences de l'entreprise, que le tableau suivant détaille.

Rôle serveur	Nombre déployé	Stockage du système d'exploitation	Stockage des données (max)	Suggestion de configuration des performances
Contrôleurs de domaine / Serveurs DNS	2	40 Go		RAID 1 moyen
Serveurs Web	4	40 Go	30 Go	RAID 1 ou 5 moyen

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Rôle serveur	Nombre déployé	Stockage du système d'exploitation	Stockage des données (max)	Suggestion de configuration des performances
Serveurs de fichiers	2	40 Go	1 000 Go	RAID 5 moyen
Serveurs de base de données	3	40 Go	900 Go	RAID 1 ou 10 - performances élevées
Serveurs Exchange	4	40 Go	3 500 Go	RAID 5 moyen

Stratégie de stockage d'A. Datum Toronto

Numéro de référence du document : BS0905/1

Auteur du document	Brad Sutton
Date	5 septembre

Présentation des exigences

Pour planifier une stratégie de stockage pour atteindre les objectifs suivants :

- Fournir le stockage suffisant pour virtualiser les serveurs répertoriés.
- Fournir la haute disponibilité si possible.
- Identifier les risques et goulots d'étranglement.

Informations supplémentaires

- Fournissez une autre solution moins coûteuse qui offre la même disponibilité.

Tâches et questions

1. Les serveurs fournis ont une seule carte réseau intégrée de 10 Go avec toutes les dernières configurations iSCSI ; pour la redondance vous souhaitez en acquérir davantage ; il y a trois emplacements PCI Express disponibles. Que devez-vous acheter ?
2. L'équipe réseau avec laquelle vous travaillez vous informe que le coût et les délais seront importants pour implémenter un réseau iSCSI distinct. Le réseau actuel est relativement récent et dispose d'environ 10 Go de capacité bien que limité en nombre de connexions. Vous devez indiquer à l'équipe le nombre de connexions de 1 ou 10 Go qui seront nécessaires.
3. Vous envisagiez d'avoir un autre serveur hôte en tant qu'hôte de maintenance, mais le budget ne le permet pas. Quelle autre solution pourriez-vous proposer ?
4. Vous avez identifié la protection des données comme un risque et un goulot d'étranglement potentiels. Qu'est-ce qui en serait la cause et comment pourriez-vous résoudre le problème ?
5. Quel rôle ou quelle fonctionnalité Windows Server pouvez-vous activer pour continuer à exécuter vos ordinateurs virtuels en cas de défaillance d'un composant de stockage réseau, tel qu'une carte réseau ou un commutateur réseau ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Lire la documentation fournie avec le produit.
2. Mettre à jour le document de proposition en fonction du plan d'action planifié.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.
4. Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur.

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation fournie dans le manuel du stagiaire.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

- Répondez aux questions de la section Propositions du document de stratégie de stockage d'A. Datum Toronto.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions avec celles du corrigé de l'atelier pratique.

▶ Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Préparez-vous à discuter de vos propositions avec la classe.

Exercice 2 : Planification d'une infrastructure réseau pour la virtualisation

Scénario

L'équipe réseau chez A. Datum a fourni les informations suivantes pour la configuration réseau dans le centre de données de Toronto.

Nom/identificateur VLAN	Objectif	Adresses IP
VLAN3/3	Serveurs de virtualisation	172.16.1.0/24
VLAN4/4	Serveurs d'infrastructure	172.16.2.0/24
VLAN5/5	Serveurs d'applications	172.16.3.0/24
VLAN6/6	Réseau de sauvegarde	172.16.4.0/24
VLAN7/7	Réseau iSCSI	172.16.5.0/24

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous devez planifier la configuration du réseau virtuel pour la configuration VMM du centre de données de Toronto. A. Datum envisage de virtualiser certains serveurs pour une organisation partenaire. Les adresses IP de ces serveurs sont identiques à celles de certains ordinateurs virtuels que l'équipe d'A. Datum envisage de déployer dans le centre de données de Toronto. Vous devez vérifier que vous pouvez déployer les deux groupes d'ordinateurs virtuels sur les mêmes serveurs Hyper-V, et qu'ils peuvent communiquer entre eux sur le réseau.

Stratégie de virtualisation réseau d'A. Datum Toronto	
Numéro de référence du document : BS0906/1	
Auteur du document Date	Brad Sutton 8 septembre

Présentation des exigences

Planifiez une stratégie de virtualisation réseau afin d'atteindre les objectifs suivants en :

- Acceptant plusieurs ordinateurs virtuels Hyper-V avec la même adresse IP sur le même hôte.
- Acceptant que le trafic transite entre les ordinateurs virtuels isolés situés sur différents hôtes Hyper-V.

Propositions

1. Parmi les réseaux répertoriés, lesquels devriez-vous virtualiser pour atteindre l'objectif ?
2. Où et comment pouvez-vous configurer des réseaux virtualisés ?
3. Quelle est la procédure de configuration des réseaux virtualisés ?
4. Existe-t-il d'autres moyens d'héberger les ordinateurs virtuels qui se chevauchent ?
5. Où pouvez-vous rechercher les commandes Windows PowerShell pour configurer la virtualisation réseau ?
6. Vous avez attribué le pilote du filtre de virtualisation réseau au commutateur Ethernet virtuel, qui est associé à la carte réseau physique. Est-ce correct ?

Les tâches principales de cet exercice sont les suivantes :

1. Lire la documentation fournie avec le produit.
2. Mettre à jour le document de proposition en fonction du plan d'action planifié.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.
4. Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur.

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation et le scénario fournis.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

- Répondez aux questions de la section Propositions du document de stratégie de virtualisation réseau d'A. Datum Toronto.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions avec celles du corrigé de l'atelier pratique.

▶ Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Préparez-vous à discuter de vos propositions avec la classe.

Exercice 3 : Implémentation d'une infrastructure de stockage pour la virtualisation

Scénario

A. Datum a décidé d'implémenter le stockage d'ordinateurs virtuels dans le centre de données de Toronto et dans les deux centres régionaux à l'aide d'un déploiement de stockage iSCSI. Vous devez configurer les cibles iSCSI et les initiateurs iSCSI pour activer ce déploiement.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les cibles iSCSI pour le déploiement d'ordinateurs virtuels.
2. Configurer les initiateurs iSCSI.

▶ Tâche 1 : Configurer les cibles iSCSI pour le déploiement d'ordinateurs virtuels

Ajouter le service du rôle de serveur cible iSCSI

1. Sur **LON-SVR1**, dans le Gestionnaire de serveur, ajoutez le rôle **Serveur cible iSCSI** (situé sous Services de fichiers et iSCSI).

Créer un pool de stockage

1. Sur **LON-SVR1**, ouvrez **Gestion du disque**, puis créez trois disques virtuels (VHDX) de 50 Go. Ceux-ci doivent être nommés et localisés comme suit :
   - **E:\iSCSI1.vhdx**.
   - **E:\iSCSI2.vhdx**.
   - **E:\iSCSI3.vhdx**.
2. **Initialiser** les trois disques.
3. Fermez la fenêtre Gestion des disques.
4. Sur LON-SVR1, dans, **Services de fichiers et de stockage**, cliquez sur **Pools de stockage**.
5. Dans la section POOLS DE STOCKAGE, créez un nouveau pool de stockage nommé **VMPool** qui utilise les trois nouveaux disques.
6. Suivez l'Assistant Nouveau pool de stockage en acceptant les paramètres par défaut. Dans la page **Résultats**, cliquez sur **Créer un disque virtuel lorsque l'Assistant se ferme**, puis cliquez sur **Fermer**. L'Assistant Nouveau disque virtuel se lance.
7. Suivez l'assistant, puis dans la page **Nom du disque dur virtuel**, dans le champ **Nom**, tapez **VMStorage**. Choisissez la mise en service **Parity** (Parité) et **Fin**, et conservez la taille de 100 Go.
8. Fermez la page **Résultats**.
9. Lorsque l'Assistant Nouveau volume se lance, suivez-le et dans la page **Serveur et disque**, dans la zone Disque, cliquez sur **VMStorage Disque virtuel**. Dans la page **Taille**, laissez **(99,9) Go**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Dans la page **Lettre de lecteur ou dossier**, conservez la Lettre du lecteur **F**. Dans la page **Paramètres du système de fichiers**, tapez **VMStorage** pour le **Nom de volume**.
11. Dans le volet Services de fichiers et de stockage, cliquez sur **iSCSI**.
12. Dans le volet DISQUES VIRTUELS iSCSI, créez un Nouveau disque virtuel iSCSI.
13. Sous **Emplacement de stockage**, cliquez sur **F**, et utilisez **iSCSIDisk1** pour le **Nom du disque dur virtuel iSCSI**. Appliquez la taille de **99 Go**, puis créez une **cible iSCSI** nommée **LON-SVR1**.
14. Dans la page **Indiquer les serveurs d'accès**, tapez **Adresse IP**, puis tapez **172.16.0.31**.
15. Exécutez l'Assistant en conservant les paramètres par défaut, puis cliquez sur **Fermer**.
16. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES**, puis dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
17. Créez un autre disque virtuel iSCSI sur **C:** nommé **iSCSIDisk2**.
18. Appliquez la taille de **5 Go**.
19. Attribuez **LON-SVR1** pour la cible.

▶ Tâche 2 : Configurer les initiateurs iSCSI

Configurer les initiateurs iSCSI

1. Sur **LON-HOST1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, **Initiateur iSCSI**, puis lorsque vous y êtes invité, démarrez le service Microsoft iSCSI, avant de cliquer sur **Oui**.
2. Dans la page **Cibles**, dans le champ **Cible**, tapez **172.16.0.12**. Cliquez sur **Connexion rapide**, cliquez sur **Terminer**, puis cliquez sur **OK** pour fermer la page.
3. Sur **LON-HOST1**, maintenez la touche Windows appuyée, appuyez sur **X**, puis cliquez sur **Gestion du disque**.
4. Recherchez le nouveau **disque de 99 Go**, mettez-le en ligne avant de l'initialiser, puis créez un Nouveau volume simple. Conservez la taille par défaut, attribuez la lettre **V**, puis ajoutez le nom **VMStorage**.
5. Fermez la fenêtre **Gestion des disques**.

Exercice 4 : Implémentation d'une infrastructure réseau pour la virtualisation

Scénario

Vous devez maintenant configurer l'infrastructure réseau du déploiement de virtualisation.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer des réseaux logiques que votre création requiert.
2. Configurer la virtualisation réseau.
3. Attribuer des ordinateurs virtuels aux réseaux d'ordinateurs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Configurer des réseaux logiques que votre création requiert

Créer le réseau logique

1. Sur **LON-VMM1**, sur la barre des tâches, cliquez sur le bouton **Console Virtual Machine Manager**.
2. Dans l'espace de travail Ensemble fibre optique, créez un **réseau logique** nommé **Réseau de production de Toronto**. Entrez une **description** d'**Adatum Toronto – Réseau logique de production**, puis cliquez sur **Autoriser les nouveaux réseaux d'ordinateurs virtuels créés sur ce réseau logique à utiliser la virtualisation de réseau**. Cliquez sur **Suivant**.
3. Dans la page **Sites réseau**, cliquez sur **Ajouter**, puis dans la section **Groupes hôtes pouvant utiliser ce site réseau**, sélectionnez **Tous les ordinateurs hôtes**.
4. Cliquez sur **Insérer une ligne**, puis cliquez dans le champ **Réseau local viruel**. Tapez **0**, cliquez sur le champ **Sous-réseau IP**, puis tapez **172.16.3.0/24**, cliquez sur **Suivant**, puis sur **Terminer**.
5. Fermez la fenêtre Travaux.

Créer un pool IP

1. Dans l'espace de travail Ensemble fibre optique, créez et attribuez un **Pool d'adresses IP** nommé **Applications de Toronto** au site réseau **Réseau de production de Toronto**. Dans la page **Site réseau**, cliquez sur **Utiliser un site réseau existant**, sélectionnez **Réseau de production de Toronto_0**, cliquez dans la zone de liste déroulante **Sous-réseau IP**, sélectionnez **172.16.3.0/24**, puis cliquez sur **Suivant.** Réservez la plage comprise entre 172.16.3.100 et 172.16.3.120 pour les adresses IP réservées pour les adresses IP virtuelles d'équilibrage de charge (VIP), puis attribuez 172.16.3.1 pour la passerelle. Dans le champ de description, tapez **Pool IP de l'application de production de Toronto**.

Créer un profil de port natif

1. Créez un **Profil de port natif** nommé **Carte réseau par défaut de Toronto**. Il doit correspondre à un profil de port de liaison montante que vous attribuez au site du réseau de production de Toronto, et sur lequel vous activez la virtualisation réseau.

Créer un commutateur logique

1. Créer un commutateur logique nommé **Commutateur logique de Toronto**, puis associez-le à la **Carte réseau par défaut de Toronto**.
2. Ajoutez les classifications de port et les profils de port de carte réseau virtuelle pour ce qui suit :
   - **Gestion des hôtes/Gestion de l'ordinateur hôte**
   - **Charge de travail de migration dynamique/Migration en direct**
   - **Charge de travail du cluster hôte/Cluster**
   - **Bande passante élevée/Carte à haute bande passante**
3. Fermez la fenêtre Travaux.

Ajouter la carte de bouclage Microsoft

1. Sur **LON-HOST1**, ouvrez le Panneau de configuration, ouvrez le Gestionnaire de périphériques, puis cliquez avec le bouton droit sur **LON-HOST1**, cliquez sur **Ajouter un matériel d'ancienne génération**. L'Assistant Ajout de matériel se lance.
2. Suivez l'Assistant, choisissez l'option **Installer le matériel que je sélectionne manuellement dans la liste (utilisateur expérimenté)**, ajoutez des Cartes réseau, le fabricant de cartes réseau est Microsoft et le type est **Carte de bouclage Microsoft KM-TEST**. Terminez l'Assistant.

Actualiser LON-HOST1

1. Sur **LON-VMM1**, ouvrez la console Virtual Machine Manager.
2. Cliquez sur l'espace de travail **Ensemble fibre optique**, développez **Serveurs**, **Tous les ordinateurs hôtes**, développez **Hôtes de London**, cliquez avec le bouton droit sur **lon-host1**, puis sur **Actualiser**.

Mettre les hôtes Hyper-V à jour pour utiliser les réseaux logiques

1. Depuis l'espace de travail Ensemble fibre optique, cliquez avec le bouton droit sur **lon-host1**, sur **Propriétés**, **Commutateurs virtuels**, **Nouveau commutateur virtuel**, puis sur **Nouveau commutateur logique**. Sous Cartes physiques, cliquez sur la liste déroulante **Carte**, puis sélectionnez **Carte de bouclage Microsoft KM-TEST.**
2. Dans la page Propriétés, cliquez sur **Matériel**, puis faites défiler l'écran et développez **Cartes réseau**. Cliquez sur la **Carte de bouclage Microsoft KM-TEST** ; vous pouvez voir que la carte est disponible pour le placement.
3. Cliquez sur **Connectivité de réseau logique** qui est répertorié sous la Carte de bouclage Microsoft KM-TEST, puis à droite de la page Matériel sous **Connectivité de réseau logique**, cliquez sur **Réseau de production de Toronto**, sur **OK**, lisez l'avertissement, puis cliquez sur **OK**.

▶ Tâche 2 : Configurer la virtualisation réseau

Activer le pilote du filtre de virtualisation réseau Windows

1. Sur LON-HOST1, dans le Gestionnaire de serveur, cliquez sur **Serveur local**, puis dans la zone **PROPRIÉTÉS**, cliquez sur **172.16.0.31, Compatible IPv6**. La page **Connexions réseau** s'affiche.
2. Dans la page **Connexions réseau**, cliquez avec le bouton droit sur la carte physique, puis sélectionnez **Propriétés**.
3. Activez le **Pilote du filtre de virtualisation réseau Windows**, puis cliquez sur **OK**.

Actualiser LON-HOST1

1. Sur **LON-VMM1**, ouvrez la console Virtual Machine Manager.
2. Cliquez sur l'espace de travail **Ensemble fibre optique**, développez **Hôtes de London**, cliquez avec le bouton droit sur **lon-host1**, puis sur **Actualiser**.

Configurer un réseau d'ordinateurs virtuels pour les serveurs d'applications à l'aide de la virtualisation réseau

1. Dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Ordinateurs virtuels et services**. Dans le ruban, cliquez sur **Créer un réseau d'ordinateurs virtuels**.
2. Dans la page **Nom**, dans le champ **Nom**, tapez **Réseau d'ordinateurs virtuels Applications de Toronto**, cliquez sur le champ **Description**, puis tapez **Serveurs d'application de Toronto**. Cliquez dans la zone de liste déroulante **Réseau logique**, sélectionnez **Réseau de production de Toronto**, puis cliquez sur **Suivant**.
3. Dans la page **Isolation**, cliquez sur **Isoler l'aide de la virtualisation réseau Hyper-V**, puis sur **Suivant**.
4. Dans la page **Sous-réseaux d'ordinateurs virtuels**, cliquez sur **Ajouter**, et dans le champ **Nom**, tapez **Serveurs d'application de Toronto**. Dans le champ **Sous-réseau**, tapez **172.16.3.0/24**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans la page **Passerelle**, laissez l'option **Aucune connectivité** sélectionnée, puis cliquez sur **Suivant**. Examinez le résumé, puis cliquez sur **Terminer**.
6. Fermez la fenêtre Travaux.
7. Répétez les étapes 1 à 6 pour créer un réseau d'ordinateurs virtuels nommé **Réseau d'ordinateurs virtuels Applications_Partenaire de Toronto**, puis utilisez le même sous-réseau.

Créer des pools IP de réseau d'ordinateurs virtuels

1. Dans l'espace de travail Ordinateurs virtuels et services, cliquez sur **Réseaux d'ordinateurs virtuels**, cliquez sur **Réseau d'ordinateurs virtuels Applications de Toronto**, puis cliquez avec le bouton droit et sélectionnez **Créer un pool d'adresses IP**.
2. Dans la page **Nom**, cliquez sur le champ **Nom**, puis tapez **Pool IP du réseau d'ordinateurs virtuels Applications de Toronto**. Vérifiez que le réseau d'ordinateurs virtuels est défini sur **Réseau d'ordinateurs virtuels Applications de Toronto** et que le sous-réseau d'ordinateurs virtuels est défini sur **Serveurs d'application de Toronto (172.16.3.0/24)**, puis cliquez sur **Suivant**.
3. Dans la page **Plage d'adresses IP**, conservez les paramètres par défaut, puis cliquez sur **Suivant**.
4. Dans la page **Passerelle**, cliquez sur **Suivant**, puis dans la page **DNS**, cliquez sur **Suivant**. Dans la page **WINS**, cliquez sur **Suivant**, puis dans la page **Résumé**, cliquez sur **Terminer**. Fermez la fenêtre Travaux.

▶ Tâche 3 : Attribuer des ordinateurs virtuels aux réseaux d'ordinateurs virtuels

Attribuez des ordinateurs virtuels aux réseaux d'ordinateurs virtuels

1. Dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Ordinateurs virtuels et services**. Dans le ruban, cliquez sur la moitié supérieure du bouton **Créer un ordinateur virtuel**.
2. Dans la page **Sélectionner une source**, cliquez sur **Créer l'ordinateur virtuel avec un disque dur virtuel vide**, puis sur **Suivant**.
3. Dans la page **Spécifier l'identité de l'ordinateur virtuel**, dans le champ **Nom de l'ordinateur virtuel**, tapez **TOR-CRM1**, puis cliquez sur **Suivant**.
4. Dans la page **Configurer le matériel**, cliquez sur **Carte réseau 1**, puis sous **Connectivité**, cliquez sur **Connecté à un réseau d'ordinateurs virtuels**. Cliquez sur **Parcourir**, puis sélectionnez **Réseau d'ordinateurs virtuels Applications de Toronto**, puis cliquez sur **OK**. Sous la section **Profil de port**, cliquez dans la zone de liste déroulante **Classification**. Il s'agit de l'emplacement où vous pouvez attribuer les profils de carte virtuelle de port natif. Sélectionnez **Bande passante élevée** et cliquez sur **Suivant**.
5. Dans la page **Sélectionner la destination**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner l'ordinateur hôte**, dans la section Détails, cliquez sur **Explication de l'évaluation**, vous devriez voir le message indiquant que : **Cette destination répond à toutes les conditions requises de cet ordinateur virtuel**, puis cliquez sur **Suivant**.
7. Dans la page **Configurer les paramètres**, conservez les paramètres par défaut, puis cliquez sur **Suivant**. Dans la page **Ajouter des propriétés**, cliquez sur **Suivant**, puis dans la page **Résumé**, cliquez sur **Créer**.
8. Fermez la fenêtre Travaux.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vérification de l'ordinateur virtuel

1. Depuis l'espace de travail Ordinateurs virtuels et services, vérifiez les propriétés de réseau de TOR-CRM1, puis confirmez qu'une adresse IP lui a été attribuée et qu'il fait partie du réseau d'ordinateurs virtuels adéquat.

▶ Pour préparer le module suivant

- N'éteignez pas les ordinateurs virtuels, car vous en aurez besoin pour le module suivant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

La bande passante de stockage et de réseau est cruciale pour la planification. Recherchez toujours les goulots d'étranglement et calculez la quantité de données qui effectuera le transfert point à point. Par exemple, si vous hébergez 500 serveurs sur un réseau SAN et planifiez une analyse antivirus, quel sera l'impact ?

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Les ordinateurs virtuels sont tous suspendus.	
Problèmes de connectivité iSCSI aléatoires.	
Les migrations dynamiques échouent, la connectivité est mauvaise sur les ordinateurs virtuels.	

Questions de contrôle des acquis

Question : Quel avantage présente les commutateurs logiques ?

Problèmes réels et scénarios

Après la création des différents réseaux logiques et réseaux d'ordinateurs virtuels, vous ne pourrez pas supprimer un objet VMM à cause d'une erreur liée à une dépendance sur un modèle provisoire. Le cas échéant, vous pourrez supprimer le modèle à l'aide de Windows PowerShell.

Dans la console VMM, dans le ruban, cliquez sur **Windows PowerShell**, puis à l'invite de commandes, tapez la commande suivante, puis appuyez sur Entrée :

Get-SCVMTemplate | where {$_.Name -like "Temporary*"}

Examinez la sortie, puis vérifiez que le seul élément répertorié est le modèle provisoire douteux, et que vous ne disposez pas des modèles valides dont le nom contient la mention « temporaire ».

Supprimez le modèle problématique en tapant la commande suivante à l'invite de commandes, puis en l'appuyant sur Entrée :

Get-SCVMTemplate | where {$_.Name -like "Temporary*"} | Remove-SCVMTemplate

Cette opération devrait supprimer le modèle dépendant, ce qui vous permettra de supprimer des objets, tels qu'un réseau d'ordinateurs virtuels.

Outils

Microsoft Assessment and Planning Toolkit (MAP)
http://go.microsoft.com/fwlink/?LinkID=285277.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4

Planification et déploiement d'ordinateurs virtuels

Table des matières :

Vue d'ensemble du module **4-1**

Leçon 1 : Planification de la configuration des ordinateurs virtuels **4-2**

Leçon 2 : Préparation aux déploiements d'ordinateurs virtuels avec VMM **4-18**

Leçon 3 : Déploiement d'ordinateurs virtuels **4-31**

Atelier pratique : Planification et implémentation d'une stratégie de déploiement et de gestion d'ordinateurs virtuels **4-42**

Contrôle des acquis et éléments à retenir **4-57**

Vue d'ensemble du module

Pour planifier et déployer des ordinateurs virtuels, vous devez analyser les charges de travail existantes, identifier les ressources et la configuration requise pour les applications, puis configurer les ordinateurs virtuels appropriés pour le déploiement sur les meilleurs hôtes disponibles. Dans ce module, vous allez apprendre à configurer des ordinateurs virtuels, des profils réutilisables et des modèles aidant au déploiement. Vous allez également examiner les charges de travail spécifiques des applications et découvrir les options relatives aux migrations d'ordinateurs physiques et virtuels.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- planifier des configurations d'ordinateurs virtuels ;
- planifier et configurer les profils et les modèles Microsoft® System Center 2012 - Virtual Machine Manager (VMM) pour implémenter un déploiement VMM ;
- planifier et implémenter un déploiement d'ordinateur virtuel dans VMM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification de la configuration des ordinateurs virtuels

La première étape de l'implémentation de la virtualisation de serveur consiste à évaluer l'environnement de serveur actuel de votre organisation et à déterminer les composants à virtualiser. Vous pouvez utiliser la virtualisation pour répondre aux nombreux problèmes de la plupart des organisations. Cependant, tirer le plus grand profit de la virtualisation implique une soigneuse planification. Cette leçon offre une vue d'ensemble du processus et des outils disponibles pour évaluer et planifier la virtualisation dans une organisation.

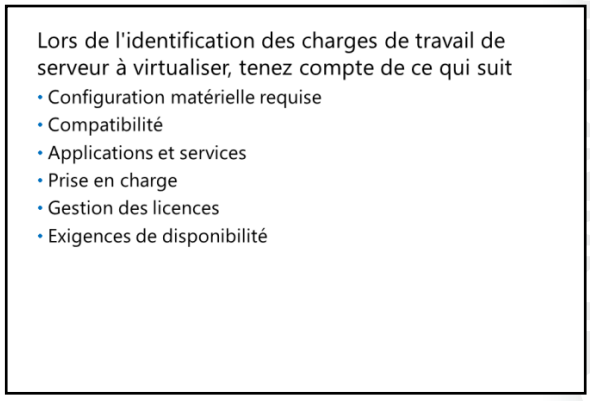
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- présenter les éléments à prendre en compte à la virtualisation de rôles serveur ;
- sélectionner les accélérateurs de solutions appropriés pour vous aider à déterminer les charges de travail de serveur à virtualiser ;
- décrire les composants d'un ordinateur virtuel ;
- décrire les éléments à prendre en compte pour planifier la configuration des ordinateurs virtuels ;
- planifier la virtualisation Microsoft SQL Server® ;
- planifier la virtualisation Microsoft Exchange Server ;
- planifier la virtualisation Microsoft SharePoint® Server ;
- planifier la virtualisation de services de domaine (AD DS) Microsoft Active Directory®.

Éléments à prendre en compte pour la virtualisation des rôles serveur

La virtualisation est une technologie reconnue que bon nombre d'organisations ont adoptée. Les entreprises développent souvent une stratégie d'implémentation de serveur qui vise à virtualiser tous les nouveaux systèmes et ceux remplacés. C'est seulement lorsqu'il existe une raison valable de ne pas virtualiser qu'elles songent à la nécessité de déployer un matériel physique comme alternative. Cela marque une évolution de l'informatique de serveur. Avec des fonctionnalités d'hyperviseur qui se sont améliorées, la virtualisation de charges de travail d'ordinateur plus volumineuses et plus consommatrices de ressources est devenue une pratique acceptée.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez désormais utiliser Windows Server® 2012 pour déployer des serveurs avec jusqu'à 320 processeurs logiques et 4 To de mémoire système. Cela permet également d'offrir de nouvelles fonctions pour les charges de travail virtuelles et constitue une amélioration importante sur les hyperviseurs antérieurs.

Le tableau suivant fournit une vue d'ensemble de l'évolution des fonctions d'ordinateur virtuel Windows Server 2012 Hyper-V®. Il vous aidera à comprendre et prendre en compte la virtualisation de charges de travail plus intensives.

	Date de version	Mémoire vive (RAM)	Nombre de processeurs (virtuels)	Stockage (par lecteur)
Microsoft Virtual Server 2005 R2 Service Pack 1 (SP1)	2007	3,6 gigaoctets (Go)	1	127 Go
Hyper-V dans Windows 2008	2008	64 Go	4	2 000 Go
Hyper-V dans Windows 2008 R2 SP1	2009	64 Go	4	2 000 Go
Hyper-V dans Windows 2012	2012	1 téraoctet	64	64 téraoctets

Les ressources et les performances ne sont pas les seuls éléments à prendre en compte lors de l'implémentation d'une solution de virtualisation de serveur, c'est pourquoi il est important d'examiner tous les aspects de la configuration requise d'une application avant de déterminer si vous pouvez l'héberger virtuellement.

Choix des rôles serveur à virtualiser

Vous devez prendre en compte certains facteurs lorsque vous choisissez de virtualiser des charges de travail de serveurs :

- Configuration matérielle requise. En général, les ordinateurs virtuels requièrent approximativement les mêmes ressources qu'un serveur physique. Par exemple, si un serveur physique utilise actuellement 1 Go de mémoire RAM, vous devez alors vous attendre à ce que l'ordinateur virtuel utilise la même quantité de RAM, en supposant qu'il exécute le même système d'exploitation et les mêmes applications que le serveur physique. Si un seul ordinateur virtuel consomme davantage que la moitié de la charge de travail de l'hôte, vous devez déterminer si la virtualisation est appropriée ou si le dimensionnement de l'hôte est adapté.
- Compatibilité. Vous devez également déterminer si l'application peut être exécutée dans un environnement de virtualisation. Les applications d'entreprise vont des programmes les plus simples aux applications multiniveaux distribuées les plus complexes. Vous devez prendre en compte les besoins des applications distribuées en termes de composants spécifiques. Il s'agit notamment de besoins spécifiques pour communiquer avec d'autres composants de l'infrastructure ou pour accéder directement au matériel du système. Vous pouvez facilement virtualiser certains serveurs. Toutefois, il se peut que certains composants doivent continuer d'être exécutés sur du matériel dédié.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Applications et services. Les applications et services qui présentent des exigences matérielles ou de pilotes spécifiques ne conviennent généralement pas à la virtualisation. Une application peut ne pas être adaptée à la virtualisation d'applications si elle contient des pilotes bas de gamme qui requièrent l'accès direct au matériel système. Cela peut s'avérer impossible via une interface de virtualisation ou affecter les performances.
- Prise en charge. Vous devez déterminer si un environnement virtualisé prendra en charge votre système d'exploitation et les applications requises. Vérifiez les règles de prise en charge de fournisseur pour le déploiement du système d'exploitation et de l'application à l'aide de technologies de virtualisation.
- Gestion des licences. Vous devez également évaluer si vous pouvez attribuer une licence d'utilisation à l'application dans un environnement virtuel. Les coûts réduits liés aux licences de plusieurs applications ou systèmes d'exploitation peuvent finalement s'ajouter et être un réel facteur de changement en faveur de la virtualisation.
- Exigences de disponibilité. La plupart des organisations disposent de certaines applications qui doivent être quasiment toujours disponibles pour les utilisateurs. Certaines applications fournissent des options intégrées permettant une haute disponibilité, d'autres en revanche ne peuvent pas facilement devenir hautement disponibles en dehors d'un environnement d'ordinateur virtuel. Lorsque vous envisagez de virtualiser ou non un serveur, évaluez si l'application a des options de haute disponibilité, si un environnement d'ordinateur virtuel les prend en charge, et si vous pouvez utiliser le clustering avec basculement pour rendre l'ordinateur virtuel hautement disponible.

Le but de la plupart des organisations est d'utiliser tous les serveurs de façon appropriée, qu'ils soient physiques ou virtuels. Vous pouvez utiliser entièrement certains rôles serveur, comme les serveurs SQL Server ou Exchange Server Mailbox, en déployant des instances SQL Server supplémentaires ou en déplaçant davantage de boîtes aux lettres sur le serveur. Dans certains cas, vous pouvez virtualiser les charges de travail du serveur dans un scénario, mais pas dans un autre. Par exemple, dans un très grand domaine, avec des milliers d'utilisateurs qui se connectent en même temps, il peut ne pas s'avérer pratique de virtualiser un contrôleur de domaine. Cependant, pour un domaine plus restreint ou le déploiement d'une filiale, la virtualisation des contrôleurs de domaine peut être la meilleure solution.

Utilisation des accélérateurs de solutions Microsoft

Pour aider les organisations à développer et fournir une stratégie de virtualisation, Microsoft a mis en place des accélérateurs de solutions gratuits qui permettent d'accélérer l'évaluation, la planification et le déploiement de ses technologies, telles que Windows Server 2012 et la virtualisation.

Les accélérateurs de solutions de la virtualisation Microsoft offrent des orientations et des outils pour vous aider à concevoir et implémenter la virtualisation. Ils incluent
- MAP
- Guides de planification d'infrastructure et de conception
- Virtual Machine Servicing Tool 2012

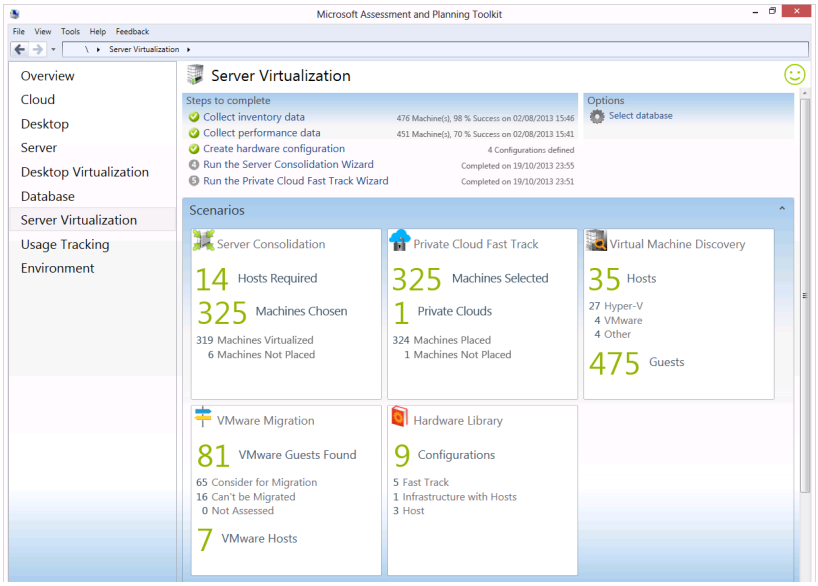
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les accélérateurs de solutions de la virtualisation Microsoft suivants sont disponibles :

- Microsoft Assessment and Planning (MAP) Toolkit.

  Boîte à outils MAP, tableau de bord de virtualisation de serveur



- Vous pouvez utiliser MAP pour évaluer si tout est prêt pour le déploiement sur l'ensemble du réseau, en particulier si vous pouvez migrer vers un environnement virtuel les technologies Microsoft telles que les serveurs, les bureaux et les applications. Grâce à MAP, vous pouvez désormais déterminer quels serveurs vous pouvez mettre à niveau vers Windows Server 2012, quels serveurs vous pouvez migrer vers des ordinateurs virtuels sur Hyper-V dans Windows Server 2008, et quels ordinateurs clients vous pouvez mettre à niveau vers Windows® 7. MAP est l'un des accélérateurs de solutions de virtualisation. Il est le principal outil permettant d'identifier les applications, les bureaux et les serveurs les mieux adaptés à la virtualisation.

  La boîte à outils MAP effectue les fonctions clés suivantes :

  - Inventaire matériel. MAP utilise un processus fiable qui n'utilise pas d'agent pour recueillir et organiser les ressources système et les informations de périphériques à travers votre réseau depuis un ordinateur en réseau unique. L'outil MAP renvoie entre autres des informations liées au système d'exploitation, à la mémoire système ainsi qu'aux pilotes et applications installés. MAP enregistre ces informations dans une base de données locale, puis les utilise pour vous fournir des rapports et des recommandations spécifiques. MAP utilise des technologies déjà disponibles dans votre environnement informatique pour réaliser un inventaire et des évaluations. Ces technologies incluent WMI (Windows Management Instrumentation), le Service d'accès à distance au Registre, le protocole SNMP (Simple Network Management Protocol), AD DS et le service Explorateur d'ordinateurs.

Vous pouvez utiliser MAP pour dresser l'inventaire des systèmes d'exploitation suivants :

- Windows 8
- Windows 7
- Windows Vista®
- Windows XP Professionnel
- Microsoft Office 2010 et versions précédentes
- Windows Server 2012
- Windows Server 2008 ou Windows Server 2008 R2
- Windows Server 2003 ou Windows Server 2003 R2
- Windows 2000 Professionnel ou Windows 2000 Server
- Windows Internet Explorer® 9 et versions précédentes
- Hyper-V
- Microsoft Lync®
- System Center Configuration Manager
- Microsoft Forefront® Endpoint Protection
- SQL Server
- VMware vSphere
- VMware vCenter
- VMware ESX
- VMware ESXi
- Serveur VMware
- Distributions Linux sélectionnées
- Découverte de la pile d'applications LAMP
- MySQL
- Oracle
- Sybase

o Analyse des données. MAP réalise une analyse détaillée de la compatibilité entre le matériel et le périphérique pour la migration vers Windows 8, Windows 7, Windows Server 2012, Windows Server 2008 R2, SQL Server 2012, SQL Server 2008 R2, Microsoft Office 2010 et Office 365™. L'outil aide à rassembler des mesures de performances et à générer des recommandations de consolidation de serveurs qui identifient les serveurs les mieux adaptés à la consolidation de serveurs. Il vous aide également à placer les serveurs physiques dans un environnement virtualisé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

  - Rapport de préparation. MAP génère des rapports contenant des résultats récapitulatifs et détaillés de l'évaluation de chaque scénario de migration et fournit ces résultats dans des documents Microsoft Excel® et Microsoft Word. Les rapports de préparation sont disponibles pour de nombreuses technologies, y compris Windows 8 et Windows Server 2012.

    MAP aide également à rassembler des mesures de performances et à générer des recommandations de consolidation de serveurs qui identifient les serveurs les mieux adaptés à la virtualisation de serveurs. Il vous aide également à placer les serveurs physiques dans un environnement virtualisé.

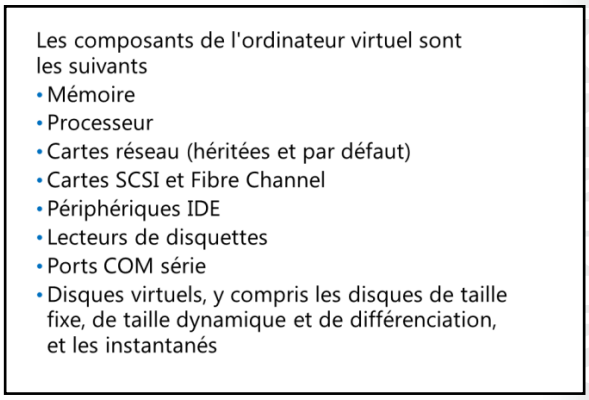
    La dernière version permet de planifier la migration vers le nouvel Office 2013, la migration vers la dernière version de Windows Server et des systèmes d'exploitation clients, ainsi que la migration de charges de travail plus volumineuses vers Windows Azure™.

- Guides de planification d'infrastructure et de conception. Les manuels gratuits Infrastructure Planning and Design (IPD) décrivent les éléments d'architecture à prendre en compte et rationalisent les processus de conception pour la planification de technologies d'infrastructure Microsoft. Chaque guide couvre un scénario ou une technologie d'infrastructure unique, telle que la virtualisation de serveur, la virtualisation des applications et l'implémentation des services de terminal. Le guide Windows Server Virtualization fournit des conseils pour planifier et implémenter la virtualisation de serveur sur Hyper-V.
- Guide de sécurité Hyper-V. L'implémentation de la virtualisation peut augmenter le nombre de problèmes de sécurité à prendre en compte car vous devez sécuriser à la fois l'ordinateur hôte et les ordinateurs virtuels. Le guide de sécurité de Hyper-V fournit des instructions et des recommandations pour répondre à des questions de sécurité principales concernant la virtualisation de serveur.
- Virtual Machine Servicing Tool 2012. Vous devez réfléchir à la façon dont vous allez vous assurer que des mises à jour sont exécutées sur les ordinateurs virtuels que vous démarrez seulement de temps en temps ou que vous stockez dans la bibliothèque Virtual Machine Manager. Virtual Machine Servicing Tool 2012 fournit des conseils et des outils automatisés pour maintenir ces ordinateurs virtuels à jour. Associé à Windows Server Update Services (WSUS) ou à System Center 2012 Configuration Manager, l'outil de maintenance peuvent fournir les informations suivantes :
- Maintenance des ordinateurs virtuels hors connexion dans la bibliothèque Virtual Machine Manager.
- Maintenance des ordinateurs virtuels arrêtes sur un hôte.
- Maintenance des modèles d'ordinateurs virtuels.
- Maintenance des disques durs virtuels hors connexion dans une bibliothèque Virtual Machine Manager.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Composants d'ordinateur virtuel

Lorsque vous créez un ordinateur virtuel, vous pouvez le personnaliser en définissant ses paramètres. Vous pouvez configurer les composants logiques suivants :



- Processeur. Vous pouvez configurer de un à 64 processeurs virtuels pour un ordinateur virtuel. Le nombre de processeurs ne peut pas dépasser le nombre de cœurs de processeur que vous installez sur le serveur hôte.
- Mémoire. Allouez suffisamment de mémoire pour l'ordinateur virtuel et pour les rôles qui seront hébergés par l'ordinateur virtuel. Vous pouvez attribuer entre 8 mégaoctets (Mo) et 1 téraoctet de mémoire. La limite supérieure ne peut pas dépasser la quantité de mémoire installée sur le serveur hôte.
    - Vous pouvez choisir entre la mémoire statique et la mémoire dynamique. La mémoire dynamique vous permet d'attribuer une valeur à la quantité de mémoire pour le démarrage, y compris une valeur minimum et un maximum, et de choisir un pourcentage pour la mise en mémoire tampon.
- Lecteur de disquette. Vous pouvez attribuer uniquement un lecteur de disquette virtuel pour monter les fichiers de disquette virtuels qui sont stockés dans la bibliothèque Virtual Machine Manager.
- Ports de communication (COM). Permet d'attribuer jusqu'à deux ports COM virtuels. Vous configurez les ports COM virtuels pour communiquer avec l'ordinateur physique local ou distant via des canaux nommés.
- Carte vidéo Microsoft RemoteFX®3D. Permet d'utiliser des ressources sur une carte vidéo physique de support sur l'hôte. Vous pouvez attribuer jusqu'à quatre écrans et utiliser des résolutions allant jusqu'à 1920x1200.
- Périphériques IDE. Permet d'utiliser jusqu'à quatre périphériques d'environnement de développement intégré (IDE) virtuels. Vous pouvez utiliser ces périphériques pour les lecteurs de CD ou DVD virtuels pour lesquels vous utilisez des images .iso que vous stockez dans la bibliothèque Virtual Machine Manager, puis que vous copiez sur l'hôte local à partir de la bibliothèque. Vous pouvez également utiliser ces périphériques pour les disques durs virtuels. Tous les ordinateurs virtuels qui démarrent à partir d'un disque localement attribué doivent avoir la partition de démarrage des systèmes d'exploitation qu'ils prennent en charge sur un lecteur IDE.
- Cartes réseau. Vous pouvez utiliser deux types de carte pour la mise en réseau virtuelle d'invités. La première carte réseau (celle par défaut) fournit une mise en réseau haute performance et requiert l'installation de services d'intégration sur l'ordinateur virtuel. Un ordinateur virtuel peut avoir jusqu'à huit cartes réseau par défaut. L'autre carte est la carte réseau héritée, qui émule un type de carte matérielle spécifique et prend en charge l'environnement PXE (Pre-Boot Execution Environment) pour exécuter l'installation réseau d'un système d'exploitation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Cartes SCSI. Vous pouvez attacher jusqu'à quatre cartes SCSI (Small Computer System Interface), et chaque carte peut prendre en charge jusqu'à 64 disques virtuels, ce qui signifie que vous pouvez avoir jusqu'à 256 disques virtuels. Vous devez installer les services d'intégration pour utiliser les cartes SCSI virtuelles.
- Carte Fibre Channel. Vous pouvez utiliser une carte Fibre Channel pour accéder au stockage Fibre Channel directement à partir du système d'exploitation invité.
- Disques virtuels. Le rôle de l'ordinateur virtuel détermine le type de disque virtuel que vous choisissez d'utiliser. Un disque virtuel est portable. Vous pouvez le déplacer vers un autre disque physique, un autre ordinateur ou même un réseau SAN (Storage Area Network). Vous pouvez également monter des disques virtuels sous Windows, puis modifier leur contenu. Hyper-V prend en charge les types de disque virtuel suivants :
    - Disques de différenciation. Vous pouvez utiliser la différenciation dans une relation parent-enfant avec un autre disque. Les modifications apportées au disque enfant ne sont pas inscrites sur le disque parent. La différenciation conduit à un développement plus rapide d'ordinateurs virtuels.

 **Remarque :** Bien que vous puissiez utiliser VMM pour gérer les ordinateurs virtuels, vous ne pouvez pas créer de disques de différenciation dans VMM.

    - Disques de taille dynamique. Ces types de disque sont utiles pour développer de nouveaux ordinateurs virtuels.
    - Disques fixes. Ces disques fournissent de meilleures performances que les disques de taille dynamique. Un disque fixe dispose uniquement de l'espace disque dur que vous spécifiez lors de sa création. Si vous avez besoin de davantage d'espace, vous devez développer le disque, joindre un autre disque dur virtuel ou utiliser un disque direct.
    - Disque dur virtuel automatique (.avhd). Le fait d'effectuer une capture instantanée d'un ordinateur virtuel crée automatiquement un disque de différenciation .avhd.

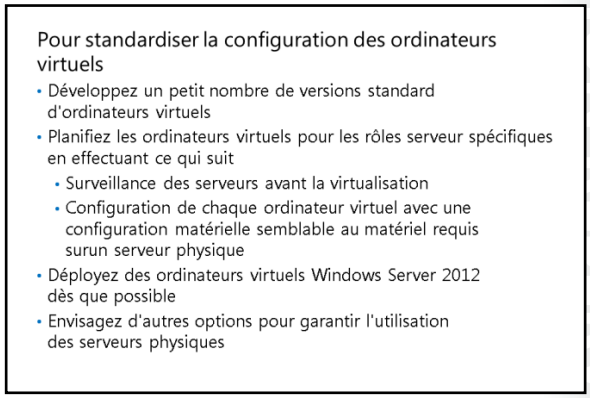
Lorsque vous créez un ordinateur virtuel, vous disposez de plusieurs options pour créer ou attacher un disque dur virtuel. Vos choix dépendent des différents scénarios, comme le décrit la liste suivante :

- Créer un VHD. Il s'agit de l'option par défaut dans l'Assistant Nouvel ordinateur virtuel. Vous spécifiez l'emplacement dans lequel vous voulez créer et installer le disque dur virtuel et le fichier de configuration, ou c'est VMM Manager qui les créera et les stockera dans l'emplacement par défaut.
- Utiliser un disque dur virtuel existant. Vous avez peut-être créé un disque dur virtuel à l'aide de l'Assistant Nouveau disque dur virtuel, ou vous utilisez peut-être le même disque dur à partir d'un autre ordinateur virtuel.
- Attacher un disque dur virtuel ultérieurement. Vous créez l'ordinateur virtuel, mais vous attachez un disque dur virtuel ultérieurement, éventuellement après l'utilisation de l'Assistant Nouveau disque dur virtuel.
- Instantanés d'ordinateurs virtuels. Lorsque vous créez une capture instantanée d'un ordinateur virtuel, VMM l'enregistre dans un sous-dossier du dossier où vous avez créé l'ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification de la configuration des ordinateurs virtuels

Un objectif important lors du développement d'une stratégie de virtualisation est de simplifier et de standardiser l'ordinateur hôte et la configuration d'ordinateur virtuel autant que possible. Tenez compte des instructions générales suivantes qui s'appliquent à tous les ordinateurs virtuels :



- Développez un petit nombre de versions standard d'ordinateurs virtuels. Pour simplifier le déploiement et la gestion des ordinateurs virtuels, développez un ensemble de versions standard d'ordinateurs virtuels. Par exemple, envisagez de créer une version de serveur bas de gamme standard, une version de serveur intermédiaire et une version de serveur haut de gamme, puis attribuez une unité centrale (CPU) standard et une configuration de mémoire pour chaque rôle. Vous devez également configurer chacun des ordinateurs virtuels avec une partition système standard de 50 Go, et fournir des disques supplémentaires pour stocker les données ou installer des applications. Vous pouvez envisager d'utiliser des contrôleurs SCSI pour tous les disques durs autres que ceux contenant la partition de démarrage et la partition système. Avec Windows Server 2012, vous pouvez ajouter de nouveaux disques durs virtuels connectés à un contrôleur SCSI sans redémarrer le serveur.
- Planifiez les ordinateurs virtuels pour les rôles serveur spécifiques. Vous devez pouvoir utiliser la même configuration de base du disque et du système d'exploitation pour configurer la plupart des ordinateurs virtuels, mais les conditions requises physiques réelles pour chaque ordinateur virtuel varient. Par exemple, certains ordinateurs virtuels auront besoin de beaucoup plus de mémoire RAM ou de ressources processeur que d'autres. Pour concevoir la configuration physique requise pour un ordinateur virtuel, prenez en compte les éléments suivants :
    - Surveillez les serveurs avant de les virtualiser. Collectez des données de performances sur les serveurs afin d'évaluer les performances d'applications spécifiques sur les serveurs physiques. Si une application utilise un pourcentage très inférieur de ressources matérielles sur un serveur physique, déployez un serveur virtuel ayant beaucoup moins de capacité d'exécuter la même application.
    - Configurez chaque serveur virtuel avec une configuration matérielle semblable au matériel requis pour l'application sur les serveurs physiques. Le fait que vous virtualisiez un serveur ne modifie pas les ressources matérielles dont le serveur a besoin.

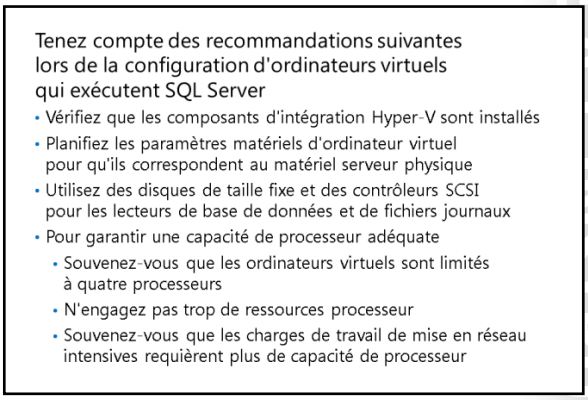
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Déployez des ordinateurs virtuels Windows Server 2012 dès que possible. Utilisez la mémoire dynamique, et recherchez et examinez toutes les instructions de support concernant la virtualisation et la mémoire dynamique pour toute application que vous hébergerez sur votre ordinateur virtuel.
- Envisagez d'autres options pour garantir l'utilisation des serveurs physiques. Un des objectifs de la virtualisation de serveur est de vérifier que vous utilisez tous les serveurs, physiques ou virtuels, de façon appropriée. Vous pouvez utiliser entièrement certains rôles serveur, comme les serveurs SQL Server ou Exchange Server Mailbox, en déployant des instances SQL Server supplémentaires ou en déplaçant davantage de boîtes aux lettres sur le serveur.

Lorsque vous réfléchissez à la virtualisation, examinez les applications et servez-vous de l'affinité et de l'anti-affinité. L'*affinité* est le processus consistant à regrouper certains ordinateurs virtuels sur un seul hôte, alors que l'*anti-affinité* empêche certains ordinateurs d'être déployés ou de résider sur les mêmes nœuds de cluster.

Planification d'ordinateurs virtuels pour SQL Server

L'une des charges de travail du serveur que les entreprises virtualisent est SQL Server. Cela s'avère particulièrement pratique dans les environnements de développement, de test et de formation qui requièrent des serveurs SQL et dans lesquels vous exécutez souvent des nouvelles installations. Si vous planifiez le déploiement de nouveaux serveurs SQL ou envisagez un projet de consolidation SQL, vous devez songer à la virtualisation, qui fournira une utilisation maximale de votre matériel.



Tenez compte des recommandations suivantes lors de la configuration d'ordinateurs virtuels qui exécutent SQL Server :

- Veillez à installer les composants d'intégration Hyper-V sur l'ordinateur virtuel invité. En outre, utilisez des cartes réseau standard plutôt que des cartes réseau héritées lors de la configuration du réseau pour l'ordinateur virtuel. Ces deux options optimisent les performances des ordinateurs virtuels.
- Envisagez de configurer les paramètres matériels afin que les ordinateurs virtuels correspondent aux paramètres matériels que vous configureriez sur un serveur physique pour la même charge de travail.
- Planifiez le stockage de l'ordinateur virtuel. Un des composants les plus importants pour garantir des performances optimales pour chaque instance SQL Server consiste à vérifier que le système de stockage a une taille et une configuration appropriées. Le matériel de stockage doit fournir suffisamment de débit d'E/S et une capacité de stockage adéquate pour répondre aux besoins actuels et futurs des ordinateurs virtuels planifiés. Vous pouvez maintenant utiliser un disque .vhdx pour gérer des lecteurs d'une taille allant jusqu'à 64 téraoctets, ou utiliser Fibre Channel directement dans l'ordinateur virtuel. Introduit dans Windows Server 2012, le format de fichier .vhdx fournit une capacité de stockage beaucoup plus importante que le format .vhd existant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Suivez les meilleures pratiques pour configurer les disques pour les journaux de transactions et le stockage de base de données. Bien que les disques directs fournissent les meilleures performances pour SQL Server, le manque de portabilité peut rendre le déploiement plus compliqué. Les disques de taille fixe fournissent presque les mêmes performances et sont généralement la meilleure option de disque pour SQL Server.
- Les ordinateurs virtuels Hyper-V doivent utiliser un contrôleur IDE pour le démarrage et les partitions système mais vous devez utiliser les contrôleurs SCSI synthétiques pour les disques contenant des bases de données SQL Server et des journaux.
- Fournissez la capacité adéquate de processeur. Un deuxième composant essentiel de la planification des performances de SQL Server est la capacité du processeur. Lorsque vous concevez un hôte de virtualisation qui doit s'exécuter sur plusieurs ordinateurs virtuels SQL Server, vous devez vérifier que les ressources de processeur physiques cumulées de l'hôte sont suffisantes pour répondre aux besoins de tous les ordinateurs virtuels invités. Comme lorsque vous déployez plusieurs instances SQL Server sur un serveur physique, le seul moyen de garantir des performances adéquates consiste à tester complètement le déploiement. Lors de l'exécution de SQL Server sur un ordinateur virtuel, vous devez tenir compte des limitations relatives au processeur :
    - En utilisant Hyper-V, vous pouvez attribuer jusqu'à 64 cœurs de processeur à un ordinateur virtuel. Si vous utilisez des hôtes de virtualisation de grande taille, vous ne devez pas solliciter les ressources processeur de façon excessive. Cela peut se produire lorsque le nombre total de cœurs de processeur logiques que vous configurez sur tous les ordinateurs virtuels invités est supérieur au nombre réel de cœurs de processeur physiques disponibles sur le serveur. La sollicitation excessive des cœurs de processeur peut affecter considérablement les performances du serveur lorsque tous les ordinateurs virtuels sont utilisés de façon intensive.
    - Les charges de travail élevées de mise en réseau entraîneront une surcharge du processeur plus importante et un plus grand impact sur les performances d'un ordinateur virtuel. Pendant la planification, pensez à utiliser l'association de cartes réseau d'invité, la virtualisation d'E/S SR-IOV et la file d'attente d'ordinateurs virtuels si ces fonctionnalités sont prises en charge.
- Les versions de SQL Server qui prennent en charge l'ajout de mémoire à chaud prennent également en charge la mémoire dynamique. Toutefois, lorsque les versions antérieures de SQL Server sont prises en charge, elles voient uniquement la mémoire de démarrage attribuée.



Liens de référence :

- Pour plus d'informations sur l'exécution de SQL Server avec la mémoire dynamique Hyper-V (SQL Server 2008 R2), accédez à http://go.microsoft.com/fwlink/?LinkID=285284.
- Pour plus d'informations sur la stratégie de prise en charge des produits Microsoft SQL Server exécutés dans un environnement de virtualisation de matériel, accédez à http://go.microsoft.com/fwlink/?LinkID=285286.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification d'ordinateurs virtuels pour Exchange Server

Vous pouvez utiliser un environnement de virtualisation pour exécuter tous les rôles serveur Exchange Server 2007, Exchange Server 2010 et Exchange Server 2013, à l'exception du rôle de messagerie unifiée, qui est pris en charge à partir d'Exchange Server 2010 SP1. Les ordinateurs virtuels ne prennent pas en charge le rôle serveur de messagerie unifiée en raison de la nécessité de réponses en temps réel associée aux communications vocales.

Lors de la conception d'ordinateurs virtuels pour Exchange Server
- Utilisez des règles de calibrage de serveur standard
- Configurez le stockage approprié
- N'utilisez pas d'instantanés d'ordinateurs virtuels
- Configurez des ressources processeur adéquates
- Réfléchissez à la façon d'utiliser Hyper-V et la haute disponibilité native d'Exchange Server
- Tenez compte des besoins d'E/S

Tenez compte des instructions suivantes lors de la virtualisation de serveurs Exchange :

- Utiliser un calibrage de serveur standard. L'exécution d'Exchange Server 2007 et d'Exchange Server 2010 sur un ordinateur virtuel invité ne modifie pas les exigences de conception d'Exchange Server du point de vue de l'application. L'ordinateur virtuel invité Exchange Server doit toujours avoir la taille appropriée pour la gestion de la charge de travail.
- Configurer le stockage approprié. Le stockage utilisé par l'ordinateur virtuel Exchange Server peut être des lecteurs de disque dur virtuel, du stockage direct SCSI ou du stockage iSCSI (Internet SCSI). À l'instar des serveurs SQL Server, le stockage physique fournit les meilleures performances, toutefois il ne prend pas en charge les disques virtuels de taille dynamique ou les lecteurs de différenciation.

  Vous devez utiliser des numéros d'unités logiques distincts sur les baies RAID (Redundant Array of Independent Disks) pour le système d'exploitation hôte, chaque disque du système d'exploitation invité et l'ensemble des supports de stockage de l'ordinateur virtuel. De même qu'avec les serveurs physiques, il est préférable de créer des numéros d'unité logique distincts pour chaque base de données et ensemble de fichiers journaux de transactions.
- N'utilisez pas d'instantanés d'ordinateurs virtuels. Les instantanés d'ordinateurs virtuels ne tiennent pas compte des applications et leur utilisation peut avoir des conséquences inattendues pour les applications serveur contenant des données d'état (Exchange Server, par exemple). Par conséquent, les ordinateurs virtuels Exchange Server ne prennent pas en charge les instantanés.
- Configurer des ressources processeur adéquates. Exchange Server prend en charge un rapport de processeurs virtuels/processeurs logiques de deux sur un maximum. Par exemple, un système biprocesseur qui utilise des processeurs quadruple cœur contient huit processeurs logiques dans le système hôte. Sur un système avec cette configuration, n'allouez pas plus de seize processeurs virtuels à l'ensemble des ordinateurs virtuels invités. Si vous utilisez beaucoup les processeurs pour toutes les instances de l'ordinateur virtuel, une sollicitation excessive affectera considérablement les performances. Dans ces scénarios, n'attribuez pas aux ordinateurs virtuels un nombre de processeurs virtuels supérieur au nombre de cœurs de processeur sur l'ordinateur hôte.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Haute disponibilité pour serveurs Exchange. Exchange Server 2007 et Exchange Server 2010 fournissent plusieurs options de haute disponibilité. Pour les rôles serveur tels que les serveurs d'accès au client, les rôles serveur de transport Hub et les rôles serveur de transport Edge, vous pouvez déployer plusieurs serveurs pour chaque rôle afin de vérifier que le rôle serveur est disponible si une seule défaillance du serveur se produit. Pour les serveurs de boîtes aux lettres, Exchange Server 2007 fournit plusieurs solutions de clustering d'échange telles que la réplication continue en cluster (CCR) et les clusters à copie unique (SCCs). Exchange Server 2010 fournit des groupes de disponibilité de la base de données (DAG). Ces solutions fournissent différentes options pour le basculement automatique en cas de défaillance de serveur.

  Avec Hyper-V, vous pouvez rendre les ordinateurs virtuels hautement disponibles en les déployant dans un cluster de basculement. Vous pouvez utiliser le clustering avec basculement pour rendre hautement disponibles les ordinateurs virtuels qui exécutent le serveur d'accès au client, le rôle serveur de transport Hub et le rôle serveur de transport Edge.

  Vous ne pouvez pas associer les options de haute disponibilité du serveur de boîte aux lettres Exchange Server au clustering avec basculement. Par exemple, vous pouvez déployer un serveur de boîtes aux lettres sur un ordinateur virtuel, puis configurer les ordinateurs virtuels pour utiliser la réplication continue en cluster (CCR) ou les groupes de disponibilité de la base de données (DAG). Toutefois, vous ne pouvez pas configurer les ordinateurs virtuels en tant qu'ordinateurs virtuels hautement disponibles dans un cluster de basculement.

  Cela signifie que vous devez choisir entre le clustering avec basculement Hyper-V et l'une des options de clustering de serveur de boîtes aux lettres Exchange Server lorsque vous activez la haute disponibilité pour les serveurs de boîtes aux lettres. Nous recommandons les options de clustering d'Exchange car selon l'option choisie, vous pouvez utiliser des fonctionnalités telles que des copies multiples de la base de données de boîtes aux lettres et le clustering tenant compte des applications. Cependant, le clustering avec basculement ne peut pas le détecter s'il existe un problème avec Exchange.

- Performances du serveur de boîtes aux lettres. Les goulots d'étranglement les plus courants en termes de performances pour les serveurs de boîtes aux lettres sont les E/S de disque ainsi les E/S du réseau. Lorsque vous exécutez des serveurs de boîtes aux lettres dans un environnement virtuel, les ordinateurs virtuels doivent partager cette bande passante d'E/S avec l'ordinateur hôte et d'autres serveurs de l'ordinateur virtuel que vous déployez sur le même hôte. Si un seul ordinateur virtuel est en cours d'exécution sur le serveur physique, les E/S de disque et de réseau disponibles pour l'ordinateur virtuel sont presque équivalentes à celles disponibles sur un serveur physique. Toutefois, un serveur de boîtes aux lettres très sollicité peut consommer toute la bande passante d'E/S disponible, ce qui le rend incapable d'héberger les ordinateurs virtuels supplémentaires sur ce serveur physique.

 **Remarque :** Exchange Server ne prend pas en charge la fonctionnalité de mémoire dynamique dans Hyper-V.

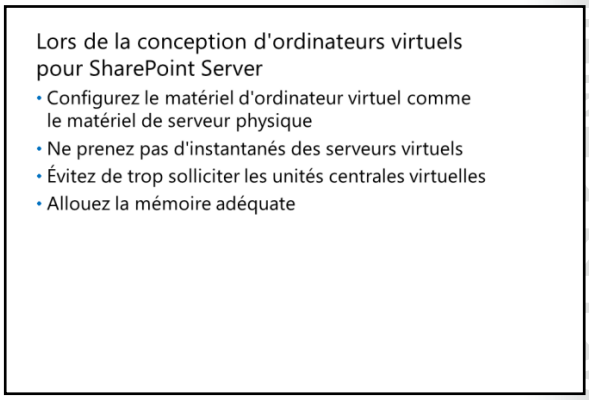
 **Liens de référence :**

- Pour plus d'informations sur la virtualisation avec Exchange Server 2010, accédez à http://go.microsoft.com/fwlink/?LinkID=285290.
- Pour plus d'informations sur la virtualisation avec Exchange Server 2013, accédez à http://technet.microsoft.com/fr-fr/library/jj619301(v=exchg.150).aspx.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification d'ordinateurs virtuels pour SharePoint Server

Une des options courantes relatives à l'utilisation des ordinateurs virtuels concerne le déploiement de Microsoft SharePoint Foundation 2010 et Microsoft SharePoint Server.



Tenez compte des recommandations suivantes pour déployer Windows SharePoint Services ou SharePoint Server sur un ordinateur virtuel :

- Veillez à configurer chaque ordinateur virtuel avec la même capacité matérielle que celle dont un serveur physique aurait besoin. En outre, tenez compte des performances supplémentaires requises sur l'ordinateur hôte pour chaque ordinateur virtuel.
- Ne prenez pas d'instantanés des serveurs virtuels qui se connectent à une batterie de serveurs SharePoint. Si vous le faites, les services de minuteur et les applications de recherche peuvent se désynchroniser pendant le processus d'instantané. Pour prendre des instantanés du serveur, commencez par détacher le serveur de la batterie de serveurs.
- Évitez de trop solliciter le nombre de processeurs virtuels. Hyper-V permet d'allouer davantage de processeurs virtuels que de processeurs physiques. Cela engendre toutefois des problèmes de performances du fait que le logiciel de l'hyperviseur doive transférer les contextes du processeur dans un fichier d'échange. Ce n'est un problème que si les ordinateurs virtuels sont utilisés de façon très intensive.
- Veillez à attribuer la quantité de mémoire adéquate à chaque ordinateur virtuel. Une mémoire inadaptée aura une plus grande influence sur les performances du serveur. La quantité de mémoire requise dépend de la charge de travail du serveur ; par conséquent, vous devez tester et optimiser la configuration de la mémoire pour chaque scénario.
- Choisissez l'implémentation de stockage appropriée. Si vous exécutez uniquement les serveurs Web frontaux ou les serveurs de requêtes sur les ordinateurs virtuels, les performances du disque ne sont pas aussi importantes qu'elles le seraient si l'image hébergeait le rôle d'index ou une base de données SQL Server. Si l'image héberge le rôle d'index, vous devez utiliser un disque dur virtuel de taille fixe ou un disque physique.
- Considérez la surveillance comme un élément de conception d'une batterie SharePoint virtualisée. System Center 2012 - Operations Manager fournit des packs d'administration, qui sont présentés dans un module ultérieur et permettent de surveiller le système d'exploitation Windows Server, Hyper-V, SQL Server, Internet Information Services (IIS), SharePoint et votre matériel de serveur. Vous pouvez créer une base de référence pour la batterie SharePoint Server à l'aide de ces packs d'administration, configurer l'alerte en cas d'erreur et surveiller les performances en cours attentivement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les centres de ressources pour SharePoint Server 2010 et SharePoint Server 2013 présentent des guides de topologie et de planification qui guident spécifiquement les administrateurs recherchant à générer les batteries de serveurs SharePoint virtualisés.

Liens de référence :

- Pour le centre de ressources SharePoint Server 2010, accédez à http://go.microsoft.com/fwlink/?LinkID=285291.
- Pour le centre de ressources SharePoint Server 2013, accédez à http://go.microsoft.com/fwlink/?LinkID=285292.

Planification d'ordinateurs virtuels pour AD DS

La virtualisation des contrôleurs de domaine AD DS n'est pas un nouveau processus, et vous devez prendre en compte certains risques. En règle générale, vous pouvez atténuer ces risques en suivant quelques recommandations de base, notamment :

Windows Server 2012 introduit une nouvelle virtualisation plus sûre des contrôleurs de domaine y compris le clonage

- N'effectuez pas de migrations P2V (physique-à-virtuel) en ligne.
- N'arrêtez pas ou ne suspendez pas les contrôleurs de domaine.
- Ne restaurez pas les instantanés des contrôleurs de domaine.
- Pensez à générer des serveurs virtuels, puis à les promouvoir au rang de contrôleurs de domaine et à rétrograder les serveurs physiques.

Avant Windows Server 2012, les contrôleurs de domaine virtualisés ne contenaient aucune technologie spécifique pour adapter la virtualisation ou en tirer parti. Windows Server 2012 introduit une prise en charge de virtualisation sans risque des contrôleurs de domaine AD DS, spécifiquement pour les plateformes de l'hyperviseur qui ont l'identificateur de génération d'ordinateur virtuel (VM GENID). Lorsque Windows Server 2012 détecte l'identificateur de génération d'ordinateur virtuel, il fournit des mesures pour protéger l'environnement AD DS, à condition que vous restauriez l'ordinateur virtuel à une version précédente.

Documentation supplémentaire : Pour plus d'informations sur l'identificateur de génération d'ID virtuel, accédez à http://go.microsoft.com/fwlink/?LinkID=260709.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

En plus de leur fournir une protection, vous pouvez désormais cloner les contrôleurs de domaine Windows Server 2012. Cela signifie que les clones peuvent s'identifier en tant que clones. Jusqu'à présent, vous deviez utiliser l'outil de préparation du système (Sysprep) pour préparer un serveur Windows puis déployer les services de contrôleur de domaine une fois ce serveur déployé, ce qui permet de simplifier la récupération d'urgence.

Lors de la virtualisation des contrôleurs de domaine pour les systèmes de production, évaluez la sélection élective des ordinateurs virtuels et utilisez l'anti-affinité pour éviter de placer les contrôleurs de domaine sur le même nœud de cluster.

Documentation supplémentaire : Pour une présentation de la virtualisation AD DS, accédez à http://go.microsoft.com/fwlink/?LinkID=285289.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Préparation aux déploiements d'ordinateurs virtuels avec VMM

VMM fournit une solution pour créer et enregistrer des ordinateurs virtuels, des modèles et des profils, ce qui permet d'accélérer la remise d'un ordinateur virtuel et de réduire les erreurs de configuration. Après la génération des modèles et des profils, vous pouvez déléguer des autorisations pour vous assurer que les administrateurs peuvent déployer uniquement le nouvel ordinateur virtuel sur la base du modèle validé et attribué.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- expliquer comment configurer un ordinateur virtuel dans VMM ;
- expliquer comment configurer des profils de systèmes d'exploitation invités ;
- expliquer comment configurer des profils matériels ;
- expliquer comment configurer des profils SQL Server ;
- expliquer comment configurer des profils d'application ;
- expliquer comment configurer des modèles d'ordinateur virtuel ;
- expliquer comment configurer des modèles de service ;
- décrire les éléments à prendre en compte pour planifier des profils et des modèles VMM.

Démonstration : Configuration d'un ordinateur virtuel dans VMM

Au cours de cette démonstration, vous allez apprendre à configurer un ordinateur virtuel à l'aide de VMM.

Procédure de démonstration

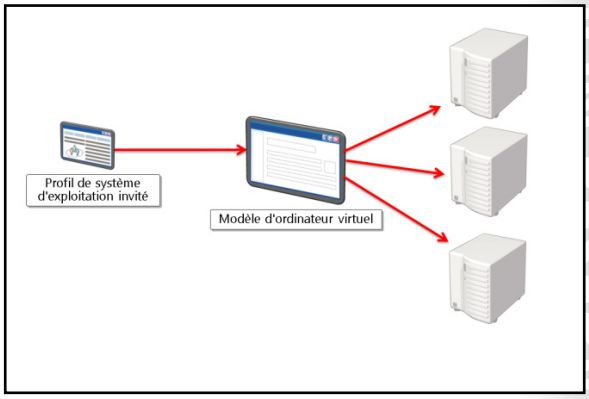
Configuration d'un ordinateur virtuel

1. Démarrez la console VMM.
2. Cliquez sur l'espace de travail **Ordinateurs virtuels et services**, dans le ruban, cliquez sur **Créer un ordinateur virtuel**, dans la zone de liste déroulante, sélectionnez et cliquez sur **Créer un ordinateur virtuel**.
3. Utilisez l'Assistant Créer un ordinateur virtuel pour créer un ordinateur virtuel à partir d'un disque dur virtuel vide.
4. Dans la page Configurer le matériel de l'Assistant Créer un ordinateur virtuel, configurez le matériel virtuel pour votre ordinateur virtuel, puis cliquez sur **Enregistrer sous** pour enregistrer un profil matériel.
5. Parcourez les autres pages de configuration, en examinant soigneusement toutes les options de déploiement d'un ordinateur virtuel.
6. Notez que lorsque vous atteignez la page **Sélectionner l'ordinateur hôte**, une évaluation de la sélection élective évalue les options en fonction de la configuration sélectionnée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de profils de système d'exploitation invité

Un profil de système d'exploitation invité contient les paramètres du système d'exploitation que vous utilisez pendant un déploiement d'ordinateurs virtuels. Vous pouvez l'utiliser comme l'un des éléments constitutifs de la création d'un modèle d'ordinateur virtuel.



Vue d'ensemble du profil de système d'exploitation invité

Un système d'exploitation invité désigne un système d'exploitation qui s'exécute sur un ordinateur virtuel dans Windows Server à l'aide de la technologie Hyper-V. Lorsque vous installez un système d'exploitation invité sur plusieurs ordinateurs virtuels, vous réalisez rapidement que de nombreux ordinateurs virtuels contiennent des paramètres système similaires, tels que l'appartenance à un domaine ou à un groupe de travail, les clés de produit, le fuseau horaire et le mot de passe de l'administrateur local.

Pour prendre en charge un processus de déploiement automatisé et standardisé d'ordinateurs virtuels, vous pouvez créer et utiliser un système d'exploitation invité. Les profils de système d'exploitation invité contiennent un ensemble de paramètres de système d'exploitation que le processus de déploiement d'ordinateurs virtuels importe dans un modèle d'ordinateur virtuel. Le modèle d'ordinateur virtuel fournit une configuration du système d'exploitation cohérente pour un ordinateur virtuel que vous créez en utilisant le modèle.

Vous pouvez utiliser un profil de système d'exploitation invité pour fournir les paramètres de configuration prédéfinis pour le système d'exploitation invité. Ces paramètres sont notamment :

- informations d'identité ;
- mot de passe de l'administrateur local ;
- clé du produit ;
- fuseau horaire ;
- version du système d'exploitation ;
- rôles et les fonctionnalités serveur ;
- appartenance à un groupe de travail ou à un domaine ;
- références du fichier de réponses.

Le *profil de système d'exploitation invité* est un objet de base de données que vous créez et consultez depuis l'espace de travail Bibliothèque dans la console VMM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Création d'un profil de système d'exploitation invité

Pour créer un profil de système d'exploitation invité, procédez comme suit :

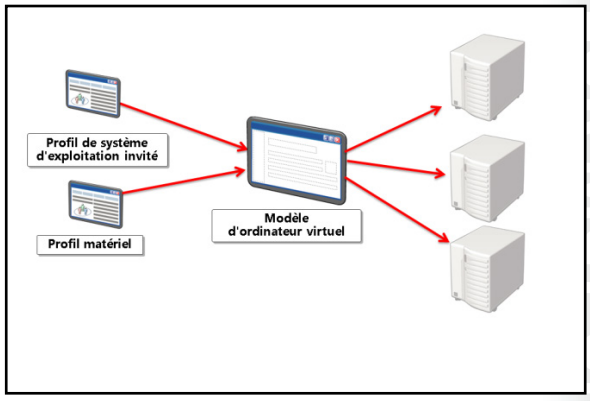
1. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**.
2. Dans le volet de navigation, développez **Profils**, puis cliquez sur **Profils de système d'exploitation invité**. Tous les profils existants s'affichent dans le volet de résultats.
3. Dans l'onglet **Accueil**, cliquez sur **Créer**, puis sur **Profil de système d'exploitation invité**. La boîte de dialogue **Nouveau profil de système d'exploitation invité** s'ouvre.
4. Dans la page **Général**, indiquez le Nom et la Description du profil.
5. Dans la page **Profil de système d'exploitation invité**, configurez les paramètres selon vos besoins, puis cliquez sur **OK**.

   Dans la page **Profil de système d'exploitation invité**, vous pouvez configurer les paramètres suivants :

   - **Paramètres généraux**. Cette section inclut des paramètres tels que le nom de l'ordinateur, le mot de passe de l'administrateur local, la clé de produit, le fuseau horaire et le type de système d'exploitation que vous déploierez sur l'ordinateur virtuel.
   - **Rôles et fonctions** Cette section permet de sélectionner un ou plusieurs rôles serveur et fonctionnalités que vous souhaitez installer sur l'ordinateur virtuel que vous déployez.
   - **Mise en réseau**. Cette section permet de spécifier le groupe de travail ou le domaine que l'ordinateur virtuel doit joindre.
   - **Scripts**. Cette section permet de comprendre les paramètres supplémentaires, que vous spécifiez dans un fichier Unattend.xml ou un fichier de Sysprep.inf ou via des commandes que vous configurez dans la section [GUIRunOnce] de la clé de Registre.

Configuration des profils matériels

Un profil matériel permet de définir un ensemble standard de paramètres matériels que vous souhaitez utiliser lors d'un déploiement d'ordinateurs virtuels. Il s'agit d'un autre élément constitutif que vous pouvez spécifier lorsque vous construisez votre modèle d'ordinateur virtuel.



Vue d'ensemble des profils matériels

Un profil matériel contient des spécifications pour différents composants matériels tels que le nombre de processeurs, l'allocation de mémoire, les périphériques IDE, la configuration de la carte SCSI et la configuration de la carte réseau. Bien que vous puissiez déployer un ordinateur virtuel sans profil matériel, l'utilisation d'un profil matériel en association avec un modèle d'ordinateur virtuel garantit la cohérence du déploiement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Création d'un profil matériel

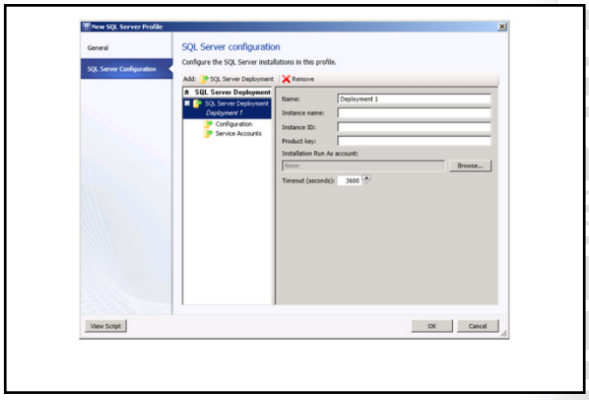
Pour créer un profil matériel, procédez comme suit :

1. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**.
2. Dans le volet de navigation, développez **Profils**, puis cliquez sur **Profils matériels**. Tous les profils existants s'affichent dans le volet de résultats.
3. Dans l'onglet **Accueil**, cliquez sur **Créer**, puis sur **Profil matériel**. La boîte de dialogue **Nouveau profil matériel** s'ouvre.
4. Dans la page **Général**, indiquez le Nom et la Description du profil.
5. Dans la page **Profil matériel**, configurez les paramètres selon vos besoins, puis cliquez sur **OK**.

   Dans la page **Profil matériel**, vous pouvez configurer les paramètres suivants :

   - **Compatibilité**. Ce paramètre fournit une option pour sélectionner un profil de capacité préconfiguré, qui garantit que le profil matériel répond aux exigences spécifiques en matière de capacité matérielle.
   - **Général**. Cette section permet de configurer des paramètres relatifs au processeur, à la mémoire, au lecteur de disquettes, aux ports COM et à la carte vidéo.
   - **Configuration de bus**. Cette section permet de configurer les paramètres des périphériques IDE et des cartes SCSI.
   - **Cartes réseau**. Cette section permet de spécifier des paramètres de connectivité pour une ou plusieurs cartes réseau.
   - **Avancé**. Cette section fournit plusieurs paramètres relatifs à la disponibilité, à la récupération de centre de données, à la configuration du BIOS et aux priorités de processeur et mémoire.

Configuration de SQL Server à l'aide de profils SQL Server



Bon nombre d'applications Web et de services multiniveaux utilisent SQL Server pour la fonctionnalité de base de données. Vous devez souvent déployer des applications de base de données pour prendre en charge des services virtualisés dans le cloud privé. Vous pouvez utiliser un profil SQL Server comme élément constitutif pour déployer des instances de SQL Server sur des ordinateurs virtuels.
Un profil SQL Server fournit les éléments constitutifs pour configurer une instance préparée de SQL Server sur une image d'ordinateur virtuel. Ce profil contient des paramètres de configuration pour chaque instance qui a été au préalable préparée sur l'ordinateur virtuel.

Pour créer un profil SQL Server, procédez comme suit :

1. Ouvrez la console VMM, puis cliquez sur l'espace de travail **Bibliothèque**.
2. Dans le volet de navigation, développez **Profils**, puis cliquez sur **Profils SQL Server**.

3. Dans le ruban, cliquez sur **Créer**, puis sur **Profil SQL Server**. La boîte de dialogue **Nouveau profil SQL Server** s'ouvre.
4. Dans la page **Général**, indiquez le **Nom** et la **Description** du profil.
5. Dans la page **Configuration de SQL Server**, pour chaque instance que vous devez configurer, cliquez sur **Déploiement de SQL Server**, puis configurez les paramètres suivants :
   - **Nom**. Permet de spécifier le nom du déploiement sur SQL Server dans le profil. Chaque instance aura un nom unique pour l'identification. Ce paramètre est obligatoire.
   - **Nom de l'instance**. Permet de spécifier le nom de l'instance SQL Server. Ce paramètre est obligatoire.
   - **ID de l'instance**. Permet d'entrer l'ID de l'instance que vous avez documenté lorsque vous avez préparé l'image SQL Server. Ce paramètre est obligatoire.
   - **Clé du produit**. Utilisez ce paramètre facultatif pour spécifier la clé de produit pour SQL Server. Si vous ne configurez pas ce paramètre, c'est la version d'évaluation qui s'installe.
   - **Compte d'identification de l'installation**. Utilisez ce paramètre facultatif pour spécifier le compte d'identification avec lequel vous souhaitez exécuter l'installation de SQL Server. Si vous ne spécifiez pas de compte, l'installation utilise le compte de service de l'ordinateur virtuel.
   - **Délai (secondes)**. Utilisez ce paramètre facultatif pour spécifier une fenêtre d'expiration dans laquelle l'installation de SQL Server doit se terminer. Par défaut, cette valeur est configurée à 3 600 secondes, ou 1 heure.
6. Cliquez sur **Configuration**, puis configurez les paramètres suivants :
   - **Source du média**. Permet d'indiquer le chemin d'accès au dossier de support d'installation. Vous pouvez placer le support localement sur le disque dur virtuel, ou spécifier un chemin d'accès à un partage réseau. Si vous utilisez un partage réseau, vous devez configurer le compte d'identification de l'installation avec des informations d'identification par l'intermédiaire desquelles l'accès au partage réseau est autorisé, et vous devez définir les privilèges d'administrateur pour l'ordinateur virtuel invité. Ce paramètre est obligatoire.
   - **Administrateurs SQL Server**. Permet d'indiquer les utilisateurs ou groupes qui doivent appartenir au rôle Administrateur système. Ce paramètre est obligatoire.
   - **Mode de sécurité**. Utilisez ce paramètre facultatif pour choisir entre l'authentification Windows (celle par défaut) et l'authentification SQL Server.
   - **Compte d'identification du mot de passe d'administrateur système**. Si, sous **Mode de sécurité**, vous avez sélectionné **Authentification SQL Server**, utilisez ce paramètre pour fournir le mot de passe du compte de l'administrateur système.
   - **TCP/IP**. Utilisez TCP/IP pour les connexions à distance. Ce paramètre facultatif active le protocole TCP/IP pour le service SQL Server.
   - **Canaux nommés**. Utilisez des canaux nommés pour les connexions à distance. Vous pouvez utiliser ce paramètre facultatif pour activer le protocole de canaux nommés pour le service SQL Server.
   - **Fichier de configuration SQL Server**. Utilisez ce paramètre facultatif pour spécifier un fichier de configuration SQL Server. Le fichier doit résider sur un partage de bibliothèque Virtual Machine Manager.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Cliquez sur **Comptes de service**, puis configurez les paramètres suivants :
   - **Compte d'identification du service SQL Server**. Permet d'indiquer le compte à utiliser avec le service SQL Server. Ce paramètre est obligatoire.
   - **Compte d'identification du service de l'agent SQL Server**. Permet d'indiquer le compte à utiliser avec le service Agent SQL Server. Ce paramètre est obligatoire.
   - **Compte d'identification des services de création de rapports**. Utilisez ce paramètre facultatif pour spécifier le compte à utiliser avec Reporting Services.

Configuration de profils d'application

Quand vous déployez un service avec VMM, il contient souvent les applications qui s'intègrent à des services Web ou à une instance SQL Server. Vous pouvez configurer et déployer des profils d'application pour fournir les paramètres d'installation et de configuration que VMM utilisera pour déployer des types spécifiques d'application avec un service.

Les profils d'application fournissent les instructions pour installer des applications afin d'assurer la prise en charge d'un service géré par VMM. Ces profils prennent en charge les types d'application suivants
- Applications de la couche Données de SQL Server
- Applications de serveur App-V
- Applications Web
- Scripts

Vue d'ensemble des profils d'application

Quand vous déployez un ordinateur virtuel dans le cadre d'un service, les profils d'application fournissent des instructions de configuration pour l'installation de types d'application spécifiques. Les profils d'application prennent en charge les types d'application suivants :

- Applications de la couche Données de SQL Server. SQL Server 2008 R2 prend en charge un nouveau type de package appelé application de la couche Données. Une application de la couche Données contient l'intégralité de la base de données et des objets d'instance que l'application utilise. Elle est généralement destinée aux applications de niveau service.
- Applications de serveur App-V. La virtualisation d'applications serveur Microsoft (serveur App-V) est une technologie qui crée des packages d'applications virtuels que vous déployez sur des serveurs exécutant l'agent de virtualisation d'applications serveur Microsoft (agent du serveur App-V). Un package d'applications virtuelles ne requiert pas une installation locale ; cependant, il fonctionne comme s'il s'agit d'une application installée localement. Lorsque vous créez un package Server App-V, le séquenceur App-V de serveur surveille une installation d'application classique et enregistre les informations requises pour que l'application s'exécute dans un environnement virtuel.

  Une fois le package Server App-V créé, vous pouvez l'importer dans la bibliothèque Virtual Machine Manager pour qu'il soit accessible à partir d'un profil d'application.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Application Web. Une *application Web* est un package stocké au sein de la bibliothèque Virtual Machine Manager et qui renferme le contenu, les sites Web, les certificats et les paramètres de Registre d'une application Web. Vous pouvez inclure et déployer des applications Web avec l'outil de déploiement Web de Microsoft. Lors du déploiement d'une application Web selon les spécifications d'un profil d'application, VMM utilise également cet outil pour déployer cette application en tant que service.
- Scripts. Lors du déploiement d'un ordinateur virtuel dans le cadre d'un service, vous pouvez également utiliser le profil d'application pour exécuter des scripts. Vous utilisez ces scripts au cours des phases de préinstallation et de post-installation d'une application spécifique. Par exemple, vous devrez peut-être copier les fichiers de configuration mis à jour dans une application Web déployée, ou vous pouvez être amené à exécuter des commandes d'application virtuelle spécifiques pour finaliser un déploiement d'application virtuelle.

Création d'un profil d'application

Pour créer un profil d'application, procédez comme suit :

1. Ouvrez la console VMM, puis cliquez sur l'espace de travail **Bibliothèque**.
2. Dans le volet de navigation, développez **Profils**, puis cliquez sur **Profils d'application**.
3. Dans le ruban, cliquez sur **Créer**, puis sur **Profil d'application**. La boîte de dialogue **Nouveau profil d'application** s'ouvre.
4. Dans la page **Général**, indiquez le **Nom** et la **Description** du profil d'application.
5. Dans la zone de liste déroulante **Compatibilité**, cliquez sur **Général** pour autoriser tous les types d'application prise en charge dans le profil. Vous pouvez également utiliser la sélection **Hôte d'application SQL Server** si vous utilisez ce profil d'application pour déployer une application de la couche Donnée SQL Server sur un ordinateur SQL Server existant. La fait de sélectionner cette option vous autorise uniquement à ajouter des packages d'applications de la couche Données et des scripts SQL Server.
6. Dans la page **Configuration de l'application**, cliquez sur **Compatibilité de système d'exploitation**, puis sélectionnez les systèmes d'exploitation invités compatibles avec l'application.
7. Cliquez sur **Ajouter**, puis sélectionnez le type d'application approprié. Notez que vous ne pouvez ajouter un script d'application qu'après avoir ajouté une application.
8. Pour chaque application ou script que vous avez ajouté, configurez les paramètres appropriés.
9. Cliquez sur **OK** pour accepter les paramètres de configuration d'application.

Déploiement d'un profil d'application

À l'instar d'un profil SQL Server, vous pouvez uniquement utiliser un profil d'application lorsque vous déployez un ordinateur virtuel dans le cadre d'un service.

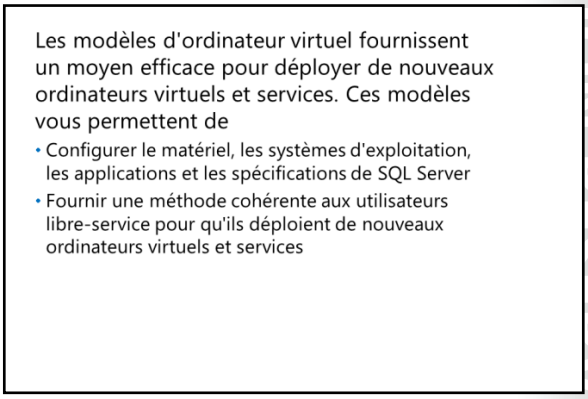
Pour configurer un modèle de service à utiliser lors du déploiement d'une application avec un service, utilisez le concepteur de modèles de service dans VMM. Vous avez deux possibilités pour spécifier une configuration d'application dans un modèle de service :

- Créez un modèle d'ordinateur virtuel, puis spécifiez les paramètres de configuration d'application. Vous pouvez ensuite utiliser le modèle d'ordinateur virtuel lorsque vous créez le modèle de service.
- Modifiez les propriétés d'une couche de service et spécifiez le profil d'application manuellement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de modèles d'ordinateur virtuel

Pour créer des ordinateurs virtuels, vous utilisez des modèles d'ordinateur virtuel. Vous pouvez ensuite ajouter ces modèles à des niveaux dans un modèle de service. Le modèle d'ordinateur virtuel combine également bon nombre des paramètres que vous configureriez dans les profils matériels, les profils de système d'exploitation invité, les profils d'application et les profils SQL Server.



Vue d'ensemble d'un modèle d'ordinateur virtuel

Lorsque vous créez un ordinateur virtuel, vous pouvez soit dériver la source de ce nouvel ordinateur virtuel à partir d'un ordinateur virtuel existant ou d'un disque dur, soit baser le nouvel ordinateur virtuel sur un modèle d'ordinateur virtuel. Si vous utilisez un ordinateur virtuel stocké ou un disque dur virtuel, vous ne pouvez personnaliser que les paramètres matériels. Il n'existe aucune option pour ajouter des informations supplémentaires telles que la configuration du système d'exploitation ou les applications. Cependant, un modèle d'ordinateur virtuel fournit davantage de flexibilité et d'efficacité pour le déploiement d'ordinateurs virtuels. L'utilisation d'un modèle d'ordinateur virtuel présente les avantages suivants :

- Vous pouvez configurer le matériel, le système d'exploitation, les applications et les spécifications de SQL Server.
- Vous pouvez créer des ordinateurs virtuels ou des modèles de service.
- Vous pouvez partager un modèle d'ordinateur virtuel avec des rôles libre-service pour assurer la cohérence du processus de déploiement d'ordinateur virtuel.

Lorsque vous créez un modèle d'ordinateur virtuel, vous pouvez configurer les éléments suivants :

- Profil matériel. Vous pouvez configurer les paramètres matériels directement dans le modèle d'ordinateur virtuel, ou spécifier un profil matériel préconfiguré. Vous pouvez également enregistrer les modifications en tant que nouveau profil matériel qui est stocké dans la bibliothèque Virtual Machine Manager. La principale différence entre la configuration matérielle dans le modèle d'ordinateur virtuel et la configuration matérielle dans le profil matériel est que dans le modèle d'ordinateur virtuel, vous pouvez créer, supprimer et configurer des disques au besoin.
- Profil de système d'exploitation invité. Dans le modèle d'ordinateur virtuel, vous pouvez configurer les paramètres de profil de système d'exploitation invité manuellement, ou importer les paramètres d'un modèle de profil de système d'exploitation invité préconfiguré. Si vous n'avez pas besoin de personnaliser le système d'exploitation, dans la page **Configurer le système d'exploitation** de l'**Assistant Créer un modèle d'ordinateur virtuel**, vous pouvez sélectionner **Aucune – personnalisation non requise**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Profil d'application. Vous pouvez configurer les paramètres de profil d'application manuellement, importer des paramètres depuis un profil d'application préconfiguré, ou choisir de ne pas installer certaines applications.
- Profil SQL Server. Vous pouvez configurer les paramètres d'installation de SQL Server manuellement, les importer à partir d'un profil SQL Server préconfiguré, ou choisir de ne pas indiquer de paramètres de configuration de SQL Server dans le modèle d'ordinateur virtuel.

Création d'un modèle d'ordinateur virtuel

VMM fournit plusieurs méthodes que vous pouvez utiliser pour créer des modèles d'ordinateur virtuel. Cependant, vous devez comprendre les implications pour chaque méthode. Le tableau suivant décrit les méthodes et les éléments à prendre en compte pour chaque méthode.

Méthode	Éléments à prendre en compte
Créer un modèle d'ordinateur virtuel à partir d'un disque dur virtuel qui est stocké dans la bibliothèque Virtual Machine Manager.	Le disque dur virtuel source a généralement un système d'exploitation qui a été installé et préparé à l'aide de l'outil Sysprep. Si vous choisissez d'utiliser un disque dur virtuel source qui n'est pas préparé avec Sysprep, vous pouvez configurer un modèle d'ordinateur virtuel non personnalisé contenant le profil de système d'exploitation invité qui est défini sur **Aucune – personnalisation non requise**.
Créer un modèle d'ordinateur virtuel à partir d'un modèle d'ordinateur virtuel qui est stocké dans la bibliothèque Virtual Machine Manager.	Vous pouvez utiliser les paramètres d'un modèle d'ordinateur virtuel préconfiguré comme base pour un nouveau modèle d'ordinateur virtuel. Tous les paramètres préconfigurés et modifiés sont enregistrés dans un nouveau modèle qui est stocké et mis à disposition dans la bibliothèque Virtual Machine Manager.
Créer un modèle d'ordinateur virtuel à partir d'un ordinateur virtuel existant qui est déployé sur un hôte.	Vous pouvez uniquement choisir un ordinateur virtuel source qui est déployé sur un hôte, et non un ordinateur virtuel stocké dans la bibliothèque. Vous configurez les paramètres d'ordinateur virtuel dans le modèle, puis vous généralisez les disques virtuels de l'ordinateur virtuel à l'aide de Sysprep. Ensuite, vous déplacez l'ordinateur virtuel dans un partage de bibliothèque Virtual Machine Manager, où il ne devient plus disponible sur l'hôte. Vous avez toujours la possibilité de modifier le modèle d'ordinateur virtuel si nécessaire.
Importer un modèle préconfiguré.	Vous pouvez utiliser l'Assistant Importation de package pour importer des modèles préconfigurés qui ont été configurés dans d'autres plateformes de virtualisation. Pour démarrer cet assistant, cliquez sur le bouton Importer un modèle dans le ruban.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de modèles d'ordinateur virtuel

Pour créer un modèle d'ordinateur virtuel à partir d'un disque dur virtuel qui est stocké dans la bibliothèque Virtual Machine Manager, procédez comme suit :

1. Ouvrez la console VMM, puis cliquez sur l'espace de travail **Bibliothèque**.
2. Dans le volet de navigation, développez **Modèles**, puis cliquez sur **Modèles d'ordinateur virtuel**.
3. Dans le ruban, cliquez sur **Créer un modèle d'ordinateur virtuel**. L'Assistant Créer un modèle d'ordinateur virtuel s'ouvre.
4. Dans la page **Sélectionner une source**, sélectionnez une des options suivantes, puis cliquez sur Suivant:
   - Utiliser un modèle d'ordinateur virtuel existant ou un disque dur virtuel stocké dans la bibliothèque.
   - À partir d'un ordinateur virtuel existant qui est déployé sur un ordinateur hôte.
5. Dans la page **Identité du modèle d'ordinateur virtuel**, indiquez le **Nom du modèle d'ordinateur virtuel** et sa **Description**.
6. Dans la page **Configurer le matériel**, configurez les paramètres de profil matériel affichés ou sélectionnez un profil matériel préconfiguré, puis effectuez les modifications nécessaires.
7. Dans la page **Configurer le système d'exploitation**, configurez les paramètres affichés pour le profil de système d'exploitation invité ou sélectionnez un profil préconfiguré, puis effectuez les modifications nécessaires.
8. Dans la page **Configurer les applications**, configurez les paramètres de profil d'application affichés ou sélectionnez un profil préconfiguré, puis effectuez les modifications nécessaires.
9. Dans la page **Configurer SQL Server**, configurez les paramètres de profil SQL Server affichés ou sélectionnez un profil préconfiguré, puis effectuez les modifications nécessaires.
10. Dans la page **Résumé**, cliquez sur **Créer**.

Configuration de modèles de service

Le déploiement d'un nouveau service nécessite un haut niveau d'automatisation et de composants prédéfinis et requiert également la prise en charge du logiciel de gestion. C'est la raison pour laquelle VMM propose des modèles de service. Un modèle de service est un modèle qui encapsule tout ce qui est nécessaire pour déployer et exécuter la nouvelle instance d'une application. De la même façon qu'un utilisateur de cloud privé peut créer des ordinateurs virtuels à la demande, un utilisateur peut également utiliser les modèles de service pour installer et démarrer de nouvelles applications à la demande.

Un modèle de service encapsule tous les composants nécessaires pour déployer et exécuter une nouvelle instance d'une application. Lorsque vous utilisez des modèles de service, gardez à l'esprit les points suivants

- Les administrateurs créent des modèles de service dans VMM
- Les propriétaires d'application déploient les services selon le modèle de service
- Les utilisateurs utilisent App Controller ou la console VMM pour déployer le service selon le modèle

Informations incluses dans le modèle de service

Le modèle de service comprend des informations sur les ordinateurs virtuels déployés dans le cadre du service. Le modèle de service comprend également les applications qu'il convient d'installer sur les ordinateurs virtuels, ainsi que la configuration de réseau nécessaire pour le service, y compris l'utilisation de services d'équilibrage de charge. Le modèle de service peut également utiliser des modèles d'ordinateurs virtuels existants. Même si vous pouvez définir le service sans utiliser de modèle d'ordinateur virtuel existant, il est beaucoup plus facile de créer un modèle si vous avez déjà créé des modèles d'ordinateur virtuel. Après la création du modèle de service, vous pouvez le configurer en vue de son déploiement en sélectionnant le modèle puis en cliquant sur l'option **Configurer le déploiement** dans le ruban.

Processus de déploiement d'un nouveau service

Lorsque vous utilisez des modèles de service dans VMM, le processus de déploiement d'un nouveau service ou d'une nouvelle application se déroule comme suit :

1. L'administrateur système crée et configure les modèles de service dans VMM à l'aide du concepteur de modèles de services.
2. Le propriétaire de l'application (par exemple, un développeur qui doit déployer l'environnement de l'application) ouvre le portail System Center 2012 - App Controller et demande un nouveau déploiement de service selon les modèles de service disponibles auxquels il peut avoir accès. L'utilisateur peut ensuite déployer le service vers un cloud privé auquel un utilisateur a accès. Comme alternative à App Controller, l'utilisateur peut également utiliser la console VMM.
3. Une demande est soumise et évaluée par le serveur de gestion VMM. VMM recherche les ressources disponibles dans le cloud privé, puis calcule le quota de l'utilisateur et vérifie que le cloud privé est apte à héberger le déploiement de service demandé.
4. Lorsque le service est créé automatiquement, les ordinateurs virtuels et les applications (le cas échéant) sont déployés sur l'hôte sélectionné par VMM.
5. Le propriétaire de l'application parvient à contrôler les ordinateurs virtuels des services via le portail App Controller ou via le protocole RDP (Remote Desktop Protocol).

Si une approbation manuelle s'avère nécessaire pour la création des ressources, vous pouvez utiliser System Center 2012 - Service Manager pour créer des flux de travail à cet effet.

Configuration de modèles de service

Chaque modèle de service que vous créez dans VMM contient plusieurs paramètres que vous pouvez configurer. Vous accédez à ces paramètres en ouvrant la fenêtre Propriétés du modèle de service que vous créez.

La liste suivante fournit des explications sur les propriétés de modèle de service les plus importantes :

- Nom. Il s'agit d'un modèle de service qui apparaît dans la bibliothèque VMM. Les utilisateurs libre-service verront ce nom, vous laissant le rendre descriptif.
- Version. Valeur indiquant la version du modèle de service. Cette valeur est importante quand vous mettez à jour un service, car elle vous permet d'identifier la version du modèle de service. Chaque fois que vous créez un modèle de service et effectuez un déploiement selon le modèle, vous ne pouvez pas y apporter d'autres modifications. Si vous souhaitez le modifier, vous devez créer une autre version.

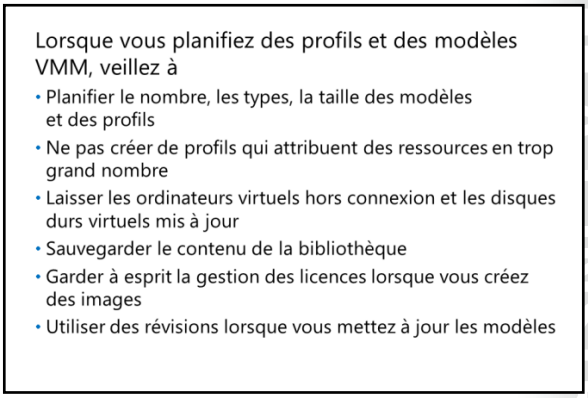
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Dépendances. Dans le paramètre Dépendances, vous pouvez afficher les objets dérivés d'un modèle de service spécifique et les ressources de bibliothèque qui sont référencées dans le modèle. Vous ne pouvez pas apporter de modifications à ce stade.
- Accès. Vous pouvez définir le propriétaire du modèle de service dans ce paramètre. Vous pouvez également répertorier les utilisateurs libre-service qui peuvent utiliser ce modèle de service pour déployer un service. Si vous souhaitez offrir aux utilisateurs libre-service la possibilité de déployer des services en utilisant la console VMM ou App Controller, vous devez les ajouter à la liste d'accès pour le modèle de service.

Nous vous recommandons de configurer tous les paramètres de modèle de service avant de commencer à déployer des services basés sur ce modèle.

Planification de profils et de modèles VMM

Dans le cadre de la stratégie de virtualisation et de la conception d'infrastructure, prenez en compte les différents modèles, disques virtuels stockés, profils matériels, profils d'applications invitées et profils de base de données dont vous aurez besoin. Planifiez le nombre de systèmes d'exploitation déployés et l'emplacement auquel les fichiers doivent être stockés. La liste suivante résume certains éléments à prendre en compte pour utiliser les profils et les modèles :



- Utilisation d'éléments de bibliothèque. Envisagez de créer un plan pour le nombre de modèles dont vous pensez avoir besoin et configurez tout ou partie de ces modèles avant de lancer le déploiement. Envisagez de ne conserver que le nombre de fichiers .vhd requis. Dans un environnement hôte mixte, envisagez de posséder à la fois les formats .vhd et .vhdx. Supprimez les profils et les modèles hérités et inutilisés. Sauvegardez une bibliothèque de temps en temps, et si vous devez récupérer une image antérieure, vous pouvez la récupérer à partir de la sauvegarde.
- Essayez de maintenir la bibliothèque Virtual Machine Manager nettoyée et d'éviter la position abandonnée virtuelle. Supprimez les ordinateurs virtuels et les disques durs virtuels inutilisés. La position abandonnée virtuelle comprend les fichiers hors connexion, qui risquent d'être stockés sur des serveurs de fichiers et d'infrastructure autres que les hôtes.
- Si vous devez posséder les mêmes modèles et fichiers sur plusieurs bibliothèques Virtual Machine Manager, vous pouvez envoyer les fichiers volumineux hors connexion, puis les importer à l'emplacement nécessaire. Si vous devez éviter d'utiliser des liens de petits réseaux étendus (WAN), configurez des objets équivalents à plusieurs emplacements pour les ressources de déploiement de virtualisation dont vous avez besoin et que vous ne souhaitez pas voir déployées via un réseau étendu (WAN).
- Performances. Examinez l'incidence de la gestion d'un grand nombre de fichiers hors connexion. Si vous les mettez à jour, veillez à instaurer une collaboration au sein des grandes organisations en vous assurant qu'aucune personne n'utilise des images pendant qu'une autre tente de les déployer.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Prenons l'exemple d'un profil matériel standard. Si vous définissez la configuration de base pour tous vos serveurs virtuels en leur attribuant une quantité de mémoire, de processeurs et d'espace disque trop importante, les ressources sont gaspillées et la valeur complète de la virtualisation n'est pas atteinte.
- Gestion des licences. Vous pouvez utiliser des profils de système d'exploitation invité pour appliquer les exigences en matière de gestion des licences. Par exemple, vous pouvez préconfigurer une image pour le site Web Microsoft Developer Network (MSDN), puis l'attribuer aux développeurs qui ont l'accord de MSDN. Prenez en compte la gestion de licences lorsque vous utilisez un modèle basé sur un autre ordinateur. Vérifiez que seules les personnes censées utiliser un modèle l'utilisent.
- Intégration de systèmes, automatisation et libre-service. VMM et ses bibliothèques sont la source à partir de laquelle d'autres applications sont déployées. Si nécessaire, créez plusieurs bibliothèques avec la sécurité appropriée et assurez-vous que les fichiers et les images déployés sont à jour.
- Modèles de service. Lorsque vous créez des services d'applications qui montent en charge, prenez en compte les versions et les révisions et tentez de conserver leur cohérence. Par exemple, si vous avez un modèle pour une application à trois niveaux, quand vous mettez à jour les niveaux, vous devez veiller à incrémenter les révisions convenablement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Déploiement d'ordinateurs virtuels

La virtualisation est une grande technologie qui apporte haute disponibilité et portabilité aux applications et aux services qui en sont initialement dépourvus ou qui se révèlent très coûteux. Le déploiement d'ordinateurs virtuels est un composant clé dans une stratégie de virtualisation d'organisations, et vous devez maîtriser ces options pour gagner du temps et réduire les charges de travail futures tout en améliorant la cohérence de la configuration des ordinateurs virtuels.

Dans cette leçon, vous allez découvrir les méthodes que vous pouvez utiliser pour déployer les ordinateurs virtuels à partir de VMM, et vous allez étudier les méthodes et les outils pour les conversions P2V et V2V.

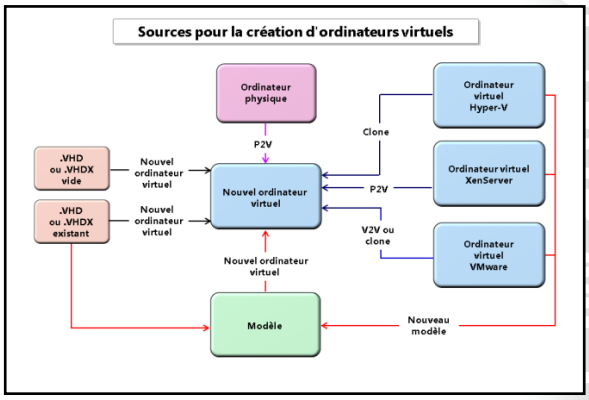
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- expliquer comment déployer des ordinateurs virtuels à l'aide de VMM ;
- expliquer comment configurer la sélection élective d'ordinateur virtuel dans VMM ;
- décrire le processus des conversions d'ordinateur P2V dans VMM ;
- décrire les éléments à prendre en compte pour les conversions P2V ;
- décrire le processus des conversions d'ordinateur V2V dans VMM ;
- décrire les éléments à prendre en compte pour les conversions V2V ;

Déploiement d'ordinateurs virtuels dans VMM

L'avantage que présente l'utilisation d'un environnement virtualisé géré à l'aide de VMM est la flexibilité qu'il offre pour créer et déployer rapidement de nouveaux ordinateurs virtuels. Avec VMM, vous pouvez créer manuellement un nouvel ordinateur virtuel avec de nouveaux paramètres de configuration et un nouveau disque dur. Vous pouvez ensuite déployer ce nouvel ordinateur virtuel à partir de l'une des sources suivantes :



- Un fichier .vhd ou .vhdx existant (vierge ou préconfiguré).
- Un modèle d'ordinateur virtuel.
- Un modèle de service.

Vous pouvez créer des ordinateurs virtuels en convertissant un ordinateur physique existant, en clonant un ordinateur virtuel existant, ou à partir d'un disque virtuel vierge ou d'un disque virtuel préconfiguré qui contient un système d'exploitation préparé avec Sysprep. VMM fournit quatre modèles de disque dur virtuel vierges (VHD ou VHDX) que vous pouvez utiliser pour créer des disques :

- Disque vierge VHD - Petit.
- Disque vierge VHD - Grand.
- Disque vierge VHDX - Petit.
- Disque vierge VHDX - Grand.

Vous pouvez également utiliser un disque dur virtuel vierge quand vous souhaitez utiliser un système d'exploitation avec PXE. À défaut, vous pouvez placer une image .iso sur un DVD-ROM virtuel puis installer un système d'exploitation sur le lecteur vide. Il s'agit d'une manière efficace de créer une image source d'un ordinateur virtuel que vous pourrez utiliser pour référence ultérieure. Pour installer le système d'exploitation sur un ordinateur virtuel de ce type, vous pouvez utiliser un fichier d'image .iso de la bibliothèque ou du disque local, puis mapper un lecteur physique à partir de l'ordinateur hôte ou lancer l'installation du système d'exploitation invité via un démarrage du service réseau.

Vous pouvez également choisir des disques durs virtuels existants lors du déploiement d'un système d'exploitation à partir duquel VMM ne peut pas créer de modèle, par exemple un système d'exploitation autre que Windows.

Lorsque vous créez un nouvel ordinateur virtuel à l'aide d'un disque dur virtuel existant (VHD ou VHDX), vous créez en fait une configuration d'ordinateur virtuel qui est associée au fichier. VMM crée une copie du fichier source pour vous éviter d'avoir à déplacer ou modifier le fichier d'origine.

Dans ce scénario, le fichier source doit répondre aux conditions suivantes :

- Vous devez laisser le mot de passe Administrateur non spécifié sur le disque dur virtuel dans le cadre du processus SysPrep.
- Vous devez installer les services d'intégration sur l'ordinateur virtuel.
- Vous devez utiliser Sysprep pour préparer le système d'exploitation pour la duplication.

Déploiement à partir d'un modèle

Le déploiement à partir d'un modèle crée un ordinateur virtuel à partir d'un modèle de la bibliothèque Virtual Machine Manager. Le modèle est une ressource de bibliothèque, qui établit la liaison avec un disque dur virtuel doté d'un système d'exploitation généralisé, de paramètres matériels et de paramètres de système d'exploitation invité. Vous utilisez les paramètres du système d'exploitation invité pour configurer les paramètres du système d'exploitation tels que le nom de l'ordinateur, le mot de passe d'administrateur local et l'appartenance au domaine. Les profils de système d'exploitation invité vous permettent de préconfigurer les rôles et fonctionnalités seront déployés pour Windows Server 2008 R2 et systèmes d'exploitation Windows Server plus récents.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le processus de déploiement ne modifie pas le modèle que vous pouvez réutiliser plusieurs fois. Les conditions requises suivantes s'appliquent si vous souhaitez déployer un nouvel ordinateur virtuel à partir d'un modèle :

- Vous devez installer un système d'exploitation pris en charge sur le disque dur virtuel utilisé avec le modèle.
- Vous devez laisser le mot de passe Administrateur sur le disque dur virtuel vierge (VHD ou VHDX) dans le cadre du processus Sysprep. Toutefois, le mot de passe Administrateur pour le profil du système d'exploitation invité ne doit pas être vide.
- Pour les modèles personnalisés, vous devez préparer le système d'exploitation sur le disque dur virtuel en supprimant les informations d'identité de l'ordinateur. Pour les systèmes d'exploitation Windows, vous pouvez préparer le disque dur virtuel à l'aide de l'outil Sysprep.

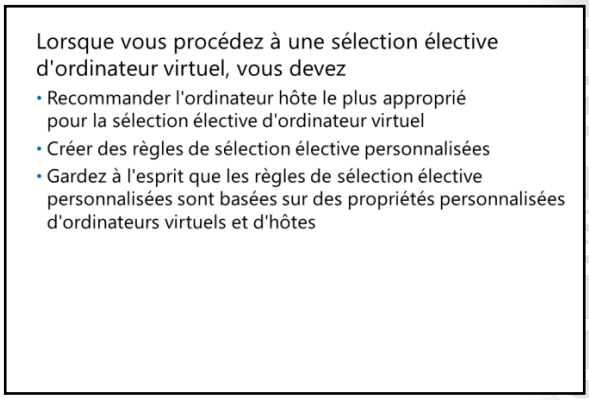
Déploiement vers et depuis la bibliothèque Virtual Machine Manager

Lors du processus de déploiement d'ordinateurs virtuels, vous pouvez effectuer le déploiement sur une bibliothèque lorsque vous sélectionnez la destination. Si vous déployez un ordinateur virtuel à partir de la bibliothèque Virtual Machine Manager, vous supprimez l'ordinateur virtuel de la bibliothèque, puis vous le placez sur l'hôte sélectionné. Lorsque vous utilisez cette méthode, vous devez fournir les détails suivants dans l'Assistant Déploiement de l'ordinateur virtuel :

- Hôte du déploiement. Le modèle que vous utilisez fournit une liste d'hôtes potentiels et leurs évaluations.
- Chemin d'accès des fichiers d'ordinateur virtuel sur l'hôte.
- Réseaux virtuels à utiliser pour l'ordinateur virtuel. Une liste des réseaux virtuels existants sur l'hôte vous est présentée. Vous pouvez y choisir un réseau virtuel.

Configuration de la sélection élective d'ordinateur virtuel dans VMM

Dans VMM, la sélection élective d'un ordinateur virtuel permet à VMM d'évaluer la capacité des hôtes, puis suggère l'hôte de virtualisation le plus approprié pour le déploiement. La dernière version de Microsoft System Center 2012 – Virtual Machine Manager étend cette fonctionnalité avec plus de cent contrôles de sélection élective d'ordinateur virtuel et ajoute la prise en charge de règles de sélection élective personnalisées.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sélection élective d'ordinateur virtuel gérée par VMM

Les règles de sélection élective que vous définissez au niveau du groupe d'hôtes vous permettent de gérer la sélection élective d'ordinateurs virtuels sur des hôtes spécifiques au sein d'un groupe d'hôtes. Généralement, VMM tente toujours de recommander l'hôte le plus approprié pour la sélection élective d'ordinateur virtuel en évaluant les hôtes. Cependant, en spécifiant des règles de sélection élective personnalisées, vous pouvez définir vos propres règles pour la sélection élective ou son blocage.

Si vous déployez un ordinateur virtuel et optez pour un déploiement sur un hôte ou un cloud privé, vous pouvez également configurer les paramètres d'utilisation prévue, ce qui peut affiner davantage les évaluations d'hôte basées sur l'utilisation anticipée des ressources. Avec ces paramètres, vous pouvez ajuster les éléments suivants :

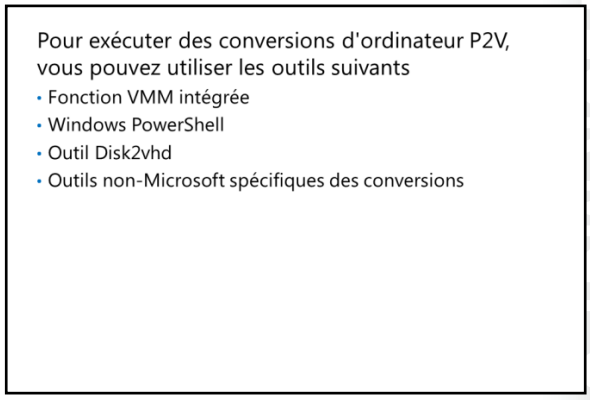
- Utilisation prévue en pourcentage du processeur.
- Disque, espace disque physique et E/S de disque prévues par seconde.
- Réseau, utilisation prévue en mégabits par seconde (Mbps).

Règles de sélection élective personnalisées

Les règles de sélection élective personnalisées sont basés sur des propriétés personnalisées d'hôte et d'ordinateur virtuel. Sur chaque hôte, vous pouvez définir des valeurs pour 10 propriétés personnalisées prédéfinies, et vous pouvez définir vos propres propriétés personnalisées et leurs valeurs. De même, vous pouvez définir des propriétés personnalisées pour chaque ordinateur virtuel. Lorsque vous définissez des règles de sélection élective personnalisées au niveau d'un groupe d'hôtes, vous pouvez définir une règle qui utilise une propriété personnalisée comme condition d'autorisation ou de blocage du déploiement d'ordinateurs virtuels sur un hôte de ce groupe. Par exemple, vous pouvez définir une règle spécifiant qu'une valeur de propriété personnalisée spécifique doit correspondre à la fois sur l'hôte et sur l'ordinateur virtuel, sinon le déploiement de l'ordinateur virtuel n'est pas autorisé.

Conversion d'ordinateur P2V

VMM fournit un assistant intégré avec une fonction permettant d'exécuter des conversions d'ordinateur P2V. Cet assistant de conversion P2V vous guide tout au long des étapes de configuration, puis déploie un agent sur le serveur que vous convertissez. La plupart des systèmes d'exploitation Windows peuvent être convertis à partir de Windows XP Service Pack 3 (SP3) pour les clients, et à partir de Windows Server 2003 Service Pack 2 (SP2) pour les serveurs.



Documentation supplémentaire :
Pour obtenir une liste des systèmes d'exploitation pris en charge pour la conversion P2V accédez à http://go.microsoft.com/fwlink/?LinkID=285288.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lors du processus de conversion P2V, VMM génère des images cible des disques durs source. Il crée également des fichiers .vhd pour le nouvel ordinateur virtuel en utilisant les images de disque comme base. En outre, VMM crée pour l'ordinateur virtuel une configuration matérielle qui est similaire, voire identique au matériel de l'ordinateur physique.

Le nouvel ordinateur virtuel a la même identité que l'ordinateur physique sur lequel il est basé. Nous vous recommandons de ne pas utiliser simultanément un ordinateur physique et son réplica virtuel. Une fois la conversion P2V effectuée, vous devez généralement déconnecter l'ordinateur physique du réseau et le désaffecter.

La conversion P2V s'achève en mode connecté ou déconnecté. En mode connecté, le système d'exploitation source s'exécute pendant le processus de conversion. En mode déconnecté, le système d'exploitation ne s'exécute pas et la conversion se produit dans l'environnement de préinstallation Windows (Windows PE).

L'Assistant Conversion P2V VMM est la méthode recommandée pour convertir quelques ordinateurs physiques. Cependant, pour des conversions par lot, envisagez d'utiliser l'interface de ligne de commande Windows PowerShell®.

Processus P2V VMM

Pour convertir un ordinateur physique en ordinateur virtuel à partir de la console VMM, procédez comme suit :

1. Ouvrez la console VMM, puis cliquez sur l'espace de travail **Ordinateurs virtuels et services**.
2. Dans le ruban, cliquez sur **Créer un ordinateur virtuel**, puis sur **Convertir un ordinateur physique**. L'Assistant Conversion de serveur physique (P2V) s'ouvre.
3. Dans la page **Sélectionner une source**, tapez le nom cible ou l'adresse IP de l'ordinateur que vous souhaitez convertir. Vous pouvez également choisir de parcourir l'ordinateur. Entrez les informations d'identification du domaine, ou si la cible ne figure pas sur le domaine, fournissez ses informations d'identification d'administration locales, puis cliquez sur **Suivant**.
4. Dans la page **Spécifier l'identité de l'ordinateur virtuel**, tapez un nom et une description, puis cliquez sur **Suivant**.
5. Dans la page Informations système, cliquez sur Analyser le système.
6. Dans la page **Configuration du volume**, sélectionnez les volumes à convertir, puis activez la taille et le type du nouveau disque dur virtuel (dynamique ou fixe). Cliquez sur **Options de conversion**, choisissez une conversion en ligne ou hors connexion, puis cliquez sur **Suivant**.
7. Si vous avez sélectionné Conversion hors connexion, dans la page **Options de conversion hors connexion**, configurez les paramètres IP, puis cliquez sur **Suivant**.
8. Dans la page **Configuration de l'ordinateur virtuel**, sélectionnez le nombre de processeurs requis et la quantité de mémoire pour l'ordinateur virtuel, puis cliquez sur **Suivant**.
9. Sélectionnez l'ordinateur hôte, le chemin d'accès et le réseau comme vous le feriez pour déployer un nouvel ordinateur virtuel, puis cliquez sur **Suivant** dans chaque page.
10. Examinez et résolvez les problèmes répertoriés dans la page **Informations de conversion**, puis cliquez sur **Suivant**.
11. Vérifiez la page **Résumé**, puis cliquez sur **Créer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Conditions préalables à la conversion P2V VMM

Pour la conversion d'un ordinateur physique en ordinateur virtuel, le serveur source doit avoir au moins au 512 Mo de RAM et ne peut pas contenir de volumes d'une taille supérieure à 2 040 Go. Il doit avoir un BIOS ACPI (Advanced Configuration and Power Interface). Windows PE ne s'installera pas sur un BIOS non ACPI. La source doit être accessible pour les deux instances VMM et les hôtes de destination, et VMM doit pouvoir installer un agent temporaire. Cela signifie que si le serveur est situé derrière un pare-feu, il doit être disponible.

Autres méthodes de conversion

Outre l'Assistant Conversion P2V VMM, vous pouvez utiliser les méthodes suivantes autonomes ou autres que Microsoft :

- Windows PowerShell : Vous pouvez créer des scripts Windows PowerShell pour convertir les hôtes physiques en hôtes virtuels.

Le script Windows PowerShell suivant est un exemple qui requiert le module VMM Windows PowerShell. Il exécute une migration P2V.

Exemple de script PowerShell pour exécuter une conversion P2V

```
$computername = [nom de l'ordinateur]
$targethostgroup = Get-SCVMHostGroup -Name [nom du groupe de l'hôte de destination]
$cred = Get-Credential
$computerconfiguration = New-SCComputerConfiguration -SourceComputerName $computername -
Credential $cred
($computerconfiguration.ErrorList.Count -eq 0)
$jobgroup = [System.Guid]::NewGuid()
for ($i=1; $ -le $computerconfiguration.NetworkAdapters.Count; $i++)
{ New-SCVirtualNetworkAdapter -JobGroup $jobgroup -MACAddress
$computerconfiguration.NetworkAdapters[$i].MACAdress -MACAddressType Static }
$totaldiskspaceBytes = 0
for ($i=1; $i -le $computerconfiguration.Volumes.Count; $i++)
{ $totaldiskspaceBytes += $computerconfiguration.Volumes[$i].Size }
$totaldiskspacegigabytes = $totaldiskspaceBytes / 1073741824
$name = "Profil matériel temporaire " + [System.Guid]::NewGuid().toString()
$memory = $computerconfiguration.MemoryMB
$cpucount = $computerconfiguration.CPUCount
$processortype = $computerconfiguration.CPUType
$hardwareprofile = New-SCHardwareProfile -HighlyAvailable $true -Name $name -JobGroup
$jobgroup -MemoryMB $memory -CPUCount $cpucount -CPUType $processortype
$vmhostrating = Get-SCVMHostRating -VMHostGroup $targethostgroup -VMName $computername -
JobGroup $jobgroup -HardwareProfile $hardwareprofile -DiskSpaceGB
$totaldiskspacegigabytes
($vmhostrating[$bestindex].DeploymentErrorList.Count -eq 0)-
and($vmhostrating[$bestindex].ZeroRatingReasonList.Count -eq 0)
Get-SCVirtualNetworkAdapter -HardwareProfile $hardwareprofile | Remove-
SCVirtualNetworkAdapter
Remove-SCHardwareProfile -HardwareProfile $hardwareprofile
$path = $vmhostrating[$bestindex].PreferredVolume.ToString() + “[un chemin d'accès au
dossier]”
New-SCP2V -SourceComputerName $computername -VMHost $vmhostrating[$bestindex].VMHost -
Name [nom de l'ordinateur virtuel] -Path $path -MemoryMB $memory –Credential $cred -
RunAsynchronously
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Disk2vhd. Vous pouvez utiliser l'outil gratuit Windows Sysinternals Disk2vhd, qui permet d'effectuer une copie en ligne à l'aide de la fonctionnalité Capture instantanée de volume dans les systèmes d'exploitation Windows Server.

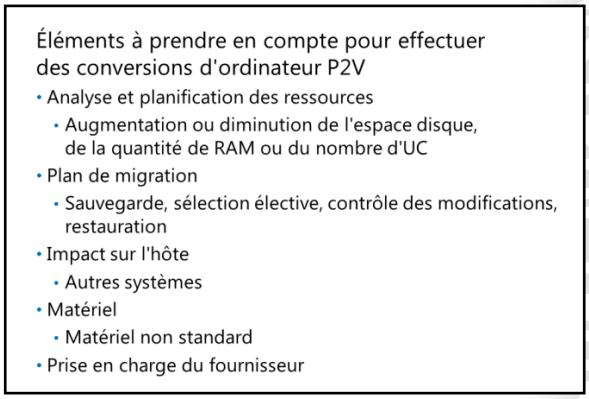
Documentation supplémentaire : Pour plus d'informations et pour télécharger Disk2vhd, accédez à http://go.microsoft.com/fwlink/?LinkID=285293.

- Autres outils non-Microsoft. Vous pouvez également utiliser d'autres outils non-Microsoft, la sauvegarde et les technologies de mise en miroir pour migrer la conversion P2V. Certaines sont spécifiquement créés à cet effet, alors que d'autres ne pourront peut-être pas être conçus avec la conversion comme objectif. Bon nombre des technologies de sauvegarde offrent un agent ou un outil de récupération complète, qui restaure un serveur complètement en un matériel non identique, y compris un ordinateur virtuel.

Liens de référence : Pour plus d'informations sur les conditions préalables à la conversion P2V VMM et les systèmes d'exploitation pris en charge, accédez à http://go.microsoft.com/fwlink/?LinkID=285288.

Implémentation de conversions P2V

La liste suivante résume certains éléments à prendre en compte lors des conversions P2V :



- Planification des ressources. Une des premières étapes de la planification d'une conversion P2V consiste à déterminer si le système ou l'application cible est pris(e) en charge pour la conversion P2V. Par exemple, nous vous déconseillons d'exécuter des migrations P2V pour les contrôleurs de domaine Active Directory, même si elles sont prises en charge si certaines conditions sont remplies.
- Avant de démarrer les conversions P2V, analysez les ressources d'ordinateur physique et leur utilisation actuelle. La boîte à outils MAP peut exécuter cette analyse et fournir un rapport de consolidation de serveurs. Planifiez les ressources d'ordinateur virtuel avec précaution. Voici certains éléments à prendre en compte pour les ressources :
    - Mémoire. Quelle quantité de mémoire est installée dans l'ordinateur physique, et quelle quantité est utilisée, en particulier pendant les heures de pointe ? Existe-t-il des applications exécutées sur l'ordinateur physique qui prennent en charge la mémoire dynamique ?
    - Processeur. Combien de processeurs l'ordinateur physique possède-t-il, quel est leur type et à quelle vitesse fonctionnent-ils ? Si vous passez d'un serveur équipé de l'ancien processeur double cœur de 3,8 gigahertz (GHz) à quatre sockets à un hôte Hyper-V doté d'un processeur quatre cœurs de 2,0 GHz à deux sockets, les performances seront-elles acceptables ? Veillez à tester les performances de vos systèmes, et idéalement, à déterminer une base de référence pour comprendre quels serveurs et applications peuvent accepter une baisse des performances au profit de la haute disponibilité et de la portabilité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

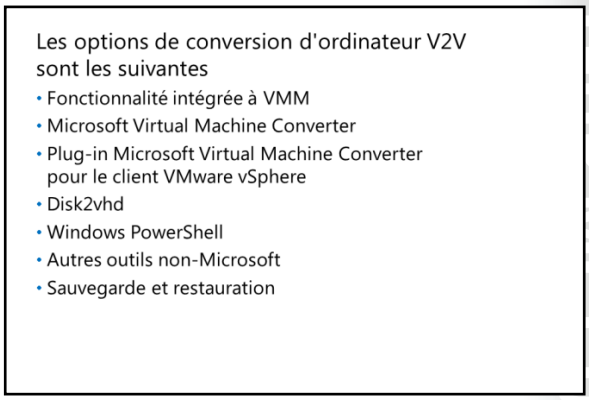
  - Réseau. Surveillez l'utilisation du réseau et vérifiez que les applications ne sont pas liées à une adresse MAC (Media Access Control) spécifique. Examinez les performances du réseau et assurez-vous que les nouveaux ordinateurs virtuels disposeront des ressources réseau adéquates. Prenez en compte le sous-réseau source et les sous-réseaux de destination, et vérifiez que leurs réseaux locaux virtuels (VLANs) sont en place.
  - Disques. Prenez en compte la capacité de vos serveurs actuels et planifiez leur croissance. Si vous disposez de rapports indiquant les tendances de croissance du stockage, cela vous aidera. Sinon, vous pouvez éventuellement examiner les tendances des données de sauvegarde pour prévoir la croissance du volume de données. Veillez à surveiller les E/S par seconde requises et vérifiez si le serveur hôte de destination fournit l'équivalent. Envisagez de limiter les ordinateurs virtuels si nécessaire.

- Planification de la migration. Prenez en compte le temps et l'impact des conversions P2V ; si vous effectuez plusieurs migrations, vérifiez que l'infrastructure sous-jacente peut simplifier les conversions que vous envisagez d'exécuter simultanément et que l'incidence sur les systèmes de production est minime voire inexistante. Effectuez des essais de migration sur des systèmes de test pour déterminer le délai moyen dont vous aurez besoin par migration, et incluez dans votre plan le temps de restauration. Vérifiez que votre système et votre application peuvent être testés avant que les utilisateurs aient besoin de se connecter. Il existe d'autres éléments à prendre en compte pour la planification de la migration :
  - Plan général. Tenez à jour un document ou une feuille de calcul contenant tout ce que vous devez savoir sur les applications ou les systèmes que vous migrez. Ces informations doivent comprendre l'adresse MAC, les propriétaires d'application et le numéro de téléphone du fournisseur de l'application ou du développeur.
  - Veillez à posséder un mot de passe d'administrateur local opérationnel et assurez-vous de disposer de tous les mots de passe d'application dont vous avez besoin. Si vous ne possédez pas les droits et les connaissances de l'administrateur réseau, assurez-vous qu'une personne répondant à ces critères soit disponible en cas de besoin.
  - Veillez à disposer de listes de contrôle de prémigration et de post-migration. Ajoutez-les aux listes et vérifiez-les par rapport à celles publiées en ligne et dans la documentation. Vérifiez tout ce qui pourrait vous conduire à la restauration d'un système.
  - Effectuez une sauvegarde de l'ordinateur que vous allez convertir. Veillez à disposer d'un plan de restauration. Vérifiez les travaux planifiés tels que les balayages antivirus et les sauvegardes, et coordonnez la migration convenablement.
  - Traitez en tant que service les applications distribuées qui couvrent plusieurs serveurs. Examinez l'incidence du déplacement d'un composant, puis essayez d'organiser les composants dans le plan de conversion. Prenez en compte la sélection élective. Par exemple, ne mettez pas une batterie complète de serveurs Web sur un même serveur. Utilisez les fonctionnalités de sélection élective intelligente et utilisez les options d'utilisation prévue lorsque cela est possible.
- Procédez au nettoyage. Nettoyez les données inutiles et défragmentez si possible. Cela permet de réduire la quantité de données déplacées du serveur physique source vers votre ordinateur virtuel cible et d'améliorer les performances du transfert de données.
- Arrêtez la source. Lorsque vous dupliquez un ordinateur, veillez à ne pas mettre en ligne simultanément les anciens ordinateurs et les nouveaux.

- Vérifiez l'analyse. Examinez le type d'analyse en place. Envisagez de publier les alertes sur le blocage pendant le processus de conversion. Par exemple, pensez à réactiver l'appel du mode de maintenance d'Operations Manager lorsque vous êtes prêt. Pensez à effectuer un suivi de l'utilisation pour la rétrofacturation, étant donné que les différents serveurs fonctionneront sur des hôtes consolidés. Votre direction peut souhaiter facturer un service ou une société en fonction du pourcentage d'utilisation des ressources.
- Impact sur l'hôte. Veillez à prévoir l'impact sur votre serveur hôte. Par exemple, il peut s'agir non seulement de l'impact de l'exécution des ordinateurs virtuels que vous migrez, mais également de l'incidence des balayages antivirus et des sauvegardes. Vont-ils être exécutés dans les temps, auront-ils un impact sur les autres invités ?
- Planification de la sauvegarde et de la récupération. Prenez en compte le mode de sauvegarde des systèmes physiques et veillez à planifier les sauvegardes en conséquence. Par exemple, vous pouvez désormais sauvegarder l'ordinateur virtuel à la fois en interne au niveau application du système d'exploitation, et en externe au niveau de l'ordinateur virtuel.
- Gestion des licences. Vérifiez que vous êtes à jour et en conformité avec les modifications en matière de gestion de licences qui peuvent être requises dans le cadre de la migration.
- Matériel non standard. Certaines applications requièrent un matériel personnalisé tel qu'un dongle. Si vous possédez un matériel personnalisé, vous devez contacter le fournisseur pour examiner la compatibilité et les solutions alternatives en matière de virtualisation.
- Résolution de noms. Prenez en compte l'examen de la résolution de noms et assurez-vous qu'AD DS fonctionne comme prévu avant de débuter une conversion.
- Prise en charge du fournisseur. Si nécessaire, confirmez que l'application exécutée sur l'ordinateur physique sera prise en charge dans un environnement virtualisé.

Conversions d'ordinateur V2V

VMM vous permet de convertir les ordinateurs virtuels VMware existants en ordinateurs virtuels qui s'exécutent sur la plateforme Hyper-V. Ce processus est appelé *conversion V2V*. Il permet aux administrateurs de consolider un environnement virtuel qui exécute différentes plateformes virtuelles sans avoir à déplacer les données ni à reconstruire les ordinateurs virtuels à partir de zéro.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

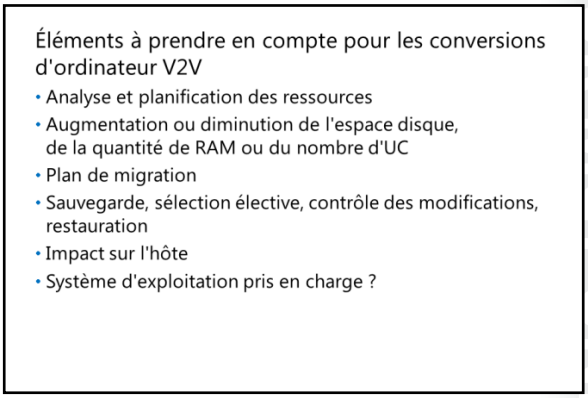
VMM permet de copier les ordinateurs virtuels VMware existants et de créer des ordinateurs virtuels Hyper-V. Vous pouvez copier les ordinateurs virtuels VMware qui sont situés sur des hôtes de serveur VMware ESX ou dans des bibliothèques Virtual Machine Manager. Même si V2V est appelé une conversion, V2V est une opération en lecture seule qui ne supprime ni n'affecte l'ordinateur virtuel source d'origine. En outre, le terme *conversion* désigne uniquement le processus de conversion d'ordinateurs virtuels VMware. Le terme *migration* est utilisé pour les serveurs virtuels. Pendant le processus de conversion, VMM convertit les fichiers VMware .vmdk en fichiers .vhd, et rend le système d'exploitation de l'ordinateur virtuel compatible avec les technologies de virtualisation de Microsoft. L'ordinateur virtuel que l'Assistant Conversion V2V VMM crée correspond aux propriétés de l'ordinateur virtuel VMware, y compris le nom, la description, la mémoire et les attributions disque-bus. Les autres outils ou méthodes pour la conversion V2V sont les suivants :

- Microsoft Virtual Machine Converter. Microsoft Virtual Machine Converter est un outil accélérateur de solution simple à utiliser, gratuit et autonome qui est mené par un Assistant. Cet outil effectue une copie de l'ordinateur virtuel source tout en laissant la source intacte.
- Plug-in Microsoft Virtual Machine Converter pour le client VMware vSphere. Le plug-in Microsoft Virtual Machine Converter pour le client VMware vSphere enrichit le menu contextuel du client vSphere pour faciliter la conversion de l'ordinateur virtuel VMware en ordinateur virtuel basé sur Hyper-V.
- Disk2vhd, outils dédiés non-Microsoft, sauvegarde et technologies de mise en miroir. Disk2vhd (qui a été présenté dans une leçon précédente) fonctionnera, mais peut nécessiter des pilotes et des modifications sur l'ordinateur source pour qu'il démarre avec succès. D'autres outils non-Microsoft sont également susceptibles de fonctionner avec différents degrés d'intervention manuelle.

Liens de référence : Pour plus d'informations sur Microsoft Virtual Machine Converter, accédez à http://go.microsoft.com/fwlink/?LinkID=285296.

Éléments à prendre en compte pour les conversions V2V

Bon nombre des éléments à prendre en compte qui s'appliquent à P2V s'appliquent également à V2V. Les principales différences sont que le serveur source est déjà virtualisé. Vous avez donc une idée précise des tendances de performances et pouvez planifier l'accueil de l'ordinateur virtuel de façon appropriée.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Voici quelques éléments à prendre en compte pour les conversions V2V :

- Vérifiez que le système d'exploitation, y compris le niveau de correctif, est pris en charge par l'outil utilisé pour le processus de conversion et que Hyper-V prend en charge le système d'exploitation source. Assurez-vous que toutes les conditions préalables sont remplies.
- Si la conversion V2V est effectuée pour résoudre un problème de performances, assurez-vous que ce problème est lié aux ressources, et non à la configuration.
- Pour les ordinateurs virtuels s'exécutant sur d'autres hyperviseurs, utilisez l'Assistant Conversion P2V VMM.
- Utilisez MAP pour définir en référence les ordinateurs virtuels existants, puis réduisez ou augmentez leur taille en fonction des besoins.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et implémentation d'une stratégie de déploiement et de gestion d'ordinateurs virtuels

Scénario

Maintenant que la société A. Datum Corporation a implémenté les composants d'hôte, de stockage et réseau de l'infrastructure de virtualisation, l'étape suivante consiste à planifier et implémenter le déploiement d'ordinateurs virtuels.

L'un des principaux objectifs du projet de déploiement est de virtualiser autant de serveurs que possible. Dans le cadre de la planification de la virtualisation, vous devez déterminer quels serveurs sont candidats à la virtualisation, notamment les serveurs physiques que vous pouvez convertir en ordinateurs virtuels. Vous devez également planifier la stratégie de déploiement et de gestion des ordinateurs virtuels pour simplifier et standardiser le déploiement.

Objectifs

- Planifier des conversions de serveur P2V.
- Planifier des ordinateurs virtuels et des modèles de service.
- Configurer des profils et des modèles VMM.
- Déployer des ordinateurs virtuels à l'aide de modèles VMM.

Configuration de l’atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22414B-LON-DC1 22414B-LON-VMM1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible. Vérifiez que **22414B-LON-DC1** et **22414B-LON-VMM1** sont exécutés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Planification des conversions de serveurs P2V (physical-to-virtual)

Scénario

Une des exigences de projet chez A. Datum est de convertir autant de serveurs physiques que possible en ordinateurs virtuels. Vous devez créer une liste prioritaire qui détermine quels serveurs physiques doivent être convertis en ordinateurs virtuels. Vous devez également identifier les éléments à prendre en compte pour implémenter des conversions P2V.

Stratégie de virtualisation de serveur	
Numéro de référence du document : BS0905/1	
Auteur du document Date	Brad Sutton 12 septembre

Présentation des exigences :

Planifiez une stratégie de consolidation et de conversion de serveurs pour qu'elle réponde aux objectifs suivants :

- Analysez les serveurs actuels et indiquez la procédure à suivre pour que l'équipe chargée du contrôle des modifications et des risques autorise la migration.
- Migrez les serveurs physiques vers de nouveaux hôtes de virtualisation en utilisant les outils de conversion lorsque cela est possible.

Informations supplémentaires

- Vous possédez sept nouveaux hôtes Windows Server 2012 Hyper-V, chacun disposant de 96 Go de RAM et de 2 processeurs à 6 cœurs. Un administrateur de stockage a fourni le stockage et examiné les E/S par seconde et vous a confirmé que vous n'avez aucun souci de stockage ou de capacité. Vous disposez d'un cluster à trois nœuds dans le réseau de périmètre et d'un cluster à quatre nœuds pour les serveurs internes. Vous ne possédez pas d'hôte de maintenance.

Propositions

1. Tous les serveurs peuvent-ils être convertis en utilisant le processus de conversion P2V intégré à VMM ?
2. Comment accélérer le processus de conversion ? Par exemple, existe-t-il des serveurs que vous pouvez convertir en exécutant des scripts ? Si oui, lesquels ?
3. Comment pouvez-vous distribuer les serveurs ?
4. Étant donné que vous ne disposez pas d'hôte de maintenance, quel plan pouvez-vous utiliser pour importer les serveurs physiques ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Services et rôles :

Nom du serveur	Rôles installés	Utilisation du processeur	Processeurs et cœurs	Version du système d'exploitation Windows	Mémoire/ utilisation
Siège social					
LON-EX1	Exchange Server 2010 : Accès au client et transport Hub	75%	Deux processeurs double cœur	2008 Entreprise Service Pack 2 (SP2)	8 Go/4 Go
LON-EX2	Exchange Server 2010 : Boîte de réception	75%	Deux processeurs double cœur	2008 Entreprise SP2	8 Go/6 Go
LON-EX3	Exchange Server 2010 : Boîte de réception	75%	Deux processeurs double cœur	2008 Entreprise SP2	8 Go/6 Go
LON-SQL1a LON-SQL1b	SQL Server (en cluster)	80%	Deux processeurs quatre cœurs	2003/Enterprise /SP 2	16 Go/ 10 Go
LON-SQLD1	SQL Server (développement)	20%	Un processeur quatre cœurs	2008 R2 Standard SP1	8 Go/6 Go
LON-WEBD1	IIS, développement	15%	Un processeur double cœur	2008 R2 Standard SP1	4 Go/2 Go
LON-CA	Services de certificats Active Directory (AD CS) : Autorité de certification racine d'entreprise (CA)	25%	Un processeur double cœur	2008 Standard SP2	8 Go/2 Go
LON-DC1	AD DS	60%	Un processeur double cœur	2008 Standard SP2	8 Go/3 Go
LON-DC2	AD DS	60%	Un processeur double cœur	2008 Standard SP2	8 Go/3 Go

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Nom du serveur	Rôles installés	Utilisation du processeur	Processeurs et cœurs	Version du système d'exploitation Windows	Mémoire/ utilisation
LON-DC3	AD DS	60%	Un processeur double cœur	2008 Standard SP2	8 Go/3 Go
LON-INF1	Protocole DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System)	50%	Deux processeurs double cœur	2008 Standard SP2	4 Go/2 Go
LON-INF2	DHCP, DNS	50%	Deux processeurs double cœur	2008 Standard SP2	4 Go/2 Go
Réseau de périmètre					
LON-PER-NS1	DNS	25%	Deux processeurs double cœur	2003 R2 SP3	4 Go/1 Go
LON-PER-NS2	DNS	25%	Deux processeurs double cœur	2003 R2 SP3	4 Go/1 Go
LON-RADIUS	Serveur NPS (Network Policy Server)	35%	Deux processeurs double cœur	2008 R2 SP1	4 Go/2 Go
LON-WEB1 LON-WEB2 LON-WEB3 LON-WEB4 LON-WEB5 LON-WEB6 LON-WEB7 LON-WEB8	IIS	75%	Deux processeurs double cœur	2008 R2 Standard SP1	8 Go/5 Go
LON-VPN1 LON-VPN2	Service de routage et d'accès à distance	25%	Deux processeurs double cœur	2000 Server Service Pack 4 (SP4)	4 Go/2 Go
LON-EX-EDGE1	Serveur de transport Edge Exchange Server 2010	40%	Deux processeurs quatre cœurs	2008 Entreprise SP2	8 Go/4 Go

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Lire la documentation fournie avec le produit.
2. Mettre à jour le document de proposition en fonction du plan d'action planifié.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.
4. Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur.

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation et le scénario fournis.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

- Répondez aux questions de la section Propositions du document Stratégie de virtualisation.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions avec celles du corrigé de l'atelier pratique.

▶ Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Préparez-vous à discuter de vos propositions avec la classe.

Résultats : À la fin de cet exercice, vous devriez avoir examiné et planifié la virtualisation et la consolidation.

Exercice 2 : Planification des modèles d'ordinateurs virtuels et de services

Scénario

Pour simplifier le déploiement des ordinateurs virtuels chez A. Datum, vous devez concevoir des modèles d'ordinateur virtuel et de service qui peuvent être utilisés pour déployer ces ordinateurs virtuels. Ces modèles devraient simplifier les déploiements d'ordinateur virtuel les plus courants chez A. Datum. Vous pouvez également souhaiter utiliser une plage des profils. Initialement, vous allez travailler avec l'équipe de développement de Toronto, qui transfère l'administration sur ses hôtes de virtualisation du développement. Elle a fourni un exemple de configuration basé sur une configuration courante de ses ateliers de développement.

Document de référence des modèles de services de développement	
Numéro de référence du document : BS0906/1	
Auteur du document Date	Brad Sutton 14 septembre
Présentation des exigences Planifier des modèles et des profils pour les objectifs de virtualisation des équipes de développement : • Planifier les détails d'un service de déploiement rapide pour les développeurs qui redéploient fréquemment des ordinateurs virtuels pour les systèmes d'exploitation serveur et clients.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Document de référence des modèles de services de développement
Tâches et questions 1. Renseignez certains des éléments de profil ci-après pour aider à créer le modèle de service de développement. 2. De combien de profils matériels, de profils de système d'exploitation invité et de profils SQL Server avez-vous besoin ? 3. Devez-vous utiliser des modèles de services ou d'ordinateurs virtuels existants ?

Bureau de Toronto					
Nom du serveur	**Rôles installés**	**Utilisation du processeur**	**Processeurs et cœurs**	**Version du système d'exploitation Windows**	**Mémoire/ utilisation**
TOR-DDC1	AD DS	15%	Un processeur double cœur	2008 R2 Standard SP1	2 Go/1 Go
TOR-SQLD1	SQL Server 2008 R2 Reporting Services Analysis Services	25%	Un processeur quatre cœurs	2008 R2 Standard SP1	6 Go/5 Go
TOR-WEBD1	IIS	15%	Un processeur double cœur	2008 Entreprise SP2	4 Go/2 Go
TOR-CLD1	N/A	80%	Un processeur double cœur	Windows XP SP3	2 Go/1 Go
TOR-CLD2	N/A	20%	Un processeur quatre cœurs	Windows 7 SP1	4 Go/2 Go

Exemple :

Profil matériel		
Option/paramètre	**Valeur**	**Valeur supplémentaire**
Nom	SQL Server	
Description	Exemple de serveur de développement	
Capacité	Hyper-V	XenServer
Processeur virtuel	2	
Mémoire	2.048	Statique

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Profil matériel		
Option/paramètre	**Valeur**	**Valeur supplémentaire**
Nom		
Description		
Capacité		
Processeur virtuel		
Mémoire		

Profil matériel		
Option/paramètre	**Valeur**	**Valeur supplémentaire**
Nom		
Description		
Capacité		
Processeur virtuel		
Mémoire		

Profil matériel		
Option/paramètre	**Valeur**	**Valeur supplémentaire**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Profil matériel		
Option/paramètre	**Valeur**	**Valeur supplémentaire**

Profil de système d'exploitation invité		
Option/paramètre	**Valeur**	**Valeur supplémentaire**
Nom	Serveurs SQL de développement (WS2008R2SP1)	
Description	MSDN Windows 2008 R2	
Nom de l'ordinateur	TOR-SQLD#	
Mot de passe administrateur	Pa$$w0rd	
Clé du produit	XXXX-XXXX-XXXX-XXXX-XXXX	
Système d'exploitation	Édition 64 bits de Windows Server 2008 R2 Standard	
Rôles		
Fonctionnalités	Microsoft .NET Framework 3.5.1	
Domaine/groupe de travail	Adatum.com	
Utilisateur du domaine/mot de passe	ADATUM\Administrateur	Pa$$w0rd

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Profils de systèmes d'exploitation invités		
Option/paramètre	**Valeur**	**Valeur supplémentaire**
Nom		
Description		
Nom de l'ordinateur		
Mot de passe administrateur		
Clé du produit		
Système d'exploitation		
Rôles		
Fonctionnalités		
Domaine/groupe de travail		
Utilisateur du domaine/ mot de passe		

Profils de systèmes d'exploitation invités		
Option/paramètre	**Valeur**	**Valeur supplémentaire**
Nom		
Description		
Nom de l'ordinateur		
Mot de passe administrateur		
Clé du produit		
Système d'exploitation		
Rôles		
Fonctionnalités		
Domaine/groupe de travail		
Utilisateur du domaine/mot de passe		

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Profil SQL Server		
Option/paramètre	**Option/paramètre**	**Option/paramètre**
Nom		
Description		
Nom de déploiement SQL Server		
Nom de l'instance		
ID de l'instance		
ID de produit		
Exécuter en tant que		
Source du média		
Administrateurs		
Mode de sécurité		
Administrateur système		
TCP/IP / Canaux nommés		
Comptes de service		

Les tâches principales de cet exercice sont les suivantes :

1. Lire la documentation fournie avec le produit.
2. Mettre à jour le document de proposition en fonction du plan d'action planifié.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.
4. Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur.

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation et le scénario fournis.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

- Répondez aux questions de la section Propositions du document de référence des modèles de services de développement.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions avec celles du corrigé de l'atelier pratique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Préparez-vous à discuter de vos propositions avec la classe.

Résultats : À la fin de cet exercice, vous devriez avoir planifié un modèle de service de base basé sur l'infrastructure existante.

Exercice 3 : Configuration des profils et des modèles VMM

Scénario

Maintenant que vous avez terminé la conception des profils et des modèles VMM, vous allez implémenter une partie de la solution. Selon la conception de ces modèles et de ces profils, vous allez créer un profil de système d'exploitation invité, un profil matériel et un profil SQL Server. Ensuite, vous allez créer un ordinateur virtuel et un modèle de service.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer un profil de système d'exploitation invité.
2. Configurer un profil matériel.
3. Configurer un profil SQL Server.
4. Configurer un modèle d'ordinateur virtuel.
5. Configurer un modèle de service.

▶ Tâche 1 : Configurer un profil de système d'exploitation invité

Configurer un profil de système d'exploitation invité

(Remarque : si nécessaire, effectuez les étapes 1 et 2 pour démarrer la console VMM)

1. Sur LON-VMM1, dans la barre de tâches, cliquez sur **Console Virtual Machine Manager**.
2. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session Microsoft Windows** est activée, puis cliquez sur **Connecter**. La console VMM s'ouvre.
3. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Profils**, puis cliquez sur **Profils de système d'exploitation invité**.
4. Dans le ruban, cliquez sur **Créer**, puis sur **Profil de système d'exploitation invité**.
5. Dans la boîte de dialogue **Nouveau profil de système d'exploitation invité**, dans la page **Général**, configurez les paramètres suivants :
   - Nom : **Profil de système d'exploitation TOR-WEB**
   - Description : **Profil de système d'exploitation invité du nouveau serveur Web de développement**
6. Cliquez sur **Profil de système d'exploitation invité**.
7. Dans la page **Profil de système d'exploitation invité**, sous **Paramètres généraux**, cliquez sur **Informations d'identité**.
8. Dans la zone de texte **Nom de l'ordinateur**, tapez **TOR-WEB#**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Cliquez sur **Mot de passe de l'administrateur**, puis sur **Spécifier le mot de passe du compte d'administrateur local**. Dans les zones de texte **Mot de passe** et **Confirmer**, tapez **Pa$$w0rd**.
10. Cliquez sur **Clé du produit**, puis dans la zone **Clé du produit**, tapez **XC9B7-NBPP2-83J2H-RHMBY-92BT4**.
11. Cliquez sur **Système d'exploitation**, puis vérifiez que **64-bit edition of Windows Server 2012 Standard** (Édition 64 bits de Windows Server 2012 Standard) est sélectionné.
12. Sous **Mise en réseau**, cliquez sur **Domaine / groupe de travail**.
13. Cliquez sur **Domaine**, puis dans la zone de texte **Domaine**, tapez **adatum.com**.
14. Sous **Informations d'identification du domaine**, cliquez sur **Spécifiez les informations d'identification à utiliser pour joindre le domaine**.
15. Dans la zone de texte **Utilisateur du domaine**, tapez **ADATUM\Administrateur**. Dans les zones de texte **Mot de passe** et **Confirmer**, tapez **Pa$$w0rd**.
16. Cliquez sur **OK** pour fermer la boîte de dialogue **Nouveau profil de système d'exploitation invité**.

▶ Tâche 2 : Configurer un profil matériel

Configurer un profil matériel

1. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Profils**, puis cliquez sur **Profils matériels**.
2. Dans le ruban, cliquez sur **Créer**, puis sur **Profil matériel**.
3. Dans la boîte de dialogue **Nouveau profil matériel**, dans la page **Général**, configurez les paramètres suivants :
   - Nom : **WsStd2012**
   - Description : **Profil matériel pour les nouveaux serveurs Windows Server 2012**
4. Cliquez sur **Profil matériel**.
5. Dans la page **Profil matériel**, sous **Compatibilité**, cliquez sur **Profils de capacité du cloud**.
6. Activez la case à cocher **Hyper-V**.
7. Dans la section **Général**, cliquez sur **Processeur**, puis activez la case à cocher **Autoriser la migration vers un ordinateur hôte d'ordinateur virtuel avec une version de processeur différente**.
8. Cliquez sur **Mémoire**, vérifiez que **Statique** est sélectionné, puis modifiez l'option **Mémoire de l'ordinateur virtuel** sur **1024 Mo**.
9. Dans la section Cartes réseau, cliquez sur **Carte réseau 1**. Sous **Connectivité**, cliquez sur **Connecté à un réseau d'ordinateurs virtuels**, puis sélectionnez **Réseau externe**.
10. Cliquez sur **OK** pour fermer la boîte de dialogue **Nouveau profil matériel**. Le nouveau profil s'affiche dans le volet de résultats.

▶ Tâche 3 : Configurer un profil SQL Server

Configurer un profil SQL Server

1. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Profils**, puis cliquez sur **Profils SQL Server**.
2. Dans le ruban, cliquez sur **Créer**, puis sur **Profil SQL Server**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la boîte de dialogue **Nouveau profil SQL Server**, dans la page **Général**, configurez les paramètres suivants :
   - Nom : **SQLDev1**
   - Description : **Modèle pour les nouveaux serveurs SQL**
4. Cliquez sur **Configuration de SQL Server**.
5. Dans la page **Configuration de SQL Server**, en regard de **Ajouter**, cliquez sur **Déploiement de SQL Server**. Un nouveau déploiement sur SQL Server est ajouté au modèle.
6. Configurez les paramètres suivants :
   - Dans le champ **Nom**, tapez **SQLDev1**.
   - Dans le champ Nom de l'instance, tapez **MSSQLSERVER**.
   - Dans le champ ID de l'instance, tapez **DefaultInstance**.
7. Sous **Compte d'identification de l'installation**, cliquez sur **Parcourir**. Dans la boîte de dialogue **Parcourir les comptes d'identification**, cliquez sur **Administrateur**, puis sur **OK**.
8. Cliquez sur **Configuration**.
9. Dans la zone de texte **Source du média**, tapez **C:\SQLInstall**.
10. Dans la zone Administrateurs SQL Server, tapez **ADATUM\Administrateur**, puis cliquez sur **Ajouter**.
11. En regard de **Mode de sécurité**, vérifiez qu'**Authentification Windows** est sélectionné.
12. Activez la case à cocher **Utiliser TCP\IP pour activer les connexions distantes**.
13. Cliquez sur **Comptes de service**.
14. Sous **Compte d'identification du service SQL Server**, cliquez sur **Parcourir**.
15. Dans la boîte de dialogue **Parcourir les comptes d'identification**, cliquez sur **Administrateur**, puis sur **OK**.
16. Sous **Compte d'identification du service SQL Server**, cliquez sur **Parcourir**.
17. Dans la boîte de dialogue **Parcourir les comptes d'identification**, cliquez sur **Administrateur**, puis sur **OK**.
18. Sous **Compte d'identification des services de création de rapports**, cliquez sur **Parcourir**.
19. Dans la boîte de dialogue **Parcourir les comptes d'identification**, cliquez sur **Administrateur**, puis sur **OK**.
20. Cliquez sur **OK** pour fermer la boîte de dialogue **Nouveau profil SQL Server**.

▶ Tâche 4 : Configurer un modèle d'ordinateur virtuel

Configurer un modèle d'ordinateur virtuel

1. Sur LON-VMM1, ouvrez l'Explorateur de fichiers.
2. Dans la barre d'adresses, tapez **\\LON-HOST1\e$\Program Files\Microsoft Learning\Base**, puis appuyez sur Entrée.
3. Cliquez avec le bouton droit sur le fichier **Base12A-WS12-TMP_FR.vhd**, puis cliquez sur **Copier**.
4. Dans la barre d'adresses, tapez **\\lon-vmm1\MSSCVMMLibrary\vhds**, puis appuyez sur Entrée. Dans une zone vide, cliquez avec le bouton droit de la souris, puis cliquez sur **Coller**. Le processus de copie du fichier prend quelques minutes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Serveurs de bibliothèque\LON-VMM1.Adatum.com\MSSCVMMLibrary**, puis cliquez sur **VHDs**.
6. Vérifiez que la copie du fichier est terminée, cliquez avec le bouton droit sur **VHDs**, puis cliquez sur **Actualiser**.
7. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Modèles**, puis cliquez sur **Modèles d'ordinateur virtuel**.
8. Dans le ruban, cliquez sur **Créer un modèle d'ordinateur virtuel**.
9. Dans l'Assistant Créer un modèle d'ordinateur virtuel, dans la page **Sélectionner une source**, cliquez sur **Utiliser un modèle d'ordinateur virtuel existant ou un disque dur virtuel stocké dans la bibliothèque**, puis sur **Parcourir**.
10. Dans la boîte de dialogue **Sélectionner la source du modèle d'ordinateur virtuel**, cliquez sur Base12A-WS12-TMP_FR.vhd, puis sur **OK**.
11. Dans la page **Sélectionner une source**, cliquez sur **Suivant**.
12. Dans la page **Identité du modèle d'ordinateur virtuel**, configurez les options suivantes, puis cliquez sur **Suivant** :
    - Nom du modèle d'ordinateur virtuel : **Serveur d'applications Web ADATUM**
    - Description : **Serveur Web hébergeant l'application Web ADATUM**
13. Dans la page **Configurer le matériel**, dans la zone de liste déroulante **Profil matériel**, cliquez sur **WsStd2012**. Notez que les paramètres du profil matériel sont importés dans le modèle. Cliquez sur **Suivant**.
14. Dans la page Configurer le système d'exploitation, dans la zone de liste déroulante Profil de système d'exploitation invité, cliquez sur Profil de système d'exploitation TOR-WEB.
15. Sous **Rôles et fonctions**, cliquez sur **Rôles**.
16. Activez la case à cocher **Serveur Web (IIS)**, puis cliquez sur **Suivant**.
17. Dans la page **Configurer les applications**, dans la zone de liste déroulante **Profil d'application**, cliquez sur **Aucune – n'installer aucune application**, puis sur **Suivant**.
18. Dans la page **Configurer SQL Server**, dans la zone de liste déroulante **Profil SQL Server**, cliquez sur **Aucun - aucun paramètre de configuration SQL Server**, puis sur **Suivant**.
19. Dans la page **Résumé**, cliquez sur **Créer**.

▶ Tâche 5 : Configurer un modèle de service

Configurer un modèle de service

1. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Modèles**, puis cliquez sur **Modèles de service**.
2. Créez un modèle de service nommé **Service Web ADATUM** et affectez le **Serveur d'applications Web ADATUM** à la couche Application.
3. Enregistrez et validez le modèle de service.

Résultats : À la fin de cet exercice, vous devriez avoir configuré les profils et les modèles VMM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 4 : Déploiement d'ordinateurs virtuels à l'aide de modèles VMM

Scénario

Dans cet exercice, vous allez déployer un service en utilisant un modèle d'ordinateur virtuel.

Les tâches principales de cet exercice sont les suivantes :

1. Déployer des ordinateurs virtuels à l'aide du modèle de service.

▶ Tâche 1 : Déployer des ordinateurs virtuels à l'aide du modèle de service

Déployer des ordinateurs virtuels à l'aide du modèle de service

1. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Modèles**, puis cliquez sur **Modèles de service**.
2. Cliquez avec le bouton droit sur **Service Web ADATUM**, puis cliquez sur **Configurer le déploiement**.
3. Dans la boîte de dialogue **Sélectionner le nom et la destination**, dans la zone de texte **Nom**, tapez **Service Web ADATUM**, puis cliquez sur **OK**.
4. Dans la fenêtre Déployer le service - Service Web ADATUM, vérifiez que la couche a été placée sur un hôte. Vous devrez peut-être cliquer sur **Actualiser l'aperçu** pour mettre à jour les résultats.
5. Dans la fenêtre Déployer le service - Service Web ADATUM, dans le ruban, cliquez sur **Déployer le service**.
6. Dans la boîte de dialogue **Déployer le service**, cliquez sur **Déployer**. Dans quelques minutes, la fenêtre Travaux s'ouvrira.
7. Analysez le déploiement du service à l'aide de la fenêtre Travaux. Le déploiement du service durera approximativement 10 minutes.
8. Une fois le service déployé, cliquez sur l'espace de travail **Ordinateurs virtuels et services**.
9. Dans le ruban, cliquez sur **Services**.
10. Dans le volet de résultats, cliquez avec le bouton droit sur **Service Web ADATUM**, puis cliquez sur **Arrêt**.

▶ Pour préparer le module suivant

- N'éteignez pas les ordinateurs virtuels, car vous en aurez besoin pour le module suivant.

Résultats : À la fin de cet exercice, vous devriez avoir déployé un service de couche en utilisant un modèle d'ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

Comme pour la plupart des projets informatiques, un contrôle approprié de la planification et des modifications contribuera au succès global pendant la virtualisation. L'analyse des performances et des ressources est une partie essentielle de la gestion de l'infrastructure de virtualisation. Par conséquent, une partie de votre stratégie d'implémentation et de conversion doit inclure ces tâches pour que vous puissiez maintenir les niveaux de performances et éviter des scénarios où les performances baissent.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Impossibilité d'effectuer une conversion P2V à CSV sur VMM si l'espace disque est insuffisant sur le lecteur local	

Outils

Pour plus d'informations sur Virtual Machine Servicing Tool 2012 et pour télécharger cet outil, accédez à http://go.microsoft.com/fwlink/?LinkID=285295.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 5

Planification et implémentation d'une solution d'administration de la virtualisation

Table des matières :

Vue d'ensemble du module **5-1**

Leçon 1 : Planification et implémentation de l'automatisation de System Center 2012 **5-2**

Leçon 2 : Planification et implémentation de l'administration de System Center 2012 **5-10**

Leçon 3 : Planification et implémentation des options de libre-service dans System Center 2012 **5-17**

Atelier pratique : Planification et implémentation d'une solution d'administration pour la virtualisation **5-24**

Contrôle des acquis et éléments à retenir **5-36**

Vue d'ensemble du module

Ce module vous préparera à concevoir un modèle d'administration que vous pouvez utiliser pour gérer la virtualisation à l'aide de Microsoft® System Center 2012. Vous verrez et utiliserez les composants de System Center 2012, y compris Microsoft System Center 2012 – Virtual Machine Manager (VMM), Microsoft System Center 2012 – Orchestrator et Microsoft System Center 2012 – App Controller. Utilisez ces composants pour déléguer des fonctions d'administration, planifier le libre-service de base, concevoir et implémenter l'automatisation. Les compétences acquises dans ce module sont le fondement des blocs de construction de base utilisés pour faire fonctionner une infrastructure de technologie de l'information (IT) qui est semblable ou équivalente à celle du cloud computing.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- planifier l'automatisation d'un environnement d'ordinateur virtuel à l'aide de l'intégration d'Orchestrator et de System Center 2012 ;
- planifier un modèle d'administration délégué à l'aide de VMM ;
- planifier le libre-service dans un environnement d'ordinateur virtuel avec VMM et App Controller.

Leçon 1
Planification et implémentation de l'automatisation de System Center 2012

Cette leçon fournit une vue d'ensemble générale des options d'automatisation des flux de travail administratifs de System Center 2012 pour la virtualisation.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- expliquer les options globales d'automatisation de la gestion de la virtualisation à l'aide de System Center 2012.
- comprendre les avantages de l'intégration des composants de System Center, en particulier de VMM et d'Orchestrator.

Conception de l'automatisation dans System Center 2012

Lorsque vous pensez à l'automatisation, vous pensez probablement à la réduction des charges de travail et à la suppression des tâches répétitives. Cependant, l'automatisation des processus peut également améliorer la vitesse de la fourniture de services et fournir un résultat plus fiable et plus cohérent en supprimant ou en limitant le risque d'erreurs humaines.

Si vous envisagez d'automatiser les processus, vous devez tenir compte des éléments suivants

- La sécurité, et si vous souhaitez utiliser l'accès basé sur les rôles, et vérifiez que vous pouvez auditer les activités en fonction de vos exigences métier
- Planifications, et comment et quand l'automatisation doit fonctionner
- L'infrastructure, et la planification des besoins tels que la réservation des pools d'adresses IP, en vérifiant que l'espace disque adéquat est disponible dans les réseaux SAN pour améliorer les services ou les ordinateurs virtuels
- Les processus métier, identifiez les participants et configurez-les en conséquence dans les flux de travail d'approbation et de notification
- L'utilisation des applets de commande Windows PowerShell dans les scénarios où les activités ne répondent pas aux besoins des flux de travail
- L'utilisation des quotas pour contrôler l'allocation des ressources
- Le déploiement des runbooks les plus rentables en premier

Orchestrator est le composant principal que vous pouvez utiliser pour concevoir l'automatisation dans votre centre de données. Vous pouvez également l'utiliser pour automatiser les processus métier et système.

Voici un exemple de processus orienté vers la virtualisation qui est adapté à l'automatisation :

1. Un utilisateur formule une demande de nouvel ordinateur virtuel au service technique.
2. L'équipe du service technique vérifie les informations sur les ressources, émet un ticket, puis envoie un message électronique au responsable informatique pour l'approbation du coût.
3. L'équipe du service technique reçoit l'approbation du responsable informatique, puis met à jour le ticket et l'assigne à un administrateur système.
4. L'administrateur système crée l'ordinateur virtuel, puis envoie une demande à l'équipe de contrôle des modifications pour l'approbation de la connexion au réseau d'entreprise.
5. L'administrateur système reçoit l'approbation de l'équipe de contrôle des modifications, puis termine le déploiement et contacte l'utilisateur pour vérifier que la demande a bien été satisfaite.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. L'utilisateur confirme que l'ordinateur virtuel fonctionne correctement, mais souhaite vérifier si l'ordinateur virtuel est sauvegardé et analysé.
7. L'administrateur système renvoie le ticket à l'équipe du service technique, qui envoie ensuite un autre message électronique au responsable informatique pour l'approbation du coût.
8. L'équipe du service technique reçoit l'approbation du responsable informatique, puis la transmet aux équipes chargées des opérations pour déployer l'agent d'analyse et l'agent de sauvegarde.
9. Le service technique confirme à l'utilisateur que le ticket peut être fermé.

Vous pouvez automatiser ces étapes et les fournir sous la forme d'une offre de libre-service. Microsoft System Center 2012 - Service Manager vous permettra de créer des formulaires et des processus qui peuvent avertir les personnes appropriées cherchant à obtenir une approbation, et de gérer le processus complet de façon automatisée. La meilleure solution consiste à approuver au préalable certains types de déploiements pour que System Center 2012 puisse apporter ce que l'utilisateur demande. System Center 2012 avertit ensuite les équipes appropriées qu'il existe un nouvel ordinateur virtuel, que l'ordinateur virtuel a été livré, et qu'il analyse et protège l'ordinateur virtuel. Les formulaires visibles par l'utilisateur final peuvent contenir des informations sur les coûts et inviter les utilisateurs finaux à sélectionner des sauvegardes et des services d'analyse.

Meilleures pratiques pour la conception de runbooks

Les runbooks constituent une collection de routines et de procédures conçues pour que les administrateurs ou les opérateurs les utilisent dans la surveillance des systèmes informatiques, de l'infrastructure réseau et des applications. Ils peuvent être physiques sous la forme de livre ou dans le cas d'Orchestrator de type logiciel.

Lors de la conception d'un runbook, vous devez documenter le processus et connaître les étapes nécessaires pour le créer. Prenez en compte les données nécessaires pour le démarrage du flux de travail, ainsi que celles nécessaires par chaque activité du runbook. Pensez à la façon dont vous gérerez les erreurs et à la façon dont votre résultat final se présentera. Essayez de pas faire en sorte que le runbook soit trop grand ou trop compliqué. Coloriez et nommez les liens, puis nommez les activités et les liens avec des descriptions correspondant à leur finalité.

La liste suivante répertorie d'autres éléments à prendre en compte pour l'automatisation des processus de System Center 2012 :

- Sécurité. Documentez les autorisations requises par l'automatisation. En outre, posez plusieurs questions, y compris : qui va créer les runbooks et qui va les modifier ? Qui va les exécuter ? Qui va auditer ce qui a été exécuté et quelles sont les autorisations dont l'auditeur a besoin ?
- Planifications. Vous pouvez automatiser de nombreuses tâches répétitives, telles que les tâches opérationnelles quotidiennes. L'automatisation peut être bénéfique à de nombreuses équipes, à vous de voir si vos processus manuels actuels s'adaptent au modèle d'automatisation et comment déterminer si vous pouvez tirer parti de l'automatisation. Par exemple, une tâche manuelle de 20 minutes peut devenir une tâche manuelle de deux minutes, ce qui est évidemment un grand avantage.
- Infrastructure. Songez aux tâches que vous pouvez automatiser, puis rassemblez les informations nécessaires pour les implémenter manuellement. Vous pouvez ensuite voir comment vous pouvez automatiser et approuver au préalable ce processus. Par exemple, vous pouvez obtenir la liste des adresses IP dont l'utilisation peut-être approuvée au préalable.
- Processus métier. Déterminez le responsable de l'approbation des déploiements et des coûts, puis tentez d'obtenir l'approbation au préalable pour que l'automatisation puisse se produire. Vous devez ensuite déterminer la personne à prévenir en matière de déploiements.

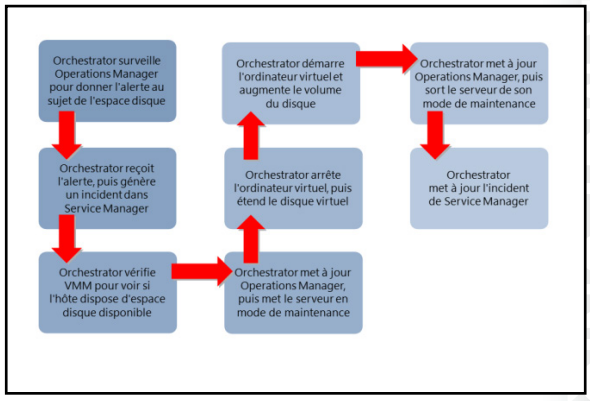
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Intégration. Intégrez les composants de System Center 2012 et passez en revue les avantages des packs d'intégration. Utilisez les exemples de runbooks et le Cloud Services Process Pack qui proposent de nombreuses offres par défaut que vous pouvez personnaliser.
- Windows PowerShell®. Si les activités requises n'existent pas pour les runbooks d'automatisation, vous devez déployer un service tiers et vous pourrez tirer parti des scripts Windows PowerShell dans les runbooks.
- Quotas. Si vous disposez d'offres de libre-service, vous devez placer des quotas à des niveaux raisonnables, puis analyser la capacité et récupérer les ressources inutilisées.
- Performances. Prenez en compte le nombre et la fréquence des tâches d'automatisation en cours d'exécution. Par exemple, si vous disposez de 50 runbooks qui analysent différents événements, quel est l'impact sur les performances sur le serveur Runbook Server et sur chacun des serveurs que vous automatisez ? Pour le serveur que vous manipulez, prenez en compte le passage d'un processus manuel à un processus automatisé, car l'automatisation peut se comporter différemment.
- Liste de processus. Créez une liste de candidats potentiels à l'automatisation, puis prenez en compte le temps, l'effort et la complexité de chacun. Essayez de trier la liste pour que le meilleur retour sur investissement se trouve au début, puis déterminez la durée d'une tâche et son coût.
- Coûts. Si l'automatisation des processus est une nouveauté pour votre organisation, vous possédez probablement une liste de possibilités en matière d'automatisation. Prenez en compte le coût de création de chacune par rapport au retour sur investissement, ce qui peut vous aider à hiérarchiser les runbooks à créer en premier.

Liens de référence :

- Pour plus d'informations sur la mise en route d'Orchestrator, accédez à la page http://go.microsoft.com/fwlink/?LinkID=285301.
- Afin d'obtenir des exemples de runbooks pour les composants de System Center 2012, accédez à la page http://go.microsoft.com/fwlink/?LinkID=285297.

Automatisation de la gestion de la virtualisation à l'aide d'Orchestrator



Orchestrator possède une série de packs d'intégration comprenant les activités de virtualisation qui vous permettent de concevoir les flux de travail des administrateurs ou des utilisateurs libre-service. Il existe des packs d'intégration pour chacun des composants de System Center 2012 et plusieurs packs de fournisseurs tiers, y compris les packs de Hewlett-Packard, d'IBM et de VMware.

Ces activités vous permettent de créer une série de tâches manuelles. Par exemple, vous pouvez fournir un nouvel ordinateur virtuel, puis ajouter l'ordinateur virtuel à un travail de sauvegarde Microsoft System Center 2012 – Data Protection Manager (DPM).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si l'activité que vous souhaitez effectuer n'a pas été créée dans un pack d'intégration, vous pouvez ensuite utiliser l'activité Exécuter le script Windows PowerShell VMM pour appeler un script et exécuter la fonction de votre choix.

Les quatre activités ci-dessous sont des exemples d'activités de Runbook fournis avec le pack d'intégration VMM et sont dans un ordre que vous pourrez utiliser pour un flux de travail simple :

- Arrêter un ordinateur virtuel
- Créer un point de contrôle
- Mettre à jour une carte réseau
- Démarrer un ordinateur virtuel

Lors de l'utilisation d'Orchestrator avec VMM, vous pouvez créer des runbooks que vous pouvez invoquer manuellement ou automatiquement. Voici un exemple de runbook que vous pouvez créer avec des étapes qui interagissent avec plusieurs composants de System Center 2012. Cet exemple de runbook suppose que vous installiez les packs d'intégration de System Center 2012 pour Service Manager, Microsoft System Center 2012 - Operations Manager et VMM. Voici les exemples d'étapes de runbooks :

1. Orchestrator analyse Operations Manager pour donner l'alerte en cas d'espace disque faible sur un ordinateur virtuel.
2. Orchestrator voit cette alerte, puis génère un incident dans Service Manager.
3. Orchestrator vérifie VMM pour confirmer que le serveur hôte dispose d'espace disque disponible. Si l'espace n'est pas suffisant, il met à jour l'incident, puis envoie un courrier électronique de notification. Si l'espace est suffisant, l'automatisation continue d'exécuter les activités prédéfinies.
4. Orchestrator met à jour Operations Manager et met l'ordinateur virtuel en mode de maintenance pour empêcher d'autres alertes concernant ce serveur.
5. Orchestrator arrête l'ordinateur virtuel, puis étend le disque virtuel.
6. Orchestrator démarre l'ordinateur virtuel, puis augmente le volume du disque.
7. Orchestrator met à jour Operations Manager, puis sort le serveur de son mode de maintenance.
8. Orchestrator met à jour l'incident de Service Manager.

Cet exemple, qu'un analyste du service technique peut exécuter de façon interactive, peut être exécuté sous la forme d'un ou de plusieurs runbooks. Par exemple, vous pouvez créer le runbook de sorte qu'il demande à l'analyste du service technique de l'exécuter à un moment donné. Ensuite, vous pouvez le configurer pour le suspendre jusqu'à ce moment-là, puis le reprendre lorsque l'analyste l'exécute. Cela serait judicieux sur un système de production qui ne peut pas être arrêté pendant les heures de travail.

Démonstration : Création d'un runbook de base

Procédure de démonstration

Créer un runbook de base

1. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'icône Accueil apparaisse, cliquez sur l'**icône Accueil**, l'interface utilisateur Windows apparaîtra. Cliquez sur **Runbook Designer**.
2. Créez un dossier pour stocker vos nouveaux runbooks, puis nommez le dossier **22414 Runbooks**.

3. Cliquez avec le bouton droit sur le dossier **22414 Runbooks**, cliquez sur **Nouveau**, sur **Runbook** et en haut du volet central, cliquez avec le bouton droit sur **Nouveau Runbook**, cliquez sur **Renommer**, sur **Oui** pour confirmer la modification de ce runbook, tapez **Analyse de la bibliothèque VMM**, puis appuyez sur Entrée.
4. Dans le volet de droite, sous Activités, cliquez sur **Gestion de fichiers**, puis cliquez sur l'activité **Analyser le dossier** et faites-la glisser au milieu du volet central.
5. Cliquez avec le bouton droit sur l'activité **Analyser le dossier**, cliquez sur **Renommer**, puis tapez **Analyse de la bibliothèque VMM**.
6. Cliquez avec le bouton droit sur **Analyse de la bibliothèque VMM**, cliquez sur **Propriétés**, et à gauche, cliquez sur **Général**. Dans la page **Informations générales**, dans le champ **Description**, tapez **Ce runbook analyse la bibliothèque VMM pour les nouveaux disques durs virtuels**.
7. À gauche, cliquez sur **Détails**, dans la section Dossier à analyser, dans le champ **Chemin d'accès**, tapez **\\LON-VMM1\MSSCVMMLibrary**, puis cliquez sur **Inclure les sous-dossiers**.
8. Dans la section Filtres de fichier, cliquez sur **Ajouter** et dans la page **Paramètres de filtre**, cliquez sur la zone de liste déroulante **Nom**, cliquez sur **Nom du fichier** et dans le champ **Valeur**, tapez ***.vhd**, puis cliquez sur **OK**.
9. À gauche, cliquez sur **Déclencheurs** et dans la section Déclencher si, cliquez sur la case à cocher à côté de **Nombre de fichiers**. Cliquez sur la zone de liste déroulante sous **Nombre de fichiers**, puis sélectionnez **greater than** et dans le champ à côté de **supérieur à**, tapez **0**.
10. À gauche, cliquez sur **Authentification** et dans le champ **Nom d'utilisateur**. Tapez **ADATUM\Administrateur** et dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Terminer**.
11. À droite, sous Activités, cliquez sur **Notification**, puis cliquez sur l'activité **Envoyer un message du journal des événements** et faites-la glisser au milieu du volet central et à droite de l'activité Analyse de la bibliothèque VMM.
12. Placez le pointeur de la souris sur l'activité Analyse de la bibliothèque VMM et une petite flèche apparaîtra sur la droite. Placez le pointeur de la souris sur la flèche et celui-ci doit prendre la forme d'une croix. Cliquez sur la **flèche**, puis faites-la glisser dans **Envoyer un message du journal des événements**. Un lien avec une flèche doit maintenant apparaître entre les deux activités.
13. Cliquez avec le bouton droit sur le lien entre les deux activités, cliquez sur **Propriétés**, puis lorsque la page **Lier Propriétés** s'affiche, examinez le filtre, puis cliquez sur **Terminer**.
14. Cliquez avec le bouton droit sur **Envoyer un message du journal des événements**, cliquez sur **Propriétés**, puis dans la page **Détails**, dans la section Propriétés, dans le champ **Ordinateur**, tapez **LON-OR1**. Dans le champ **Message**, tapez **Un fichier de disque dur virtuel a été créé ou mis à jour dans la bibliothèque LON-VMM1**. Dans la section Gravité, cliquez sur **Avertissement**, puis sur **Terminer**.
15. Dans le ruban, cliquez sur **Enregistrer**, puis sur **Exécuter**. Dans la barre des tâches de Windows, cliquez sur l'icône **Explorateur de fichiers**, puis dans le champ de la **barre d'adresses**, tapez **\\lon-vmm1\MSSCVMMLibrary\VHDs**.
16. Dans le ruban de la fenêtre des disques durs virtuels, cliquez sur **Affichage**, puis sélectionnez la case à cocher à côté d'**Extensions de noms de fichiers**.
17. Cliquez avec le bouton droit sur le fichier **Disque vierge – Grand.vhd**, cliquez sur **Copier**, cliquez avec le bouton droit sur un espace vide dans la fenêtre de l'Explorateur de fichiers, puis cliquez sur **Coller**. Un nouveau fichier nommé Disque vierge – Grand– Copie.vhd est créé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Déplacez la souris sur le coin inférieur gauche. L'icône **Accueil** s'affiche. Cliquez sur l'icône **Accueil**, jusqu'à ce que l'interface utilisateur Windows apparaisse, puis tapez **Événement** et cliquez sur **Observateur d'événements**. Au centre, dans le volet Résumé des événements d'administration, cliquez sur le bouton Développer (+) à côté d'**Avertissement** et vous verrez qu'il existe un ID de l'événement avec l'identificateur 1 et une source d'Orchestrator Runbook. Double-cliquez sur **Événement Orchestrator**, puis examinez l'événement.
19. Fermez l'**Observateur d'événements**, puis la fenêtre de l'Explorateur de fichiers. Dans le ruban, cliquez sur **Arrêter**, puis sur **Orchestration Console**. Examinez la console Orchestration et dans le Résumé, sous Statistiques des instances, vous devez voir une opération Réussite.
20. Fermez Orchestration Console, puis fermez le Runbook Designer.

Démonstration : Intégration d'Orchestrator et de VMM

Procédure de démonstration

Installer le pack d'intégration System Center pour VMM

1. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'icône **Accueil** apparaisse, cliquez avec le bouton droit sur l'icône **Accueil**, puis cliquez sur **Exécuter**. Dans la page Exécuter, cliquez dans le champ Ouvrir et tapez **\\lon-dc1\labfiles\module5\ system_center_2012_orchestrator_integration_packs.exe**, puis cliquez sur **OK**. Dans la page Choose Directory For Extracted Files, conservez le répertoire par défaut, puis cliquez sur **OK**. Dans la page **Extraction Complete (Extraction terminée)**, cliquez sur **OK**.
2. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'icône Accueil apparaisse, cliquez sur l'icône **Accueil**, puis lorsque l'interface utilisateur Windows apparaît, puis cliquez sur **Deployment Manager**.
3. Dans la console Deployment Manager, cliquez avec le bouton droit sur **Packs d'intégration**, puis cliquez sur **Inscrire le pack d'intégration auprès d'Orchestrator Management Server**.
4. Dans la page **Bienvenue**, cliquez sur **Suivant**, puis dans la page **Sélectionner les packs d'intégration ou les correctifs logiciels**, cliquez sur **Ajouter**.
5. Dans la page **Ouvrir**, dans le champ **Nom du fichier**, tapez **\\lon-dc1\Labfiles\Module5\ SC2012_Virtual_Machine_Manager_Integration_Pack.oip**. Cliquez sur **Ouvrir**, le pack d'intégration figure à présent dans la liste, cliquez sur **Suivant**, puis dans la page **Fin de l'Assistant Inscription des packs d'intégration**, cliquez sur **Terminer**. Dans la page **Contrat de Licence Utilisateur Final**, cliquez sur **Accepter**.
6. Attendez que l'inscription soit terminée, cliquez pour développer **Orchestrator Management Server**, puis cliquez sur **Packs d'intégration**.
7. Cliquez avec le bouton droit sur **System Center Integration Pack for System Center 2012 Virtual Machine Manager**, puis cliquez sur **Déployer le pack d'intégration sur le serveur Runbook Server ou sur Runbook Designer**.
8. Dans la page **Bienvenue**, cliquez sur **Suivant**, et dans la page **Déployer les packs d'intégration ou les correctifs logiciels**, activez la case à cocher à côté de **System Center Integration Pack for System Center 2012 Virtual Machine Manager**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Dans la page **Sélection de l'ordinateur**, dans le champ **Ordinateur**, tapez **LON-OR1**, cliquez sur **Ajouter**, puis sur **Suivant**.
10. Dans la page **Options d'installation**, cliquez sur **Suivant**, puis dans la page **Dernière étape**, cliquez sur **Terminer**.
11. Passez en revue les entrées du journal, puis fermez le Gestionnaire de déploiement Orchestrator.

Définir la stratégie d'exécution de Windows PowerShell

1. Sur **LON-OR1**, dans la barre des tâches, cliquez avec le bouton droit sur **Windows PowerShell**, puis sous Tâches, cliquez sur **Exécuter en tant qu'administrateur**.
2. À l'invite Windows PowerShell, tapez **set-executionpolicy remotesigned**, appuyez sur Entrée, tapez **O**, puis appuyez sur Entrée.
3. Fermez la fenêtre Windows PowerShell.
4. Sur **LON-VMM1**, dans la barre des tâches, cliquez avec le bouton droit sur **Windows PowerShell**, sous Tâches, cliquez sur **Exécuter en tant qu'administrateur**.
5. À l'invite Windows PowerShell, tapez **set-executionpolicy remotesigned**, appuyez sur Entrée, tapez **O**, puis appuyez sur Entrée.
6. Fermez la fenêtre Windows PowerShell.

Activer les hôtes approuvés par la Gestion à distance

1. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche de l'écran, l'icône Accueil apparaît. Cliquez avec le bouton droit sur l'icône **Accueil**, puis cliquez sur **Exécuter**. Dans la page **Exécuter**, dans le champ **Ouvrir**, tapez **gpedit.msc**, puis cliquez sur **OK**.
2. À gauche, sous Stratégie Ordinateur local, cliquez pour développer **Modèles d'administration**, faites défiler l'écran, puis développez **Composants Windows** et **Gestion à distance de Windows (WinRM)**.
3. À gauche, cliquez sur **Client WinRM**, puis à droite, sous le client WinRM, double-cliquez sur **Hôtes approuvés**.
4. Dans la page **Hôtes approuvés**, cliquez sur **Activé**. Dans le champ **TrustedHostsList**, tapez **LON-VMM1**, puis cliquez sur **OK**.
5. Fermez l'Éditeur de stratégies de groupe.

Configurer le pack d'intégration System Center pour VMM

1. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'interface utilisateur Windows apparaisse, puis cliquez sur **Runbook Designer**.
2. Dans le menu situé en haut, cliquez sur **Options**, puis sur **SC 2012 Virtual Machine Manager**.
3. Dans la page **Prerequisite Configuration**, cliquez sur **Add** (Ajouter) et dans la page **Add Configuration** (**Ajouter une configuration**), dans le champ **Name (Nom)**, tapez **LON-VMM1**, puis cliquez sur le bouton Parcourir **(...)**.
4. Dans la page Item Selection **(Sélection d'éléments)**, cliquez sur **System Center Virtual Machine Manager**, puis sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans la page Add Configuration (**Ajouter une configuration**), sous Properties (Propriétés), dans le champ VMM Administrator Console (**Console Administrateur VMM**), tapez **LON-VMM1**. Dans le champ VMM Server (**Serveur VMM**), tapez **LON-VMM1**, puis dans le champ **User** (Utilisateur), tapez **ADATUM\Administrateur**. Supprimez le texte du champ **Domain** (Domaine). Dans le champ Password **(Mot de passe)**, tapez **Pa$$w0rd**.
6. Dans le champ **Authentication Type (remote only)** (Type d'authentification (à distance uniquement)), cliquez sur le bouton **Parcourir**, sur **Negociate** (Négocier), puis sur **OK**.
7. Cliquez sur **OK**, dans la page **Prerequisite Configuration**, puis cliquez sur **Terminer**.
8. Dans la console Runbook Designer, dans la section Activités à droite, cliquez sur **SC 2012 Virtual Machine Manager**, puis passez en revue les activités.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Planification et implémentation de l'administration de System Center 2012

Cette leçon fournit une vue d'ensemble générale des options dans System Center 2012 pour déléguer l'administration de la virtualisation avec VMM, App Controller et Orchestrator.

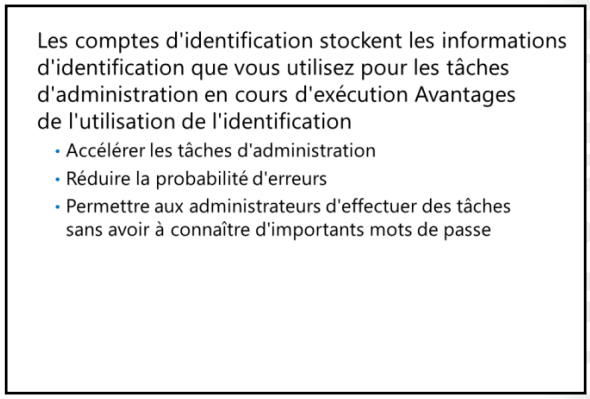
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les comptes d'identification dans System Center 2012 ;
- expliquer comment déléguer les options d'administration dans VMM ;
- expliquer comment déléguer les options d'administration dans Orchestrator ;
- expliquer comment déléguer les options d'administration dans App Controller ;
- décrire les éléments à prendre en compte pour déléguer l'administration dans System Center 2012.

Vue d'ensemble des comptes d'identification dans System Center 2012

Dans VMM, les comptes d'identification servent de conteneurs aux informations d'identification stockées qui autorisent les utilisateurs à exécuter des tâches d'administration. Par exemple, un compte d'identification stocke les informations d'identification de l'utilisateur pour se connecter à XenServer, ou pour découvrir et ajouter un stockage tiers.



Seuls les administrateurs et les administrateurs délégués peuvent créer et gérer des comptes d'identification. Les administrateurs en lecture seule ne peuvent afficher que les noms des comptes associés aux comptes d'identification qui sont dans l'étendue de leur rôle d'utilisateur.

Pour créer un compte d'identification :

1. Ouvrez la console VMM.
2. Cliquez sur l'espace de travail **Paramètres**.
3. Dans le ruban, cliquez sur **Créer un compte d'identification**.
4. Tapez un nom (Name) et une description (Description) pour les informations d'identification que vous voulez stocker.
5. Tapez les informations d'identification dans les champs **Nom d'utilisateur** et **Mot de passe**.
6. Désélectionnez **Valider les informations d'identification du domaine**. Ceci est facultatif.
7. Cliquez sur **OK** pour créer un compte d'identification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

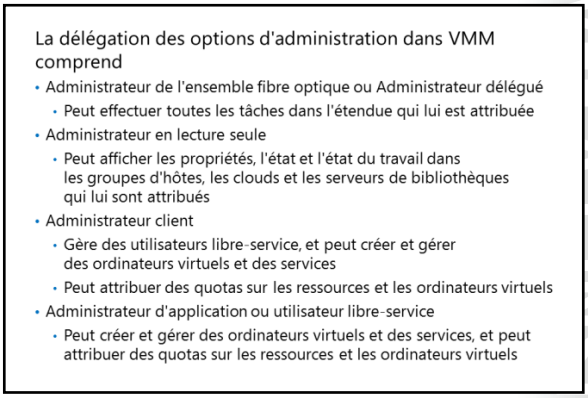
Sécurité des informations d'identification pour les comptes d'identification

VMM utilise l'interface de programmation d'applications de protection des données (DPAPI) de Windows pour fournir des services de protection de données au niveau du système d'exploitation afin de pouvoir stocker et retirer les informations d'identification des comptes d'identification.

Pendant l'installation d'un serveur d'administration VMM, vous pouvez utiliser la gestion distribuée de clés pour enregistrer les clés de chiffrement dans les services de domaine Active Directory® (AD DS), plutôt que de stocker les clés de chiffrement sur l'ordinateur sur lequel vous installez le serveur de gestion VMM. Cependant, notez que si vous installez un serveur VMM en cluster, vous devez stocker les clés de chiffrement dans AD DS.

Délégation des options d'administration dans VMM

VMM fournit quatre profils administratifs que vous pouvez attribuer aux *clouds* qui, dans VMM, font référence à un regroupement logique de ressources sur site, telles que le stockage, les réseaux, les hôtes, les équilibrages de charge et les bibliothèques. Une fois que vous avez créé un cloud dans VMM, vous pouvez déléguer une autorisation d'administrateur en fonction des responsabilités. La création d'un cloud dans VMM définit l'étendue de l'accès administrateur, que vous pouvez regrouper dans les hôtes des services ou les groupes géographiques.



Voici les rôles administratifs que vous pouvez attribuer dans VMM, y compris le rôle en lecture seule qui convient aux auditeurs :

- Administrateur de l'ensemble fibre optique (administrateur délégué). Les administrateurs délégués peuvent effectuer des tâches sur les objets dans leur étendue. Les administrateurs délégués ne peuvent pas modifier les paramètres VMM, ou ajouter et supprimer des membres du rôle d'utilisateur Administrateur.
- Administrateur en lecture seule. Les administrateurs en lecture seule peuvent afficher les propriétés, l'état et l'état du travail dans les groupes d'hôtes, clouds et serveurs de bibliothèques qui leur sont attribués. Les administrateurs en lecture seule ne peuvent pas modifier des objets.
- Administrateur client. Les administrateurs clients gèrent les utilisateurs libre-service et les réseaux d'ordinateurs virtuels. Ils peuvent créer, déployer et gérer leurs propres ordinateurs virtuels et services en utilisant la console VMM ou App Controller. Un rôle d'utilisateur d'administrateur client spécifie les tâches que les utilisateurs libre-service peuvent effectuer sur leurs ordinateurs virtuels et services. Les administrateurs clients peuvent placer des quotas sur les ressources informatiques et les ordinateurs virtuels contrôlant efficacement la quantité de ressources qu'un utilisateur libre-service peut déployer.
- Administrateur d'application ou utilisateur libre-service. Les utilisateurs libre-service peuvent créer, déployer et gérer leurs propres ordinateurs virtuels et services en utilisant la console VMM ou App Controller. Un rôle d'utilisateur libre-service spécifie les actions que l'utilisateur peut effectuer sur son ordinateur virtuel et ses services. Les administrateurs d'application peuvent également placer des quotas sur les ressources informatiques et les ordinateurs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

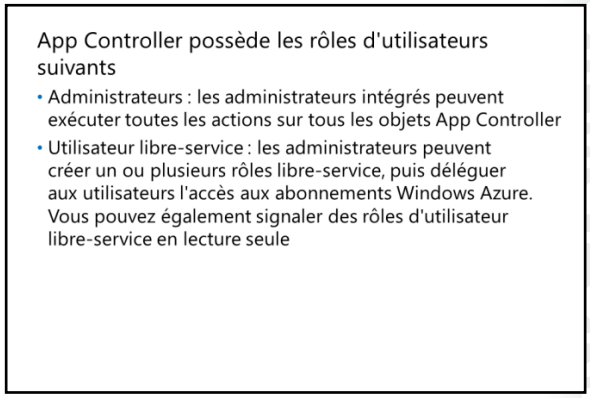
Lorsque vous créez des rôles d'utilisateur, vous pouvez attribuer des groupes d'utilisateurs à partir d'AD DS en sélectionnant plusieurs ressources, telles que les groupes d'hôtes, clouds et serveurs de bibliothèques, puis attribuer des comptes d'identification. La possibilité d'attribuer des comptes d'identification est très utile, en particulier si vous voulez déléguer l'administration de l'ensemble fibre optique et permettre aux administrateurs de la virtualisation d'ajouter le stockage à partir d'un réseau de zone de stockage (SAN), mais que vous ne souhaitez pas indiquer le nom d'utilisateur et le mot de passe réels du matériel de stockage.

Pour créer un rôle d'utilisateur dans VMM :

1. Dans la console VMM, cliquez sur **Paramètres**.
2. Cliquez pour développer **Sécurité**, puis cliquez sur **Créer un rôle d'utilisateur**.
3. Dans la page **Nom et description**, dans le champ **Nom**, tapez le nom. Dans le champ **Description**, tapez une description pour ce nouveau rôle d'utilisateur, puis cliquez sur **Suivant**.
4. Dans la page **Profil**, cliquez sur un profil pour ce rôle, puis cliquez sur **Suivant**.
5. Dans la page **Membres**, cliquez sur **Ajouter**, tapez le nom d'un compte, cliquez sur **OK**, puis sur **Suivant**.
6. Dans la page **Étendue**, activez les cases à cocher des ressources à inclure dans l'étendue, puis cliquez sur **Suivant**.
7. Dans la page **Serveurs de bibliothèque**, cliquez sur **Ajouter**, sélectionnez les serveurs de bibliothèque à inclure dans le rôle (pour sélectionner plusieurs serveurs de bibliothèque, maintenez la touche Maj enfoncée en les sélectionnant), cliquez sur **OK**, puis cliquez sur **Suivant**.
8. Dans la page **Comptes d'identification**, cliquez sur **Ajouter**, sélectionnez les comptes d'identification à inclure dans le profil (pour sélectionner plusieurs comptes d'identification, maintenez la touche Maj enfoncée en les sélectionnant), cliquez sur **OK**, sur **Suivant**, puis sur **Terminer**.

Délégation des options d'administration dans App Controller

App Controller possède deux types d'utilisateur : les administrateurs et les utilisateurs libre-service. Le groupe Administrateurs intégré peut exécuter toutes les actions d'administration sur tous les objets App Controller. Ce rôle est créé pendant l'installation et s'applique aux membres du groupe Administrateurs local du serveur sur lequel vous installez App Controller.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les administrateurs peuvent créer un ou plusieurs rôles libre-service, puis délèguent l'accès aux abonnements Windows Azure™. Vous pouvez également accorder des autorisations en lecture seule au rôle libre-service.

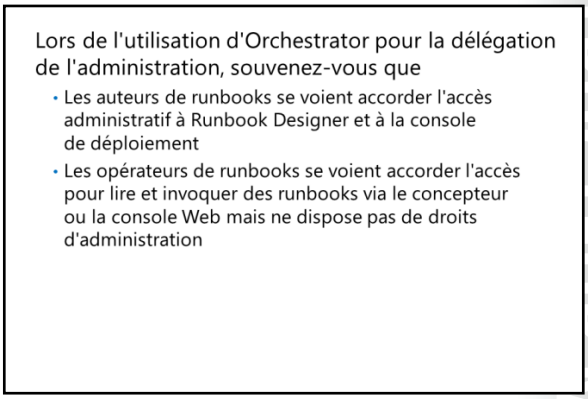
Remarque : La création des rôles dans la console App Controller s'adresse tout particulièrement aux abonnements Windows Azure ou aux connexions du fournisseur de services. Afin de créer des rôles d'utilisateurs délégués pour une connexion VMM, vous devez créer le rôle dans VMM.

Pour créer un rôle d'utilisateur dans App Controller :

1. Dans la console App Controller, double-cliquez sur **Paramètres**, puis sur **Rôles utilisateur**.
2. Dans la page **Rôles utilisateur**, cliquez sur **Nouveau** et dans la section Général, tapez un nom et une description. Éventuellement, vous pouvez cliquer sur **Rôle utilisateur en lecture seule**.
3. Dans la section Membres, cliquez sur **Ajouter**, dans le champ **Entrer le nom de l'objet à sélectionner**, tapez un nom d'utilisateur ou de groupe au format **domaine\utilisateur**, puis cliquez sur **Ajouter**.
4. Dans la section Étendue, sélectionnez **Abonnements Windows Azure** et/ou **Connexions au fournisseur de services** pour ce rôle.

Délégation des options d'administration dans Orchestrator

Orchestrator possède deux types de rôles d'utilisateur : Auteurs de runbooks et opérateurs de runbooks.



- Auteurs de runbooks. Lorsque vous installez Orchestrator, System Center 2012 vous invite à sélectionner un groupe Windows local ou un groupe de domaine Active Directory. Ce groupe vous permet d'attribuer des autorisations pour utiliser le Runbook Designer et le Gestionnaire de déploiement, que les utilisateurs peuvent utiliser pour déployer les packs d'intégration sur les serveurs Runbook Server. Les utilisateurs de ce groupe peuvent :
  - afficher, modifier et exécuter les runbooks existants, et créer des runbooks ;
  - déployer de nouveaux serveurs Runbook Server ;
  - déployer de nouvelles instances de Runbook Designers ;
  - inscrire et déployer les packs d'intégration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

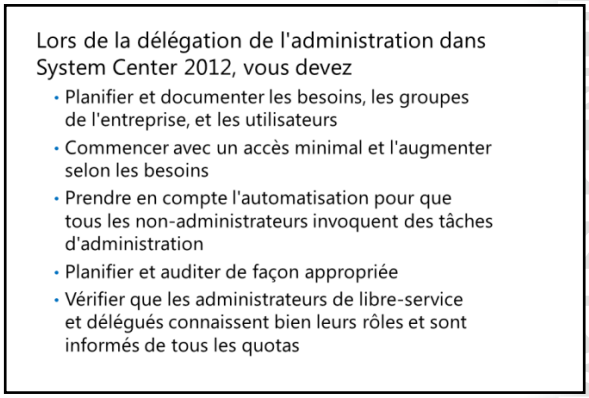
- Orchestrator vous permet également d'accorder les autorisations suivantes au niveau des runbooks :
  - Lecture : active l'exécution du runbook.
  - Écriture : active l'exécution et la modification du runbook.
  - Contrôle total : active la lecture, la modification et l'attribution des autorisations des utilisateurs pour le runbook.
- Opérateurs de runbooks. Les utilisateurs à qui vous avez accordé des autorisations de contrôle total dans les auteurs de runbooks peuvent attribuer des autorisations aux opérateurs en procédant comme suit :
  1. Dans Runbook Designer, dans le volet Connexions, cliquez sur le dossier **Runbook**.
  2. Sous le dossier **Runbook**, cliquez avec le bouton droit sur un **runbook** ou un **dossier** contenant plusieurs runbooks, puis cliquez sur **Autorisations**. La page **Autorisation** s'ouvre, à partir de la page **Autorisation**, vous pouvez cliquer sur **Ajouter** pour donner à un autre utilisateur ou groupe de sécurité l'accès au runbook, puis sélectionnez l'utilisateur ou le groupe de sécurité à partir de l'ordinateur local ou du domaine.
  3. Dans la page **Autorisations**, vous pouvez attribuer les autorisations suivantes sur les runbooks :
     - Autorisez l'utilisateur ou le groupe de sécurité à afficher et à exécuter le runbook, en activant la case à cocher **Autoriser** à côté de **Read** (Lecture).
     - Autorisez l'utilisateur ou le groupe de sécurité à modifier le runbook, en activant la case à cocher **Autoriser** à côté de **Write** (Écriture).
     - Pour permettre à l'utilisateur ou au groupe de sécurité de modifier les autorisations pour le runbook, activez la case à cocher **Autoriser** à côté de **Full Control** (Contrôle total).
  4. Lorsque vous avez ajouté et attribué des autorisations, cliquez sur **OK** pour fermer la boîte de dialogue **Autorisations pour Runbook**.

 **Liens de référence :** Pour plus d'informations sur la planification de la sécurité d'Orchestrator, accédez à la page http://go.microsoft.com/fwlink/?LinkID=285302.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour la délégation de l'administration dans System Center

Vous devez prendre en compte soigneusement les meilleures pratiques suivantes lorsque vous déléguez l'administration dans System Center 2012 :



- Sécurité. Prenez en compte les besoins d'entreprise et les rôles existants et déterminez s'ils correspondent aux rôles de System Center 2012 ou si vous devez créer des rôles. Vous devez documenter les exigences soigneusement, puis planifiez la délégation de l'administration en conséquence.
  Si possible, créez un environnement de test, puis testez les capacités des administrateurs délégués. Assurez-vous que vous définissez et définissez clairement l'étendue des administrateurs délégués dans chaque application. Examinez l'administration déléguée régulièrement, supprimez tous les comptes qui ne sont pas nécessaires et supprimez tout accès temporaire accordé qui n'est plus nécessaire. En outre, définissez les limites logiques et créez des groupes d'hôtes, clouds et serveurs de bibliothèques. Déléguez uniquement les responsabilités d'administration lorsque leur nécessité est clairement définie.
- Infrastructure. Prenez en compte les fonctions que les administrateurs délégués doivent exécuter. Doivent-ils être capables d'ajouter des équilibrages de charge et des réseaux SAN ? Doivent-ils être capables de créer leurs propres packs d'analyse ou juste attribuer les packs d'analyse existants ? Vous pouvez utiliser les comptes d'identification pour masquer les informations d'identification système essentielles.
- Formation. Fournissez une formation adaptée au personnel à qui vous accordez des rôles d'administration
- Mises à jour. Lisez toujours les informations cumulatives des mises à jour. Si la nouvelle fonctionnalité devient disponible, vous devez déterminer si elle est disponible via des privilèges existants.

Démonstration : Créer un administrateur délégué dans VMM

Dans cette démonstration, vous allez créer un administrateur délégué dans VMM.

Procédure de démonstration

Configurer l'administration déléguée dans VMM

1. Sur LON-VMM1, dans la barre de tâches, cliquez sur **Console Virtual Machine Manager**.
2. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session Microsoft Windows** est activée, puis cliquez sur **Connecter**. La console Virtual Machine Manager (VMM) s'ouvre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la console VMM, cliquez sur l'espace de travail **Paramètres**, puis dans le ruban, cliquez sur **Créer un rôle d'utilisateur**.
4. Entrez le nom **DevAdmin** et la description **Administrateurs de l'équipe de développement**, puis cliquez sur **Suivant**.
5. Cliquez sur **Administrateur de l'ensemble fibre optique (administrateur délégué)**, puis cliquez sur **Suivant**.
6. Cliquez sur **Ajouter**, tapez **Rob Cason**, cliquez sur **OK**, puis sur **Suivant**.
7. Cliquez sur **Tous les ordinateurs hôtes**, cliquez sur **Suivant**, sur **Ajouter**, sélectionnez **LON-VMM1.Adatum.com**, puis cliquez sur **OK**. Cliquez sur **Suivant**.
8. Cliquez sur **Ajouter**, sélectionnez **Administrateur**, cliquez sur **OK**, puis cliquez sur **Suivant**. Examinez le résumé, puis cliquez sur **Terminer**.
9. Fermez la fenêtre Travaux.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Planification et implémentation des options de libre-service dans System Center 2012

Cette leçon fournit une vue d'ensemble générale des options de System Center 2012 que vous pouvez utiliser pour fournir des capacités de libre-service aux utilisateurs finaux et aux administrateurs délégués. Elle fournit une vue d'ensemble des options de libre-service dans les composants de System Center 2012, y compris VMM, Orchestrator et App Controller et décrit comment vous pouvez activer le libre-service pour les différents groupes de votre organisation, tels que les administrateurs de filiales ou les administrateurs des groupes d'entreprise.

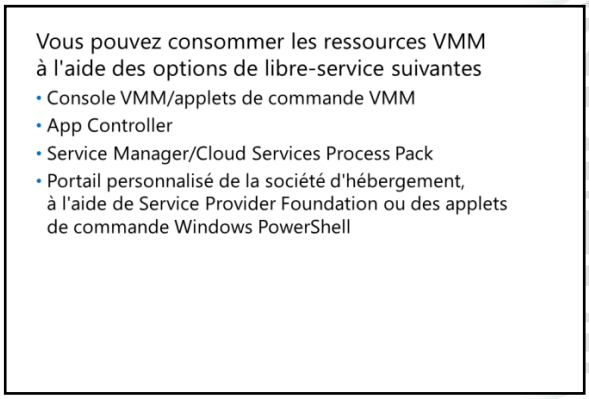
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options de libre-service dans VMM ;
- décrire les options de libre-service dans App Controller ;
- décrire les options de libre-service dans Orchestrator.

Activation des options de libre-service dans VMM

Avant de pouvoir utiliser la fonctionnalité de libre-service dans VMM, vous devez créer des ressources afin de fournir une étendue pour le libre-service. Dans VMM, vous créez puis alignez les clouds en fonction des besoins de votre entreprise. Par exemple, vous pouvez créer un cloud Ressources Humaines (RH), ainsi que les ordinateurs virtuels nécessaires et vous pouvez attribuer des autorisations à un administrateur RH qui peut gérer ces ordinateurs virtuels ou en déployer de nouveaux. Vous pouvez également utiliser des clouds comme unités logiques pour rassembler des informations sur la réévaluation des coûts et sur les coûts d'exploitation de relais par cloud, si vous intégrez Operations Manager.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Avant Microsoft System Center 2012 Service Pack 1 – Virtual Machine Manager Service Pack 1 (SP1), VMM comprenait un portail libre-service facultatif. Cependant, le portail libre-service VMM a été supprimé et remplacé par App Controller. VMM 2012 SP1 comprend les options de libre-service suivantes :

- Console VMM. Les utilisateurs peuvent déployer des ressources dans l'étendue qui leur est attribuée à l'aide de la console VMM. Vous pouvez déployer la console aux utilisateurs libre-service ou à une installation RemoteApp Windows Server® 2012 et publier le tout aux utilisateurs finaux. L'avantage de cette approche est que vous avez potentiellement moins de consoles à gérer. Le tableau suivant répertorie les actions que vous pouvez attribuer à un rôle d'utilisateur libre-service.

Nom	Description
Auteur	Créer des modèles d'ordinateur virtuel et de service.
Point de contrôle	Créer et gérer des points de contrôle d'ordinateur virtuel.
Point de contrôle (restaurer uniquement).	Restaurer mais ne peut pas créer de points de contrôle d'ordinateur virtuel.
Déployer	Créer des ordinateurs virtuels et des services à partir de disques durs virtuels (VHD) ou de modèles.
Déployer (à partir d'un modèle uniquement)	Créer des ordinateurs virtuels à partir de modèles uniquement.
Administrateur local	Accorder des droits d'administrateur local sur des ordinateurs virtuels.
Suspendre et reprendre	Suspendre et reprendre des ordinateurs virtuels et des services.
Recevoir	Recevoir des ressources d'autres utilisateurs libre-service.
Se connecter à distance	Se connecter à distance aux ordinateurs virtuels.
Supprimer	Supprimer des ordinateurs virtuels et des services.
Enregistrer	Enregistrer des ordinateurs virtuels et des services.
Partager	Partager des ressources avec d'autres utilisateurs libre-service.
Éteindre	Éteindre des ordinateurs virtuels.
Démarrer	Démarrer des ordinateurs virtuels et des services.
Arrêter	Arrêter des ordinateurs virtuels et des services.
Stocker et redéployer	Stocker des ordinateurs virtuels dans la bibliothèque et les redéployer.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Applets de commande VMM. Vous pouvez utiliser les applets de commande Windows PowerShell pour effectuer toutes les étapes que vous effectuez à l'aide de VMM. Vous pouvez ainsi utiliser vos propres applications personnalisés qui peuvent appeler les applets de commande Windows PowerShell pour fournir des ressources et administrer un environnement virtualisé.
- App Controller. Les utilisateurs peuvent accéder à App Controller pour voir et gérer les ressources étendues que vous attribuez dans VMM. App Controller remplace le portail libre-service VMM à partir de VMM 2012 SP1.
- Service Manager. Pour des solutions de libre-service plus complètes, les utilisateurs peuvent accéder au portail libre-service de Service Manager. Le portail libre-service de Service Manager est basé sur Microsoft SharePoint® 2013 et vous pouvez le personnaliser facilement. Outre le portail prêt à l'emploi de Service Manager, il existe également le Cloud Services Process Pack, un pack d'automatisation et de processus avec l'infrastructure en tant que service (IaaS) activée qui tire parti des capacités d'un déploiement intégré de System Center et utilise VMM, Service Manager et Orchestrator.
- Service Manager/ Cloud Services Process Pack. En déployant le Cloud Services Process Pack, vous pouvez utiliser les formulaires préconfigurés, les offres de demande et de service qui fournissent l'automatisation et le libre-service d'un modèle informatique d'infrastructure IaaS. Le Cloud Services Process Pack fournit un certain nombre d'offres de demande pour Service Manager et les runbooks correspondants pour Orchestrator pour que vous puissiez configurer ces demandes automatiquement à l'aide de VMM.
- Hébergement des ressources. Dans Orchestrator SP1, Microsoft propose une technologie facultative appelée Service Provider Foundation. Cette technologie est destinée aux sociétés d'hébergement qui possèdent un portail libre-service existant. Elle apporte une intégration nécessaire aux composants de System Center 2012 pour fournir des ressources via des portails existants. En outre, les nouveaux portail et API de gestion des services vous permettent d'offrir une plateforme semblable à celle de Windows Azure, qui propose des offres de site Web et d'ordinateur virtuel.

Démonstration : Création de clouds privés VMM

Dans cette démonstration, vous allez apprendre à créer un cloud et à déléguer l'administration dans VMM.

Procédure de démonstration

Créer un cloud privé

1. Sur LON-VMM1, dans la barre de tâches, cliquez sur **Console Virtual Machine Manager**.
2. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session Microsoft Windows** est activée, puis cliquez sur **Connecter**. La console VMM s'ouvre.
3. Cliquez sur l'espace de travail **Ordinateurs virtuels et services**.
4. Dans le ruban, cliquez sur **Créer un cloud**.
5. Dans la page **Général**, dans le champ **Nom**, tapez **Développement de London** et dans le champ **Description**, tapez **Cloud Développement de London**, puis cliquez sur **Suivant**.
6. Dans la page **Ressources**, sélectionnez **Tous les ordinateurs hôtes**, puis cliquez sur **Suivant**.
7. Dans la page **Réseaux logiques**, sélectionnez **Réseau externe**, puis cliquez sur **Suivant**.

8. Dans la page **Équilibrages de charge**, sélectionnez **Microsoft Network Load Balancing (NLB)** (Équilibrage de charge réseau Microsoft (NLB)), puis cliquez sur **Suivant**.
9. Dans la page **Modèles d'adresse IP virtuelle**, cliquez sur **Suivant**.
10. Dans la page **Classifications de port**, cliquez sur **Équilibrage de la charge réseau**, cliquez sur **Bande passante moyenne**, sur **Faible bande passante**, puis sur **Suivant**.
11. Dans la page **Stockage**, cliquez sur **Suivant**.
12. Dans la page **Bibliothèque**, dans la section **Partages de bibliothèque en lecture seule**, cliquez sur **Ajouter**. Sélectionnez **MSSCVMMLibrary**, cliquez sur **OK**, puis sur **Suivant**.
13. Dans la page **Capacité**, passez en revue les options de capacité. Supprimez la coche à côté de chaque ressource sélectionnée, puis attribuez ce qui suit :
    - 8 processeurs virtuels
    - 12 gigaoctets (Go) de mémoire
    - 250 Go de stockage
    - Quota personnalisé (points) : 15
    - 8 ordinateurs virtuels
14. Cliquez sur **Suivant**.
15. Dans la page **Profils de capacité**, sélectionnez **Hyper-V**, puis cliquez sur **Suivant**.
16. Vérifiez la page **Résumé**, puis cliquez sur **Terminer**.
17. Fermez la fenêtre Travaux.

Accorder l'accès au cloud Développement de London

1. Cliquez sur l'espace de travail **Ordinateurs virtuels et services**, cliquez avec le bouton droit sur **Clients**, puis sur **Créer un rôle d'utilisateur**.
2. Dans la page **Nom et description**, dans le champ **Nom**, tapez **DevSS**. Dans le champ **Description**, tapez **Rôle de libre-service de l'équipe de Développement de London**, puis cliquez sur **Suivant**.
3. Dans la page **Profil**, cliquez sur **Administrateur d'application (utilisateur libre-service)**, puis sur **Suivant**.
4. Dans la page **Membres**, cliquez sur **Ajouter** et dans la page **Sélectionnez des utilisateurs, des ordinateurs ou des groupes**, tapez **anat**, cliquez sur **OK**, puis sur **Suivant**.
5. Dans la page **Étendue**, cliquez sur **Développement de London**, puis cliquez sur **Suivant**.
6. Dans la page **Quotas**, vérifiez les quotas au niveau des rôles et des utilisateurs, puis cliquez sur **Suivant**.
7. Dans la page **Mise en réseau**, cliquez sur **Ajouter** et dans la page **Sélectionner des réseaux d'ordinateurs virtuels**, cliquez sur **Réseau externe**, sur **OK**, puis sur **Suivant**.
8. Dans la page **Ressources**, cliquez sur **Suivant**.
9. Dans la page **Actions**, cliquez sur **Sélectionner tout**, puis cliquez sur **Suivant**.
10. Dans la page **Comptes d'identification**, cliquez sur **Ajouter**, sur **Administrateur**, sur **OK**, puis sur **Suivant**.
11. Dans la page **Résumé**, vérifiez les paramètres, puis cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Connecter App Controller à VMM

1. Sur **LON-VMM1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'icône **Accueil** apparaisse, cliquez sur l'icône **Accueil**, puis lorsque l'interface utilisateur Windows apparaît, cliquez sur **App Controller**.
2. Dans la page **Entrez vos informations d'identification pour vous connecter**, dans le champ **Nom d'utilisateur**, tapez **ADATUM\Administrateur** et dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Connexion**.
3. Dans la page **Vue d'ensemble**, sous État, cliquez sur **Connecter un serveur Virtual Machine Manager et des clouds**. Dans la page **Ajouter une nouvelle connexion VMM**, cliquez sur le champ **Nom de la connexion**, puis tapez **LON-VMM1.adatum.com**. Dans le champ Description, tapez **Accès au serveur VMM de London**. Dans le champ **Nom du serveur**, tapez **LON-VMM1.adatum.com**, puis cliquez sur **OK**.
4. Dans la page **Vue d'ensemble**, dans le coin supérieur droit du navigateur, cliquez sur **Déconnexion**.

Configuration des options de libre-service dans Orchestrator

Orchestrator possède une console Web qui requiert la version 4 de Silverlight® ou une version plus récente. La console permet aux administrateurs et aux opérateurs d'effectuer les actions suivantes :

La console Orchestrator libre-service fournit un emplacement aux opérateurs et auteurs de runbooks pour

- Démarrer, arrêter et examiner des runbooks
- Accéder aux informations sur l'historique et l'état d'exécution des runbooks
- Examiner les événements consignés par les serveurs Runbook Server et les serveurs d'administration

- afficher la liste de runbooks et de serveurs Runbook Server ;
- afficher l'historique et l'état d'exécution des runbooks ;
- afficher une définition générale des runbooks ;
- démarrer et arrêter des runbooks ;
- examiner les événements que les runbooks et les serveurs d'administration créent.

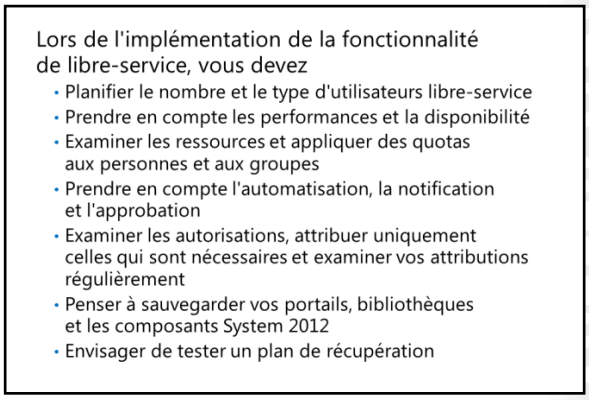
La console Orchestrator offre un sous-ensemble de la fonctionnalité proposée par le Runbook Designer, vous pouvez y accéder de la manière suivante :

- Ouvrez un navigateur, puis dans la barre d'adresses, tapez **http://<nom de l'ordinateur>:<numéro du port>**, où le nom de l'ordinateur est le nom du serveur sur lequel le service Web est installé, et le port est le numéro de port sélectionné pendant la configuration du service Web. Le port 82 est le port par défaut.
- Utilisez la console Runbook Designer, vous pouvez y accéder en cliquant sur **Orchestration Console** dans la barre d'outils.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Implémentation du libre-service dans System Center 2012

Vous comprenez à présent le libre-service et l'administration déléguée dans System Center 2012, vous pouvez commencer à faire correspondre les exigences métier. L'installation de VMM propose des options pour offrir la fonctionnalité de libre-service, et App Controller, Service Manager et Orchestrator étendent les capacités de libre-service encore plus loin. Cependant, avant de déterminer les composants à déployer pour pouvoir offrir des capacités de libre-service, vous devez déterminer les exigences métier.



La liste suivante répertorie les aspects à prendre en compte avant d'implémenter les capacités de libre-service :

- Planification. Lorsque vous déployez et mettez à niveau des applications, vous devez toujours planifier le déploiement en premier. Si vous souhaitez déployer la fonctionnalité de libre-service, il n'y a aucune exception à cette règle. La nature hautement personnalisable et extensible des composants de System Center 2012 peut faire varier considérablement le déploiement des capacités de libre-service en fonction du temps et des efforts nécessaires au déploiement. Si vous souhaitez commencer la planification du déploiement du libre-service, vous devez tenir compte des dernières informations et ressources disponibles sur TechNet, telles que l'implémentation de produits et la configuration requise. En outre, vous devez vérifier toute architecture de référence et tirer parti des informations et des aide-mémoire associés présents dans les guides d'infrastructure et de planification pour chaque composant que vous envisagez de déployer.
- Recherchez des guides relatifs au cloud privé Microsoft, pour autant que ces guides portent sur le libre-service d'infrastructure et d'application. Cloud Services Process Pack, faites correspondre les exigences métier aux capacités des produits et envisagez un déploiement en plusieurs parties si vous devez effectuer de nombreuses configurations pendant votre déploiement. Calculez le retour sur investissement prévu pour les zones principales de libre-service et déterminez si ce que vous voulez obtenir est disponible prêt à l'emploi. En outre, vous devez rechercher les consultants ou développeurs expérimentés qui peuvent créer et étendre les packs d'administration. Procédez à une planification de bout en bout pour chaque demande de libre-service et pensez à utiliser les organigrammes pour créer les processus métier et techniques que vous devrez utiliser. Enfin, prenez en compte les avantages de l'automatisation des demandes de libre-service.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Sécurité. Vous devez inclure les problèmes potentiels de sécurité dans la planification documentée du déploiement de vos systèmes. Utilisez les contrôles d'accès basés sur les rôles, nous vous recommandons d'attribuer au moins les privilèges requis pour que chaque rôle réponde à vos besoins, et de fournir uniquement aux utilisateurs l'accès ou la visibilité aux outils dont ils ont besoin. Par exemple, vous ne devrez peut-être pas rendre chaque catalogue ou offre de portail de service visible et accessible pour chaque utilisateur. Si votre organisation effectue des contrôles de sécurité de l'accès au système, vous voudrez peut-être vérifier régulièrement l'accès en libre-service par rapport à vos offres pour garantir que les autorisations restent comme vous le vouliez. Par exemple, vérifiez que les utilisateurs ne peuvent pas supprimer d'ordinateurs virtuels s'ils ne doivent pas disposer de cette capacité.
- Performances et ressources. Prenez en compte les incidences sur les ressources et les performances pouvant se produire lorsque vous déplacez la capacité de déploiement de l'équipe serveurs vers une équipe du service technique, ou vers les développeurs et les professionnels de projet et de support. De nombreuses personnes peuvent potentiellement demander et déployer des services simultanément. Vos ressources peuvent s'épuiser rapidement. Déterminez comment réguler la gestion du déploiement et du cycle de vie de vos systèmes. Par exemple, si vous permettez aux utilisateurs d'utiliser des sauvegardes de serveurs en libre-service et que vous automatisez le déploiement de l'agent, vous devez envisager ce qui risque de se passer si quelqu'un demande la sauvegarde de chaque serveur au cours d'une nuit en particulier. Cela peut paralyser un réseau ou provoquer l'épuisement des ressources de stockage avant que d'autres systèmes plus essentiels ne soient sauvegardés.
- Sauvegarde. Vérifiez que vous sauvegardez votre produit System Center 2012 régulièrement.
- Récupération d'urgence. Réfléchissez à l'impact potentiel si votre offre de libre-service n'est plus disponible et veillez à disposer d'un plan pour récupérer l'offre de libre-service et déployer les services manuellement, si nécessaire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et implémentation d'une solution d'administration pour la virtualisation

Scénario

A. Datum Corporation a déployé plusieurs serveurs virtualisés, et il est apparu de plus en plus clairement qu'elle devra simplifier la gestion de son environnement. Certains groupes de l'entreprise demandent un accès supplémentaire à l'environnement virtuel et exigent plus de contrôle sur le déploiement et la configuration de leurs ordinateurs virtuels. En outre, ils souhaitent pouvoir initier des tâches de gestion dans l'environnement virtuel.

Comme le nombre d'hôtes physiques et d'ordinateurs virtuels augmente, les administrateurs de System Center 2012 chez A. Datum continuent d'être surchargés par des tâches d'administration. Par conséquent, pour réduire le temps que les administrateurs passent sur des tâches régulières, ils souhaiteraient déléguer certaines des tâches les plus courantes et prévisibles qu'ils effectuent.

Objectifs

- Planifier la délégation de l'administration et du libre-service dans System Center 2012.
- Implémenter le libre-service et la délégation de l'administration dans VMM.
- Implémenter l'automatisation des processus dans System Center 2012.

Configuration de l’atelier pratique

Durée approximative : 60 minutes

Ordinateur(s) virtuel(s)	22414B-LON-DC1 22414B-LON-VMM1 22414B-LON-OR1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible. Avant de commencer cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, ouvrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22414B-LON-OR1**, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **Administrateur**
   - Mot de passe : **Pa$$w0rd**
   - Domaine : **ADATUM**
5. Vérifiez que **22414B-LON-DC1** et **22414B-LON-VMM1** sont exécutés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configuration de l'automatisation des processus dans System Center

Scénario

L'équipe d'administration du développement a installé la console Orchestrator et souhaite que vous l'aidiez à la configurer pour créer des flux de travail qui automatiseront le déploiement d'ordinateurs virtuels.

Les tâches principales de cet exercice sont les suivantes :

1. Installer et configurer les packs d'intégration System Center.
2. Configurer l'automatisation dans Orchestrator.

▶ Tâche 1 : Installer et configurer les packs d'intégration System Center

Installer le pack d'intégration System Center pour VMM

1. Sur LON-DC1, dans la barre des tâches, cliquez sur **Explorateur de fichiers**.
2. Dans l'Explorateur de fichiers, accédez à **E:\Labfiles\Module5**.
3. Double-cliquez sur **System_Center_2012_Orchestrator_Integration_Packs.EXE**. Cliquez sur **Ok**, puis une nouvelle fois sur **OK** pour fermer le message **Extraction Complete** (Extraction terminée).
4. Fermez l'Explorateur de fichiers.
5. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'icône **Accueil** apparaisse, cliquez sur l'icône **Accueil**, puis lorsque la page de démarrage apparaît, cliquez sur **Deployment Manager**.
6. À l'aide de la console Orchestrator Deployment Manager, inscrivez et déployez le **pack d'intégration Virtual Machine Manager**, situé dans **\\lon-dc1\Labfiles\Module5\SC2012_Virtual_Machine_Manager_Integration_Pack.oip**.
7. Déployez le pack sur **LON-OR1**.
8. Passez en revue les Entrées de journal, puis fermez Orchestrator Deployment Manager.

Définissez la stratégie d'exécution de Windows PowerShell sur RemoteSigned.

1. Sur **LON-OR1**, dans la barre des tâches, cliquez avec le bouton droit sur **Windows PowerShell**, puis sous Tâches, cliquez sur **Exécuter en tant qu'administrateur**.
2. À l'invite Windows PowerShell, tapez **set-executionpolicy remotesigned**, appuyez sur Entrée, tapez **O**, puis appuyez sur Entrée.
3. Fermez la fenêtre Windows PowerShell.
4. Sur **LON-VMM1**, dans la barre des tâches, cliquez avec le bouton droit sur **Windows PowerShell**, puis sous Tâches, cliquez sur **Exécuter en tant qu'administrateur**.
5. À l'invite Windows PowerShell, tapez **set-executionpolicy remotesigned**, appuyez sur Entrée, tapez **O**, puis appuyez sur Entrée.
6. Fermez la fenêtre Windows PowerShell.

Activer les hôtes approuvés par la Gestion à distance

1. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche de l'écran jusqu'à ce que l'icône **Accueil** apparaisse, cliquez avec le bouton droit sur l'icône **Accueil**, puis cliquez sur **Exécuter**. Dans la page **Exécuter**, dans le champ **Ouvrir**, tapez **gpedit.msc**, puis cliquez sur **OK**.
2. À gauche, sous **Stratégie Ordinateur local\Configuration ordinateur**, cliquez pour développer **Modèles d'administration**, puis développez **Composants Windows** et **Gestion à distance de Windows (WinRM)**.
3. Cliquez sur **Client WinRM**, puis à droite, sous Client WinRM, double-cliquez sur **Hôtes approuvés**.
4. Dans la page **Hôtes approuvés**, cliquez sur **Activé** et dans le champ **TrustedHostsList**, tapez **LON-VMM1**, puis cliquez sur **OK**.
5. Fermez l'Éditeur de stratégie de groupe local.

Configurer le pack d'intégration System Center pour VMM

1. Sur **LON-OR1**, cliquez sur l'écran Accueil, puis sur **Runbook Designer**.
2. Dans le menu situé en haut, cliquez sur **Options**, puis sur **SC 2012 Virtual Machine Manager**.
3. Dans la page **Prerequisite Configuration**, cliquez sur **Add** (Ajouter) et dans la page **Add Configuration** (Ajouter une configuration), dans le champ **Name** (Nom), tapez **LON-VMM1**, puis cliquez sur le bouton Parcourir.
4. Dans la page **Item Selection** (Sélection d'éléments), cliquez sur **System Center Virtual Machine Manager**, puis sur **OK**.
5. Dans la page **Add Configuration** (Ajouter une configuration), ajoutez les détails suivants :
   - VMM Administrator Console = **LON-VMM1**
   - VMM Server = **LON-VMM1**
   - User = **ADATUM\Administrateur**
   - Domain : supprimez le texte
   - Password = **Pa$$w0rd**
   - Authentication Type (Remote only) = **Negociate**
6. Cliquez sur **OK**, puis dans la page **Prerequisite Configuration**, cliquez sur **Terminer**.

▶ Tâche 2 : Configurer l'automatisation dans Orchestrator

Créer un runbook de base

1. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'icône **Accueil** apparaisse, cliquez sur l'icône **Accueil**, puis lorsque l'interface utilisateur Windows apparaît, cliquez sur **Runbook Designer**.
2. À gauche, dans le volet Connexions, cliquez avec le bouton droit sur **Runbook**, cliquez sur **Nouveau**, puis sur **Dossier**. Appuyez sur la touche Suppr, tapez **22414 Runbooks**, puis appuyez sur Entrée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Cliquez avec le bouton droit sur le dossier **22414 Runbooks**, cliquez sur **Nouveau**, sur **Runbook** et en haut du volet central, cliquez avec le bouton droit sur **Nouveau Runbook**, cliquez sur **Renommer**, sur **Oui** pour confirmer la modification de ce runbook, tapez **Analyse de la bibliothèque VMM**, puis appuyez sur Entrée.
4. Dans le volet de droite, sous Activités, développez **Gestion de fichiers**, puis cliquez sur l'activité **Analyser le dossier** et faites-la glisser au milieu du volet central.
5. Cliquez avec le bouton droit sur l'activité **Analyser le dossier**, cliquez sur **Renommer**, puis tapez **Analyse de la bibliothèque VMM**. Appuyez sur Entrée.
6. Cliquez avec le bouton droit sur **Analyse de la bibliothèque VMM**, cliquez sur **Propriétés**, et à gauche, cliquez sur **Général**. Dans la page **Informations générales**, dans le champ **Description**, tapez **Ce runbook analyse la bibliothèque VMM pour les nouveaux disques durs virtuels**.
7. Cliquez sur **Détails** et dans la section Dossier à analyser, dans le champ **Chemin d'accès**, tapez **\\LON-VMM1\MSSCVMMLibrary**, puis cliquez sur **Inclure les sous-dossiers**.
8. Dans la section **Filtres de fichiers**, cliquez sur **Ajouter** et dans la page **Paramètres de filtre**, cliquez sur la zone de liste déroulante **Nom**, cliquez sur **Nom du fichier** et dans le champ **Valeur**, tapez ***.vhd**, puis cliquez sur **OK**.
9. À gauche, cliquez sur **Déclencheurs** et, dans la section **Déclencher si**, activez la case à cocher **Nombre de fichiers** cliquez sur la zone de liste déroulante **Nombre de fichiers** sélectionnez **greater than**, puis dans le champ **greater than**, tapez **0**.
10. Cliquez sur **Authentification** et dans le champ **Nom d'utilisateur**, tapez **ADATUM\Administrateur** et dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Terminer**.
11. Sous Activités, cliquez sur **Notification**, puis cliquez sur l'activité **Envoyer un message du journal des événements** et faites-la glisser au milieu du volet central et à droite de l'activité **Analyse de la bibliothèque VMM**.
12. Placez le pointeur de la souris sur l'activité **Analyse de la bibliothèque VMM** et une petite flèche doit apparaître sur la droite. Placez le pointeur de la souris sur la flèche et celui-ci doit prendre la forme d'une croix. Cliquez sur la flèche, puis faites-la glisser dans **Envoyer un message du journal des événements**. Un lien avec une flèche doit maintenant apparaître entre les deux activités.
13. Cliquez avec le bouton droit sur la flèche entre les deux activités, cliquez sur **Propriétés**, puis lorsque la page **Lier Propriétés** s'affiche, vérifiez le filtre, puis cliquez sur **Terminer**.
14. Cliquez avec le bouton droit sur **Envoyer un message du journal des événements**, cliquez sur **Propriétés** et dans la page **Détails**, dans la section Propriétés, dans le champ **Ordinateur**, tapez **LON-OR1**, puis dans le champ **Message**, tapez **Un fichier de disque dur virtuel a été créé ou mis à jour dans la bibliothèque LON-VMM1**. Dans la section Gravité, cliquez sur **Avertissement**, puis sur **Terminer**.
15. Dans le ruban, cliquez sur **Enregistrer**. Dans le ruban, cliquez sur **Exécuter**.
16. Dans la barre des tâches de Windows, cliquez sur l'icône **Explorateur de fichiers** et dans le champ de la **barre d'adresses**, tapez **\\lon-vmm1\MSSCVMMLibrary\VHDs**.
17. Dans le ruban de la fenêtre des disques durs virtuels, cliquez sur **Affichage**, puis sélectionnez la case à cocher à côté d'**Extensions de noms de fichiers**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Cliquez avec le bouton droit sur l'un des fichiers **Disque vierge – Grand.vhd**, cliquez sur **Copier**, puis cliquez avec le bouton droit sur un espace vide dans la fenêtre de l'Explorateur de fichiers, cliquez sur **Coller** et un nouveau fichier nommé Disque vierge – Grand – Copie.vhd est créé.
19. Basculez vers la page Accueil, tapez **Événement**, puis cliquez sur **Observateur d'événements**. Au centre, dans le volet Résumé des événements d'administration, développez **Avertissement** et vous verrez qu'il existe un ID de l'événement avec l'identificateur 1 et une source d'Orchestrator Runbook. Double-cliquez sur **Événement Orchestrator**, puis examinez l'événement.
20. Fermez l'**Observateur d'événements**, puis la fenêtre de l'Explorateur de fichiers.
21. Dans Runbook Designer, dans le ruban, cliquez sur **Arrêter**, puis sur **Orchestration Console**. Examinez la console Orchestration, puis dans le Résumé, sous Statistiques des instances (historique), vous devez voir une opération Réussite.
22. Fermez Orchestration Console.

Créer un runbook de base à l'aide des activités VMM

1. Dans Orchestrator Runbook Designer, dans le volet Connexions, développez **Runbook**, cliquez avec le bouton droit sur le dossier **22414 Runbooks**, cliquez sur **Nouveau**, sur **Runbook** et en haut du volet central, cliquez avec le bouton droit sur **Nouveau Runbook**, cliquez sur **Renommer**, sur **Oui** pour confirmer la modification de ce runbook, tapez **Point de contrôle VM**, puis appuyez sur Entrée.
2. Sous Activités, cliquez sur **SC 2012 Virtual Machine Manager**, cliquez sur l'activité **Shut Down VM** (Arrêter l'ordinateur virtuel) et faites-la glisser dans l'espace de travail central, puis cliquez sur l'activité **Create CheckPoint** (Créer un point de contrôle) et faites-la glisser dans l'espace de travail central, en la plaçant à droite de l'activité **Shut Down VM** (Arrêter l'ordinateur virtuel).
3. Cliquez sur l'activité **Start VM** (Démarrer l'ordinateur virtuel) et faites-la glisser dans l'espace de travail central, en la plaçant à droite de l'activité **Create CheckPoint** (Créer un point de contrôle).
4. Placez le pointeur de la souris sur l'activité **Shut Down VM** (Arrêter l'ordinateur virtuel), puis lorsqu'une petite flèche apparaît à droite, placez le pointeur de la souris sur la flèche et celui-ci doit prendre la forme d'une croix. Cliquez sur la flèche, puis faites-la glisser dans **Create CheckPoint** (Créer un point de contrôle). Un lien avec une flèche doit apparaître entre les deux activités.
5. Répétez l'étape précédente, cette fois pour créer un lien entre l'activité **Create CheckPoint** (Créer un point de contrôle) et l'activité Start VM (Démarrer l'ordinateur virtuel).
6. Cliquez avec le bouton droit sur **Shut Down VM** (Arrêter l'ordinateur virtuel), cliquez sur **Propriétés** et dans la page **Properties** (Propriétés), dans la section Configuration, cliquez sur **...** à côté du champ **Name** (Nom). Lorsque la page **Item Selection** (Sélection d'éléments) s'ouvre, cliquez sur **LON-VMM1**, puis cliquez sur **OK**.
7. Dans la section Properties (Propriétés), cliquez dans le champ **VM ID** (ID de l'ordinateur virtuel), puis cliquez sur **...** pour parcourir les options de la page VM ID (ID de l'ordinateur virtuel), cliquez sur l'ID qui commence par **(TOR-WEB1.Adatum.com)**, cliquez sur **OK**, puis sur **Terminer**.
8. Cliquez avec le bouton droit sur l'activité **Create CheckPoint** (Créer un point de contrôle), cliquez sur **Propriétés** et dans la page **Properties** (Propriétés), dans la section Configuration, cliquez sur **...** à côté du champ **Name** (Nom). Lorsque la page **Item Selection** (Sélection d'éléments) s'ouvre, cliquez sur **LON-VMM1**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Dans la section **Properties** (Propriétés), cliquez dans le champ **VM ID** (ID de l'ordinateur virtuel), cliquez sur **...** pour parcourir les options de la page **VM ID** (ID de l'ordinateur virtuel), cliquez sur l'ID qui commence par **(TOR-WEB1.Adatum.com)**, puis cliquez sur **OK**.
10. Cliquez sur **Optional Properties** (Propriétés optionnelles) et dans la page **Add/Remove Property** (Ajouter/Supprimer une propriété), cliquez sur **Description**. Cliquez sur **>>**, sur **Name** (Nom), sur **>>**, sur **OK** et dans la section Propriétés, dans le champ **Description**, tapez **Point de contrôle VM initial du service Web**, puis dans le domaine **Name** (Nom), tapez **Image de départ**, puis cliquez sur **Terminer**.
11. Cliquez avec le bouton droit sur l'activité **Start VM** (**Démarrer l'ordinateur virtuel**), cliquez sur **Propriétés**, puis dans la page **Properties** (Propriétés), dans la section Configuration, cliquez sur **...** à côté du champ **Name** (Nom). Lorsque la page **Item Selection** (Sélection d'éléments) s'ouvre, cliquez sur **LON-VMM1**, puis cliquez sur **OK**.
12. Dans la section Properties (Propriétés), cliquez dans le champ **VM ID** (ID de l'ordinateur virtuel), puis cliquez sur **...** pour parcourir les options de la page VM ID (ID de l'ordinateur virtuel), cliquez sur l'ID qui commence par **(TOR-WEB1.Adatum.com)**, cliquez sur **OK**, puis sur **Terminer**.
13. Sur LON-OR1, dans la console Runbook Designer, dans le ruban, cliquez sur **Enregistrer**.
14. Sur **LON-VMM1**, dans la barre de tâches, cliquez sur **Console Virtual Machine Manager**.
15. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session Microsoft Windows** est activée, puis cliquez sur **Connecter**. La console VMM s'ouvre.
16. Cliquez sur l'espace de travail **Ordinateurs virtuels et services**.
17. Confirmez que l'ordinateur virtuel TOR-WEB1 est en cours d'exécution. Si ce n'est pas le cas, cliquez avec le bouton droit sur **TOR-WEB1**, cliquez sur **Marche**, puis attendez que l'ordinateur virtuel démarre.
18. Dans le ruban d'Orchestrator Runbook Designer, cliquez sur **Exécuter**.
19. Dans la console Virtual Machine Manager, le serveur TOR-WEB1 doit maintenant s'arrêter. Créez le point de contrôle, puis redémarrez-le. Lorsque l'ordinateur virtuel TOR-WEB1 démarre, cliquez pour sélectionner **TOR-WEB1**, puis dans le ruban, cliquez sur **Gérer les points de contrôle**. Vous devez voir le point de contrôle de l'image de départ. Cliquez sur **OK**, puis fermez la console Virtual Machine Manager.
20. Sur **LON-OR1**, fermez Orchestrator Runbook Designer.

Résultats : À la fin de cet atelier pratique, vous aurez installé les packs d'intégration Virtual Machine Manager, créé un runbook de base dans Orchestrator Runbook Designer et examiné la console Web Orchestrator.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Planification de la délégation administrative et du libre-service dans System Center 2012

Scénario

L'équipe de développement chez A. Datum basée à Toronto souhaiterait avoir plus de contrôle sur l'environnement virtuel dans lequel ses serveurs sont déployés. Elle veut recueillir des informations d'analyse avancées, y compris personnaliser une partie de la configuration de l'analyse. Elle veut également pouvoir créer et gérer des événements de flux de travail liés à ses environnements virtuels, et pouvoir déléguer la responsabilité de la création d'ordinateurs virtuels aux utilisateurs au sein de l'organisation.

Stratégie d'administration de la virtualisation	
Numéro de référence du document : BS0907/1	
Auteur du document Date	Brad Sutton 20 septembre

Présentation des exigences :

Planifiez une stratégie d'administration de la virtualisation afin d'atteindre les objectifs suivants :

- donner à l'équipe d'administration du groupe de développement le contrôle administratif sur ses groupes d'hôtes et ressources associées ;
- permettre à l'équipe de développement de créer des comptes en libre-service pour les développeurs et les fournisseurs afin de déployer rapidement des ordinateurs ;
- fournir à l'équipe de développement l'analyse de serveur afin d'inclure l'option de configuration de paramètres avancés spécifiques.

Informations supplémentaires :

- L'équipe de développement recommande que le service soit très dynamique et qu'il déploie des ordinateurs virtuels tous les jours à des fins développement interne des systèmes.
- En ce moment, du personnel externe est chargé de tester deux grands systèmes pendant une courte période. Les développeurs qui gèrent normalement les serveurs hôtes virtuels sont pressés par le temps à cause des tâches d'administration qu'ils doivent accomplir. La stratégie consiste à analyser et à sauvegarder tous les ordinateurs virtuels, y compris les systèmes de tests.

Propositions :

1. Quel est le rôle d'administration le mieux approprié pour atteindre les objectifs de contrôle principaux des équipes d'administration dans le groupe de développement ?
2. La plupart des développeurs auront besoin de la fonction de création des comptes en libre-service. Par conséquent, quels seront les rôles d'administration les plus adaptés pour eux ?
3. Que pouvez-vous faire pour aider à réduire les charges administratives des administrateurs du développement ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Lire la documentation fournie avec le produit.
2. Mettre à jour le document de proposition en fonction du plan d'action planifié.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.
4. Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur.

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation et le scénario fournis.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

- Répondez aux questions de la section Propositions du document Stratégie d'administration de la virtualisation.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions avec celles du corrigé de l'atelier pratique.

▶ Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Préparez-vous à discuter de vos propositions avec la classe.

Exercice 3 : Configuration de l'administration déléguée et du libre-service dans VMM

Scénario

Afin de répondre aux besoins d'administration pour l'un des groupes de l'entreprise, vous allez implémenter l'administration déléguée et le libre-service dans VMM. Vous devez configurer les rôles délégués d'administration et les rôles de libre-service, puis vérifier la configuration.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer un rôle d'administrateur délégué dans VMM.
2. Configurer l'administration du libre-service dans VMM.
3. Valider la configuration.

▶ Tâche 1 : Configurer un rôle d'administrateur délégué dans VMM

Créer un cloud privé

1. Sur **LON-VMM1**, dans la barre de tâches, cliquez sur **Console Virtual Machine Manager**.
2. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session Microsoft Windows** est activée, puis cliquez sur **Connecter**.
3. Cliquez sur l'espace de travail **Ordinateurs virtuels et service**, puis créez un cloud nommé **Développement de London**, avec la Description **Cloud Développement de London**.

4. Suivez les instructions de l'Assistant Création d'un cloud, dans la page **Ressources**, sélectionnez **Hôtes de London**.
5. Dans la page **Réseaux logiques**, sélectionnez **Réseau externe**.
6. Dans la page **Équilibrages de charge**, sélectionnez **Microsoft Network Load Balancing (NLB)** (Équilibrage de charge réseau Microsoft (NLB)).
7. Dans la page **Classifications de port**, sélectionnez **Équilibrage de la charge réseau**, **Bande passante moyenne** et **Bande passante élevée**.
8. Dans la page **Bibliothèque**, sélectionnez **MSSCVMMLibrary**.
9. Dans la page **Capacité**, passez en revue les options de capacité. Désactivez la case à cocher à côté de chaque ressource sélectionnée, puis attribuez ce qui suit :
   - 8 processeurs virtuels
   - 12 Go de mémoire
   - 250 Go de stockage
   - Quota personnalisé (points) : 15
   - 4 ordinateurs virtuels
10. Dans la page **Profils de capacité**, sélectionnez **Hyper-V**.
11. Vérifiez la page **Résumé**, cliquez sur **Terminer**, puis fermez la fenêtre Travaux.

Configurer l'administration déléguée dans VMM

1. Dans la console VMM, cliquez sur l'espace de travail **Paramètres**, puis créez un rôle d'utilisateur nommé **DevAdmin** avec la description **Administrateurs de l'équipe de développement**.
2. Suivez les instructions de l'Assistant Création d'un rôle d'utilisateur, dans la page **Profil**, sélectionnez **Administrateur de l'ensemble fibre optique (administrateur délégué)**, puis dans la page **Membres**, ajoutez **Rob Cason**.
3. Dans la page **Étendue**, sélectionnez le cloud **Développement de London** et le groupe d'hôtes **Hôtes de London**.
4. Sur les **Serveurs de bibliothèque**, sélectionnez **LON-VMM1.Adatum.com**.
5. Dans la page **Comptes d'identification**, sélectionnez le compte **Administrateur**.
6. Examinez le Résumé, cliquez sur **Terminer**, puis fermez la fenêtre Travaux.

▶ Tâche 2 : Configurer l'administration du libre-service dans VMM

Configurer le libre-service dans VMM

1. Dans la console VMM, cliquez sur l'espace de travail **Paramètres**, puis créez un rôle d'utilisateur nommé **DevFournisseurs** avec la description **Fournisseurs de l'équipe de développement**.
2. Suivez les instructions de l'Assistant Création d'un rôle d'utilisateur, puis dans la page **Profil**, sélectionnez **Administrateur d'application (utilisateur libre-service)**.
3. Dans la page **Membres**, ajoutez **Adam**.
4. Dans la page **Étendue**, sélectionnez **Développement de London**.
5. Dans la page **Mise en réseau**, sélectionnez **Réseau externe**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans la page **Ressources**, sélectionnez le **serveur d'applications Web Adatum**.
7. Dans la page **Actions**, attribuez les actions autorisées suivantes :
   - **Connexion à distance**
   - **Arrêt**
   - **Démarrer**
   - **Arrêter**
8. Dans la page **Résumé**, vérifiez les paramètres, cliquez sur **Terminer**, puis fermez la fenêtre Travaux.

▶ Tâche 3 : Valider la configuration

Vérifier la délégation de l'administration

1. Dans le menu supérieur de la console Virtual Machine Manager, au-dessus du ruban, cliquez sur la flèche, puis cliquez sur **Ouvrir une nouvelle connexion**. La page **Connexion au serveur** s'ouvre.
2. Dans la page **Connexion au serveur**, cliquez sur l'option **Spécifier les informations d'identification**, et entrez les données suivantes :
   - Nom d'utilisateur : **ADATUM\Rob**
   - Mot de passe : **Pa$$w0rd**
3. Créez un ordinateur virtuel dans le cloud Développement de London, suivez les instructions de l'Assistant Créer un ordinateur virtuel, puis dans la page **Sélectionner une source**, sélectionnez **Créer l'ordinateur virtuel avec un disque dur virtuel vide**.
4. Dans la page **Spécifier l'identité de l'ordinateur virtuel**, nommez l'ordinateur virtuel **RobVM**.
5. Dans la page **Configurer le matériel**, sélectionnez un profil de capacité **Hyper-V**.
6. Dans la page **Sélectionner la destination**, sélectionnez **Déployer l'ordinateur virtuel sur un cloud privé**.
7. Dans la page **Sélectionner le cloud**, sélectionnez **lon-host1.adatum.com**.
8. Dans la page **Résumé**, créez l'ordinateur virtuel. Fermez l'instance **DevAdmin** de la console Virtual Machine Manager.
9. Dans l'instance Administrateur de la console Virtual Machine Manager, cliquez sur l'espace de travail **Ordinateurs virtuels et services**, cliquez sur la flèche à côté de Clouds et vous devez voir le cloud Développement de London.
10. Cliquez sur le cloud **Développement de London**, puis dans le ruban, cliquez sur **Vue d'ensemble**. Notez que vous pouvez voir les rôles d'utilisateurs et les propriétaires d'ordinateur virtuel. Confirmez que vous pouvez voir les rôles DevAdmin et DevFournisseurs. Cliquez pour développer ces rôles et afficher les utilisateurs qui leur sont attribués. Examinez les détails dans cette page.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vérifier le libre-service dans VMM

1. Dans le menu supérieur de la console Virtual Machine Manager, au-dessus du ruban, cliquez sur la flèche, puis cliquez sur **Ouvrir une nouvelle connexion**. La page **Connexion au serveur** s'ouvre.
2. Connectez-vous à la console Virtual Machine Manager en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Adam**
   - Mot de passe : **Pa$$w0rd**
3. Cliquez sur l'espace de travail **Ordinateurs virtuels et services**. Cliquez sur la flèche à côté de Clouds.
4. Créez un ordinateur virtuel dans le cloud **Développement de London**.
5. Suivez les instructions de l'Assistant Créer un ordinateur virtuel, puis dans la page **Sélectionner une source**, sélectionnez **Créer l'ordinateur virtuel avec un disque dur virtuel vide**.
6. Dans la page **Spécifier l'identité de l'ordinateur virtuel**, nommez l'ordinateur virtuel **AdamVM**.
7. Dans la page **Configurer le matériel**, cliquez sur **Suivant**.
8. Une page d'avertissement doit apparaitre indiquant que vous ne disposez pas de l'autorisation requise pour effectuer cette opération. Cliquez sur **OK** pour fermer l'avertissement. Cliquez sur **Annuler**, puis sur **Oui**.
9. Fermez l'instance **DevFournisseurs** de la console Virtual Machine Manager.

Connecter App Controller à VMM

1. Sur **LON-VMM1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'icône **Accueil** apparaisse, cliquez sur l'icône **Accueil**, puis lorsque l'interface utilisateur Windows apparaît, cliquez sur **App Controller**.
2. Dans la page **Entrez vos informations d'identification pour vous connecter**, dans le champ **Nom d'utilisateur**, tapez **ADATUM\Administrateur** et dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Connexion**.
3. Dans la page **Vue d'ensemble**, sous État, cliquez sur **Connecter un serveur Virtual Machine Manager et des clouds**. Dans la page **Ajouter une nouvelle connexion VMM**, cliquez sur le champ **Nom de la connexion**, puis tapez **LON-VMM1.adatum.com**. Dans le champ Description, tapez **Accès au serveur VMM de London**. Dans le champ **Nom du serveur**, tapez **LON-VMM1.adatum.com**, puis cliquez sur **OK**.
4. Dans la page **Vue d'ensemble**, dans le coin supérieur droit du navigateur, cliquez sur **Déconnexion**.

Vérifier le libre-service dans App Controller

1. Dans la page **Entrez vos informations d'identification pour vous connecter**, dans le champ **Nom d'utilisateur**, tapez **ADATUM\Adam** et dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Connexion**.
2. Dans la page **Vue d'ensemble**, déployez un nouveau service à partir du modèle **Service Web Adatum**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la section SERVICE, cliquez sur **Configurer** et dans la page **Propriétés de Service Web ADATUM service**, nommez le service **Service Fournisseur**, puis ajoutez un Centre de coûts nommé **Développement de London**.
4. Dans la section **INSTANCE**, cliquez sur **Configurer** et dans le champ **Nom de l'ordinateur**, tapez **LON-WEB1**, cliquez sur **OK**, puis sur **Déployer**.
5. À gauche de la console App Controller, cliquez sur l'espace de travail **Travaux**. Vous devez voir le travail Créer un déploiement du service avec l'état En cours. Le déploiement prendra un certain temps, vous pouvez donc revenir à la console Virtual Machine Manager pour vérifier l'état de déploiement dans le détail.
6. Pour examiner l'état de déploiement détaillé, dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Travaux**, puis dans la section Travail en cours de exécution, cliquez sur **Créer une instance de service**. La partie inférieure de l'écran affiche les étapes individuelles et le fichier de déploiement, à l'aide de bits par seconde (bits/s) via HTTPS, vous donnera une indication de la progression.
7. Lorsque le déploiement est terminé, fermez toutes les consoles.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez les ordinateurs virtuels à leur état initial en procédant comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-VMM1**, **22414B-LON-OR1** et **22414A-TOR-SVR1**.
5. Sur **LON-HOST1**, cliquez sur l'écran Accueil, puis sur **Panneau de configuration**. Cliquez sur **Désinstaller un programme**, puis désinstallez **Microsoft System Center Virtual Machine Manager Agent (x64)** et **Microsoft System Center Virtual Machine Manager DHCP Server (x64)**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quels sont certains des avantages de l'automatisation et du libre-service ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 6

Planification et implémentation d'une stratégie d'analyse des serveurs

Table des matières :

Vue d'ensemble du module **6-1**

Leçon 1 : Planification de l'analyse dans Windows Server 2012 **6-2**

Leçon 2 : Vue d'ensemble de System Center Operations Manager **6-11**

Leçon 3 : Planification et configuration de packs d'administration **6-27**

Leçon 4 : Planification et configuration des notifications et de la création de rapports **6-34**

Leçon 5 : Configuration de l'intégration à VMM **6-40**

Atelier pratique : Implémentation d'une stratégie d'analyse des serveurs **6-47**

Vue d'ensemble du module

L'analyse est une partie essentielle de la gestion et de la maintenance des serveurs. En analysant vos serveurs, vous pourrez bien souvent identifier les problèmes potentiels et les résoudre avant qu'ils n'affectent les utilisateurs. Dans ce module, vous verrez comment utiliser les outils d'analyse inclus à Windows Server® 2012 et à Microsoft® System Center 2012 – Operations Manager (Operations Manager).

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- planifier l'analyse dans Windows Server 2012 ;
- décrire Operations Manager ;
- planifier la configuration des packs d'administration ;
- planifier la configuration des notifications et de la création de rapports ;
- configurer l'intégration d'Operations Manager et de System Center 2012 – Virtual Machine Manager (VMM).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification de l'analyse dans Windows Server 2012

Windows Server 2012 propose plusieurs outils d'analyse dans le cadre du système d'exploitation. Ces outils sont utiles pour analyser un ou plusieurs serveurs lorsque cela s'avère nécessaire. Vous pouvez utiliser des outils tels que l'Observateur d'événements, l'Analyseur de performances, le Moniteur de fiabilité, le Moniteur de ressources et le Gestionnaire de serveur pour vérifier que les serveurs fonctionnent comme prévu. Ils peuvent également être utilisés pour la résolution des problèmes.

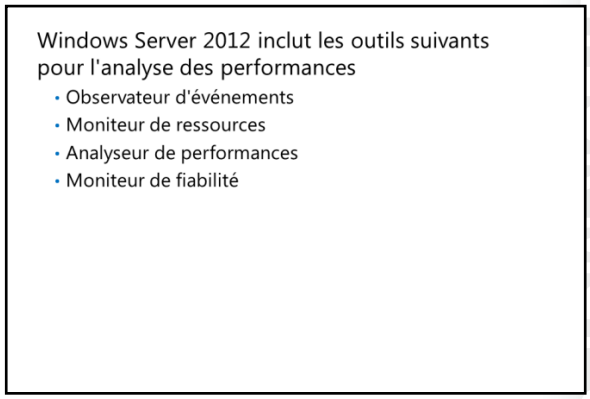
Dans un environnement virtualisé, vous devez prendre en compte certains éléments particuliers pour analyser les serveurs. Vous devez connaître la façon dont la virtualisation affecte les données que vous collectez à l'aide des outils d'analyse afin de vérifier que vous avez des informations exactes.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les outils d'analyse de Windows Server 2012 ;
- analyser plusieurs serveurs à l'aide du Gestionnaire de serveur ;
- élaborer une stratégie d'analyse ;
- décrire les éléments à prendre en compte pour l'analyse des rôles serveur ;
- comprendre les options d'analyse des serveurs dans un environnement virtualisé ;
- activer et afficher les données.

Vue d'ensemble des outils d'analyse dans Windows Server 2012



L'analyse des performances des serveurs est un moyen efficace d'identifier les problèmes de ressources potentiels avant qu'ils n'affectent les performances applicatives. En analysant les ressources (par exemple, l'utilisation au fil du temps), vous pouvez identifier des tendances et prédire à quel moment les serveurs doivent être mis à jour avec des ressources supplémentaires ou à quel moment les services doivent être déplacés vers de nouveaux serveurs. L'absence d'analyse des performances des serveurs peut se traduire par une baisse de productivité pour les utilisateurs. Généralement, les ressources les plus analysées sont l'utilisation du processeur, de la mémoire et du réseau et l'activité du disque.

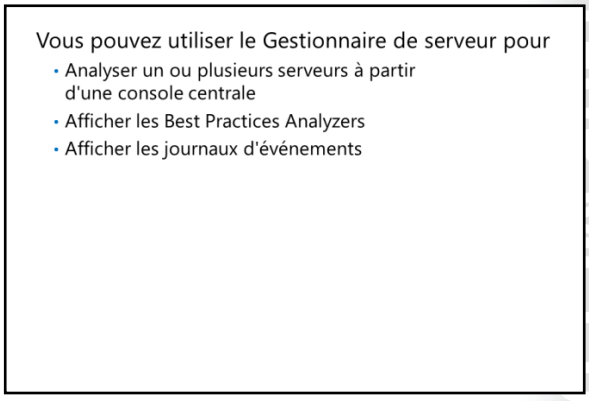
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Windows Server 2012 inclut les outils suivants, que vous pouvez utiliser pour analyser les performances des serveurs :

- Observateur d'événements : vous pouvez utiliser cet outil pour afficher les journaux d'événements, qui sont une source d'informations précieuses pour analyser Windows Server 2012 et les applications, et résoudre les problèmes connexes. Les journaux d'événements contiennent des informations, des avertissements et des erreurs. Vous pouvez utiliser le contenu des événements pour identifier la source des problèmes. Vous pouvez utiliser les abonnements de l'Observateur d'événements pour centraliser la collecte d'événements de plusieurs serveurs.
- Moniteur de ressources : vous pouvez utiliser cet outil pour analyser l'état actuel de l'utilisation des ressources sur vos serveurs. Vous pouvez analyser l'utilisation du processeur, de la mémoire et du réseau et l'activité du disque. L'utilisation des ressources est identifiée pour chaque processus qui s'exécute sur l'ordinateur. Cet outil fournit des informations similaires aux données de performances du Gestionnaire des tâches, mais les informations sont beaucoup plus détaillées.
- Analyseur de performances : vous pouvez utiliser cet outil pour analyser les compteurs de performances installés sur le serveur. Cet outil fournit des informations bien plus détaillées que celles du Moniteur de ressources, au sujet de l'activité système. Il peut également enregistrer des journaux pour une évaluation ultérieure, et déclenche des alertes quand les compteurs dépassent les limites acceptables. Vous pouvez également utiliser les rapports intégrés pour les diagnostics système et les performances système afin de résoudre les problèmes.
- Moniteur de fiabilité : vous pouvez utiliser cet outil pour afficher une vue d'ensemble de la stabilité système, de l'historique des problèmes et de l'installation logicielle. Cela vous permet de visualiser à quel moment les problèmes de stabilité ont commencé et de les corréler avec une éventuelle modification apportée à votre système, comme une nouvelle installation logicielle ou une mise à jour de pilote.

Analyse de plusieurs serveurs à l'aide du Gestionnaire de serveur

Le Gestionnaire de serveur a été totalement reconçu pour Windows Server 2012. Il constitue désormais l'outil central pour gérer vos serveurs exécutant Windows Server 2012. L'une des principales améliorations apportées au Gestionnaire de serveur est sa capacité à gérer des serveurs individuels à distance et à exécuter plusieurs serveurs en tant que groupe à partir d'un emplacement unique, ce qui simplifie l'administration.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les deux éléments du Gestionnaire de serveur utiles pour l'analyse sont :

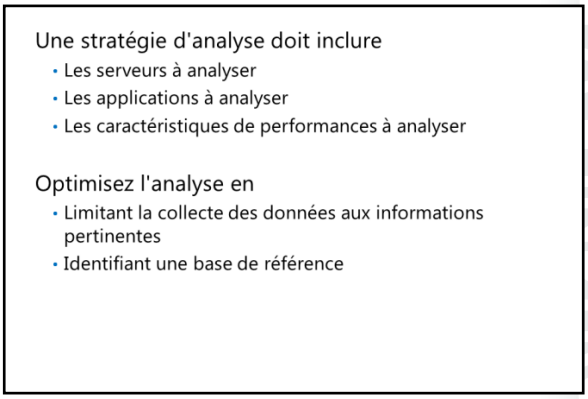
- Best Practices Analyzer : Windows Server 2012 inclut l'outil Best Practices Analyzer pour les rôles serveur. Vous pouvez utiliser l'outil BPA pour déterminer si les rôles serveur sont correctement configurés ou s'ils rencontrent des problèmes. L'analyse permet de rechercher des informations pertinentes dans les journaux d'événements.
- Journaux d'événements : vous pouvez utiliser le Gestionnaire de serveur pour afficher les journaux d'événements du serveur local ou des groupes de serveurs. Les journaux d'événements s'affichent également par rôle serveur. Vous pouvez utiliser les journaux d'événements pour identifier les erreurs ou les avertissements générés par des applications ou des rôles serveur.

Si vous utilisez régulièrement l'outil Best Practices Analyzer et examinez les journaux d'événements, vous devriez pouvoir identifier les problèmes de performances potentiels avant qu'ils n'affectent les utilisateurs.

Élaboration d'une stratégie d'analyse

Nous vous recommandons d'élaborer une stratégie d'analyse qui vous permette d'identifier les problèmes de performances et de configuration avant qu'ils n'affectent les utilisateurs. Votre stratégie d'analyse doit inclure les informations suivantes :

- Les serveurs à analyser.
- Les applications à analyser.
- Les caractéristiques de performances à analyser.



L'une des principales préoccupations des administrateurs en matière d'analyse est de savoir comment analyser l'immense quantité d'informations générées. Il n'est pas possible d'analyser chaque caractéristique d'un serveur. Au lieu de cela, vous devez déterminer les informations spécifiques dont vous avez besoin pour identifier les problèmes de performances avec précision. Cela implique d'identifier les ressources les plus déterminantes pour un rôle serveur particulier.

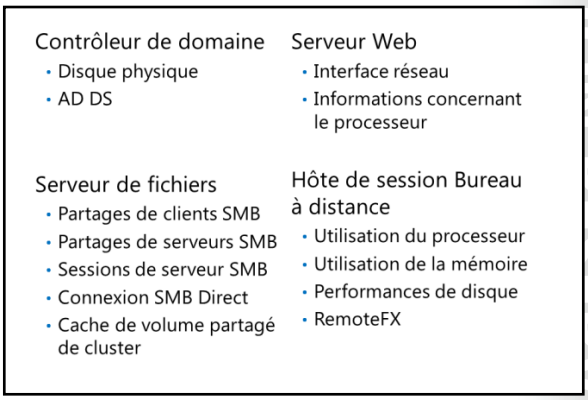
Lors de l'analyse, vous devez également comprendre les performances normales d'un serveur ou d'une application. Ce comportement normal est appelé « base de référence ». Une base de référence vous aide à identifier ce qui a changé lorsque des problèmes de performances se produisent. Par exemple, si la base de référence d'un serveur indique qu'il utilise normalement 8 gigaoctets (Go) de mémoire, vous devriez examiner l'utilisation de la mémoire lorsque les rapports indiquent que ce même serveur utilise 12 Go de mémoire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour l'analyse des rôles serveur

Les informations appropriées pour analyser un serveur varient selon les rôles serveur que vous avez installés. Chaque rôle serveur utilise différentes ressources. En conséquence, vous devez sélectionner différents compteurs de performances à analyser pour chaque rôle serveur. Cependant, indépendamment du rôle serveur, vous devez toujours identifier une base de référence pour la résolution future des problèmes.



Contrôleur de domaine

Les contrôleurs de domaine utilisent intensivement la mémoire et le disque. Une mémoire insuffisante réduit les performances des contrôleurs de domaine car les informations des services de domaine Active Directory® (AD DS) récemment consultées seront mises en cache dans la mémoire. Un débit de disque insuffisant réduit également les performances des contrôleurs de domaine.

Les compteurs de performances à analyser pour le disque et la mémoire incluent :

- Disque physique\Longueur moyenne de file d'attente du disque (doit être inférieure à 2 par pile)
- Disque physique\Longueur moy. de file d'attente lecture disque
- Disque physique\Longueur moy. de file d'attente écriture disque
- Active Directory\Taux d'accès au cache de la base de données
- Active Directory\Taille de la mémoire cache de la base de données (en mégaoctets, Mo)
- Services d'annuaire\Demandes restantes en file d'attente ATQ

Serveur de fichiers

En général, les performances du serveur de fichiers reposent sur la vitesse de la connectivité réseau, la quantité de mémoire disponible pour la mise en cache et les performances du disque. Windows Server 2012 propose un certain nombre de nouveaux compteurs de performances qui vous permettent d'analyser le partage de fichiers :

- Partages de clients SMB : fournit des informations sur les performances du client SMB (Server Message Block) accédant aux partages sur un autre serveur.
- Partages de serveurs SMB : fournit des informations sur les performances des partages SMB qui existent sur le serveur.
- Sessions de serveur SMB : fournit des informations sur les performances des sessions que les clients utilisent pour se connecter aux partages sur le serveur.
- Connexion SMB Direct : fournit des informations sur les performances de l'activité de connexion.
- Cache de volume partagé de cluster : fournit des informations sur les performances du cache de volume partagé de cluster.

Serveur Web

La plupart des serveurs Web hébergent des applications Web avec du contenu dynamique plutôt que des sites Web avec des pages Web statiques. Par conséquent, les performances des serveurs Web dépendent souvent des performances du processeur. Toutefois, outre le processeur, il doit y avoir suffisamment de capacités réseau et de performances disque. Pour garantir des performances de serveur Web optimales, vous devez envisager d'analyser les compteurs suivants :

- Interface réseau\Octets reçus/s
- Interface réseau\Octets envoyés/s
- Interface réseau\Longueur de la file d'attente de sortie (ne doit pas être supérieure à 2)
- Informations sur le processeur\% du temps processeur

Hôte de session Bureau à distance

La charge placée sur un hôte de session Bureau à distance dépend du nombre d'utilisateurs accédant au serveur et des applications qu'ils exécutent. Les applications que chaque utilisateur exécute placent une charge sur le processeur, la mémoire, le disque et la carte graphique de l'hôte de session Bureau à distance.

Pour un hôte de session Bureau à distance, vous devez analyser les compteurs suivants :

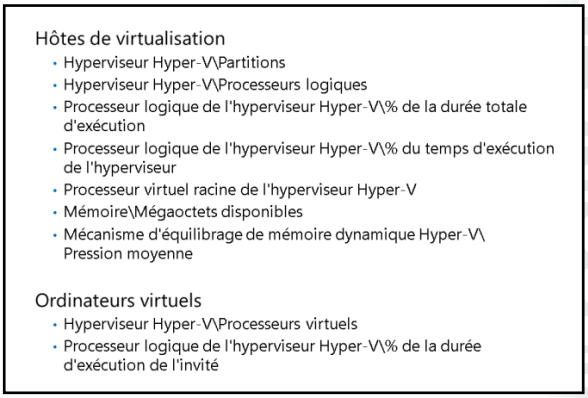
- Utilisation du processeur
- Utilisation de la mémoire
- Performances de disque
- Microsoft RemoteFX®

Documentation supplémentaire :

- Pour plus d'informations sur l'ajustement des performances de Windows Server 2012, consultez le document « Performance Tuning Guidelines for Windows Server 2012 » sur le site Web de Microsoft à l'adresse http://go.microsoft.com/fwlink/?LinkID=285313
- Reportez-vous au document « Performance Tuning Guidelines for Windows Server 2012 », à l'adresse http://go.microsoft.com/fwlink/?LinkID=285314

Options d'analyse d'un environnement de serveurs virtualisé.

Les environnements virtualisés fournissent la flexibilité nécessaire pour exécuter plusieurs ordinateurs virtuels avec différents systèmes d'exploitation sur le même ordinateur physique. Ceci afin de tirer le meilleur parti de votre matériel et de diminuer les coûts énergétiques. Cependant, la virtualisation présente également une certaine complexité en ce qui concerne l'analyse de votre environnement virtualisé.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour l'analyse, vous pouvez diviser l'environnement virtualisé en deux groupes distincts :

- Hôtes de virtualisation
- Ordinateurs virtuels

Hôtes de virtualisation

Votre environnement de virtualisation se composera d'un ou de plusieurs serveurs exécutant le rôle Hyper-V® dans Windows Server 2012. Vous pouvez utiliser l'Analyseur de performances pour analyser l'utilisation de la mémoire, du réseau et du disque sur vos serveurs hôtes, tout comme vous le faites pour tout serveur donné. Cependant, vous évaluez l'utilisation du processeur différemment, car les processeurs sont utilisés par le système d'exploitation hôte et les systèmes d'exploitation invités, exécutés sur les ordinateurs virtuels que l'hôte prend en charge. Pour surveiller l'utilisation du processeur sur un hôte Hyper-V, vous utilisez les compteurs suivants :

- Hyperviseur Hyper-V\Partitions : nombre d'ordinateurs virtuels.
- Hyperviseur Hyper-V\Processeurs logiques : nombre de processeurs logiques.
- Hyperviseur Hyper-V\Processeurs virtuels : nombre de processeurs virtuels.
- Processeur logique de l'hyperviseur Hyper-V\% de la durée totale d'exécution : temps d'activité total des processeurs logiques. Cette valeur doit être inférieure à 75 %.
- Processeur logique de l'hyperviseur Hyper-V\% du temps d'exécution de l'hyperviseur : temps d'activité des processeurs logiques pour le système d'exploitation hôte uniquement.
- Processeur virtuel racine de l'hyperviseur Hyper-V : tous les compteurs de cet objet mesurent l'utilisation du processeur pour le système d'exploitation hôte uniquement.

Vous devriez également envisager d'analyser les compteurs liés à la mémoire suivants pour votre hôte de virtualisation :

- Mémoire\Mégaoctets disponibles : vérifiez que votre hôte de virtualisation a au moins 10 % de mémoire de libres à tout moment. Si la mémoire de l'hôte tombe sous ce pourcentage, envisagez d'ajouter de la mémoire à l'hôte de virtualisation ou de réduire sa charge.
- Mécanisme d'équilibrage de mémoire dynamique Hyper-V\Pression moyenne : ce compteur mesure le pourcentage de mémoire disponible pour un ordinateur virtuel donné par rapport à la quantité de mémoire dont ce même ordinateur virtuel a besoin. Cela signifie qu'un ordinateur virtuel avec une pression moyenne de 100 a la quantité précise de mémoire dont il a besoin, alors qu'un ordinateur virtuel avec une pression moyenne de 120 % a besoin de 20 % de plus de mémoire que ce que vous lui attribuez. Idéalement, vous devriez avoir la valeur 80 ou moins pour ce compteur.



Liens de référence :

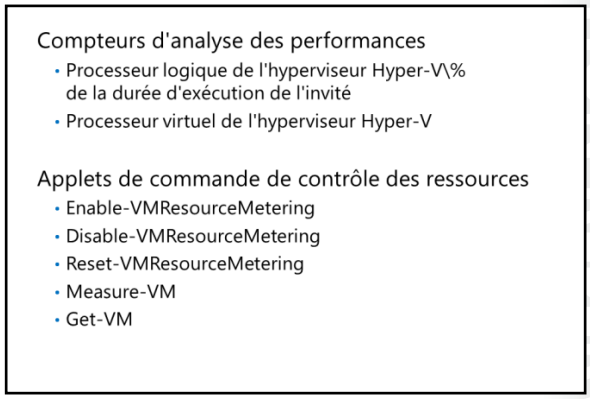
Vous pouvez vous reporter au document « Performance Tuning Guidelines for Windows Server 2012 », à l'adresse http://go.microsoft.com/fwlink/?LinkID=285313.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour l'analyse d'ordinateurs virtuels

Les organisations analysent généralement l'utilisation des ordinateurs virtuels pour deux raisons :

- Analyse des performances : vous pouvez mesurer l'utilisation du réseau, de la mémoire, du processeur, du disque et d'autres ressources pour vérifier que l'ordinateur virtuel fonctionne selon une base prédéfinie.
- Contrôle des ressources : vous pouvez mesurer l'utilisation de la bande passante, de la mémoire, du processeur et du stockage pour la planification des ressources et la comptabilité.



Analyse des performances

L'analyse des performances d'un ordinateur virtuel ressemble à celle de tout ordinateur qui exécute un système d'exploitation Windows®. À l'aide de l'analyse des performances, vous pouvez récupérer les données d'utilisation de la mémoire, du disque et du réseau. Cependant, si vous utilisez la même technique pour rassembler les données d'utilisation du processeur, les données que vous collecterez pourront ne pas être exactes. Lorsque vous analysez un ordinateur virtuel, vous ne voyez pas les informations relatives à l'hôte de virtualisation dans son ensemble.

Si vous avez un ordinateur virtuel qui exécute une application qui sollicite beaucoup le processeur et affiche 100 % d'utilisation du processeur dans le Gestionnaire des tâches, cela signifie que l'ordinateur virtuel utilise toutes les ressources de processeur qui lui sont allouées. Si vous démarrez un deuxième ordinateur sur ce même hôte de virtualisation qui affiche 100 % d'utilisation du processeur, les ressources que le deuxième ordinateur virtuel utilise sont supprimées du premier ordinateur virtuel afin que les deux ordinateurs se partagent la puissance de traitement de l'hôte à parts égales. Bien que le Gestionnaire des tâches affiche une valeur cohérente, vous devez garder à l'esprit qu'en démarrant le deuxième ordinateur virtuel, vous réduirez la puissance de traitement réelle du premier ordinateur virtuel.

Pour analyser l'utilisation du processeur au sein d'un ordinateur virtuel, vous devez utiliser l'Analyseur de performances dans le système d'exploitation hôte et analyser les compteurs suivants :

- Processeur logique de l'hyperviseur Hyper-V\% de la durée d'exécution de l'invité : ce compteur analyse la durée d'activité pour le système d'exploitation invité. Cette valeur doit être inférieure à 75 %.
- Processeur virtuel de l'hyperviseur Hyper-V : tous les compteurs de cet objet mesurent l'utilisation du processeur pour le système d'exploitation invité uniquement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des ressources

Le contrôle est une pratique très courante pour les organisations informatiques qui font des rapports sur la consommation des ressources par division au sein de la société pour laquelle elles travaillent, tout comme pour les entreprises qui fournissent des services hébergés à leurs clients. Grâce au contrôle, les sociétés et les divisions payent uniquement ce qu'elles utilisent.

Quel que soit le scénario requis par votre société, dans Windows Server 2012, Hyper-V fournit une fonctionnalité appelée « Contrôle des ressources », qui vous permet d'analyser la consommation des ressources par ordinateur virtuel au fil du temps. Les données que vous collectez restent dans l'ordinateur virtuel, même si vous le déplacez en utilisant la migration dynamique, la migration hors connexion et la migration du stockage.

Le contrôle des ressources collecte les données suivantes de chaque ordinateur virtuel analysé :

- Moyenne d'utilisation de l'UC : mesurée en mégahertz sur une période spécifique.
- Utilisation moyenne de la mémoire physique : mesurée en mégaoctets.
- Utilisation minimale de la mémoire (quantité la plus basse de mémoire physique).
- Utilisation maximale de la mémoire (quantité la plus élevée de mémoire physique).
- Quantité maximale d'espace disque allouée à l'ordinateur virtuel.
- Trafic réseau entrant total : mesuré en mégaoctets, pour une carte réseau virtuelle.
- Trafic réseau sortant total : mesuré en mégaoctets, pour une carte réseau virtuelle.

Vous pouvez configurer le contrôle des ressources et récupérer les données collectées en utilisant l'interface de ligne de commande Windows PowerShell®. Les applets de commande suivantes sont utilisées pour le contrôle des ressources :

- **Enable-VMResourceMetering** : permet le contrôle des ressources pour un ordinateur virtuel donné.
- **Disable-VMResourceMetering** : désactive le contrôle des ressources pour un ordinateur virtuel donné.
- **Reset-VMResourceMetering** : Réinitialise les compteurs de contrôle des ressources pour un ordinateur virtuel donné.
- **Measure-VM** : affiche les données de contrôle des ressources pour un ordinateur virtuel donné.
- **Get-VM** : affiche les propriétés d'un ordinateur virtuel, ce qui vous permet d'afficher la propriété **ResourceMeteringEnabled** pour déterminer si le contrôle des ressources est activé pour l'ordinateur virtuel.

Démonstration : Activation et affichage des données de contrôle des ressources

Vous ne pouvez accéder au contrôle des ressources qu'à l'aide de commandes Windows PowerShell®. Vous devez activer le contrôle des ressources pour chaque ordinateur virtuel pour lequel vous voulez collecter des données de contrôle. Une fois que vous avez activé le contrôle des ressources, Hyper-V collecte et compile les données à tout moment. Vous pouvez utiliser l'interface de ligne de commande Windows PowerShell pour afficher les données collectées ou pour réinitialiser les compteurs de contrôle.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

1. Ouvrez l'environnement d'écriture de scripts intégré Windows PowerShell.
2. Dans la fenêtre Windows PowerShell ISE, tapez les commandes suivantes, en appuyant sur Entrée à la fin de chaque ligne :

```
$vms = Get-VM | ?{$_.State –eq “Running”}
$vms
```

3. Dans la fenêtre Windows PowerShell ISE, tapez la commande suivante pour afficher les propriétés des ordinateurs virtuels en cours d'exécution, puis appuyez sur Entrée :

```
$vms | Select Name, state, ResourceMeteringEnable
```

4. Dans la fenêtre Windows PowerShell ISE, tapez la commande suivante pour activer le contrôle des ressources, puis appuyez sur Entrée :

```
$vms | Enable-VMResourceMetering
```

5. Dans la fenêtre Windows PowerShell ISE, tapez la commande suivante pour afficher les données du contrôle des ressources, puis appuyez sur Entrée :

```
$vms | Measure-VM
```

6. Dans la fenêtre Windows PowerShell ISE, tapez la commande suivante pour afficher toutes les données du contrôle des ressources pour l'ordinateur virtuel 22414B-LON-DC1, puis appuyez sur Entrée :

```
Get-VM –Name 22414B-LON-DC1 | Measure-VM
```

7. Dans la fenêtre Windows PowerShell ISE, tapez la commande suivante pour désactiver le contrôle des ressources, puis appuyez sur Entrée :

```
$vms | Disable-VMResourceMetering
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Vue d'ensemble de System Center Operations Manager

Operations Manager est un outil d'analyse de serveurs idéal pour une utilisation dans les environnements d'entreprise où un haut niveau d'automatisation est requis. Semblable à l'Analyseur de performances et à l'Observateur d'événements, Operations Manager vous permet d'afficher les informations de performances des serveurs et de résoudre les problèmes. Par ailleurs, Operations Manager centralise ces fonctionnalités pour vous permettre d'analyser des centaines de serveurs à partir d'une console centrale unique.

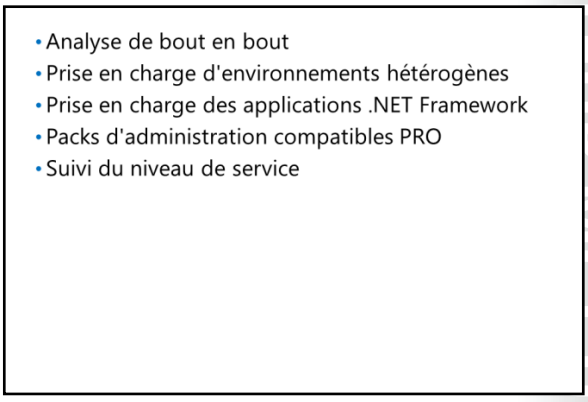
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les fonctionnalités clés d'Operations Manager ;
- décrire les composants d'Operations Manager ;
- utiliser la console Opérateur ;
- expliquer comment installer l'agent Operations Manager ;
- installer l'agent Operations Manager ;
- décrire les composants des services ACS ;
- expliquer comment déployer les services ACS ;
- collecter et afficher les données ACS ;
- décrire les éléments à prendre en compte pour le déploiement d'Operations Manager.

Fonctionnalités clés d'Operations Manager

Operations Manager fournit l'analyse de bout en bout de votre infrastructure informatique. Que votre environnement contienne des ordinateurs physiques ou virtuels, vous pouvez utiliser Operations Manager pour analyser les performances et la disponibilité de l'infrastructure. Vous pouvez afficher l'état d'intégrité des ordinateurs et des applications analysés par Operations Manager via les affichages des performances, des alertes et du tableau de bord.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Analyse de bout en bout

Operations Manager peut surveiller les applications de bout en bout. Cela signifie qu'il peut analyser l'application, le système d'exploitation sur lequel elle s'exécute, le matériel sur lequel repose le système d'exploitation et les périphériques réseau que vous utilisez pour permettre l'accès à l'application. Si vous distribuez l'application sur plusieurs systèmes, vous pouvez configurer Operations Manager pour afficher la topologie de l'application dans un espace de travail unique de sorte que les opérateurs puissent voir immédiatement où se situe le problème dans topologie.

Prise en charge d'environnements hétérogènes

Operations Manager prend en charge les systèmes d'exploitation Windows Server et les systèmes d'exploitation clients Windows, en plus des systèmes d'exploitation Linux et UNIX. Vous pouvez afficher les performances, la disponibilité et les alertes pour tous ces systèmes d'exploitation dans la même console.

Prise en charge des applications .NET Framework

Les applications qui reposent sur diverses technologies Microsoft .NET sont nombreuses. Operations Manager peut analyser les applications .NET Framework, y compris les performances du point de vue de l'utilisateur. Operations Manager inclut également les diagnostics des applications qui vous permettent d'isoler un problème en affichant les événements au niveau code qui se produisent.

Packs d'administration compatibles PRO

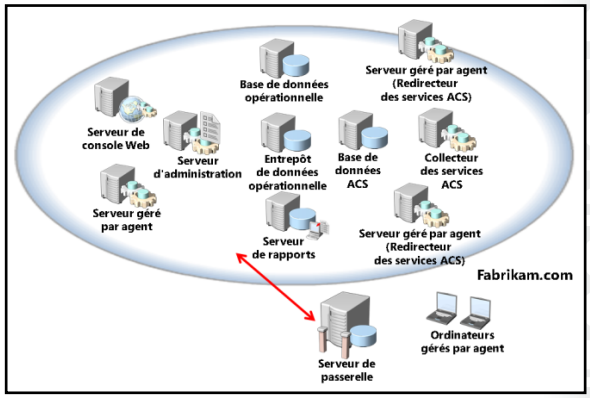
Operations Manager peut fournir des actions automatisées ou des suggestions sur une action spécifique à prendre dans l'environnement virtuel. Par exemple, un pack d'administration compatible PRO (optimisation des performances et des ressources) peut détecter s'il y a un problème avec un hôte de virtualisation et, si cela est approprié, peut automatiquement initialiser une action dans VMM pour migrer les ordinateurs virtuels vers un autre hôte de virtualisation.

Suivi du niveau de service

Vous pouvez utiliser Operations Manager pour créer des objets de suivi du niveau de service pouvant inclure vos applications sectorielles et l'infrastructure sous-jacente. Vous pouvez ensuite appliquer un objectif de niveau de service, c'est-à-dire des rapports sur la disponibilité des applications. Les rapports et les tableaux de bord d'Operations Manager peuvent ensuite incorporer ces informations, que vous pouvez utiliser pour vous aider à fournir des données de contrat de niveau de service.

Composants d'Operations Manager

Operations Manager intègre plusieurs composants qui fonctionnent ensemble pour analyser et gérer l'environnement de l'infrastructure informatique. Vous pouvez installer ces composants sur des systèmes distincts du réseau pour assurer l'évolutivité, la disponibilité et les meilleures performances de l'environnement d'Operations Manager.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'ensemble des composants d'Operations Manager que vous utilisez pour analyser un environnement donné est appelé « groupe d'administration ». Les grandes entreprises peuvent avoir plusieurs groupes d'administration qui se connectent dans une hiérarchie, et un groupe d'administration local peut recevoir les données consolidées des groupes d'administration connectés.

Les composants suivants forment un groupe d'administration d'Operations Manager :

- Rôles serveur d'Operations Manager :
  - Serveur d'administration
  - Serveur de passerelle
  - Base de données opérationnelle
  - Base de données de création de rapports Microsoft SQL Server®
  - Base de données d'entrepôt de données de création de rapports
  - Serveur de console Web
  - Collecteur des services ACS
  - Base de données ACS
  - Redirecteur des services ACS (sur les périphériques gérés par agent)
- Agents
- Console Opérateur
- Packs d'administration
- Pools de ressources
- Consoles Application Advisor et Application Diagnostics

Serveur d'administration

Le serveur d'administration d'Operations Manager est le premier composant installé dans un groupe d'administration. Il permet la communication entre les agents et le groupe d'administration, et sert de point d'administration pour la configuration du groupe d'administration.

Les agents envoient les données d'analyse vers un serveur d'administration pour inclusion à la base de données Opérateur. Si un serveur d'administration tombe en panne, un autre serveur d'administration peut assurer la charge automatiquement, ce qui fournit le basculement automatique pour la communication entre les agents et le groupe d'administration.

Pools de ressources

Vous pouvez utiliser des pools de ressources pour équilibrer la charge entre plusieurs serveurs d'administration qui font partie du même pool, ce qui fournit l'équilibrage de la charge et le basculement automatiques à l'environnement Operations Manager. Dès que vous ajoutez un serveur à un pool de ressources, il commence à répondre aux demandes automatiquement et réduit la charge sur les autres serveurs. Un seul serveur d'administration peut gérer un objet individuel à un moment donné.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Serveur de passerelle

Les serveurs de passerelle permettent la gestion des systèmes gérés par agent qui résident en dehors de la limite d'approbation du protocole Kerberos des groupes d'administration. Les agents des domaines qui ne sont pas approuvés communiquent avec la passerelle, puis le serveur de passerelle communique avec un ou plusieurs serveurs d'administration. Étant donné que le serveur de passerelle réside dans un domaine non approuvé, vous devez utiliser des certificats pour établir l'identité des systèmes gérés, du serveur de passerelle et des serveurs d'administration. En outre, le serveur de passerelle effectue la détection et l'installation, et relaie le trafic d'administration en cours vers les agents, au nom du serveur d'administration.



Remarque : Toutes les communications entre les serveurs de passerelle et les serveurs d'administration se produisent sur un port unique (TCP 5723), qui doit être ouvert sur n'importe quel pare-feu entre ces serveurs. Les serveurs de passerelle peuvent également détecter et gérer les ordinateurs UNIX et Linux via le port TCP 1270 et, selon les besoins, via le port TCP 22 (Secure Shell).

Base de données opérationnelle

La base de données opérationnelle stocke toutes les données d'analyse, d'alerte et de performances collectées des agents. Ces données comprennent les données d'événements et d'alerte, les données de performances et les données de modification d'état. Vous devez installer la base de données opérationnelle sur un serveur SQL Server 2008 R2. System Center 2012 Service Pack 1 (SP1) prendra en charge SQL Server 2012.

Base de données d'entrepôt de données de création de rapports

La base de données d'entrepôt de données de création de rapports stocke des données agrégées, utilisées pour la création de rapports. Les données collectées des agents sont stockées dans la base de données opérationnelle et dans la base de données d'entrepôt de données de création de rapport, simultanément. Le fait de disposer d'une base de données distincte pour générer des rapports réduit la charge sur la base de données opérationnelle. La base de données d'entrepôt de données stocke également les données pour longtemps.

Base de données de création de rapports SQL Server

System Center 2012 utilise SQL Server Reporting Services pour héberger et afficher les rapports. SQL Server Reporting Services utilise sa propre base de données pour stocker les définitions de rapport et mettre en cache les données de rapport.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Console Opérateur

La console Opérateur est une application Microsoft Silverlight® que les administrateurs utilisent pour gérer la plupart des fonctions typiques effectuées dans un environnement Operations Manager. La console Opérateur a cinq espaces de travail différents.

- Analyse : l'espace de travail Analyse contient plusieurs affichages, notamment Alertes actives, État de la tâche et État de Windows Server. De nouveaux affichages sont ajoutés automatiquement lorsque vous installez des packs d'administration. Vous pouvez également créer des affichages de tableau de bord, qui contiennent plusieurs espaces de travail et qui peuvent afficher les données d'un affichage distinct. Vous pouvez ensuite publier ces tableaux de bord vers Microsoft SharePoint® Server.
- Création : vous utilisez le volet Création pour personnaliser votre environnement Operations Manager en créant et en modifiant des règles, des analyseurs et des remplacements. Vous pouvez également créer vos propres packs d'administration dans l'espace de travail Création.
- Création de rapports : vous utilisez l'espace de travail Création de rapports pour afficher et créer des rapports.
- Administration : vous utilisez l'espace de travail Administration pour configurer votre environnement Operations Manager, ainsi que les notifications du programme d'installation, la sécurité et les pools de ressources.
- Mon espace de travail : vous utilisez Mon espace de travail pour accéder à vos affichages préférés et à vos recherches enregistrées. Chaque utilisateur possède ses propres paramètres pour Mon espace de travail.

Serveur de console Web

La console Web permet aux utilisateurs distants d'accéder à la plupart des fonctionnalités fournies dans la console Opérateur. Vous installez la console Web sur un ordinateur qui exécute le rôle Serveur Web. Vous sécurisez ensuite la console Web en utilisant des certificats.

Agents

L'agent Operations Manager est un service que vous pouvez installer sur les ordinateurs qu'Operations Manager gérera. L'agent collecte les données en fonction de règles et d'analyseurs, qui font partie des packs d'administration que vous déployez vers l'agent.

Packs d'administration

Les packs d'administration fournissent les éléments de base que vous utilisez pour analyser les objets gérés par Operations Manager. Les packs d'administration sont créés en tant que fichiers XML qui peuvent contenir un ou plusieurs des éléments suivants :

- Détections d'objets : les détections d'objets détectent les objets que vous souhaitez analyser en examinant les données récupérées d'un ordinateur géré par agent. La forme de détection la plus courante consiste à vérifier les données dans le Registre ou en utilisant le service Windows Management Instrumentation (WMI). Par exemple, vous pouvez lire le Registre pour trouver la version du système d'exploitation qui s'exécute sur un ordinateur donné. Si le système exécute Windows Server 2012, l'agent téléchargera le pack d'administration pour Windows Server 2012.
- Analyseurs : vous utilisez des analyseurs pour déterminer l'état d'intégrité d'un objet analysé. Il existe différents types d'analyseurs tels que les analyses d'unités, les analyses de cumul de dépendances et les analyses de cumul d'agrégats. Les analyseurs peuvent effectuer le suivi d'un service, recevoir des données de périphériques SNMP, de journaux d'événements ou de compteurs de performances, et retourner l'état d'intégrité de l'objet qu'ils analysent en fonction de critères que vous prédéfinissez.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Règles : vous utilisez les règles pour générer des alertes selon des critères prédéfinis, pour collecter des données pour les rapports ou pour exécuter une tâche planifiée.
- Tâches : vous utilisez les tâches pour exécuter des actions sur des objets analysés, par exemple redémarrer un service, en exécutant l'outil de ligne de commande **ipconfig** sur un système ou en recyclant un pool d'applications des services Internet (IIS).
- Affichages : dans la console Opérateur, les affichages présentent des informations spécifiques sur les objets analysés. Vous pouvez créer les affichages suivants :
  - Affichage Alerte : présente les alertes pour un groupe d'ordinateurs.
  - Affichage Événement : présente les événements spécifiques pour un ordinateur ou un groupe d'ordinateurs.
  - Affichage des états : présente l'état d'intégrité d'une application, d'un serveur ou d'un groupe de serveurs.
  - Affichage des performances : présente les compteurs de performances rassemblés pour un serveur donné.
  - Affichage des diagrammes : présente un diagramme contenant tous les serveurs utilisés pour effectuer une tâche ou pour héberger une application.
  - Affichage État de la tâche : présente toutes les tâches planifiées pour s'exécuter pour un serveur donné.
  - Affichage Page Web : contient un affichage auquel vous pouvez accéder sur un navigateur Web.
  - Affichage Tableau de bord : contient plusieurs espaces de travail, chacun disposant de son propre affichage, que vous pouvez publier vers SharePoint Server.
- Connaissances : les bases de connaissances fournissent de la documentation spécifique aux alertes générées par un pack d'administration donné. Les bases de connaissances contiennent des informations détaillées sur la façon de résoudre le problème lié à l'alerte. Vous pouvez personnaliser les bases de connaissances pour inclure des informations spécifiques liées à votre propre environnement d'infrastructure informatique.
- Remplacements : les remplacements vous permettent de personnaliser l'analyse par défaut fournie par les packs d'administration. Par exemple, un pack d'administration donné peut avoir un analyseur stipulant que l'état d'intégrité d'un serveur passe à « défectueux » quand sa mémoire disponible est inférieure à 10 %. Avec un remplacement, vous pouvez indiquer qu'un serveur donné peut avoir moins de mémoire disponible pendant un certain temps, sans que son état ne passe à « défectueux ».

Consoles Application Advisor et Application Diagnostics

Après avoir configuré l'Analyse des performances de l'application .NET, vous pouvez utiliser Application Advisor et Application Diagnostics pour résoudre les problèmes des applications .NET Framework. Pour commencer la résolution, Application Advisor identifie les applications qui ont généré le plus grand nombre d'alertes. La console Application Diagnostics affiche les événements liés aux performances et à la fiabilité pour les applications .NET Framework. Ces événements vous aident à identifier comment résoudre les problèmes avec l'application .NET Framework.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Collecteur des services ACS

Vous utilisez les services ACS pour collecter les événements générés par une stratégie d'audit, puis les stockez dans une base de données centralisée à l'aide de SQL Server. Une fois que les événements sont dans une base de données centralisée, les utilisateurs peuvent les filtrer et les analyser en utilisant les outils d'analyse des données de SQL Server.

Le collecteur des services ACS reçoit et traite les événements des redirecteurs des services ACS, puis envoie ces données à la base de données des services ACS. Ce traitement inclut le désassemblage des données et leur stockage dans plusieurs tables de la base de données des services ACS (ce qui réduit la redondance des données), ainsi que l'application de filtres afin que les événements inutiles ne soient pas ajoutés à la base de données des services ACS.

Base de données ACS

Vous pouvez installer la base de données ACS sur la même instance SQL Server que celle que vous utilisez pour la base de données opérationnelle ou sur une autre instance SQL Server. Si vous l'installez sur la même instance, vous pouvez afficher les rapports des services ACS directement depuis la console Opérateur. Sinon, vous accédez aux rapports via SQL Server Reporting Services (SSRS).

Redirecteur des services ACS

Le service qui s'exécute sur les redirecteurs des services ACS est inclus à l'agent Operations Manager. Par défaut, ce service est installé, mais non actif, quand vous installez l'agent Operations Manager. Vous pouvez activer ce service pour plusieurs ordinateurs d'agents à la fois en utilisant la tâche Activer la collecte d'audits. Une fois ce service activé, Operations Manager envoie tous les événements de sécurité aux services ACS et au journal de sécurité local.

Liens de référence : Pour plus d'informations sur le déploiement distribué d'Operations Manager, consultez http://go.microsoft.com/fwlink/?LinkID=285319.

Démonstration : Utilisation de la console Operations Manager

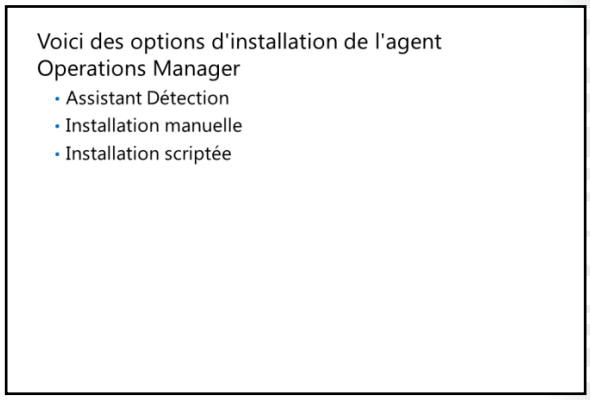
Procédure de démonstration

1. Sur l'écran d'accueil, cliquez sur **Operations Console** (Console Opérateur).
2. Dans l'espace de travail Analyse, prenez note des différents affichages disponibles sous le nœud **Operations Manager**.
3. Identifiez les différents nœuds de l'espace de travail Création.
4. Identifiez les différents nœuds de l'espace de travail Création de rapports.
5. Identifiez les différents nœuds de la console **Administration**.
6. Identifiez les différents nœuds de la console **Mon espace de travail**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options d'installation de l'agent Operations Manager

L'agent Operations Manager est disponible pour Windows XP et les ordinateurs avec de nouveaux clients, ou sur Windows Server 2003 ou de nouveaux systèmes d'exploitation serveur. Il existe également un agent Operations Manager disponible pour UNIX et Linux.



Liens de référence : Pour plus d'informations sur les systèmes d'exploitation pris en charge pour l'agent Operations Manager, reportez-vous à la page http://go.microsoft.com/fwlink/?LinkID=285321 et recherchez « Agent Operations Manager – ordinateurs Windows » dans le navigateur.

Vous pouvez installer l'agent Operations Manager pour les systèmes d'exploitation Windows de trois façons différentes. Vous pouvez utiliser l'Assistant Détection, procéder à une installation manuelle ou créer un script.

Assistant Détection

Vous pouvez utiliser l'Assistant Détection pour déployer des agents Operations Manager. Lorsque vous démarrez l'Assistant, vous pouvez choisir de détecter les ordinateurs Windows, UNIX/Linux ou des périphériques réseau. Après avoir sélectionné le type d'objet à détecter, vous pouvez choisir entre la détection automatique et la détection avancée.

- Détection automatique : la détection automatique analyse le domaine pour tous les ordinateurs Windows qui n'ont pas d'agent installé rapportant au groupe d'administration à partir de quel emplacement la détection est initialisée. Une fois l'analyse terminée, vous pouvez sélectionner vers quels ordinateurs vous souhaitez déployer l'agent.
- Détection avancée : la détection avancée vous permet de modifier l'étendue de la détection (serveurs, clients ou les deux) et de spécifier une requête LDAP à utiliser pour l'analyse (par exemple, tous les ordinateurs dont le nom commence par LON-). Vous pouvez également rechercher manuellement des ordinateurs.

La détection requiert un compte disposant de droits d'administration locaux sur les ordinateurs que vous voulez gérer. Vous pouvez fournir les informations d'identification pour le processus de détection ou utiliser le compte d'action du serveur d'administration. Vous utilisez également ces informations d'identification pour installer l'agent ou vous pouvez utiliser le compte administrateur local pour exécuter l'installation de l'agent. Dans ce cas, vous utilisez le compte administrateur local pour installer l'agent et vous utilisez le compte d'action du serveur d'administration pour la détection.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Une fois la détection terminée, vous pouvez choisir parmi la liste d'ordinateurs détectés. Les ordinateurs que vous sélectionnez sont les ordinateurs qu'Operations Manager analysera. Vous pouvez choisir si vous souhaitez que les ordinateurs soient gérés par agent ou sans agent. L'agent Operations Manager est installé sur les ordinateurs gérés par agent, tandis que le serveur d'administration effectue l'analyse sans agent à distance. Généralement, l'analyse sans agent offre moins de fonctionnalités que l'analyse gérée par agent, et n'est pas aussi évolutive. Certains Packs d'administration, tels que le pack d'administration des serveurs de domaine Active Directory, ne prennent pas en charge l'analyse sans agent.

Dans l'Assistant Détection, vous pouvez également spécifier le répertoire d'installation de l'agent et le compte d'action d'agent que l'agent utilise lors des actions. Vous pouvez modifier le compte d'action d'agent après installation, mais dans la plupart des cas, il doit être défini sur la valeur par défaut du système local. Certains packs d'administration ne fonctionnent correctement que lorsque vous utilisez le système local comme compte d'action d'agent. La documentation pour un pack d'administration inclura toutes les conditions requises pour le compte d'action d'agent.

Installation manuelle

Dans certaines circonstances, il peut être nécessaire d'installer l'agent manuellement. Cela peut être dû aux restrictions de pare-feu ou aux limites d'approbation. Par exemple, vous pourriez avoir un réseau de périmètre comprenant un serveur Web disponible au public, mais que vous avez sécurisé avec des pare-feu. En outre, ce serveur Web est dans son propre domaine ou groupe de travail, séparé du domaine et du réseau dans lesquels se trouve le groupe d'administration Operations Manager.

Dans ce scénario, vous utilisez des certificats et/ou des passerelles pour fournir la communication au serveur d'administration. En outre, vous devez installer l'agent manuellement, car les ports de pare-feu que vous utiliseriez normalement pour l'installer avec l'Assistant Détection sont bloqués.

Pour installer l'agent manuellement, vous pouvez exécuter le fichier setup.exe à partir du support Operations Manager et sélectionner l'option **Agent local**. Sinon, vous pouvez exécuter le fichier MOMAgent.msi du dossier Agent du support Operations Manager. Avec cette seconde méthode, vous pouvez ne copier que les fichiers d'agent requis sur l'ordinateur qui exécutera l'agent au lieu de copier tout le contenu du support.

Le dossier d'agent contient les fichiers d'installation de l'agent pour les versions AMD64, i386 et ia64 de l'agent. Vous pouvez exécuter le fichier MOMAgent.msi à partir du dossier approprié pour lancer la procédure d'installation de l'agent.

Installation scriptée

Vous pouvez transmettre des paramètres à MOMAgent.msi pour scripter l'installation et éviter l'Assistant d'installation. Pour installer l'agent à l'aide d'une installation scriptée, utilisez la commande suivante :

```
%WinDir%\System32\msiexec.exe /i path\Directory\MOMAgent.msi /qn
USE_SETTINGS_FROM_AD={0|1} USE_MANUALLY_SPECIFIED_SETTINGS={0|1} MANAGEMENT_GROUP=MGname
MANAGEMENT_SERVER_DNS=MSname MANAGEMENT_SERVER_AD_NAME =MSname SECURE_PORT=PortNumber
ACTIONS_USE_COMPUTER_ACCOUNT={0|1} ACTIONSUSER=UserName ACTIONSDOMAIN=DomainName
ACTIONSPASSWORD=Password
```

Vous pouvez utiliser la commande ci-dessus avec un script de connexion ou même avec un programme System Center 2012 Configuration Manager pour effectuer l'installation sur les ordinateurs existants.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Installation de l'agent Operations Manager

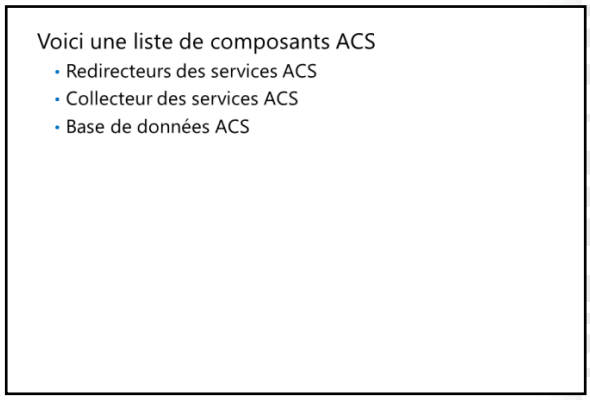
Dans cette démonstration, vous allez découvrir une méthode d'installation de l'agent Operations Manager.

Procédure de démonstration

- Exécutez l'Assistant Détection pour déployer le client Operations Manager sur les serveurs réseau.

Que sont les services ACS (Audit Collection Services) ?

Les services ACS permettent de collecter les enregistrements générés par une stratégie d'audit, puis de les stocker dans une base de données centralisée. Par défaut, quand vous implémentez une stratégie d'audit sur un ordinateur qui exécute un système d'exploitation Windows, cet ordinateur enregistre automatiquement tous les événements générés par la stratégie d'audit dans son journal de sécurité local. Cela est valable pour les stations de travail clientes Windows et les serveurs Windows. Dans les organisations où les exigences de sécurité sont strictes, les stratégies d'audit peuvent rapidement générer de très nombreux événements.



En utilisant les services ACS, vous pouvez consolider différents journaux de sécurité dans une base de données que vous pouvez gérer de manière centralisée, puis filtrer et analyser les événements à l'aide des outils d'analyse des données et de création de rapports fournis par SQL Server. Avec les services ACS, seul un utilisateur ayant reçu le droit d'accéder spécifiquement à la base de données ACS peut exécuter des requêtes et créer des rapports sur les données collectées.

Les services ACS requièrent les composants suivants :

- Redirecteurs des services ACS
- Collecteur des services ACS
- Base de données ACS

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Redirecteur des services ACS

Le service de redirecteur des services ACS fait partie de l'agent Operations Manager. Il est installé par défaut sur tous les ordinateurs sur lesquels l'agent est déployé. Cependant, ce service n'est pas activé tant que vous n'exécutez pas la tâche Activer la collecte d'audits à partir de la console Opérateur. Une fois ce service activé, tous les événements de sécurité sont envoyés au collecteur des services ACS et au journal de sécurité local.

Collecteur des services ACS

Le collecteur des services ACS reçoit et traite les événements des redirecteurs des services ACS, puis envoie ces données à la base de données des services ACS. Ce traitement inclut le désassemblage des données qui permet de placer ces dernières dans plusieurs tables de la base de données des services ACS (ce qui réduit la redondance des données), ainsi que l'application de filtres afin que les événements inutiles ne soient pas ajoutés à la base de données des services ACS.

Le nombre de redirecteurs des services ACS pouvant être pris en charge par un seul collecteur des services ACS et la base de données des services ACS peut varier, en fonction des facteurs suivants :

- Le nombre d'événements que votre stratégie d'audit génère.
- Le rôle des ordinateurs que les redirecteurs des services ACS analysent (comme le contrôleur de domaine par opposition au serveur membre).
- Le niveau des activités sur l'ordinateur.
- Le matériel sur lequel le collecteur des services ACS et la base de données des services ACS s'exécutent.

Si votre environnement contient trop de redirecteurs des services ACS pour un seul collecteur des services ACS, vous pouvez installer plusieurs collecteurs des services ACS. Toutefois, chaque collecteur des services ACS doit avoir sa propre base de données des services ACS.

Les conditions requises pour un collecteur des services ACS sont les suivantes :

- Un serveur d'administration Operations Manager.
- Un membre d'un domaine Active Directory.
- Au moins 1 Go de RAM, avec 2 Go recommandés.
- Au moins un processeur de 1,8 GHz, avec un processeur de 2,8 GHz recommandé.
- Au moins 10 Go d'espace disque disponible, avec 50 Go recommandés.

Sur chaque ordinateur sur lequel vous prévoyez d'installer le collecteur des services ACS, vous devez télécharger et installer la dernière version des composants Microsoft Data Access à partir du site Web de Microsoft.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Base de données ACS

La base de données des services ACS est le référentiel central pour les événements générés par une stratégie d'audit dans un déploiement des services ACS. La base de données des services ACS peut se trouver sur le même ordinateur que le collecteur des services ACS, mais pour de meilleures performances, chaque élément doit être installé sur un serveur dédié.

Les conditions requises pour une base de données des services ACS sont les suivantes :

- SQL Server 2005 ou SQL Server 2008. Vous pouvez choisir une installation existante ou nouvelle de SQL Server.
- Au moins 1 Go de RAM, avec 2 Go recommandés.
- Au moins un processeur de 1,8 GHz, avec un processeur de 2,8 GHz recommandé.
- Au moins 20 Go d'espace disque disponible, avec 100 Go recommandés.

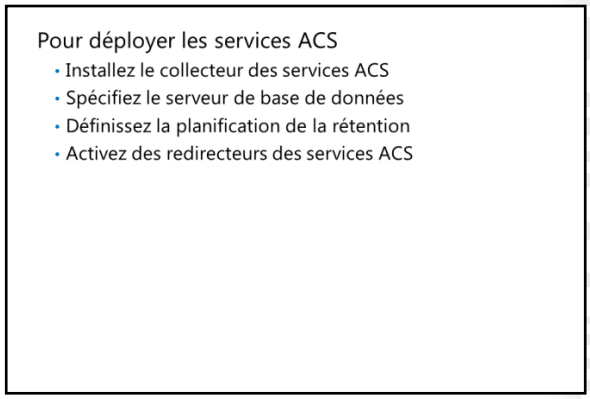
Liens de référence :

- Pour plus d'informations sur la façon de filtrer les événements des services ACS pour UNIX et Linux, consultez http://go.microsoft.com/fwlink/?LinkID=290803.
- Pour plus d'informations sur l'utilisation du contrôle d'accès dynamique avec les services ACS, consultez http://go.microsoft.com/fwlink/?LinkID=285318.

Si vous utilisez l'édition Standard de SQL Server, la base de données doit être interrompue pendant les opérations de maintenance quotidiennes. Par conséquent, la file d'attente du collecteur des services ACS peut se remplir de demandes de redirecteurs des services ACS. Lorsqu'une file d'attente de collecteur des services ACS est pleine, les redirecteurs des services ACS sont déconnectés du collecteur des services ACS de planification et configuration des notifications et de la création de rapports. Les redirecteurs des services ACS déconnectés se reconnectent une fois la maintenance de la base de données terminée, puis la base de données traite la file d'attente. Pour qu'aucun événement d'audit ne soit perdu, assurez-vous d'allouer assez d'espace disque au journal de sécurité locale sur tous les redirecteurs des services ACS. Cependant, dans ce cas, il peut y avoir une courte période considérée comme un risque de sécurité, car les événements sont décalés par rapport à l'activité réelle. Si vous utilisez l'édition Entreprise de SQL Server, vous pouvez éviter ce problème car la base de données ne s'arrête pas pendant la maintenance.

Déploiement des services ACS (Audit Collection Services)

Pour utiliser les services ACS, vous devez déployer au moins un collecteur des services ACS, une base de données des services ACS par collecteur, des redirecteurs des services ACS et la création de rapports des services ACS.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Installation de collecteurs et de bases de données des services ACS

Pour installer un collecteur et une base de données des services ACS, procédez comme suit :

1. Ouvrez une session sur le serveur avec un compte disposant d'informations d'identification d'administration locales.
2. Sur le support d'installation d'Operations Manager, exécutez **Setup.exe**, puis cliquez sur **Services ACS**. Pour analyser des ordinateurs UNIX et Linux, cliquez sur **Services ACS pour UNIX/Linux**.
3. Dans la page d'**accueil** de l'Assistant Programme d'installation du collecteur des services ACS, cliquez sur **Suivant**.
4. Dans la page **Contrat de licence**, lisez le contrat, cliquez sur **J'accepte les termes du contrat de licence**, puis sur **Suivant**.
5. Dans la page **Options d'installation de la base de données**, cliquez sur **Créer une nouvelle base de données**, puis sur **Suivant**.
6. Dans la page **Source de données**, dans la zone **Nom de la source de données**, tapez le nom que vous souhaitez utiliser comme nom de source de données ODBC (Open Database Connectivity) pour votre base de données des services ACS (par défaut, ce nom est **OpsMgrAC**), puis cliquez sur **Suivant**.
7. Dans la page **Base de données**, si la base de données est sur un serveur indépendant de celui du collecteur des services ACS, cliquez sur **Serveur de base de données distant**, puis tapez le nom d'ordinateur du serveur de base de données qui hébergera la base de données pour cette installation des services ACS. Sinon, cliquez sur **Serveur de base de données exécuté localement**.
8. Dans le champ **Nom d'instance du serveur de base de données**, tapez le nom de la base de données qui sera créée pour les services ACS, puis cliquez sur **Suivant**. Si vous laissez ce champ vide, le nom par défaut **OpsMgrAC** sera utilisé. Dans le champ **Nom de la base de données**, le nom de base de données par défaut **OperationsManagerAC** est écrit automatiquement. Vous pouvez laisser le nom par défaut ou le mettre en surbrillance et taper un autre nom.
9. Dans la page **Authentification de la base de données**, sélectionnez l'une des méthodes d'authentification. Si le collecteur et la base de données des services ACS sont membres du même domaine, sélectionnez **Authentification Windows**. Sinon, sélectionnez **Authentification SQL**, puis cliquez sur **Suivant**.

Remarque : Si vous sélectionnez **Authentification SQL**, puis cliquez sur **Suivant**, la page **Informations d'identification de la base de données** s'affiche. Dans la zone **Nom de connexion SQL**, entrez le nom du compte d'utilisateur qui a accès à SQL Server et le mot de passe pour ce compte dans la zone **Mot de passe SQL**, puis cliquez sur **Suivant**.

10. Dans la page **Options de création de la base de données**, cliquez sur l'une des deux options suivantes, puis sur **Suivant** :
    - **Utiliser les répertoires de données et de fichiers journaux par défaut de SQL Server** pour utiliser les dossiers par défaut de SQL Server ou
    - **Spécifier les répertoires** et entrez le chemin complet, y compris la lettre de lecteur, de l'emplacement que vous souhaitez utiliser pour la base de données et le fichier journal des services ACS. Par exemple, C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data.

11. Dans la page **Planification de rétention des événements**, cliquez sur **Heure locale de maintenance quotidienne de la base de données**. Choisissez une heure où le nombre d'événements de sécurité prévus est bas car les performances de la base de données seront affectées pendant la maintenance. Dans la zone **Nombre de jours pendant lesquels conserver les événements**, tapez le nombre de jours pendant lesquels les services ACS doivent conserver les événements dans la base de données des services ACS avant de les supprimer au cours du nettoyage de la base de données. La valeur par défaut est de 14 jours. Cliquez sur **Suivant**.
12. Dans la page **Format d'horodatage des services ACS stocké**, choisissez **Local** ou **Heure UCT** (autrefois, GMT), puis cliquez sur **Suivant**.
13. La page **Résumé** affiche la liste des actions que le programme d'installation effectuera pour installer les services ACS. Passez la liste en revue, puis cliquez sur **Suivant** pour commencer l'installation.

 **Remarque :** Si une boîte de dialogue **Connexion à SQL Server** s'affiche et que l'authentification de base de données est définie sur **Authentification Windows**, cliquez sur la base de données correcte et vérifiez que la case à cocher **Utiliser une connexion approuvée** est sélectionnée. Sinon, désactivez la case à cocher, tapez le nom de connexion SQL et le mot de passe, puis cliquez sur **OK**.

14. Une fois l'installation achevée, cliquez sur **Terminer**.

Activation de redirecteurs des services ACS

Pour activer les redirecteurs des services ACS, procédez comme suit :

1. Connectez-vous à l'ordinateur avec un compte membre du rôle Administrateurs d'Operations Manager. Ce compte doit également posséder les droits d'un administrateur local sur chaque ordinateur d'agent que vous souhaitez activer en tant que redirecteur des services ACS.
2. Dans la console Opérateur, cliquez sur **Analyse**.
3. Dans l'espace de travail de navigation, développez **Operations Manager**, **Détails des agents**, puis cliquez sur **État d'intégrité des agents**. Cet affichage contient deux espaces de travail, et les actions de cette procédure sont exécutées dans le bon espace de travail.
4. Dans l'espace de travail des détails, cliquez sur tous les agents que vous souhaitez activer comme redirecteurs des services ACS. Vous pouvez faire des choix multiples en appuyant sur Ctrl ou Maj.
5. Dans l'espace de travail Actions, sous **Tâches du service de contrôle d'intégrité**, cliquez sur **Activer la collecte d'audits** pour ouvrir la boîte de dialogue **Exécuter la tâche - Activer la collecte d'audits**.
6. Dans la section **Paramètres de la tâche**, cliquez sur **Remplacer** pour ouvrir la boîte de dialogue **Remplacer les paramètres de la tâche**.
7. Dans la section **Remplacer les paramètres de la tâche avec les nouvelles valeurs**, cliquez sur le paramètre **CollectorServer** ; dans la colonne **Nouvelle valeur**, tapez le nom de domaine complet du collecteur des services ACS ; puis cliquez sur **Remplacer**.

 **Remarque :** Si vous activez les services ACS sur une passerelle ou le serveur d'administration et que vous ne spécifiez pas le paramètre CollectorServer, la tâche échouera avec une « erreur d'incompatibilité de type ». Pour éviter cela, fournissez une valeur pour le remplacement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

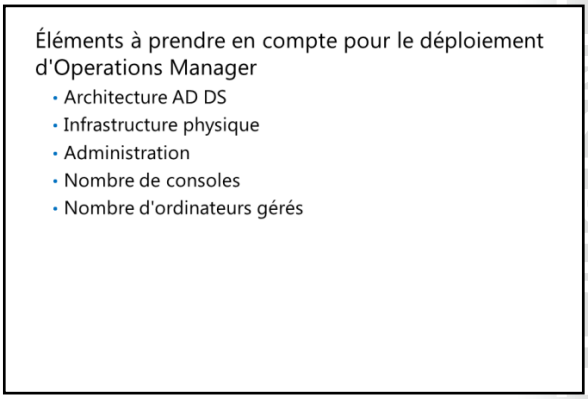
8. Dans la section **Identification de la tâche**, cliquez sur **Autre**. Dans la zone **Nom d'utilisateur**, tapez le nom d'un compte d'utilisateur qui appartient au groupe Administrateurs local sur les ordinateurs d'agents. Dans la zone **Mot de passe**, tapez le mot de passe pour ce compte d'utilisateur. Cliquez pour développer la liste **Domaine** afin d'afficher les domaines disponibles, puis cliquez sur le domaine du compte d'utilisateur.
9. Cliquez sur **Exécuter la tâche**. La boîte de dialogue **État de la tâche** s'affiche et suit la progression de la tâche.
10. Lorsque la tâche est correctement terminée, cliquez sur **Fermer**.

Liens de référence :

- Pour plus d'informations sur la configuration de certificats pour le collecteur et le redirecteur des services ACS, consultez http://go.microsoft.com/fwlink/?LinkID=285320.
- Pour plus d'informations sur l'administration des services ACS et sur l'outil AdtAdmin.exe, consultez http://go.microsoft.com/fwlink/?LinkID=285317.

Éléments à prendre en compte pour le déploiement d'Operations Manager

Vous devez prendre en compte plusieurs facteurs lorsque vous concevez votre environnement Operations Manager. Vous devez prendre en compte l'architecture AD DS, les pare-feu et la disponibilité de la bande passante entre les sites.



La liste suivante résume ces facteurs et leur relation à vos décisions de conception :

- Architecture AD DS : vous pouvez utiliser un groupe d'administration pour gérer n'importe quel ordinateur d'une forêt approuvée. Si vous devez gérer des ordinateurs externes à votre limite d'authentification Kerberos, vous devez utiliser un serveur de passerelle et des certificats.
- Infrastructure physique : la bande passante minimale requise pour les communications entre un ordinateur géré par agent et un serveur d'administration est de 64 kilobits par seconde (Kbits/s). Entre un ordinateur analysé sans agent et le serveur d'administration, la bande passante minimale requise est de 1 024 Kbits/s. Si votre bande passante passe au-dessous de ces paramètres, vous devez envisager d'utiliser plusieurs serveurs d'administration.
- Administration : si vous avez différents besoins d'analyse à différents emplacements physiques, vous pouvez envisager de déployer plusieurs groupes d'administration. Cependant, il est recommandé que la bande passante minimale entre des groupes d'administration à niveaux soit de 1 024 Kbits/s.
- Nombre de consoles Opérateur : les consoles Opérateur peuvent être utilisées par plusieurs utilisateurs de votre organisation. La limite recommandée du nombre de consoles Opérateur ouvertes simultanément est de 50 par groupe d'administration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Nombre d'ordinateurs gérés par agent par serveur d'administration : un serveur d'administration doit gérer 3 000 ordinateurs au maximum.
- Nombre d'ordinateurs gérés par agent par serveur de passerelle : il est recommandé qu'un serveur de passerelle gère 2 000 ordinateurs au maximum.
- Nombre d'ordinateurs gérés sans agent par serveur d'administration : il est recommandé qu'un serveur d'administration gère 10 ordinateurs gérés sans agent au maximum.
- Nombre d'ordinateurs AEM (analyse des exceptions sans agent) par serveur d'administration dédié : il est recommandé qu'un serveur d'administration dédié gère 25 000 ordinateurs AEM au maximum.
- Nombre d'ordinateurs analysés par client collectif par serveur d'administration : il est recommandé qu'un serveur d'administration gère 2 500 ordinateurs clients au maximum.
- Nombre d'ordinateurs gérés sans agent par groupe d'administration : il est recommandé qu'un groupe d'administration gère 60 ordinateurs gérés sans agent au maximum.
- Nombre d'ordinateurs gérés par agent par groupe d'administration : il est recommandé qu'un groupe d'administration gère 6 000 ordinateurs au maximum lors de l'utilisation de 50 consoles Opérateur ouvertes ou 15 000 lors de l'utilisation de 25 consoles ouvertes.
- Nombre d'ordinateurs AEM par groupe d'administration : il est recommandé qu'un groupe d'administration gère 100 000 ordinateurs AEM au maximum.
- Serveurs d'administration par agent pour l'hébergement multiple : il est recommandé qu'un ordinateur géré utilise l'hébergement multiple avec quatre serveurs d'administration au maximum.

 **Liens de référence :** Configuration requise : System Center 2012 SP1 - Operations Manager http://go.microsoft.com/fwlink/?LinkID=285321**.**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Planification et configuration de packs d'administration

Les packs d'administration stockent les règles d'analyse de l'intégrité de vos serveurs et de génération d'alertes dans le cas où l'état d'intégrité requiert une attention particulière. Vous devez comprendre comment importer les packs d'administration pour des applications et des rôles de serveur spécifiques. Vous devez également comprendre comment optimiser ces packs d'administration pour votre environnement afin de vous assurer que seules des alertes pertinentes sont générées.

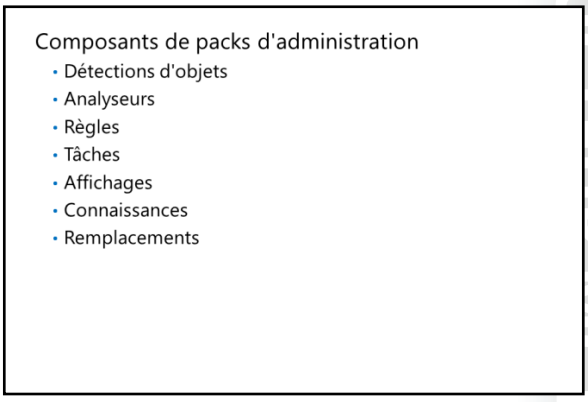
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les packs d'administration ;
- décrire la création de packs d'administration ;
- afficher des classes et des objets ;
- décrire la définition d'autorisations ;
- installer et optimiser les packs d'administration ;
- importer des packs d'administration ;
- créer des remplacements ;
- planifier l'analyse avec Operations Manager.

Vue d'ensemble des packs d'administration

Comme nous l'avons vu précédemment dans ce module, les packs d'administration fournissent les éléments de base utilisés pour analyser les objets gérés par Operations Manager. Les packs d'administration peuvent contenir un ou plusieurs des éléments suivants :

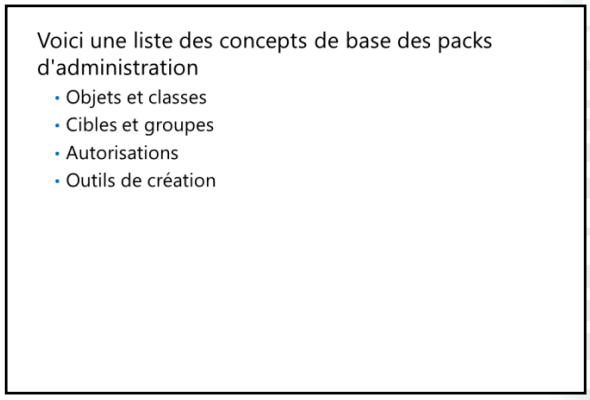


- Détections d'objets : les détections d'objets sont utilisées pour détecter les objets que vous souhaitez analyser.
- Analyseurs : les analyseurs sont utilisés pour déterminer l'état d'intégrité d'un objet analysé.
- Règles : les règles sont utilisées pour : générer des alertes selon des critères prédéfinis, collecter des données pour les rapports ou exécuter une tâche planifiée.
- Tâches : les tâches sont utilisées pour exécuter des actions sur les objets analysés.
- Affichages : les affichages sont utilisés dans la console Opérateur pour présenter des informations spécifiques sur les objets analysés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Connaissances : les bases de connaissances fournissent de la documentation propre aux alertes générées par un pack d'administration donné et contiennent des informations détaillées sur la façon de résoudre le problème lié à l'alerte.
- Remplacements : les remplacements vous permettent de personnaliser l'analyse par défaut fournie par les packs d'administration.

Création de packs d'administration



Plusieurs packs d'administration sont disponibles pour analyser des applications particulières. Ces packs d'administration sont créés par les sociétés qui fabriquent le matériel ou les logiciels dont l'analyse est permise par le pack d'administration en question. La société Microsoft elle-même publie des packs d'administration pour chaque produit (parfois même pour des fonctionnalités spécifiques de produits).

Le plus souvent, vous allez créer un pack d'administration uniquement pour le stockage de personnalisations apportées à des packs d'administration existants que vous téléchargez et déployez dans votre environnement Operations Manager. Nous vous recommandons de procéder ainsi afin d'avoir toutes vos personnalisations au même emplacement et de pouvoir facilement les sauvegarder et les envoyer ailleurs ou les restaurer, si besoin. Cela évite également de perdre vos personnalisations en cas de mises à jour d'un pack d'administration.

Cependant, vous pouvez aussi avoir besoin de créer un pack d'administration pour une application personnalisée ou du matériel ou un logiciel que votre société a créé et décidé de vendre. En outre, diverses sociétés créent et vendent des packs d'administration destinés à des applications pour lesquelles les concepteurs n'ont pas créé de pack d'administration.

Concepts de base

Avant de commencer à créer des packs d'administration, vous devez comprendre certains concepts de base et la terminologie relative aux objets analysés.

- *Objet* : un objet est l'unité de base de l'administration dans Operations Manager. Il représente un élément de votre infrastructure informatique tel qu'un ordinateur, une imprimante, un routeur. Il peut également représenter des éléments plus abstraits tels qu'AD DS, un site Web ou une application. Pour que les objets puissent être utilisés, ils doivent être détectés. Les différents packs d'administration contiennent des détections différentes pour les types d'objets qu'ils administrent. Ces détections s'exécutent à des moments différents selon le type d'objet pour lequel elles effectuent l'analyse. Les détections inspectent les propriétés des ordinateurs et des périphériques gérés par Operations Manager pour déterminer l'existence d'objets donnés dans ces périphériques analysés.
- *Classe* : une classe représente un type d'objet et chaque objet détecté par Operations Manager est dit être une instance d'une classe particulière. Les instances de la même classe partagent un ensemble de propriétés. Par exemple, chaque ordinateur a un nom d'ordinateur, un système d'exploitation et une quantité de mémoire. Ce sont les propriétés de la classe Ordinateur. Chaque ordinateur détecté peut avoir une valeur différente pour ces propriétés. Ces valeurs sont inspectées pendant la détection et renseignées pour chaque objet individuel trouvé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Cible* : lors de la création d'éléments dans un pack d'administration, vous devez spécifier une cible pour l'élément. Par exemple, lorsque vous créez un analyseur, vous devez spécifier le type d'objet qu'il analyse. Dans Operations Manager, une cible représente toutes les instances d'une classe donnée.
- *Classes d'hébergement* : la plupart des classes sont des classes enfant d'une autre classe ou hébergées par une autre classe. Par exemple, la classe Disque logique est une classe enfant de la classe Ordinateur. Il n'est pas nécessaire d'analyser un disque logique tout seul. Le disque existe uniquement à l'intérieur d'un ordinateur. Par conséquent, la classe Ordinateur est la classe hôte de la classe Disque logique.
- *Groupe* : un groupe est une collection d'objets qui peuvent être des instances de la même classe ou de différentes classes. Les groupes sont renseignés selon des critères prédéfinis qui peuvent être explicites (Groupe1 est composé des ordinateurs A, B et C) ou dynamiques (Groupe2 est composé de tous les ordinateurs exécutant SQL Server 2008 R2 Standard). Vous pouvez utiliser les groupes pour définir l'étendue des remplacements, des affichages et des rôles d'utilisateur.

 **Remarque :** Vous ne pouvez pas utiliser les groupes comme cibles, analyseurs ou règles. Les analyseurs ou les règles peuvent uniquement cibler des classes. Si vous devez limiter l'étendue d'un analyseur ou d'une règle à un groupe, vous devez créer un remplacement.

Autorisations

Pour qu'un utilisateur puisse créer un pack d'administration et des objets dans un pack d'administration, il doit avoir accès à l'espace de travail de création. Pour accéder à cet espace de travail, un utilisateur doit être membre du rôle d'utilisateur Auteur ou Administrateur dans Operations Manager. Lors de l'implémentation de la sécurité dans Operations Manager, vous pouvez limiter l'accès à des types spécifiques d'objets à l'aide d'une étendue. Si un utilisateur a uniquement accès à un ensemble précis de types d'objets (ou de classes), il ne peut créer des éléments que dans un pack d'administration qui affectera ces classes.

Outils de création

Vous pouvez utiliser plusieurs outils de création pour créer des packs d'administration et leurs objets :

- Console Opérateur : pour créer des objets d'analyse, vous pouvez utiliser différents modèles et Assistants de la console Opérateur, qui requièrent peu de connaissances sur les concepts de création. Depuis l'espace de travail de création, vous pouvez utiliser les outils suivants :
  - Modèles de pack d'administration : les modèles de pack d'administration vous permettent de créer des éléments d'analyse en fonction de scénarios prédéfinis.
  - Concepteur d'applications distribuées : le Concepteur d'applications distribuées permet de créer une seule application qui comprend plusieurs composants. Il ne vous permet pas de créer des analyseurs pour les composants de l'application. L'intégrité de chaque composant est déterminée par les analyseurs existants pour ce composant, et l'intégrité de l'application est déterminée par l'intégrité de ses différents composants.
  - Assistants de création : vous pouvez utiliser les assistants pour créer des analyseurs, des règles et des tâches.
- Microsoft Visio® Management Pack Designer : est un complément Microsoft Visio 2010 qui vous permet de créer des packs d'administration en utilisant l'interface utilisateur graphique disponible dans Visio. Vous pouvez ajouter des scénarios d'analyse à un pack d'administration en faisant glisser des formes vers un diagramme Visio.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Extensions de création Visual Studio : les extensions de création Visual Studio vous permettent de modifier le contenu XML d'un pack d'administration, tout en fournissant la fonctionnalité IntelliSense® et la possibilité de partager la création d'un pack d'administration avec plusieurs auteurs simultanément.
- Console de création de System Center Operations Manager 2007 R2 : bien qu'elle ait été créée pour Operations Manager 2007 R2, vous pouvez utiliser cette console pour créer l'administration pour Microsoft System Center Operations Manager 2007 R2 ou pour Operations Manager. Cependant, cet outil requiert des connaissances approfondies et la compréhension des éléments d'un pack d'administration. De plus, vous devez uniquement l'utiliser pour créer des packs d'administration complets pour les applications personnalisées ou les périphériques.

Démonstration : Affichage des classes et des objets

Procédure de démonstration

Ouvrez et examinez la liste des classes et des objets de la console Opérateur.

Démonstration : Définition d'autorisations

Procédure de démonstration

1. Créez un nouveau rôle Opérateur pour le groupe informatique à l'aide des paramètres suivants :
   - Nom : **Opérateurs de serveur**
   - Groupe : **Groupe d'ordinateurs Windows Server**
   - Tâches :
     - **Désactiver la collecte d'audits**
     - **Activer la collecte d'audits**
     - **Ping**
     - **Redémarrer le service Windows**
   - Analyse des affichages : **Tous les affichages sous Microsoft Windows Server**
   - Tableaux de bord des tâches : **Tableau de bord détaillé - Liste**
2. Connectez-vous à la console Operations et cliquez sur Exécuter en tant qu'autre utilisateur du groupe informatique pour tester les autorisations.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Installation et optimisation de packs d'administration

Une fois que vous aurez installé Operations Manager, vous aurez accès à des dizaines de packs d'administration directement depuis Microsoft. L'une des erreurs les plus communes faites par les administrateurs Operations Manager débutants est d'importer chaque pack d'administration qu'ils trouvent. Après tout, si le pack d'administration existe, il doit être important. N'oubliez pas que chaque pack d'administration contient des dizaines, des centaines, voire des milliers d'objets. Certains de ces objets collectent des données auprès des agents dans des intervalles très courts, données qui sont envoyées via votre réseau et stockées dans la base de données Operations Manager.

Pour personnaliser des packs d'administration, vous devez

1. Identifier les éléments à analyser
2. Importer les packs d'administration pour tester l'environnement
3. Étudier les guides des packs d'administration
4. Personnaliser les packs d'administration
5. Tester les packs d'administration
6. Exporter les personnalisations
7. Importer les personnalisations en production

Vous devez vous demander quels packs d'administration s'appliquent à votre environnement en fonction des applications et des services que vous avez besoin d'analyser. Une approche plus détaillée de l'optimisation des packs d'administration est présentée ci-dessous :

1. Identifiez les applications et les périphériques de votre infrastructure informatique que vous souhaitez voir analysés par Operations Manager.
2. Lisez le guide de chaque pack d'administration et identifiez les analyseurs, les règles et les détections qui doivent être remplacés pour votre environnement.
3. Téléchargez et importez les packs d'administration dans un environnement de test.
4. Créez un pack d'administration distinct pour stocker les personnalisations pour chaque pack d'administration que vous importez.
5. Créez vos groupes, remplacements et tout autre objet dont vous avez besoin dans vos packs d'administration.
6. Testez le pack d'administration dans votre environnement de test.
7. Exportez vos packs d'administration personnalisés.
8. Installez les packs d'administration d'origine et les packs d'administration personnalisés dans votre environnement de production.

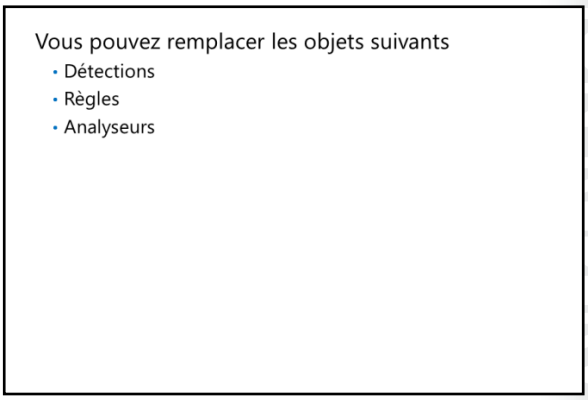
Démonstration : Importation de packs d'administration

Procédure de démonstration

- Importez le pack d'administration SQL Server vers LON-OM1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Création de remplacements



Operations Manager 2012 a deux types de packs d'administration : scellé et non scellé. Vous ne pouvez pas modifier les packs d'administration scellés sans utiliser d'outils tiers. Vous pouvez modifier les packs d'administration non scellés dans l'espace de travail Création.

La plupart des packs d'administration que vous téléchargez de Microsoft et d'autres fournisseurs seront des packs d'administration scellés, et sont donc difficiles voire impossibles à modifier. Cependant, selon la façon dont leurs détections, leurs analyseurs et leurs règles ont été créés, vous pourrez éventuellement remplacer les paramètres que leurs éléments utilisent. Étant donné que ces packs d'administration sont scellés, les remplacements créés pour eux ne peuvent pas être enregistrés dans le même pack d'administration. Par conséquent, vous devez créer un pack d'administration distinct pour les remplacements. C'est une des raisons qui vous pousseront à créer un pack d'administration distinct pour des remplacements. Même si un pack d'administration est non scellé, il est toutefois toujours recommandé de créer un pack d'administration distinct pour tout type de personnalisation que vous pouvez apporter au pack d'administration.

Avant de créer des remplacements pour les packs d'administration existants, il est très important que vous sachiez quelles règles et quels analyseurs vous remplacez, et pourquoi. Un pack d'administration peut contenir des dizaines, parfois des centaines de règles et analyseurs. Afin d'aider les administrateurs d'Operations Manager, Microsoft publie un guide pour chacun de ses packs d'administration. Veillez à lire le guide pour identifier tous les éléments qui peuvent et doivent être remplacés, selon votre environnement.

Par exemple, imaginez que vous ayez un pack d'administration contenant un analyseur d'unités indiquant que si le % du temps processeur d'un ordinateur qui exécute une application appelée Application1 dépasse 80 %, l'état d'intégrité de l'application doit être critique. Celui-ci devrait bien fonctionner sur des ordinateurs physiques, mais comme indiqué dans la leçon 1, vous ne devez pas utiliser ce compteur de performances pour des ordinateurs virtuels. Au lieu de cela, vous devriez créer un groupe contenant tous les ordinateurs virtuels exécutant Application1, puis créer un remplacement qui vise ce groupe et désactive l'analyseur. En outre, vous pourriez créer un analyseur distinct pour ces ordinateurs virtuels, qui analyse le compteur Processeur logique de l'hyperviseur Hyper-V\% de la durée d'exécution de l'invité pour l'hôte Hyper-V qui héberge l'ordinateur virtuel. Vous pourriez ensuite définir l'intégrité de l'application selon ce compteur. Vous pourriez créer ces nouveaux objets (remplacement, groupe et nouvel analyseur) dans un pack d'administration distinct.

Liens de référence : Boris's OpsMgr Tools – Updated http://go.microsoft.com/fwlink/?LinkID=285311.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification de l'analyse avec Operations Manager

Discutez de chaque question avec la classe. N'oubliez pas que les réponses varieront selon l'environnement du stagiaire. Il n'y a pas de bonne ou de mauvaise réponse ici. Mais il peut y avoir des réponses meilleures et pires que d'autres. Informez les stagiaires qu'ils doivent utiliser le moins de groupes et de serveurs d'administration possible, en fonction du nombre d'emplacements qu'ils ont et du nombre de périphériques gérés. Il en va de même pour les packs d'administration ; moins il sont nombreux, mieux c'est, en fonction des technologies qu'ils ont implémentées.

- De combien de groupes d'administration pensez-vous avoir besoin dans votre environnement actuel ?
- De combien de serveurs d'administration par groupe d'administration pensez-vous avoir besoin ?
- Quels packs d'administration pensez-vous importer ?
- Quels remplacements pourriez-vous avoir besoin de créer ?
- Utiliseriez-vous des abonnements aux événements dans l'Observateur d'événements, par opposition aux services ACS ? Pourquoi ou pourquoi pas ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4

Planification et configuration des notifications et de la création de rapports

Les notifications peuvent être utilisées pour alerter les administrateurs de serveurs si Operations Manager détecte des problèmes liés aux serveurs qu'ils administrent. Operations Manager peut envoyer des notifications via un courrier électronique, un texto, la messagerie instantanée ou en exécutant une commande. Operations Manager s'intègre également aux SQL Server Reporting Services (SSRS) pour fournir des rapports personnalisables auxquels les administrateurs peuvent accéder directement depuis la console d'Operations Manager ou en utilisant le site Web des SSRS.

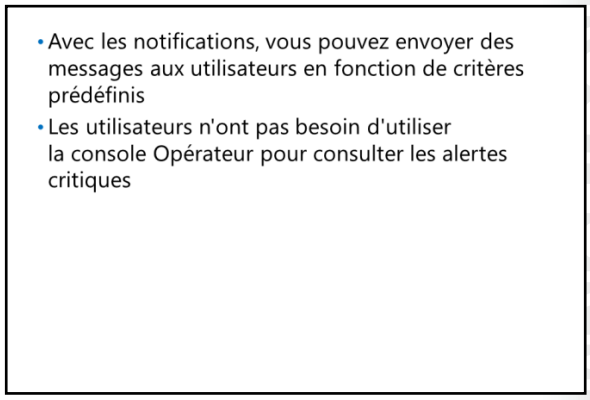
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les canaux de notification, les abonnés et les abonnements ;
- créer des canaux de notification ;
- configurer des abonnés aux notifications ;
- créer des abonnements ;
- accéder aux rapports.

Vue d'ensemble des notifications

Les utilisateurs d'Operations Manager peuvent utiliser la console Opérateur pour afficher les alertes générées par les diverses règles et divers analyseurs déployés sur l'environnement Operations Manager. Bien que la console Opérateur soit un emplacement parfait pour accéder à ces alertes, vous aurez peut-être parfois besoin que des alertes soient envoyées à un autre groupe de votre organisation, qui pourra ne pas avoir accès à la console, ou pouvez ne pas avoir un administrateur d'Operations Manager qui consulte la console fréquemment.

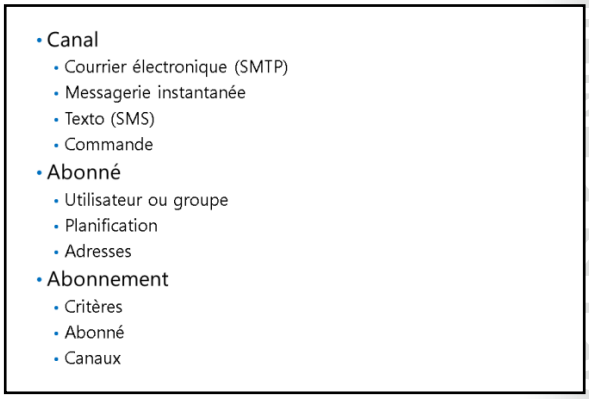


Par exemple, vous pouvez vouloir avertir les administrateurs d'une base de données de commerce électronique critique si l'état de la base de données qu'ils gèrent passe hors connexion. Il peut y avoir une ou plusieurs alertes générées par différents analyseurs ou règles qui analysent la base de données et le serveur sur lequel elle réside. En outre, les administrateurs de base de données peuvent ne pas vérifier la console Opérateur régulièrement. Dans ce cas, vous pouvez utiliser une notification pour envoyer une alerte aux administrateurs de base de données selon un ensemble de critères. Les notifications peuvent être envoyées via un courrier électronique, un texto, la messagerie instantanée ou en exécutant une commande personnalisée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des notifications

Pour utiliser des notifications, vous devez créer et configurer les objets suivants dans la console Opérateur :



- Canal : les canaux précisent le type de solution de messagerie utilisé pour la notification. Quatre types de canaux peuvent être utilisés :
  - Courrier électronique (SMTP) : pour envoyer des courriers électroniques.
  - Messagerie instantanée : pour envoyer des messages instantanés.
  - Texto (SMS) : pour envoyer des textos.
  - Commande : pour exécuter une commande personnalisée.
- Abonné : les abonnés représentent les utilisateurs ou groupes qui peuvent recevoir une notification. Chaque abonné contient les paramètres suivants :
  - Nom d'abonné : nous recommandons d'utiliser le nom du compte pour l'utilisateur ou le groupe que l'abonné représente.
  - Planification : précise les jours et heures auxquels l'abonné peut recevoir des notifications.
  - Adresses : indique une liste d'adresses pouvant utiliser l'un des canaux préconfigurés pour envoyer une notification à l'abonné.
- Abonnements : un abonnement précise qui reçoit une alerte selon un ensemble de critères. Les abonnements comprennent les éléments suivants :
  - Critères : un ensemble de conditions prédéfinies, semblables aux règles Microsoft Office Outlook®, qui peuvent être combinées pour déterminer quand une notification est envoyée.
  - Abonné : une liste d'abonnés qui doivent recevoir des notifications pour cet abonnement.
  - Canaux : la liste des canaux utilisés pour envoyer la notification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

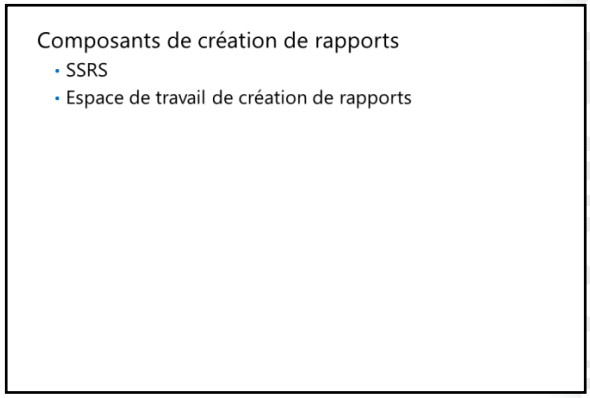
Démonstration : Configuration de notifications (facultatif)

Procédure de démonstration

1. Créez un canal de notification avec les paramètres suivants :
   - Type de canal : **Courrier électronique**
   - Serveur SMTP : **LON-SVR1.adatum.com**
   - Adresse de retour : **om@adatum.com**
2. Créez un abonné avec les paramètres suivants :
   - Nom : **ADATUM\Administrateur**
   - Planification : **Lun-Sam de 8 h 00 à 20 h 00**
   - Type de canal : **Courrier électronique**
   - Adresse de messagerie : **administrateur@adatum.com**
3. Créez un abonnement avec les paramètres suivants :
   - Nom : **Alertes SQL critiques**
   - Critères : **générée par le groupe SQL Server 2008 Computers** (Ordinateurs SQL 2008) et **de gravité « Critique »**
   - Canal : **Canal de notification SMTP**
   - Abonné : **ADATUM\Administrateur**
4. Rétablissez les ordinateurs virtuels suivants :
   - LON-DC1
   - LON-OM1
   - LON-SVR1
   - LON-SVR2

Vue d'ensemble de la création de rapports

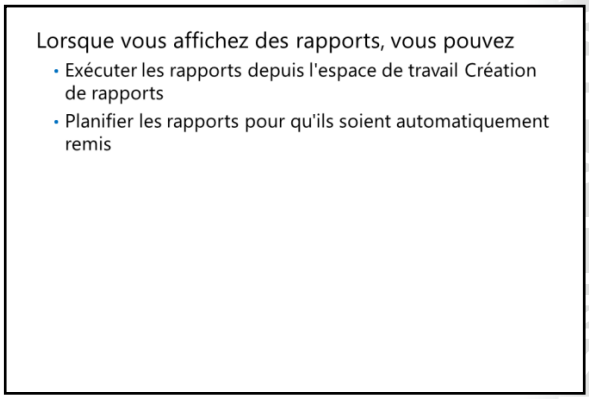
Operations Manager utilise les SSRS pour créer, gérer et enregistrer les rapports. Vous ajoutez des rapports à la console Opérateur en important un pack d'administration ou lors de la conception d'un nouveau rapport dans l'espace de travail Création de rapports.



Lorsque vous concevrez votre premier rapport à partir de l'espace de travail Création de rapports, vous serez invité à installer l'outil Générateur de rapports de SQL Server. Le Générateur de rapports est une application Web qui vous permet de générer des rapports tabulaires, de matrice et de graphique d'après des modèles créés par un administrateur de base de données.

Remarque : La création de modèles de rapports et de rapports avec le Générateur de rapports n'est pas traitée dans ce cours, mais dans le cours *10778 Implementing Data Models and Reports with SQL Server 2012 (Implémentation de modèles de données et de rapports avec SQL Server 2012)*.

Configuration des rapports et de la création de rapports



Pendant l'installation d'Operations Manager, vous êtes invité à configurer le serveur SSRS. À tout moment après l'installation, vous pouvez changer de serveur SSRS en accédant à l'espace de travail Administration et, à partir du nœud **Paramètres**, en sélectionnant **Création de rapports**. Avant de procéder ainsi, assurez-vous que vous avez installé les SSRS sur le nouveau serveur de création de rapports.

Si vous n'installez pas les SSRS et ne configurez pas Operations Manager pour qu'il utilise le serveur de création de rapports approprié, chaque rapport que vous exécuterez contiendra très probablement de nombreux paramètres. La plupart des rapports vous permettront d'agréger les données par jour, semaine ou mois. Vous devriez également pouvoir spécifier une date de début et une date de fin pour les données affichées.

Pour afficher un rapport, procédez comme suit :

1. Dans la console Opérateur, ouvrez l'espace de travail Création de rapports.
2. Accédez au rapport que vous souhaitez afficher.
3. Double-cliquez sur le rapport.
4. Sélectionnez les valeurs que vous souhaitez utiliser pour chaque paramètre.
5. Cliquez sur **Exécuter**.

Vous pouvez également planifier l'exécution de rapports et fournir le rapport à un partage de fichiers à une heure spécifique. Pour planifier un rapport, procédez comme suit :

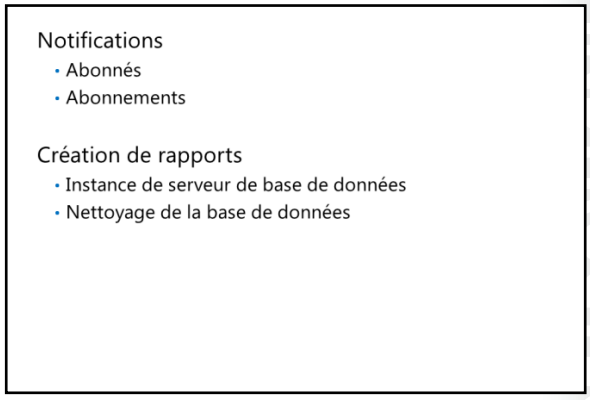
1. Dans la console Opérateur, ouvrez l'espace de travail Création de rapports.
2. Accédez au rapport dont vous souhaitez planifier l'exécution.
3. Dans le volet des tâches, cliquez sur **Planification**.
4. Dans la page **Paramètres de remise**, spécifiez une description pour la planification et sélectionnez **Partage de fichiers Windows** comme méthode de remise.
5. Dans la zone de texte **Nom du fichier**, tapez un nom pour que le fichier soit enregistré dans le partage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans la zone de texte **Chemin**, tapez le chemin du partage à utiliser.
7. Dans la zone de liste déroulante **Format du rendu**, cliquez sur le format pour le rapport.
8. Dans la zone de liste déroulante **Mode écriture**, cliquez sur l'une des options suivantes :
   - **Aucun** pour arrêter l'exécution du rapport si le fichier existe déjà
   - **Auto-incrément** pour créer un nouveau fichier chaque fois que la planification fonctionne
   - **Remplacer** pour remplacer le fichier précédent s'il existe
9. Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification utilisées pour exécuter le rapport, puis cliquez sur **Suivant**.
10. Dans la page **Planification de l'abonnement**, spécifiez une fréquence pour le rapport, puis cliquez sur **Suivant**.
11. Dans la page **Paramètres du rapport**, spécifiez les valeurs pour chaque paramètre, puis cliquez sur **Terminer**.

Éléments à prendre en compte pour implémenter des notifications et des rapports

Avant d'implémenter des notifications et des rapports, prenez en compte les éléments suivants :



- Abonnés : utilisez des groupes plutôt que des personnes pour les abonnés. Veillez à avoir un nombre d'abonnés facile à gérer et documentez les alertes qu'ils doivent recevoir. En outre, si un utilisateur ou un groupe d'utilisateurs regarde constamment la console Opérateur pour vérifier les éventuelles alertes, il n'a peut-être pas besoin d'être défini comme abonné.
- Abonnements : veillez à analyser les abonnements et demandez à l'abonné à quelle fréquence il reçoit les notifications. Il est courant qu'un environnement non optimisé remplisse les boîtes aux lettres des abonnés avec davantage de messages qu'ils ne peuvent en gérer. Dans ce cas, les abonnés ignoreront très probablement les messages. Pour éviter cela, veillez à ce que seules les alertes pertinentes fassent l'objet de notifications.
- Création de rapports : nous vous recommandons d'utiliser une instance distincte de SQL Server pour héberger la base de données d'entrepôt de données de création de rapports, la base de données opérationnelle et la base de données des SSRS. Veillez à analyser ces composants.
- Nettoyage de la base de données : passez en revue les paramètres de nettoyage de la base de données dans le nœud Paramètres de l'espace de travail Administration. Vous utilisez ces paramètres pour réduire la quantité d'espace utilisé par la base de données tout en conservant la quantité de données d'historique nécessaires à votre organisation. Prenez en compte toute réglementation à laquelle votre société puisse avoir à se plier, y compris le stockage des données analysées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 5
Configuration de l'intégration à VMM

Vous vous trouvez face à une difficulté lorsque vous utilisez Operations Manager pour analyser des environnements virtuels car les ressources matérielles, telles que la mémoire et le processeur, sont virtualisées pour les ordinateurs virtuels. La leçon 1 détaille ces problèmes et la façon de les résoudre. Si VMM gère votre environnement virtuel, vous pouvez intégrer cet environnement à Operations Manager et utiliser des packs d'administration compatibles PRO, fournis par Microsoft et des fournisseurs tiers, pour analyser votre environnement d'ordinateurs virtuels correctement. Vous pouvez utiliser une technologie appelée Conseils PRO dans VMM pour gérer les packs d'administration compatibles PRO d'Operations Manager.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- intégrer Operations Manager à VMM ;
- configurer l'intégration d'Operations Manager et de VMM ;
- décrire la fonctionnalité PRO ;
- comparer PRO et les options de placement avancées dans VMM ;
- décrire les éléments à prendre en compte pour l'implémentation de PRO ;
- configurer l'analyse avancée pour les composants de virtualisation.

Intégration d'Operations Manager à VMM

Il existe de nombreux problèmes à résoudre lorsque vous analysez des ordinateurs virtuels. Vous n'avez pas toujours le sens exact des ressources des ordinateurs virtuels lorsque vous utilisez des compteurs pour analyser les ressources matérielles en mémoire et en processeur. Il est possible que plusieurs ordinateurs virtuels soient hébergés sur le même serveur physique. Si VMM gère vos ordinateurs virtuels, vous pouvez intégrer VMM et Operations Manager pour analyser votre environnement virtuel plus efficacement. Operations Manager et VMM fournissent les fonctionnalités suivantes :

- Analyser l'intégrité et la disponibilité de l'environnement VMM
- Voir les affichages des diagrammes de l'environnement VMM
- Gérer des services PRO
- Effectuer l'intégration au mode de maintenance
- Créer des rapports à partir de VMM
- Fournir la prise en charge des SSAS pour les prévisions

- Analyse de l'intégrité et de la disponibilité des ordinateurs virtuels et des hôtes d'ordinateurs virtuels gérés par VMM.
- Analyse de l'intégrité et de la disponibilité du serveur de gestion VMM, du serveur de base de données VMM et des serveurs Web du portail libre-service VMM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Consultation des affichages des diagrammes de votre environnement virtualisé via la console Opérateur.
- Gestion des services PRO.
- Intégration au mode de maintenance.
- Création de rapports à partir de VMM.

Prise en charge des SQL Server Analysis Services (SSAS)analysant l'intégrité et la disponibilité

Vous pouvez importer le pack d'analyse System Center pour VMM pour analyser l'intégrité des ordinateurs virtuels, des hôtes VMM et des composants VMM. Vous pouvez également gérer l'installation des packs d'administration depuis VMM.

VMM utilise le kit de développement logiciel (SDK) d'Operations Manager pour remplir Operations Manager automatiquement avec les objets relatifs à VMM. Par exemple, une fois que vous aurez intégré Operations Manager et VMM, vous remarquerez qu'Operations Manager pourra détecter des objets d'ordinateurs virtuels. Cependant, si vous recherchez un objet de détection pour gérer l'ordinateur virtuel, vous ne le trouverez pas. Au lieu d'utiliser la découverte d'objets dans une gestion, VMM utilise le SDK d'Operations Manager pour créer un objet d'ordinateur virtuel automatiquement chaque fois que vous créez ou modifiez un ordinateur virtuel dans VMM.

Affichage des diagrammes

VMM utilise le SDK d'Operations Manager pour créer un affichage des diagrammes automatiquement pour chaque serveur de gestion VMM. Cet affichage des diagrammes montre la relation et l'intégrité globale pour tous les composants VMM. Cet affichage repose sur un diagramme d'application distribuée.

PRO

La fonctionnalité PRO permet d'exposer des données collectées par Operations Manager dans VMM, puis d'exécuter des actions automatisées en réponse à un groupe prédéfini de critères. Par exemple, vous pouvez utiliser PRO pour analyser l'utilisation de la mémoire sur les ordinateurs virtuels hébergés sur un cluster Hyper-V, puis exécuter automatiquement une migration dynamique de l'ordinateur virtuel d'un nœud vers un autre au cas où l'utilisation de la mémoire dépasse un seuil donné.

Vous implémentez PRO via la création de packs d'administration compatibles PRO. Le pack d'analyse System Center pour VMM contient les composants de base nécessaires à l'implémentation de packs d'administration compatibles PRO, et contient également une implémentation de base de PRO que vous pouvez utiliser dans votre environnement.

 **Liens de référence :** Pour plus d'informations, consultez System Center 2012 – Virtual Machine Manager : PRO-enabled management packs, à l'adresse http://go.microsoft.com/fwlink/?LinkID=285324.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Intégration au mode de maintenance

Les modes de maintenance de VMM et d'Operations Manager sont deux tâches complètement distinctes. Lorsque VMM migre les ressources d'un nœud de cluster Hyper-V vers un autre nœud, il place le nœud en mode de maintenance automatiquement. Toutefois, Operations Manager ne voit pas cela et déclenche des alertes pour l'hôte VMM, à moins que VMM et Operations Manager ne soient intégrés au pack d'analyse System Center pour System Center 2012 – VMM. Une fois que vous appliquez le pack d'administration, dès que VMM place un hôte en mode de maintenance, il communique avec Operations Manager de sorte que l'hôte soit également placé en mode de maintenance dans Operations Manager.

Création de rapports à partir de VMM

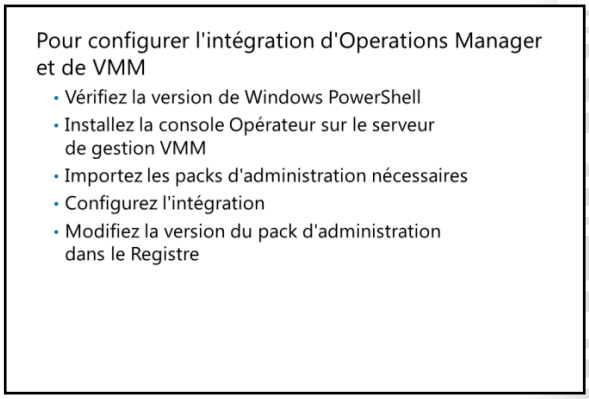
Une fois l'intégration effectuée, vous pouvez accéder aux rapports d'Operations Manager pour VMM à partir de la console VMM. Les rapports seront également disponibles dans Operations Manager.

SSAS

Vous pouvez intégrer les SSAS à VMM et Operations Manager pour fournir des rapports de prévision d'après les données collectées de l'environnement VMM. Cela vous permet de prévoir si vous aurez besoin d'ajouter des ressources à votre structure.

Configuration de l'intégration d'Operations Manager et de VMM

Avant de configurer l'intégration entre VMM et Operations Manager, assurez-vous que votre système répond aux conditions requises suivantes :



- Version Windows PowerShell appropriée : vous devez avoir Windows PowerShell 2.0 pour System Center 2012, ou Windows PowerShell 3.0 pour System Center 2012 SP1.
- Installation de la console Opérateur sur le serveur de gestion VMM.
- Importation des packs d'administration suivants vers Operations Manager :
  - Windows Server Internet Information Services 2003
  - Windows Server 2008 Internet Information Services 7
  - Windows Server Internet Information Services Library
  - SQL Server Core Library

Remarque : Nous vous recommandons également d'installer l'agent Operations Manager sur le serveur de gestion VMM et tous les hôtes VMM. En revanche, il est inutile d'installer l'agent Operations Manager sur les ordinateurs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Une fois que vous avez vérifié que votre système répond aux conditions requises, vous pouvez installer et configurer l'intégration, en procédant comme suit :

1. Dans la console VMM, ouvrez l'espace de travail Paramètres.
2. Dans le volet Paramètres, cliquez sur **Paramètres de System Center**, puis sur **Serveur Operations Manager**.
3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, cliquez sur **Propriétés**.
4. Passez en revue les informations de la page **Introduction**, puis cliquez sur **Suivant**.
5. Dans la page **Connexion à Operations Manager**, entrez le nom d'un serveur d'administration du groupe d'administration et sélectionnez un compte à utiliser pour se connecter. Vous pouvez utiliser le compte de service du serveur VMM ou indiquer un compte **Exécuter en tant que**. Ce compte doit être membre du rôle Administrateur d'Operations Manager.
6. Sélectionnez **Activer PRO**, si vous le souhaitez.
7. Sélectionnez **Activer l'intégration du mode de maintenance avec Operations Manager**, si vous le souhaitez, puis cliquez sur **Suivant**.
8. Entrez les informations d'identification pour qu'Operations Manager se connecte au serveur de gestion VMM, puis cliquez sur **Suivant**. Ce compte sera ajouté au rôle d'utilisateur Administrateur dans VMM.
9. Passez en revue les informations de la page **Résumé**, puis cliquez sur **Terminer**.

Une fois que vous avez configuré l'intégration, il peut être encore nécessaire d'apporter quelques modifications en fonction de la version du pack d'analyse System Center 2012 pour VMM que vous avez utilisée. Pour apporter ces modifications nécessaires, procédez comme suit :

1. Consultez le guide du pack d'analyse System Center pour System Center 2012 – Virtual Machine Manager pour obtenir le numéro de version du pack d'administration VMM. Vous pouvez voir le numéro de version actuel du pack d'analyse dans la console Opérateur. Vérifiez que le guide et le pack d'administration se rapportent au même numéro de version. Vous en aurez besoin à l'étape 6.
2. Ouvrez l'espace de travail Administration.
3. Dans le volet **Administration**, cliquez sur **Packs d'administration**. Faites défiler l'écran pour trouver les packs d'analyse VMM, tels que System Center 2012 Virtual Machine Manager Discovery.
4. Sur le serveur de gestion VMM, cliquez sur **Démarrer**, dans la zone de texte **Rechercher des programmes et des fichiers**, tapez **regedit**, puis appuyez sur Entrée. Si la boîte de dialogue **Contrôle de compte d'utilisateur** s'affiche, cliquez sur **Oui** pour continuer.
5. Dans l'Éditeur du Registre, localisez la clé de Registre suivante :

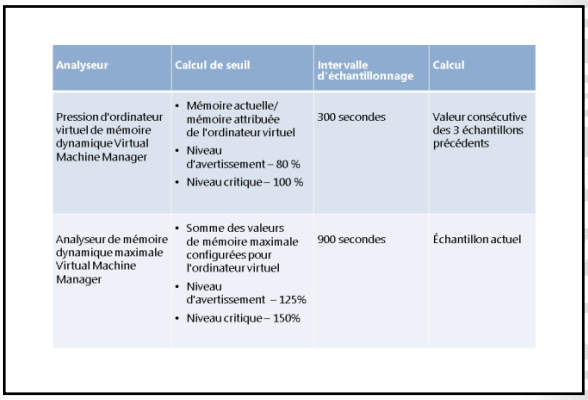
```
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Microsoft System Center Virtual Machine Manager
Server/Setup
```

6. Sous la clé, si nécessaire, mettez à jour la valeur de chaîne **CompatibleMPVersion** vers le nouveau numéro de version, puis fermez l'Éditeur du Registre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que la fonctionnalité PRO ?

PRO est une fonctionnalité qui prend en charge l'optimisation des ressources dans un environnement virtuel en fonction de la consommation des ressources par vos ordinateurs virtuels. PRO fournit un mécanisme pour lier les alertes spécifiques à Operations Manager aux actions correctives qui peuvent être exécutées manuellement ou automatiquement dans VMM. Ces alertes sont générées par des analyseurs que vous créez dans des packs d'administration compatibles PRO.



Analyseur	Calcul de seuil	Intervalle d'échantillonnage	Calcul
Pression d'ordinateur virtuel de mémoire dynamique Virtual Machine Manager	• Mémoire actuelle/ mémoire attribuée de l'ordinateur virtuel • Niveau d'avertissement – 80 % • Niveau critique – 100 %	300 secondes	Valeur consécutive des 3 échantillons précédents
Analyseur de mémoire dynamique maximale Virtual Machine Manager	• Somme des valeurs de mémoire maximale configurées pour l'ordinateur virtuel • Niveau d'avertissement – 125% • Niveau critique – 150%	900 secondes	Échantillon actuel

Les packs d'administration compatibles PRO définissent les classes, groupes et analyseurs cibles utilisés pour analyser les performances et la disponibilité des ordinateurs virtuels, des hôtes, des applications et du matériel utilisé dans un environnement de virtualisation. Microsoft et des fournisseurs tiers proposent des packs d'administration compatibles PRO pour certains de leurs produits. Vous pouvez également créer votre propre pack d'administration compatible PRO en suivant les instructions fournies par Microsoft dans http://go.microsoft.com/fwlink/?LinkID=285322.

Lorsqu'une alerte qui vise une classe PRO dans Operations Manager est déclenchée, un conseil PRO est créé dans VMM. Un conseil PRO peut inclure une action pour résoudre l'alerte exécutée à partir d'Operations Manager. L'action peut être exécutée automatiquement ou peut nécessiter l'approbation d'un administrateur VMM. Les conseils PRO peuvent exécuter la migration dynamique d'un ordinateur virtuel d'un nœud vers un autre dans un cluster Hyper-V, d'après des seuils de performances, ou déplacer l'ordinateur virtuel vers un hôte complètement nouveau en cas de défaillance matérielle.

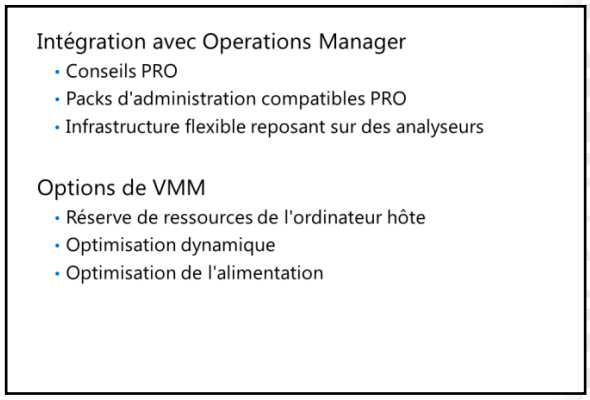
Le pack d'analyse VMM comprend plusieurs packs d'administration compatibles PRO qui définissent les classes et les groupes de base prenant en charge PRO et fournissent des analyseurs pour optimiser les performances des hôtes et des ordinateurs virtuels en fonction de seuils de processeur et de mémoire.

Le pack d'analyse VMM fournit plusieurs analyseurs compatibles PRO que vous pouvez utiliser. Le tableau suivant montre deux des analyseurs les plus courants.

Analyseur	Calcul de seuil	Intervalle d'échantillonnage	Calcul
Pression d'ordinateur virtuel de mémoire dynamique Virtual Machine Manager	Mémoire actuelle/mémoire attribuée de l'ordinateur virtuel Niveau d'avertissement – 80 % Niveau critique – 100 %	300 secondes	Valeur consécutive des 3 échantillons précédents
Analyseur de mémoire dynamique maximale Virtual Machine Manager	Somme des valeurs de mémoire maximale configurées pour l'ordinateur virtuel Niveau d'avertissement – 125 % Niveau critique – 150 %	900 secondes	Échantillon actuel

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comparaison de PRO et des options de placement avancées dans VMM



Bien que l'utilisation de conseils PRO fonctionne bien, ces derniers requièrent l'intégration à Operations Manager. Cela signifie que les clients sans Operations Manager ne peuvent pas les utiliser. Pour les clients qui n'utilisent pas Operations Manager, VMM offre la prise en charge des paramètres d'optimisation des ressources suivants :

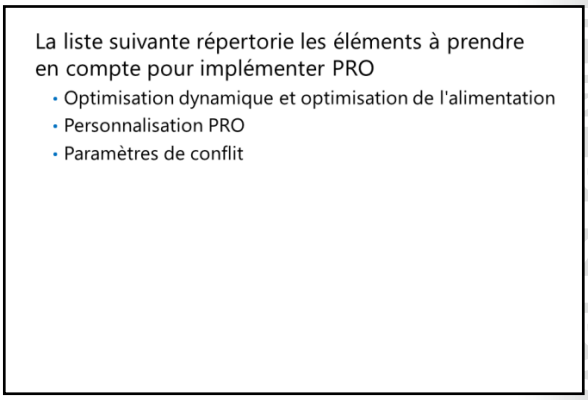
- Réserves de ressources de l'ordinateur hôte : ces réserves permettent de mettre de côté des ressources pour le système d'exploitation hôte afin que lorsqu'un ordinateur virtuel est créé ou déplacé vers l'hôte, l'action ne se produise que si les ressources mises de côté pour le système d'exploitation hôte peuvent être conservées.
- Optimisation dynamique : l'optimisation dynamique est utilisée pour migrer automatiquement des ordinateurs virtuels d'un hôte vers un autre, en fonction de seuils de ressources.
- Optimisation de l'alimentation : l'optimisation de l'alimentation est utilisée pour migrer des ordinateurs virtuels d'un hôte vers un autre au cours de périodes de faible utilisation de sorte qu'un hôte puisse être arrêté afin d'économiser l'énergie.

La fonctionnalité PRO fournit beaucoup plus de flexibilité que l'optimisation dynamique ou l'optimisation de l'alimentation, car elle peut être utilisée pour analyser n'importe quel objet de l'environnement VMM avant d'exécuter l'action. Par exemple, avec PRO, un analyseur peut vérifier les performances du stockage utilisé pour héberger des fichiers pour un ordinateur virtuel. Si les performances de l'ordinateur virtuel tombent sous (ou dépassent) une valeur établie, alors PRO peut migrer l'ordinateur virtuel. Cela ne peut pas être réalisé avec l'optimisation dynamique ou l'optimisation de l'alimentation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour implémenter PRO

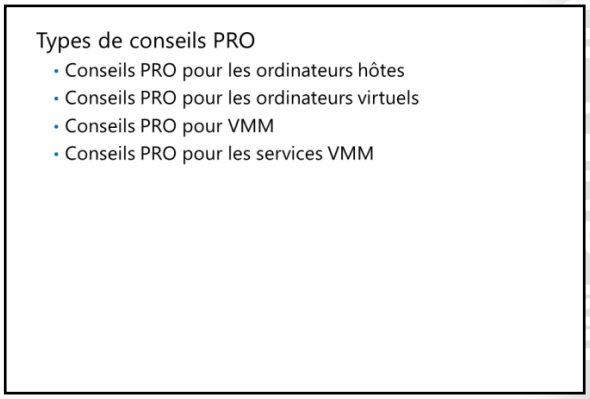
Avant de décider d'implémenter PRO, vous devez prendre en compte les facteurs suivants :



- Optimisation dynamique et optimisation de l'alimentation : si vous n'avez pas d'autres exigences que l'analyse de l'utilisation du processeur et de la mémoire, l'optimisation dynamique et l'optimisation de l'alimentation sont une meilleure option que PRO.
- Personnalisation : assurez-vous de comprendre les fonctions disponibles via les packs d'analyse VMM. Le guide du pack d'analyse VMM contient la liste complète des règles et des analyseurs disponibles avec le pack d'administration. Vous devrez créer tout autre élément dont vous pourriez avoir besoin pour votre environnement.
- Paramètres de conflit : si vous utilisez actuellement l'optimisation dynamique et l'optimisation de l'alimentation, puis que vous procédez à l'intégration à Operations Manager, vous devez soit désactiver l'optimisation dynamique et l'optimisation de l'alimentation, soit modifier leurs paramètres pour éviter d'éventuels conflits avec les analyseurs du pack d'administration compatible PRO.

Configuration de l'analyse avancée pour les composants de virtualisation

L'un des avantages de l'utilisation des packs d'administration compatibles PRO est la souplesse. L'utilisation de packs d'administration compatibles PRO fournit l'analyse pour les environnements virtualisés gérés par VMM et Operations Manager. Cependant, cette même flexibilité peut également gêner l'utilisation de PRO, car elle requiert une excellente compréhension de la création de packs d'administration et de l'architecture PRO implémentée par le pack d'analyse VMM.



Les packs d'administration compatibles PRO peuvent contenir quatre types de conseils PRO :

- Conseils PRO pour les ordinateurs hôtes : les conseils PRO pour les ordinateurs hôtes peuvent implémenter des actions (telles que la migration d'un ordinateur virtuel) afin de restaurer un état sain pour un ordinateur hôte en fonction de l'utilisation des ressources ou d'autres mesures de performances et d'intégrité sur l'ordinateur hôte. C'est ainsi que l'optimisation dynamique et les réserves de l'hôte sont implémentées dans VMM.
- Conseils PRO pour les ordinateurs virtuels : les conseils PRO pour les ordinateurs virtuels peuvent implémenter des actions (telles qu'une mise à jour de la configuration qui restaure un état sain pour un ordinateur virtuel) en fonction de l'utilisation des ressources ou d'autres compteurs de performances dans les ordinateurs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Conseils PRO pour VMM : les conseils PRO pour VMM peuvent cibler VMM pour résoudre les problèmes qui affectent plusieurs ordinateurs gérés par VMM dans tout votre environnement virtuel. Par exemple, un conseil PRO qui vise VMM peut définir une action corrective pour un problème avec une application distribuée, telle que Microsoft SharePoint, afin de créer un nouveau serveur frontal SharePoint automatiquement, basé sur la charge de l'utilisateur de votre ferme SharePoint.
- Conseils PRO pour les services VMM : les conseils PRO peuvent cibler des services VMM et des niveaux de service pour résoudre les problèmes qui affectent les instances du service et/ou du niveau. Par exemple, un conseil PRO qui vise un service peut définir une action corrective pour un niveau de service, ce qui initialise une action avec montée en puissance pour le niveau lorsque les instances de niveau existantes dépassent un seuil de performances particulier.

 **Remarque :** Pour obtenir des instructions détaillées sur la création de packs d'administration compatibles PRO, téléchargez le guide PRO-Enabled Management Pack Building à l'adresse http://go.microsoft.com/fwlink/?LinkID=285324.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation d'une stratégie d'analyse des serveurs

Scénario

A. Datum Corporation a terminé le déploiement initial de l'infrastructure Windows Server 2012 et souhaite maintenant implémenter une stratégie pour analyser l'environnement. A. Datum évalue l'utilisation des outils d'analyse de Windows Server 2012 pour certaines de ses filiales. En outre, A. Datum a installé Operations Manager au centre de données de Londres pour analyser les serveurs du centre de données.

Vous devez implémenter l'analyse des serveurs à l'aide des outils Windows Server 2012 et en utilisant Operations Manager.

Objectifs

- Configurer l'analyse des serveurs à l'aide des outils Windows Server 2012.
- Implémenter l'analyse d'Operations Manager.
- Configurer les composants d'analyse d'Operations Manager.
- Analyser les performances des serveurs.

Configuration de l'atelier pratique

Durée approximative : 75 minutes

Ordinateurs virtuels	22414B-LON-DC1 22414B-LON-OM1 22414B-LON-SVR1 22414B-LON-SVR2 22414B-TOR-SVR1 22414B-TOR-SS1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible. Avant de commencer cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, sur **Accueil**, cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22414B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
    - Nom d'utilisateur : **ADATUM\Administrateur**
    - Mot de passe : **Pa$$w0rd**

Répétez les étapes 2 à 4 pour les ordinateurs virtuels restants.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configuration de l'analyse des serveurs à l'aide de Windows Server 2012

Scénario

La société A. Datum n'a pas encore décidé si elle déploiera Operations Manager au centre de données de Toronto, alors elle évalue d'abord les outils Windows Server 2012 disponibles. A. Datum souhaite évaluer les options permettant d'analyser plusieurs serveurs en utilisant une interface unique et de collecter des informations de plusieurs serveurs dans un emplacement unique.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer le Gestionnaire de serveur pour surveiller plusieurs serveurs.
2. Configurer un ensemble de collecteurs de données.
3. Configurer un abonnement aux événements.

▶ Tâche 1 : Configurer le Gestionnaire de serveur pour surveiller plusieurs serveurs

1. Sur TOR-SVR1, configurez **Gestionnaire de serveur** pour gérer TOR-SS1, puis créez un groupe de serveurs nommé **Serveurs de Toronto** qui contient **TOR-SVR1** et **TOR-SS1**.
2. Exécutez une analyse Best Practices Analyzer sur **TOR-SS1**.
3. Configurez les alertes de performances pour TOR-SS1 avec les paramètres suivants :
   - Utilisation du processeur (%) : **75**
   - Mémoire (Mo disponibles) : **100**
4. Ajoutez le rôle de serveur Web (IIS) à TOR-SS1.

▶ Tâche 2 : Configurer un ensemble de collecteurs de données

1. Sur TOR-SVR1, dans le Gestionnaire de serveur, configurez un ensemble de collecteurs de données avec les paramètres suivants :
   - Nom : **Ressources principales**
   - Modèle : **System Performance**
2. Configurez le collecteur de données à l'aide des paramètres suivants :
   - Planification : **du lundi au vendredi à partir de 8 h 00**
   - Condition d'arrêt : **durée globale de 10 heures**
3. Collectez des données pendant 10 minutes, puis arrêtez le collecteur et analysez le rapport.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer un abonnement aux événements

1. Sur TOR-SVR1, configurez un abonnement aux événements de TOR-SS1 avec les paramètres suivants :
   - Nom : **Événements TOR-SS1**
   - Type d'événements : **Critique et erreur**
   - Journaux d'événements : **Journaux Windows**
2. Ajoutez le compte d'ordinateur pour TOR-SVR1 au groupe local **Lecteurs des journaux d'événements** dans TOR-SS1.
3. Affichez les événements transférés. Le transfert des événements peut prendre plusieurs minutes.

Résultats : Après avoir terminé cet exercice, vous devriez avoir configuré l'analyse pour les serveurs à l'aide des outils disponibles dans Windows Server 2012.

Exercice 2 : Implémentation de l'agent Microsoft System Center 2012 - Operations Manager

Scénario

A. Datum a déployé un serveur Operations Manager unique dans le centre de données de Londres. Vous devez maintenant déployer l'agent Operations Manager pour les serveurs du centre de données de Londres.

Les tâches principales de cet exercice sont les suivantes :

1. Déployer l'agent Microsoft® System Center 2012 Operations Manager (Operations Manager) à l'aide de la détection.
2. Déployer l'agent Operations Manager manuellement.

▶ Tâche 1 : Déployer l'agent Microsoft® System Center 2012 Operations Manager (Operations Manager) à l'aide de la détection

1. Déployez l'agent Operations Manager vers les ordinateurs suivants à l'aide de la détection :
   - LON-SVR1
   - LON-SVR2

▶ Tâche 2 : Déployer l'agent Operations Manager manuellement

1. Configurez LON-OM1 pour placer manuellement les agents installés en état d'attente.
2. Sur LON-DC1, installez manuellement l'agent Operations Manager avec les paramètres suivants :
   - Source de l'agent : **\\LON-OM1\C$\Programmes\System Center 2012\Operations Manager\Server\AgentManagement\amd64\MOMAgent.msi**
   - Groupe d'administration : **ADATUM**
   - Serveur d'administration : **LON-OM1**

3. Dans le Gestionnaire de serveur, vérifiez que le service System Center Management s'exécute.
4. Sur LON-OM1, approuvez LON-DC1 dans la console Opérateur et vérifiez que LON-DC1 est maintenant géré par agent.

Résultats : Après avoir terminé cet exercice, vous devriez avoir installé et vérifié l'agent Operations Manager sur les ordinateurs du centre de données de Londres.

Exercice 3 : Configuration des composants d'analyse d'Operations Manager

Scénario

Maintenant que vous avez configuré Operations Manager pour qu'il analyse les serveurs du centre de données de Londres, l'étape suivante consiste à déployer et à configurer les composants d'analyse.

Les tâches principales de cet exercice sont les suivantes :

1. Installer et configurer les packs d'administration.
2. Configurer les notifications.
3. Vérifier les compteurs de performance.

▶ Tâche 1 : Installer et configurer les packs d'administration

1. Sur LON-OM1, importez les packs d'administration SQL Server depuis **C:\Program Files (x86)\System Center Management Packs\System Center Monitoring Pack for SQL Server**.
2. Créez une gestion pour les remplacements, nommée **SQL Server 2008 (Analyse) – Remplacements**.
3. Créez un remplacement pour l'analyseur d'unités **Espace du fichier de base de données** dans la liste des analyseurs de performances pour la cible **Fichier de base de données SQL Server 2008** selon les paramètres suivants :
   - Seuil inférieur : **20**
   - Seuil supérieur : **30**

▶ Tâche 2 : Configurer les notifications

1. Créez un canal de notification avec les paramètres suivants :
   - Type de canal : **Courrier électronique**
   - Serveur SMTP : **LON-SVR1.adatum.com**
   - Adresse de retour : **om@adatum.com**
2. Créez un abonné avec les paramètres suivants :
   - Nom : **ADATUM\Administrateur**
   - Planifier : **Lun-Sam de 8 h 00 à 20 h 00**
   - Type de canal : **Courrier électronique**
   - Adresse de messagerie : **administrator@adatum.com**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Créez un abonnement avec les paramètres suivants :
   - Nom : **Alertes SQL critiques**
   - Critères : **générée par le groupe SQL Server 2008 Computers** (Ordinateurs SQL Server 2008) et **de gravité « Critique »**
   - Canal : **Canal de notification SMTP**
   - Abonné : **ADATUM\Administrateur**

▶ Tâche 3 : Vérifier les compteurs de performance

- Vérifiez la collecte des données de performances de l'exercice 1, tâche 1.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-SVR2**, **22414B-LON-OM1**, **22414B-TOR-SS1** et **22414B-TOR-SVR1**.

Résultats : Après avoir terminé cet exercice, vous devriez avoir importé et configuré le pack d'administration Microsoft SQL Server® dans Operations Manager.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 7

Planification et implémentation d'une haute disponibilité pour des services et des applications de fichiers

Table des matières :

Vue d'ensemble du module **7-1**

Leçon 1 : Planification et implémentation d'espaces de stockage **7-2**

Leçon 2 : Planification et implémentation du système de fichiers DFS **7-8**

Leçon 3 : Planification et implémentation du système de fichiers NLB **7-16**

Atelier pratique : Planification et implémentation d'une haute disponibilité pour des services et des applications de fichiers **7-21**

Vue d'ensemble du module

Les infrastructures de services de fichiers hautement disponibles requièrent habituellement un investissement important en matière de matériel et de logiciels. Avec les espaces de stockage, le système de fichiers distribués (DFS), l'équilibrage de la charge réseau (NLB) et l'utilisation des technologies iSCSI (Internet SCSI) dans Windows Server® 2012, Microsoft® permet aux sociétés de toutes les tailles de créer des infrastructures de services de fichiers hautement disponibles sans qu'il leur soit nécessaire d'investir dans du matériel nouveau et coûteux.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- expliquer comment planifier et implémenter des espaces de stockage ;
- expliquer comment planifier et implémenter le système de fichiers distribués (DFS) ;
- expliquer comment planifier et implémenter l'équilibrage de la charge réseau (NLB) ;
- expliquer comment planifier et implémenter la haute disponibilité pour des services et des applications de fichiers.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification et implémentation d'espaces de stockage

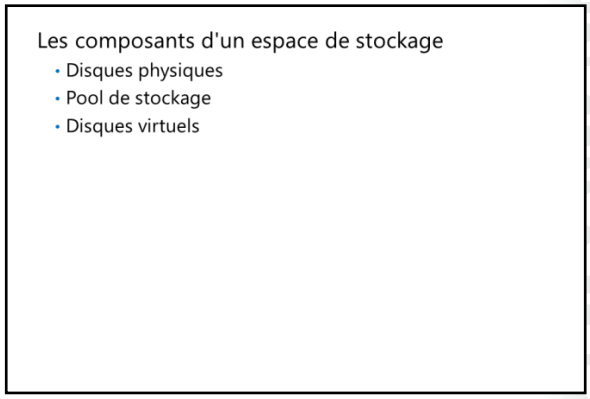
Dans cette leçon, vous découvrirez les infrastructures de stockage hautement disponibles en utilisant des espaces de stockage.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les espaces de stockage ;
- résumer les options de configuration des pools de stockage ;
- comprendre les options de redondance dans la configuration du pool de stockage ;
- décrire les espaces de stockage en cluster ;
- décrire la configuration requise pour l'implémentation d'espaces de stockage en cluster ;
- décrire le processus de configuration de l'espace de stockage en cluster.

Que sont les espaces de stockage ?



Les espaces de stockage constituent une fonctionnalité de virtualisation de stockage intégrée à Windows Server 2012 et Windows® 8. Il s'agit d'une fonctionnalité disponible à la fois pour les volumes de systèmes de fichiers NTFS et ReFS (Resilient File System), pouvant assurer la redondance et fournir un pool de stockage à différents disques internes et externes de différentes tailles et interfaces. Vous pouvez utiliser cette fonctionnalité pour ajouter des disques physiques de tout type et de toute taille à un pool de stockage, puis créer des disques virtuels hautement disponibles à partir du pool de stockage. L'avantage principal des espaces de stockage est que vous ne gérez pas de disques uniques, mais que vous pouvez gérer plusieurs disques comme une seule unité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les espaces de stockage comprennent les composants suivants :

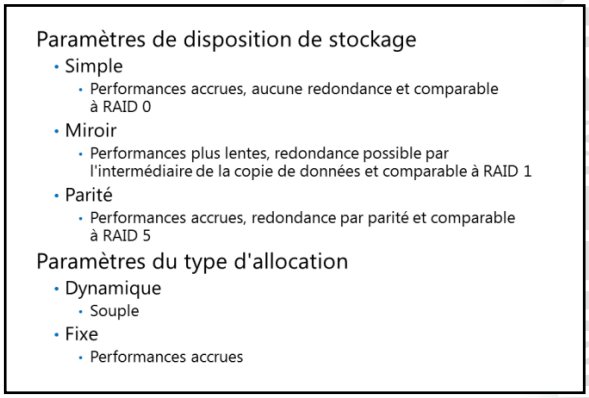
- *Disque physique*. Les disques physiques sont des disques à proprement parler, par exemple SATA (Serial ATA) ou SAS (Serial Attached SCSi, en anglais). Pour être ajoutés à un pool de stockage, les disques physiques doivent répondre aux conditions suivantes :
  - un disque physique est requis pour créer un pool de stockage. Au moins deux disques physiques sont requis pour créer un disque virtuel en miroir résilient ;
  - au moins trois disques physiques sont requis pour créer un disque virtuel avec une résilience par parité ;
  - la mise en miroir triple requiert au moins cinq disques physiques ;
  - les disques doivent être vierges et non formatés. Ils ne doivent contenir aucun volume ;
  - il est également possible de connecter des disques à l'aide de diverses interfaces de bus, notamment iSCSI SCS, SATA, SCSI, et USB (Universal Serial Bus, en anglais).

Remarque : Si vous souhaitez utiliser le clustering avec basculement avec des pools de stockage, vous ne pouvez pas utiliser de disques SATA, USB ou SCSI.

- *Pool de stockage*. Un pool de stockage est constitué d'un ou plusieurs disques physiques qu'il est possible d'utiliser pour créer des disques virtuels. Cet ensemble peut être complété par n'importe quel disque physique disponible non formaté ou non connecté à un autre pool de stockage.
- *Disque virtuel (ou espace de stockage)*. Un disque virtuel est un disque non physique, mais semblable à un disque physique du point de vue des utilisateurs et des applications. Mais les disques virtuels sont plus souples, car ils comprennent l'allocation dynamique (ou les allocations juste-à-temps) et la résilience aux défaillances de disque physique avec une fonctionnalité intégrée, par exemple la mise en miroir.

Options de configuration d'un espace de stockage

Il est possible de configurer des disques virtuels avec différents types de disposition et d'allocation de stockage. Le type de disposition et d'allocation de stockage sélectionné pendant la création du disque virtuel indique le niveau de fiabilité et de performance de ce dernier.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Disposition du stockage

La disposition du stockage d'un disque virtuel indique comment l'espace de stockage configure les disques physiques sous-jacents. Les paramètres sont les suivants :

- Simple. Ce paramètre fournit une bande définie sans parité, semblable au système RAID 0 (Redundant Array of Independent Disks). Par rapport à un seul disque, cette configuration augmente le débit et optimise la capacité. Cependant, elle n'offre aucune redondance et ne protège pas les données contre une défaillance du disque.
- Miroir. Ce paramètre fournit un miroir défini en dupliquant des données sur deux ou trois disques, semblables au RAID 1. Il améliore la fiabilité dans le cas d'une capacité réduite. Cette configuration requiert au moins deux disques pour protéger des données contre toute défaillance du disque ou au moins cinq disques pour faire face à deux défaillances simultanées du disque.
- Parity *(Parité)*. Ce paramètre fournit un agrégat par bandes avec parité distribuée en agrégeant par bandes des données et des informations de parité sur plusieurs disques, à l'instar du RAID 5. Il améliore la fiabilité dans le cas d'une capacité réduite. Cette configuration requiert au moins trois disques pour protéger des données contre une défaillance d'un seul disque. En outre, il n'est pas possible d'utiliser cette configuration dans un cluster de basculement.

Type d'allocation

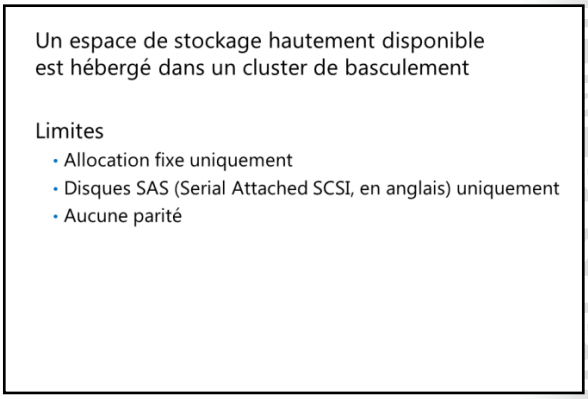
Le type d'allocation du disque virtuel détermine la façon dont l'espace est alloué au disque virtuel. Cette décision peut avoir des conséquences sur les performances du disque virtuel. Les différents types d'allocation sont les suivants :

- Dynamique. Cette allocation permet au disque virtuel de dépasser la capacité du pool de disques en allouant un volume supérieur à la quantité d'espace disponible dans le pool de disques au moment de la création. Bien qu'elle permette plus de souplesse, cette allocation se fait au détriment des performances. Cela s'explique par le fait que le moteur des espaces de stockages doit réallouer de l'espace disque du pool à mesure que la consommation du disque virtuel augmente.
- Fixe. L'allocation fixe réserve de l'espace pour le disque virtuel au moment de la création, ce qui optimise les performances. Cependant, la taille du disque doit être inférieure à l'espace disponible sur le pool. À mesure que vous ajoutez des disques physiques au pool, il est possible d'augmenter le volume du disque fixe. Cela n'aura des conséquences sur les performances que pendant l'augmentation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce qu'un espace de stockage en cluster ?

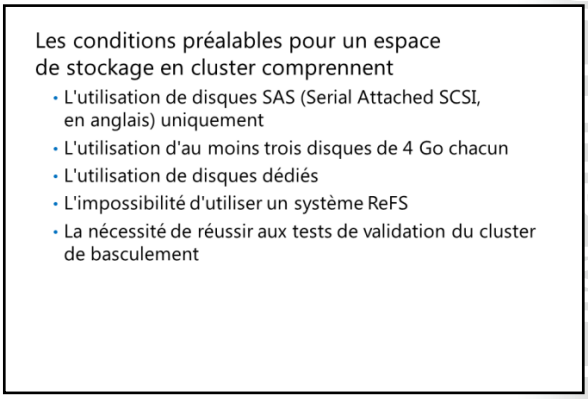
Un espace de stockage en cluster utilise le service de cluster de basculement pour fournir un espace de stockage hautement disponible. La création de l'espace de stockage est semblable à celle d'un espace de stockage standard. Bien que les espaces de stockage en cluster fournissent la haute disponibilité aux solutions de stockage, il existe quelques limites :



- Allocation fixe. Les disques virtuels qu'un espace de stockage en cluster héberge peuvent utiliser uniquement l'allocation fixe. Il est possible d'étendre des disques comme disques physiques lorsque vous ajoutez des disques physiques au pool, mais l'allocation ne peut pas être dynamique.
- Disques SAS (Serial Attached SCSI, en anglais). Il n'est possible d'utiliser des disques SAS que pour créer un espace de stockage en cluster.
- Aucune parité. Dans un espace de stockage en cluster, il est possible de créer un stockage simple uniquement ou d'y adjoindre un disque virtuel en miroir.

Configuration requise pour l'implémentation des espaces de stockage en cluster

Les espaces de stockage en cluster utilisent le service de cluster de basculement pour fournir un environnement d'espace de stockage hautement disponible. Cependant, il existe certaines exigences en matière de matériel et de logiciels qu'il convient de respecter pour qu'un environnement puisse héberger des espaces de stockage dans un cluster de basculement. Pour créer un espace de stockage en cluster, vous devez vérifier que votre environnement répond aux exigences suivantes :



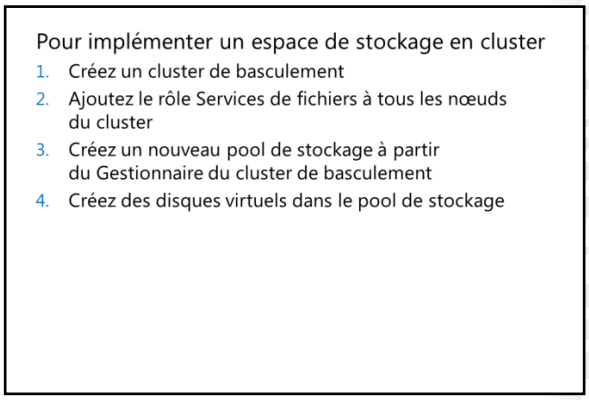
- tous les disques physiques doivent être connectés aux nœuds via une interface SAS ;
- au moins trois disques physiques, avec au moins 4 gigaoctets (Go) chacun, doivent être présents ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- tous les disques physiques doivent être dédiés au pool de stockage ;
- les espaces de stockage formatés dans le système de fichiers ReFS ne doivent pas être ajoutés au volume partagé de cluster (CSV) ;
- tous les disques physiques doivent passer les tests de validation du cluster de basculement.

Configuration d'un espace de stockage en cluster

Après avoir vérifié que les exigences d'un espace de stockage en cluster sont satisfaites, il est possible de créer un nouveau pool de stockage pour héberger votre espace de stockage en cluster. Toutefois, au lieu d'utiliser le Gestionnaire de serveur pour créer ce pool de stockage, vous aurez besoin du Gestionnaire du cluster de basculement. Avant de créer un espace de stockage en cluster, il vous faut :



1. Ajouter le **rôle cluster de basculement** sur tous les nœuds connectés aux disques physiques que vous utiliserez dans l'espace de stockage ;
2. Ajouter le **rôle services de fichiers** et les outils d'administration du **rôle services de fichiers** sur tous les nœuds du cluster de basculement.

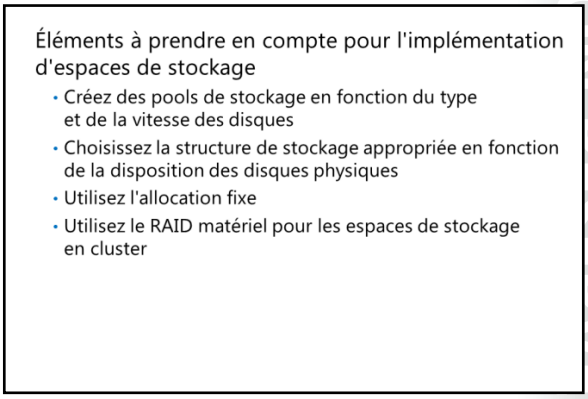
Une fois le rôle cluster de basculement configuré sur tous les nœuds qui se connectent aux disques physiques que vous utilisez dans l'espace de stockage en cluster, il est possible d'implémenter un espace de stockage en cluster en suivant la procédure suivante :

1. Ouvrez **Gestionnaire du cluster de basculement**.
2. Développez **Stockage**, cliquez avec le bouton droit sur **Pools**, puis cliquez sur **Nouveau pool de stockage**.
3. Dans l'Assistant Nouveau pool de stockage, tapez un nom pour le nouveau pool de stockage, puis cliquez sur **Suivant**.
4. Dans la page **Sélectionner les disques physiques pour le pool de stockage**, sélectionnez au moins trois disques SAS avec un minimum de 4 Go d'espace disponible, puis cliquez sur **Suivant**.
5. Dans la page **Confirmation**, cliquez sur **Fermer**. Le pool sera ajouté au cluster, puis mis en ligne.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour l'implémentation d'espaces de stockage

Les espaces de stockage fournissent la souplesse et la simplicité d'utilisation lors de la création de volumes. Cependant, cette même souplesse peut provoquer des problèmes de performances selon la façon dont vous combinez différents types de disques physiques dans le même disque virtuel. Il est nécessaire de prendre en compte l'implémentation physique sous-jacente d'un sous-système de disque avant de configurer les différents types de disques virtuels disponibles dans un espace de stockage. Lors de la création d'espaces de stockage, prenez en compte les options suivantes :



- créez des pools de stockage distincts selon le type et la vitesse des disques. Envisagez, par exemple, un pool de stockage avec trois disques : un disque SATA qui se connecte en USB 2.0 et deux disques SAS directement connectés. La création d'un disque virtuel de parité à l'aide de ce pool entraînerait une diminution des performances en raison de la plus grande lenteur d'un disque USB comparé à un disque SAS. Il est conseillé d'utiliser trois disques SAS ;
- choisissez la structure de stockage appropriée en fonction de la disposition des disques physiques. Par exemple, si vous utilisez un volume RAID matériel, deux volumes peuvent apparaître en tant que deux disques physiques distincts dans le système d'exploitation Windows Server. Cependant, chacun d'entre eux peut être un ensemble RAID 5 ou RAID 10, ce qui offre la tolérance de panne. Le choix de la parité comme disposition de stockage serait excessif. Le stockage simple augmenterait les performances, alors que le niveau physique fournirait la tolérance de panne ;
- utilisez l'allocation fixe pour de meilleures performances. L'allocation fixe réserve la quantité d'espace nécessaire pour un disque pendant l'allocation, évitant le coût de l'allocation juste-à-temps exigée par l'allocation dynamique ;
- utilisez le RAID matériel pour les espaces de stockage en cluster. Les espaces de stockage en cluster ne permettent pas la création des disques virtuels à l'aide d'une disposition de parité. Utilisez des systèmes RAID matériels pour offrir la redondance nécessaire pour les espaces de stockage en cluster.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Planification et implémentation du système de fichiers DFS

La fonctionnalité DFS de Windows Server 2012 vous permet d'exposer des dossiers partagés hébergés par différents serveurs sur votre réseau comme s'ils appartenaient à un seul serveur. En supprimant la dépendance d'un nom du serveur lors de l'accès aux partages et de la mise à disposition de la réplication des données sur les serveurs qui hébergent des partages, DFS crée un système de stockage hautement disponible sans qu'il soit nécessaire d'investir dans le matériel à tolérance de panne spécifique.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les composants de DFS ;
- examiner des scénarios d'utilisation de DFS ;
- comprendre les instructions relatives à la conception d'une disponibilité d'espace de nom DFS ;
- décrire les éléments à prendre en compte pour la configuration de références ;
- comprendre les instructions relatives à l'optimisation d'espaces de noms pour des systèmes DFS ;
- décrire les meilleures pratiques pour le déploiement d'espaces de noms pour des systèmes DFS ;
- comprendre les instructions pour la conception d'une réplication DFS.

Vue d'ensemble des composants DFS

Les DFS sont composés d'espaces de noms DFS et de la réplication DFS. Chaque composant est un rôle serveur Windows Server 2012 qu'il est possible d'utiliser séparément conjointement à un autre. Il est possible de gérer DFS en utilisant soit les outils de gestion du système de fichiers DFS, soit l'interface de ligne de commande Windows PowerShell®.

Rôles de serveur
- Espaces de noms DFS
- Réplication DFS

Modifications apportées depuis Windows Server 2008
- Windows Powershell pour les espaces de noms DFS
- Appartenance à un site pour les clients DirectAccess
- Fournisseur WMI
- Réplication pour les volumes de déduplication de données

Espace de noms DFS

Les espaces de noms DFS offre la possibilité de grouper les dossiers partagés se trouvant sur différents serveurs dans une ou plusieurs espaces de noms logiquement structurés. Chaque espace de noms apparaît aux utilisateurs comme un dossier partagé unique avec plusieurs sous-dossiers. Cependant, la structure sous-jacente de l'espace de noms peut être composée de nombreux partages de fichiers situés sur différents serveurs et dans plusieurs sites.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Réplication DFS

La réplication DFS offre la possibilité de répliquer des dossiers (y compris ceux auxquels un chemin d'accès d'espace de noms DFS fait référence) sur plusieurs serveurs et sites. La réplication DFS utilise un algorithme de compression appelé compression différentielle à distance. Cette dernière détecte les modifications appliquées aux données dans un fichier, et permet à la réplication DFS de répliquer uniquement les blocs des fichiers modifiés au lieu des fichiers complets.

Remarque : Il est possible d'utiliser la réplication DFS pour répliquer le dossier SYSVOL dans les services de domaine Active Directory® (AD DS) pour des domaines au niveau fonctionnel du domaine Windows Server 2008 ou ultérieur.

Fonctionnalités nouvelles et modifiées

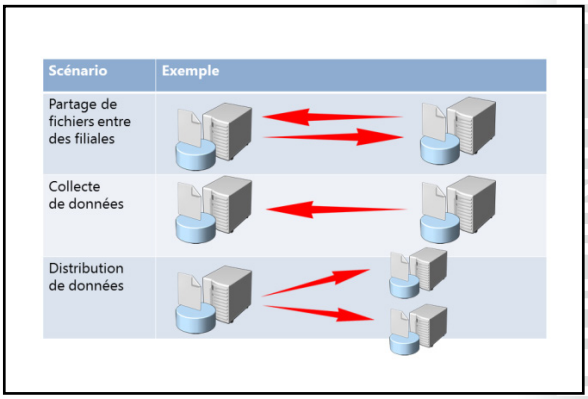
Les fonctionnalités suivantes de DFS ont été ajoutées ou modifiées dans Windows Server 2012 :

- Espaces de noms DFS :
  - appartenance à un site pour les clients DirectAccess. Offre des références optimales vers du contenu DFS aux clients distants lorsque les ordinateurs se connectent à l'aide de DirectAccess. Seuls les clients Windows 8 prennent en charge la détection de site ;
  - fournit des méthodes de gestion basées sur WMI (Windows Management Infrastructure) pour gérer les espace de noms DFS ;
  - module Windows PowerShell. Fournit des applets de commande Windows PowerShell pour gérer des espaces de noms DFS ;
  - outil en ligne de commande Dfscmd. Cette fonctionnalité a été déconseillée. Utilisez plutôt Windows PowerShell.
- Réplication DFS. Prend en charge les volumes de déduplication de données. Fournit une prise en charge pour la réplication de contenu stocké sur des volumes qui utilisent la déduplication des données.
- Service de réplication de fichiers. Cette fonctionnalité a été déconseillée. Utilisez plutôt la réplication DFS.

Scénarios d'utilisation du système de fichiers DFS

À l'aide d'espaces de noms DFS et de la réplication DFS, votre organisation peut tirer profit de plusieurs scénarios d'implémentation, parmi lesquels :

- le partage de fichiers entre des filiales ;
- la collecte de données ;
- la distribution de données.



Partage de fichiers entre des filiales

Les succursales des organisations ont tendance à partager des fichiers ou à collaborer. La réplication DFS permet de répliquer des fichiers entre ces filiales, ou d'une filiale vers un site concentrateur. Cette forme de réplication aide à réduire le trafic d'un réseau WAN, et offre la haute disponibilité en cas de défaillance d'une liaison WAN ou d'un serveur. La réplication DFS fait en sorte que lorsque des modifications sont apportées à un fichier, la réplication delta se produise pour garantir la réplication des modifications à tous les autres sites.

Remarque :

- souvenez-vous que la réplication DFS réplique uniquement les données après que l'utilisateur ferme le fichier auquel il a apporté des modifications. Par conséquent, nous déconseillons la réplication DFS pour les fichiers qui restent ouverts pendant de longues périodes, telles que les bases de données et les fichiers de disques durs utilisés par les ordinateurs virtuels ;
- il est important de se souvenir que si un fichier change dans plusieurs emplacements, la réplication DFS conserve les modifications apportées par le fichier avec le dernier horodatage. Cela signifie que les modifications peuvent être perdues lors de la réplication DFS ;
- la réplication delta copie uniquement les modifications effectuées sur un fichier, utilisant ainsi moins de bande passante pour la réplication.

Collecte de données

La réplication DFS permet de répliquer des fichiers entre toutes les filiales vers un site concentrateur. Une fois les fichiers dans le site concentrateur, il est possible de sauvegarder toutes les données immédiatement, fournissant ainsi une manière centralisée de récupérer des données. Il est possible d'utiliser ce jeu de sauvegarde centralisé comme deuxième source de sauvegarde si vous sauvegardez déjà des données au niveau local du site. En proposant une sauvegarde au niveau du site concentrateur uniquement, il est possible de réaliser des économies sur le matériel, les logiciels et la main-d'œuvre nécessaires à la sauvegarde.

Il est possible d'utiliser les espaces de noms DFS pour offrir la tolérance de panne aux accès aux fichiers. Ainsi, si un serveur de filiale échoue, les clients peuvent encore accéder aux fichiers à partir du site concentrateur.

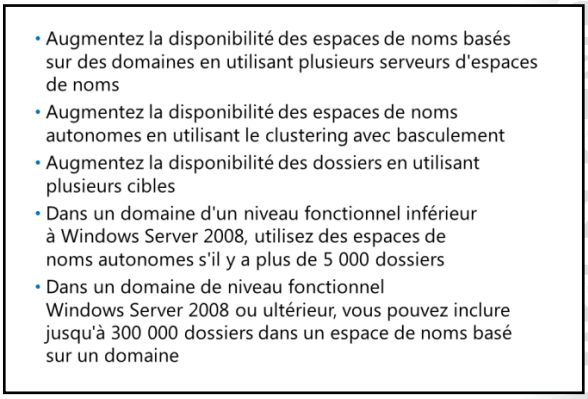
Distribution de données

Il est possible d'utiliser la réplication DFS pour répliquer des données d'un site concentrateur vers les sites de plusieurs filiales. Ce procédé rapproche les données de l'utilisateur. Il est possible d'utiliser les espaces de noms DFS pour s'assurer que les ordinateurs clients accèdent aux partages les plus proches, réduisant ainsi la consommation de bande passante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Instructions relatives à la conception d'une haute disponibilité d'espace de nom DFS

DFS redirige les utilisateurs qui ont besoin d'accéder aux dossiers dans un espace de noms DFS vers les cibles des dossiers dans l'espace de noms. Si un espace de noms est non disponible, les utilisateurs ne peuvent pas accéder aux fichiers. Pour garantir un accès ininterrompu aux fichiers, il est nécessaire de rendre un espace de noms hautement disponible.



Parmi les instructions pour l'implémentation de la disponibilité de l'espace de noms :

- AD DS stocke les espaces de noms basés sur un domaine et hébergés sur plusieurs serveurs. L'hébergement d'un espace de noms sur plusieurs serveurs rend l'espace de noms hautement disponible. Tous les serveurs qui hébergent un espace de noms doivent appartenir au même domaine ;
- un seul serveur héberge des espaces de noms autonomes, alors que les données de configuration sont stockées localement. Il est possible d'utiliser le clustering avec basculement pour augmenter la disponibilité d'un espace de noms autonome ;
- chaque dossier dans un espace de noms peut avoir une ou plusieurs cibles. Pour améliorer la disponibilité, utilisez plusieurs cibles pour chaque dossier, puis utilisez la réplication pour synchroniser des données entre des cibles de dossiers ;
- lorsque les espaces de noms DFS sont dans un domaine qui s'exécute à un niveau fonctionnel de domaine inférieur à Windows Server 2008, les utilisateurs peuvent rencontrer des problèmes de performances, comme être limités à 5 000 dossiers dans l'espace de noms. S'il est nécessaire d'utiliser un niveau fonctionnel de domaine inférieur pour la compatibilité avec les systèmes d'exploitation Windows antérieurs, utilisez les espaces de noms autonomes pour augmenter l'évolutivité au-delà de 5 000 dossiers ;
- lorsque les espaces de noms DFS sont dans un domaine fonctionnant au niveau fonctionnel de Windows Server 2008 ou ultérieur, il ne rencontre pas de dégradation des performances tant qu'il n'a pas atteint ou dépassé environ 300 000 dossiers.

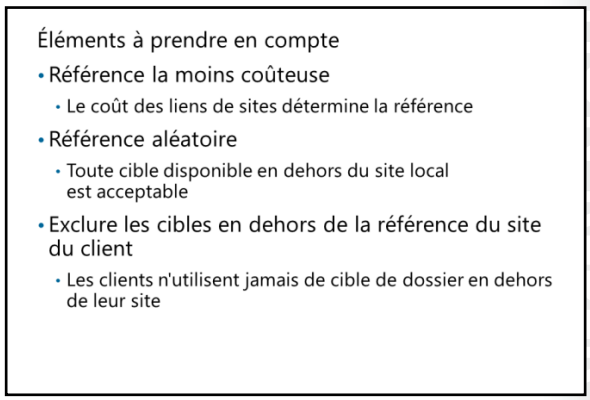
Liens de référence : Pour plus d'informations sur les espaces de noms DFS, rendez-vous à l'adresse : http://go.microsoft.com/fwlink/?LinkID=285325.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour la configuration de références

Le tri des références contrôle l'ordre dans lequel Windows Server 2012 présente les cibles de dossier aux clients. Chaque dossier utilise la configuration de la racine DFS par défaut, mais il est possible de remplacer ce paramètre.

Lorsqu'un client accède à un dossier, Windows Server 2012 lui présente une liste de cibles de dossier. Les paramètres configurés pour les références et la priorité cible déterminent l'ordre des cibles de dossier dans la liste.



Les éléments à prendre en compte pour les options des références sont les suivants :

- utilisez l'option de référence la moins coûteuse lorsque les coûts des liens de sites reflètent exactement l'ordre dans lequel vous souhaitez que les utilisateurs accèdent à des cibles. Lorsque vous sélectionnez l'option de référence la moins coûteuse, les clients utilisent d'abord une cible de dossier dans le site local. S'il n'existe aucune cible dans le site local, les clients choisissent une cible dans un autre site en se basant sur les coûts de liens de sites les plus bas ;

Remarque : Si plusieurs liens de sites ont le même coût, Windows Server 2012 sélectionne un site aléatoirement pour le client.

- utilisez l'option de référence aléatoire dès lors qu'une cible disponible en dehors du site local est acceptable. Lorsque vous sélectionnez l'option de référence aléatoire, les clients utilisent d'abord une cible de dossier dans le site local. S'il n'existe aucune cible dans le site local, les clients choisissent aléatoirement une cible dans un autre site ;
- utilisez l'option Exclure les cibles en dehors de la référence du site du client si vous souhaitez qu'aucun client n'utilise de cible de dossier en dehors de leur site. Lorsque vous sélectionnez cette option, les clients utilisent uniquement les cibles de dossier dans le site local. Si un dossier ne présente aucune cible dans le site local, les clients ne peuvent pas y accéder.

Pour définir avec précision les références et pour remplacer la configuration de référence du tri des références, utilisez la priorité cible. Les éléments à prendre en compte pour les options de priorité cible comprennent :

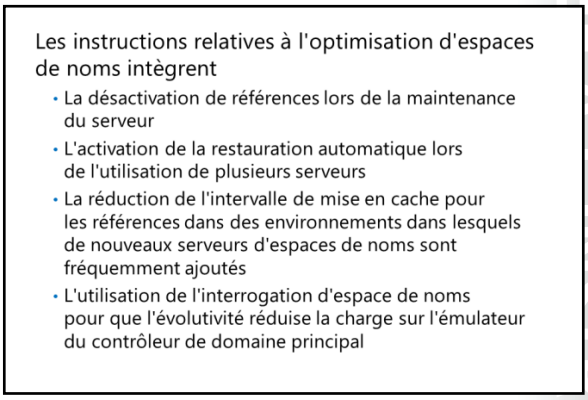
- utilisez la première des cibles présentant un coût équivalent lorsque plusieurs cibles sont dans le même site et que vous souhaitez qu'une cible soit la principale. Cela permet d'éviter les conflits de réplication. Par exemple, il est possible de stocker deux copies de données dans un site pour une haute disponibilité ;
- utilisez la dernière des cibles présentant un coût équivalent lorsque plusieurs cibles sont dans le même site et que vous souhaitez que les clients utilisent une cible uniquement lorsque les autres sont non disponibles. Par exemple, il est possible de configurer une cible devant être utilisée uniquement en tant qu'archive de sauvegarde ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- utilisez la première de toutes les cibles pour obliger Windows Server à choisir une cible en tant que cible préférée, quel que soit le coût associé au site. Cela est utile lorsque plusieurs cibles existent dans plusieurs sites, mais qu'une cible doit être la principale pour éviter les conflits de réplications. Par exemple, il est possible de conserver une copie principale des données, que les utilisateurs doivent toujours utiliser si elle est disponible, au siège social ;
- utilisez la dernière de toutes les cibles pour obliger les utilisateurs à se servir d'une cible en dernier recours, quel que soit le coût associé au site. Cela est utile lorsque plusieurs cibles existent dans plusieurs sites, mais que vous souhaitez qu'une cible soit utilisée uniquement lorsque les autres sont non disponibles. Par exemple, dans un scénario, il est possible d'utiliser une cible devant être utilisée uniquement en tant qu'archive de sauvegarde.

Instructions relatives à l'optimisation d'espaces de noms pour des systèmes DFS

Outre le tri des références et la priorité cible, pensez à d'autres options pour optimiser les espaces de noms DFS, dont ce qui suit :



- en effectuant la maintenance sur un serveur qui héberge une cible de dossier, désactivez les références pour cette dernière. Ceci permet de s'assurer que les clients ne se déconnecteront pas de la cible de dossier lorsque vous redémarrez le serveur ;
- activez la restauration automatique sur un dossier si vous souhaitez que les clients reviennent à une cible préférée une fois cette dernière disponible. Cela est utile lorsque la cible préférée est locale et que les autres cibles disponibles se trouvent uniquement sur une liaison WAN ;
- les clients mettent en cache des références vers des racines et des dossiers d'espaces de noms. Par défaut, DFS met en cache des références pour des racines d'espace de noms pendant cinq minutes et des références pour des dossiers pendant 30 minutes. Il est possible de raccourcir ces valeurs pour s'assurer que les clients trouvent plus rapidement de nouvelles racines d'espaces de noms et de nouvelles cibles de dossiers ;
- les serveurs d'espaces de noms utilisent l'interrogation d'espace de noms pour récupérer des données de configuration à partir d'AD DS. Vous avez la possibilité d'optimiser l'interrogation d'espace de noms pour la cohérence ou l'évolutivité. Lorsque vous optimisez l'interrogation d'espace de noms pour la cohérence, tous les serveurs d'espaces de noms récupèrent des données de configuration à partir de l'émulateur de contrôleur de domaine principal (PDC). Lorsque vous optimisez l'interrogation d'espace de noms pour l'évolutivité, les serveurs d'espaces de noms récupèrent des données de configuration à partir d'un contrôleur de domaine local afin de réduire la charge sur l'émulateur PDC.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Meilleures pratiques pour le déploiement d'espaces de noms pour des systèmes DFS

Window Server 2012 propose plusieurs options pour configurer des espaces de noms DFS. La configuration appropriée des espaces de noms DFS facilite l'accès aux fichiers pour les utilisateurs et évite les conflits de réplication. Les meilleures pratiques pour le déploiement d'espaces de noms DFS sont les suivantes :

- Utilisez des espaces de noms DFS pour créer une hiérarchie de dossiers unifiée
- Utilisez plusieurs cibles de dossier pour augmenter la disponibilité de chaque dossier
- Utilisez la méthode la moins coûteuse pour trier des références cibles
- Utilisez le mode d'évolutivité en cas d'utilisation de plus de 16 serveurs d'espace de noms
- Spécifiez un serveur principal à l'aide de la priorité cible pour réduire les conflits de réplication
- Activer l'énumération basée sur l'accès

- utilisez des espaces de noms DFS pour créer une hiérarchie de dossiers unifiée. Cela facilite la localisation de fichiers, les utilisateurs n'ayant en effet pas besoin de parcourir plusieurs serveurs ;
- utilisez plusieurs cibles de dossier pour augmenter la disponibilité de chaque dossier ;
- utilisez la méthode la moins coûteuse pour trier des références cibles. Dans la plupart des cas, il est préférable que les utilisateurs accèdent aux fichiers à partir d'une cible située dans le site Active Directory local ou à proximité ;
- utilisez le mode d'évolutivité en cas d'utilisation de plus de 16 serveurs d'espace de noms. Le mode d'évolutivité vérifie que les requêtes des serveurs d'espaces de noms ne surchargent pas l'émulateur PDC ;
- spécifiez un serveur principal à l'aide de la priorité cible pour réduire les conflits de réplication. Si vous spécifiez un serveur principal, tous les utilisateurs accèdent aux fichiers sur un seul serveur ;
- activez l'énumération basée sur l'accès sur l'espace de nom pour vous assurer que les utilisateurs voient uniquement les dossiers d'espaces de noms auxquels ils ont accès. Activez également l'énumération basée sur l'accès sur les cibles de dossier.

Instructions relatives à la conception d'une réplication DFS

Il est possible de contrôler la manière dont la réplication DFS effectue la réplication. La conception de la réplication DFS de manière appropriée pour votre environnement garantit des performances acceptables.

- Utilisez une topologie de réplication de maille uniquement lorsqu'il existe moins de dix membres
- Utilisez la limitation de bande passante pour garantir que la réplication ne surcharge pas les liaisons WAN
- Utilisez la compression différentielle à distance entre fichiers pour réduire le trafic de réplication
- Utilisez la réplication de filtre pour empêcher la réplication de fichiers indésirables
- Utilisez les dossiers répliqués en lecture seule quand le contenu ne doit pas être modifié
- Utilisez l'intermédiaire de taille, le conflit et les dossiers supprimés de manière adéquate
- Utilisez plusieurs petits dossiers pour simplifier le redémarrage

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour concevoir la réplication DFS, suivez les instructions suivantes :

- utilisez une topologie de réplication de maille uniquement lorsqu'il existe moins de dix membres. Dans la réplication de maille, chaque serveur réplique son contenu sur tous autres serveurs. Cela permet de simplifier la réplication et d'améliorer les performances. S'il existe plus dix membres, pensez à la topologie de réplication hub-and-spoke ;
- utilisez la limitation de bande passante pour garantir que la réplication ne surcharge pas les liaisons WAN. Cela peut être important lorsque la vitesse des liaisons WAN est basse ;
- utilisez la compression différentielle à distance entre fichiers pour réduire le trafic de réplication. La compression différentielle à distance entre fichiers identifie les modèles dans plusieurs fichiers, et utilise ces modèles pour réduire la réplication. La fonctionnalité entre fichiers est disponible sur toutes les éditions de Windows Server 2012 ;
- utilisez des filtres de réplication pour empêcher la réplication de types de fichiers indésirables. Les filtres de réplication restreignent la réplication selon des extensions de fichiers, et réduisent ainsi le trafic de réplication. Par exemple, il est possible d'empêcher la réplication de fichiers multimédias si ce contenu n'est requis ;
- utilisez des dossiers répliqués en lecture seule quand vous ne souhaitez pas qu'une réplication subisse une modification d'un client. Par exemple, quand un serveur central collecte des fichiers pour la sauvegarde, l'utilisation de dossiers répliqués en lecture seule évite de configurer manuellement les autorisations de partage en lecture seule ;
- assurez-vous de classer convenablement les dossiers intermédiaires, ainsi que ceux en conflit et supprimés. Un dossier intermédiaire avec une taille par défaut de 4 Go doit être au moins deux fois plus volumineux que le plus gros fichier répliqué. Si la taille par défaut du dossier en conflit et supprimé, qui est de 660 mégaoctets (Mo), est insuffisante, la réplication DFS peut vider les conflits avant qu'ils soient traités. Une fois que les deux dossiers atteignent 90 % d'utilisation, la réplication DFS les vide jusqu'à ce qu'ils atteignent 60 % d'utilisation ;
- utilisez plusieurs plus petits dossiers répliqués plutôt qu'un grand dossier répliqué. Si vous devez redémarrer la réplication, elle est beaucoup plus rapide de le faire sur un dossier présentant moins de contenu.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Planification et implémentation du système de fichiers NLB

NLB offre une haute disponibilité et l'évolutivité à des applications basées sur TCP/IP en partageant la charge des applications sur plusieurs serveurs. Si un serveur échoue dans un cluster d'équilibrage de charge réseau, d'autres serveurs existants pourront prendre la charge laissée par le serveur défectueux, permettant ainsi une haute disponibilité. Si le nombre d'utilisateurs de l'application augmente, il est possible d'ajouter plus de serveurs au cluster pour permettre à l'application de se mettre à l'échelle et d'offrir l'évolutivité.

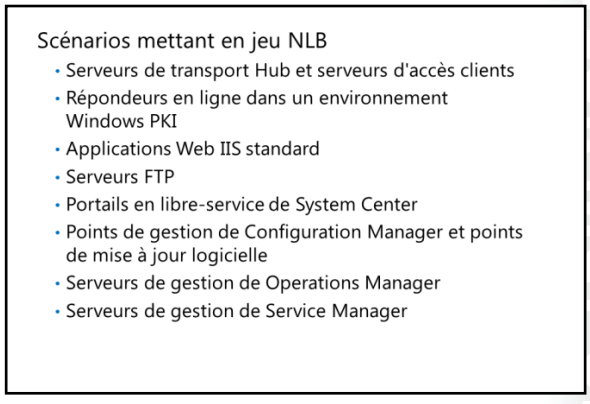
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les scénarios dans lesquels NLB offre une haute disponibilité ;
- décrire les options et les recommandations pour configurer les paramètres réseau NLB ;
- décrire les options et les recommandations pour configurer les règles des ports et d'autres paramètres de l'hôte ;
- décrire les options pour le stockage de données, qui doit être accessible aux serveurs Web du cluster NLB ;
- fournir des recommandations relatives au déploiement NLB sur des ordinateurs virtuels ;
- décrire les options d'intégration de NLB sur Microsoft System Center 2012 - Virtual Machine Manager (VMM).

Scénarios mettant en jeu NLB

Utilisez NLB pour fournir une haute disponibilité et l'évolutivité aux applications et services qui utilisent le protocole réseau TCP/IP sur un port TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol). La plupart des organisations utilisent des équilibrages de charge matérielle pour fournir une haute disponibilité et l'évolutivité à des applications Web essentielles. Pourtant, ces mêmes organisations utilisent le service NLB pour prendre en charge de plus petites applications sans entraîner de dépenses supplémentaires en matériel.



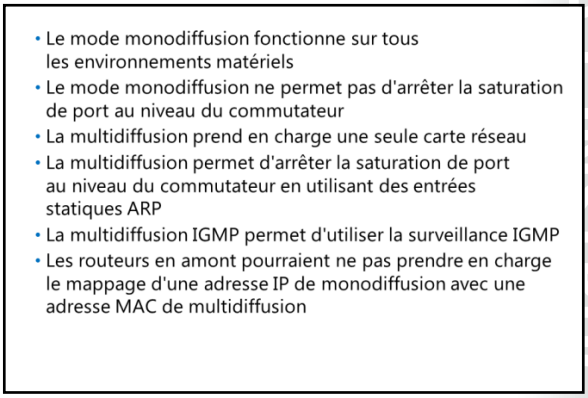
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La liste suivante répertorie certains des environnements permettant l'utilisation de NLB :

- service de répondeur en ligne dans un environnement d'infrastructure à clé publique de Windows (KPI) ;
- applications Web IIS (Internet Information Services) standard avec moins de 10 serveurs frontaux ;
- serveurs FTP (File Transfer Protocol) ;
- System Center 2012 – portail libre-service du Gestionnaire de service ;
- points de gestion et de mise à jour de logiciels du gestionnaire de configuration de System Center 2012 ;
- serveurs de gestion de System Center 2012 Operations manager ;
- serveurs de gestion de System Center 2012 Service manager.

Éléments à prendre en compte pour la configuration des paramètres réseau NLB

Les paramètres réseau NLB définissent la gestion de l'adresse MAC (Media Access Control) de l'adresse IP virtuelle du cluster. Les paquets réseau sont envoyés à l'adresse IP virtuelle du cluster, car elle doit être gérée par tous les nœuds du cluster. Il existe trois options de paramètres réseau dans NLB : monodiffusion, multidiffusion et multidiffusion IGMP (Internet Group Management Protocol).



Monodiffusion

Le mode monodiffusion est le paramètre réseau par défaut pour NLB. Dans ce mode, NLB remplace l'adresse MAC réelle de chaque serveur dans le cluster par une adresse MAC NLB commune. De cette façon, tous les paquets qui sont envoyés à l'adresse IP virtuelle du cluster sont livrés à l'aide de la même adresse MAC, et donc tous les serveurs présents dans le cluster les reçoivent. Cependant, si vous utilisez le même commutateur pour vos nœuds, vous pouvez rencontrer un problème, car chaque port dans un commutateur doit avoir sa propre adresse MAC. NLB résout ce problème en attribuant une adresse MAC distincte à chaque nœud, en modifiant le deuxième octet de l'adresse MAC commune afin qu'elle corresponde à l'ID de membre du cluster du nœud. NLB utilise ensuite une multidiffusion ARP (Address Resolution Protocol) pour envoyer des données au cluster.

Remarque : Le mode monodiffusion nécessite l'utilisation de deux cartes réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Multidiffusion

En mode multidiffusion (multidiffusion ou multidiffusion IGMP), NLB attribue une adresse IP de multidiffusion aux nœuds du cluster. Il est possible d'utiliser ce mode avec une seule carte réseau par nœud.

Remarque : Il est possible d'utiliser la multidiffusion IGMP dans un cluster NLB Windows uniquement si le commutateur auquel les nœuds sont connectés prend en charge la multidiffusion IGMP.

Éléments à prendre en compte pour la configuration des paramètres réseau NLB

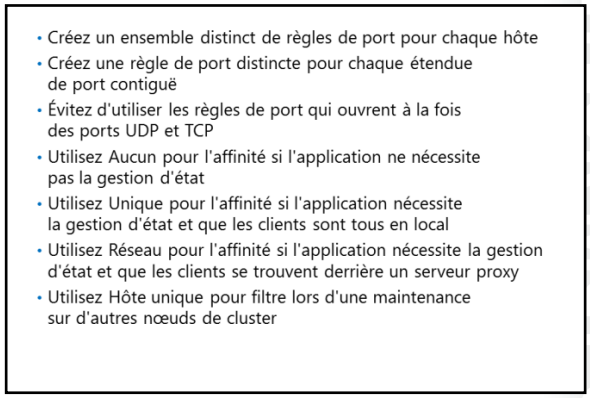
Voici une liste des éléments à prendre en compte pour la configuration des paramètres réseau NLB :

- le mode monodiffusion fonctionne sur tous les environnements matériels ;
- le mode monodiffusion ne permet pas d'arrêter la saturation de port au niveau du commutateur ;
- la multidiffusion prend en charge une seule solution de carte réseau par nœud ;
- la multidiffusion permet d'arrêter la saturation de port au niveau du commutateur en utilisant des entrées statiques ARP ;
- la multidiffusion IGMP permet d'utiliser la surveillance IGMP ;
- les routeurs en amont pourraient ne pas prendre en charge le mappage d'une adresse IP de monodiffusion (l'adresse IP du cluster) avec une adresse MAC de multidiffusion. En pareille situation, mettez à niveau ou remplacez le routeur. Sinon, la méthode de multidiffusion est inutilisable.

Éléments à prendre en compte pour la configuration des règles des ports

Lors de l'implémentation d'hôtes de cluster NLB, pensez aux options de règles de port suivantes :

- créez un ensemble distinct de règles de port pour chaque hôte ;
- évitez d'ajouter plus de ports que nécessaire pour chaque hôte ; créez une règle de port distincte pour chaque étendue de port contiguë, à l'aide de TCP ou d'UDP ;
- évitez d'utiliser les règles de port qui ouvrent à la fois des ports UDP et TCP ;
- choisissez Aucune comme option d'affinité si l'application ne nécessite pas la gestion d'état au niveau du serveur ;
- choisissez Unique comme option d'affinité si l'application nécessite la gestion d'état au niveau du serveur et si les clients sont au niveau local ;
- choisissez Réseau comme option d'affinité si l'application nécessite la gestion d'état au niveau du serveur et si les clients sont derrière un serveur proxy ;
- utilisez Hôte unique pour filtre lors d'une maintenance sur d'autres nœuds de cluster.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour la configuration du stockage de données des clusters NLB

L'utilisation la plus courante de NLB consiste à fournir une haute disponibilité et l'évolutivité aux sites Web et aux sites FTP. IIS héberge généralement ces sites. Les sites IIS fournissent l'accès aux données stockées dans le système de fichiers via les protocoles HTTP, HTTPS ou FTP. Par conséquent, tous les nœuds d'un cluster NLB doivent avoir accès aux mêmes données.

- Utilisez la réplication DFS pour répliquer des données entre tous les nœuds
- Utilisez la réplication DFS et les espaces de noms DFS pour répliquer des données vers un ensemble distinct de serveurs de fichiers
- Utilisez le clustering avec basculement avec le rôle serveur de fichiers pour stocker les données loin des nœuds

En concevant votre solution de stockage pour NLB dans IIS, prenez en considération les éléments suivants :

- utilisez DFS pour répliquer les données entre les nœuds. Cela permet de conserver une copie des données dans chaque nœud. Cependant, cette méthode ne fournit pas la tolérance de panne si le sous-système de disque est défaillant sur un nœud et si le nœud NLB est encore actif ;
- utilisez un serveur de fichiers dans le cluster pour fournir le stockage sur tous les nœuds de cluster. Cette méthode ne fournit qu'un seul point de stockage pour tous les nœuds, mais la mise à l'échelle n'est pas correcte lors de l'ajout de nœuds ;
- utilisez des serveurs de fichiers séparés et la réplication DFS pour fournir la haute disponibilité en cas de perte de disque et pour réduire la réplication entre les nœuds.

Éléments à prendre en compte pour le déploiement d'un système de fichiers NLB sur des ordinateurs virtuels

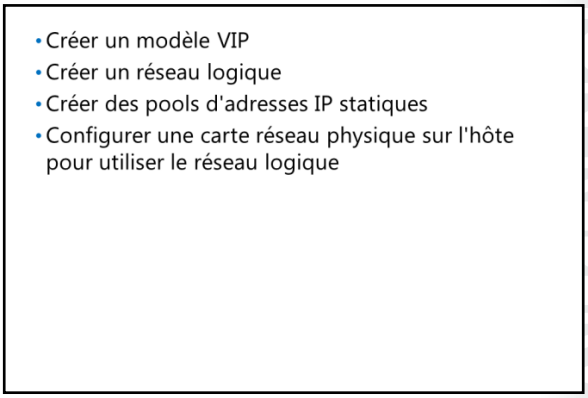
Les serveurs physiques ne constituent pas le seul type de serveurs qui peuvent tirer profit de l'utilisation de NLB. Il est possible d'utiliser NLB dans des serveurs virtualisés de la même manière que dans des serveurs physiques. Cependant, certains éléments sont à prendre en considération en matière d'environnement virtuel :

- Utilisez des réseaux virtuels distincts pour les réseaux NLB privés et publics
- Activez l'usurpation d'adresses MAC

- utilisez des réseaux virtuels distincts pour les réseaux privés et publics que NLB utilise ;
- dans les paramètres réseau de la carte que vous utilisez pour le cluster NLB, prenez soin d'activer l'usurpation des adresses MAC et indiquez l'adresse statique que vous créez pour le cluster.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion des composants NLB dans VMM



VMM vous permet de créer des ordinateurs virtuels et des services selon des modèles prédéfinis. Un modèle de service peut contenir plusieurs ordinateurs virtuels, et il est possible de configurer certains de ces ordinateurs virtuels de sorte qu'ils fonctionnent dans un cluster NLB. Avant de pouvoir utiliser NLB avec VMM, il est nécessaire de vérifier que vous répondez aux exigences suivantes. Pour ce faire :

- créez un modèle d'IP virtuelle (VIP) pour NLB ;
- créez un réseau logique et associez-le à un ou plusieurs sites réseau. Associez les sites réseau aux groupes d'hôtes sur lesquels il est possible de déployer le service ;
- créez des pools d'adresses IP statiques pour les sites réseau associés sur lesquels vous déploierez le service ;
- sur l'hôte sur lequel vous déploierez le service, prenez-soin de configurer une carte réseau physique de sorte qu'elle utilise le même réseau logique que le service.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et implémentation d'une haute disponibilité pour des services et des applications de fichiers

Scénario

Parmi les exigences économiques et techniques pour le déploiement de Windows Server 2012 chez A. Datum Corporation, la haute disponibilité pour tous les services et toutes les applications réseau est essentielle. A. Datum a identifié des services de fichiers et plusieurs applications Web comme étant des services essentiels qu'il est nécessaire de rendre hautement disponibles.

A. Datum a identifié deux exigences pour la haute disponibilité des services de fichiers :

- la perte d'un disque sur lequel les fichiers réseau sont stockés ne doit pas avoir de conséquences sur la disponibilité de ces derniers ;
- la perte d'un disque fournissant les partages de fichiers ne doit pas avoir de conséquences sur la disponibilité des fichiers stockés sur le serveur.

A. Datum a également identifié que la défaillance d'un serveur Web ne devrait pas avoir de conséquences sur la disponibilité des applications Web.

Objectives

À la fin de cet atelier pratique, les stagiaires seront à même d'effectuer les tâches suivantes :

- planifier la stratégie de haute disponibilité pour des services de fichiers ;
- planifier la stratégie de haute disponibilité pour des applications Web ;
- implémenter et valider la stratégie de haute disponibilité pour le stockage de fichiers ;
- implémenter une solution à haute disponibilité à l'aide de NLB.

Configuration de l'atelier pratique

Durée approximative : 75 minutes

Ordinateurs virtuels	22414B-LON-DC1 22414B-LON-CL1 22414B-LON-SVR1 22414B-LON-SVR2 22414B-TOR-SVR1 22414B-TOR-SS1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible.
Avant de commencer cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, sur **Accueil**, cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22414B-LON-DC1** et, dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   a. Nom d'utilisateur : **ADATUM\Administrateur**
   b. Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 et 3 pour les ordinateurs virtuels restants.

Exercice 1 : Planification d'une stratégie de haute disponibilité pour des services de fichiers

Scénario

Ces derniers mois, A. Datum a connu plusieurs pannes non planifiées, ce qui a affecté la disponibilité des services de fichiers dans l'organisation. Les pannes ont principalement touché la filiale de Toronto. Pour éviter que cela se produise, vous devez planifier un déploiement de services de fichiers qui offre la redondance totale contre la défaillance de tout composant dans le centre de données de Toronto.

Pour implémenter cette solution, A. Datum a équipé le bureau de Toronto d'un nouveau réseau SAN de zone de stockage iSCSI. Le réseau SAN iSCSI offre un certain niveau de redondance, mais l'équipe serveurs a également décidé d'implémenter des espaces de stockage et un système de fichiers DFS pour atteindre un de niveau de redondance plus élevé.

La conception de l'espace de stockage doit offrir la redondance en cas de défaillance de n'importe quel composant de stockage. Ceci comprend les serveurs, les périphériques réseau et les compartiments de stockage.

A. Datum a identifié plusieurs partages de fichiers importants qui doivent être à la disposition des utilisateurs même si le centre de données à Toronto tombe en panne. Si le centre de données tombe en panne, les utilisateurs doivent encore pouvoir accéder aux fichiers à partir d'un serveur situé à Londres.

Les tâches principales de cet exercice sont les suivantes :

1. Lire la documentation fournie avec le produit.
2. Mettre à jour le document de proposition en fonction du plan d'action planifié.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.

▶ Tâche 1 : Lire la documentation fournie avec le produit

1. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez l'explorateur de fichiers, puis accédez à et ouvrez **\\LON-DC1\E$\Labfiles\Module6\email1.docx**.
3. Lisez et examinez le fichier.
4. Fermez le document.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

1. Sur LON-CL1, dans l'Explorateur de fichiers, accédez à et ouvrez **\\LON-DC1\E$\Labfiles\Module6\Proposal1.docx**.
2. Lisez le fichier **Proposal1.docx**, puis proposez des suggestions pour traiter chacun des problèmes répertoriés.
3. Fermez le document.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

1. Sur LON-CL1, dans l'Explorateur de fichiers, accédez à et ouvrez **\\LON-DC1\E$\Labfiles\Module6\FinalProposal1.docx**.
2. Lisez les réponses dans le document **E:\Labfiles\Module6\FinalProposal1.doc**, comparez-les avec vos réponses, puis partagez vos réponses avec la classe.
3. Fermez le fichier.

Résultats : Après avoir terminé cet exercice, vous devez avoir planifié une stratégie de haute disponibilité pour des serveurs de fichiers.

Les stagiaires concevront le déploiement de l'espace de stockage. La conception doit intégrer les serveurs et composants réseau qui seront déployés, ainsi que les unités de stockage. La conception doit également contenir des remarques au sujet des fonctionnalités hautement disponibles que le déploiement inclut, comme l'association de cartes d'interface réseau (NIC) sur les serveurs, Microsoft Multipath I/O (MPIO) pour le chemin d'accès réseau, et les niveaux RAID sur le compartiment de stockage.

Les stagiaires concevront également le déploiement DFS. La conception inclura les emplacements des serveurs, les espaces de noms DFS déployés et cibles DFS. La conception doit comprendre des remarques sur la configuration pour la configuration de réplication DFS.

Exercice 2 : Planification d'une stratégie de haute disponibilité pour des applications Web

Scénario

A. Datum a déployé le site intranet de l'entreprise sur des serveurs Web Windows Server 2012. Les utilisés utilisent le site d'intranet comme référentiel pour la documentation de société. Une partie de la documentation est essentielle et doit toujours être disponible pour les utilisateurs.

La conception que vous créez pour le déploiement du site intranet doit offrir la haute disponibilité. La conception doit accepter la défaillance de tout serveur ou disque.

Les tâches principales de cet exercice sont les suivantes :

1. Lire la documentation fournie avec le produit.
2. Mettre à jour le document de proposition en fonction du plan d'action planifié.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.

UTILISATION RÉSERVÉE À L'ENSEIGNEMENT MCT UNIQUEMENT

▶ Tâche 1 : Lire la documentation fournie avec le produit

1. Sur LON-CL1, dans le serveur de fichiers, accédez à et ouvrez **\\LON-DC1\E$\Labfiles\Module6\email2.docx**.
2. Lisez et analysez le fichier.
3. Fermez le document.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

1. Sur LON-CL1, dans l'Explorateur de fichiers, accédez à et ouvrez **\\LON-DC1\E$\Labfiles\Module6\Proposal2.docx**.
2. Lisez le fichier **Proposal2.docx**, puis renseignez les suggestions pour traiter chacun des problèmes répertoriés.
3. Fermez le fichier.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

1. Sur LON-CL1, dans l'Explorateur de fichiers, accédez à et ouvrez **\\LON-DC1\E$\Labfiles\Module6\FinalProposal2.docx**.
2. Lisez les réponses dans le document **E:\Labfiles\Module6\FinalProposal2.docx**, puis comparez-les avec vos réponses. Présentez vos réponses à la classe et comparez-les avec celles fournies.
3. Fermez le fichier.

Résultats : Après avoir terminé cet exercice, vous devez avoir planifié une stratégie de haute disponibilité pour des applications Web, y compris les éléments suivants :

- votre conception de déploiement NLB doit inclure le déploiement du serveur et la conception de stockage. Utilisez les informations de l'exercice précédent pour planifier la conception du stockage ;
- votre conception doit intégrer les règles de port NLB et la conception des paramètres réseau.

Exercice 3 : Implémentation d'une solution de haute disponibilité pour le stockage de fichiers

Scénario

Vous devez implémenter l'espace de stockage et la conception DFS que vous avez créés. Vous validerez la redondance de déploiement et de test.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer une association de cartes d'interface réseau (NIC).
2. Configurer des initiateurs iSCSI et MPIO.
3. Configurer des espaces de stockage à l'aide des cibles iSCSI.
4. Valider la haute disponibilité du déploiement contre le risque de perte d'un disque.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Configurer une association de cartes d'interface réseau (NIC)

1. Connectez-vous à TOR-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez les connexions réseau et activez **Connexion au réseau local 2**, **Connexion au réseau local 3** et **Connexion au réseau local 4**.
3. Créez une nouvelle association de cartes réseau en respectant les paramètres suivants :
   - Nom : **Association d'accès iSCSI 1**
   - Cartes : **Connexion au réseau local** et **Connexion au réseau local 2**
4. Configurez les paramètres TCP/IP pour l'association d'accès iSCSI 1 à l'aide des paramètres suivants :
   - Adresse IP : **172.16.1.20**
   - Masque de sous-réseau : **255.255.0.0**
   - Passerelle par défaut : **172.16.0.1**
   - Serveur DNS préféré : **172.16.0.10**
5. Créez une nouvelle association de cartes réseau en respectant les paramètres suivants :
   - Nom : **Association d'accès iSCSI 2**
   - Cartes : **Connexion au réseau local 3** et **Connexion au réseau local 4**
6. Configurez les paramètres TCP/IP pour l'association d'accès iSCSI 2 à l'aide des paramètres suivants :
   - Adresse IP : **131.107.1.10**
   - Masque de sous-réseau : **255.255.0.0**
   - Passerelle par défaut : vide
   - Serveur DNS préféré : **172.16.0.10**

▶ Tâche 2 : Configurer des initiateurs iSCSI et MPIO

1. Sur TOR-SVR1, dans le Gestionnaire de serveur, démarrez l'Assistant Ajout de rôles et de fonctionnalités, puis installez la fonctionnalité **Multipath I/O**.
2. Dans le Gestionnaire de serveur, dans le menu **Outils**, ouvrez **Initiateur iSCSI**, puis configurez les éléments suivants :
   a. Activez le service **Initiateur iSCSI**.
   b. Établissez une **Connexion rapide** avec la cible : **172.16.1.25**
3. Dans Gestionnaire de serveur, dans le menu **Outils**, ouvrez **MPIO**, puis configurez les éléments suivants :
   a. Activez **Ajouter la prise en charge des périphériques iSCSI** sur **Découvrir plusieurs chemins**
4. Lorsque l'ordinateur a redémarré, ouvrez une session sur TOR-SVR1 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
5. Dans le Gestionnaire de serveur, dans le menu **Outils**, cliquez sur **MPIO** et vérifiez que **ID du matériel de périphérique MSFT2005iSCSIBusType_0x9** est répertorié dans la liste.

▶ Tâche 3 : Configurer des espaces de stockage à l'aide des cibles iSCSI

1. Sur TOR-SVR1, créez un pool de stockage qui utilise les paramètres suivants :
   - Nom : **iSCSIPool**
   - Disques :
     - **PhysicalDisk1 (TOR-SVR1)**
     - **PhysicalDisk2 (TOR-SVR1)**
     - **PhysicalDisk3 (TOR-SVR1)**
     - **PhysicalDisk4 (TOR-SVR1)**
     - **PhysicalDisk5 (TOR-SVR1)**
2. Dans iSCSIPool, créez un disque dur virtuel avec les paramètres suivants :
   - Nom : **DFSDisk**
   - Disposition du stockage : **Parity** (Parité)
   - Type d'allocation : **Fixe**
   - Taille : **Maximale**
3. Créez un volume avec les paramètres suivants :
   - Lettre du lecteur : **H**
   - Système de fichiers : **NTFS**
   - Nom : **Volume DFS**

▶ Tâche 4 : Valider la haute disponibilité du déploiement contre le risque de perte d'un disque

1. Sur TOR-SVR1, utilisez Windows PowerShell pour copier le fichier **C:\windows\system32\notepad.exe** sur le lecteur **H**.
2. Sur l'ordinateur hôte, dans le Gestionnaire Hyper-V, dans le volet Ordinateurs virtuels, cliquez avec le bouton droit sur **22414B-TOR-SVR1**, puis sur **Paramètres**.
3. Dans la fenêtre Paramètres pour 22414B-TOR-SVR1 sur LON-HOST1, dans le volet Matériel, cliquez sur la première occurrence de **Carte réseau héritée**. Dans la liste déroulante **Commutateur virtuel**, cliquez sur **Non connecté**, puis cliquez sur **OK**.
4. Sur TOR-SVR1, ouvrez l'explorateur de fichiers, puis cliquez sur **Volume DFS (H:)**.
5. Vérifiez que notepad.exe figure dans la liste des fichiers.
6. Sur l'ordinateur hôte, dans le Gestionnaire Hyper-V, dans le volet Ordinateurs virtuels, cliquez avec le bouton droit sur **22414B-TOR-SVR1**, puis sur **Paramètres**.
7. Dans la fenêtre Paramètres pour 22414B-TOR-SVR1 sur LON-HOST1, dans le volet Matériel, cliquez sur la première occurrence de **Carte réseau héritée**. Dans la liste déroulante **Commutateur virtuel**, cliquez sur **Réseau externe**, puis cliquez sur **OK**.

Résultats : Après avoir terminé cet exercice, vous devez avoir implémenté une solution de haute disponibilité pour un stockage de fichiers.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 4 : Implémentation d'une solution de haute disponibilité à l'aide de l'équilibrage de charge réseau

Scénario

Vous devez implémenter la conception NLB que vous avez créée. Pour ce faire, vous allez déployer un cluster NLB, configurer les paramètres en fonction de la conception, et configurer un site Web de test pour utiliser le stockage hautement disponible. Vous validerez ensuite la disponibilité du site Web en simulant une défaillance du serveur.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer un cluster d'équilibrage de la charge réseau (NLB).
2. Configurer des serveurs Web pour utiliser le stockage à haute disponibilité.
3. Valider le déploiement.

▶ Tâche 1 : Configurer un cluster d'équilibrage de la charge réseau (NLB)

1. Connectez-vous à LON-DC1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez Internet Explorer®, puis vérifiez que l'application Web est disponible sur les URL suivantes :
   - **http://LON-SVR1.adatum.com**
   - **http://LON-SVR2.adatum.com**
3. Créez un enregistrement de ressource d'hôte (A) dans DNS pour **www.Adatum.com** qui pointe vers **172.16.0.111**.
4. Installez la fonctionnalité d'équilibrage de la charge réseau sur **LON-SVR1** et **LON-SVR2**.
5. Créez un cluster NLB à l'aide des paramètres suivants :
   - Nom : **LON-NLB**
   - Mode d'opération : **multidiffusion**
   - Adresse IP du cluster : **172.16.0.111**
   - Interface réseau sur LON-SVR1 : **Connexion au réseau local**
6. Ajoutez un deuxième nœud au cluster à l'aide des paramètres suivants :
   - Noms du nœud : **LON-SVR2**
   - Interface réseau : **Connexion au réseau local**
7. Configurez le cluster de sorte qu'il utilise une règle de port unique avec les paramètres suivants :
   - Étendue du port : **80 à 80**
   - Protocoles : **TCP**
   - Mode de filtrage : **Hôte multiple**
   - Affinité : **Unique**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer des serveurs Web pour utiliser le stockage à haute disponibilité

1. Sur LON-SVR1, ouvrez la console Gestion du système de fichiers distribués DFS, et vérifiez qu'elle est configurée avec les trois serveurs d'espace de noms suivants :
   a. **LON-SVR1**
   b. **LON-SVR2**
   c. TOR-SVR1
2. Vérifiez que la réplication est configurée.
3. Fermez la console Gestion du système de fichiers distribués DFS.
4. Configurez IIS sur LON-SVR1 et LON-SVR2 pour utiliser le partage **\\adatum.com\website\wwwrroot** comme source pour le site Web par défaut.

▶ Tâche 3 : Valider le déploiement

1. Basculez vers LON-CL1, puis testez le cluster NLB à partir d'Internet Explorer à l'aide de l'URL **http://www.adatum.com**. Validez les paramètres d'affinité.
2. Arrêtez le nœud de cluster NLB auquel vous êtes connecté, puis actualisez Internet Explorer pour tester la haute disponibilité.
3. Redémarrez le nœud, puis actualisez Internet Explorer pour tester l'affinité.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, et cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-SVR2**, **22414B-LON-CL1**, **22414B-TOR-SS1** et **22414B-TOR-SVR1**.

Résultats : Après avoir terminé cet exercice, vous devez avoir implémenté une solution de haute disponibilité à l'aide de NLB.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 8

Planification et implémentation d'une infrastructure haute disponibilité à l'aide du clustering avec basculement

Table des matières :

Vue d'ensemble du module 8-1

Leçon 1 : Planification d'une infrastructure pour le clustering avec basculement 8-2

Leçon 2 : Implémentation du clustering avec basculement 8-13

Leçon 3 : Intégration du clustering avec basculement avec la virtualisation de serveur 8-21

Leçon 4 : Planification d'un cluster de basculement multisite 8-34

Atelier pratique : Planification et implémentation d'une infrastructure hautement disponible à l'aide du clustering avec basculement 8-39

Contrôle des acquis et éléments à retenir 8-49

Vue d'ensemble du module

La planification de la haute disponibilité est une partie essentielle de la conception de votre système. Pour la plupart des organisations, le temps nécessaire à l'implémentation d'un plan de récupération d'urgence est trop long ou n'est pas inclus dans le budget. Par conséquent, ces organisations utilisent la haute disponibilité afin de ne pas avoir à exécuter la récupération d'urgence.

Windows Server® 2012 inclut le clustering avec basculement pour fournir la haute disponibilité aux applications et services.

Dans ce module, vous allez apprendre à planifier et implémenter le clustering avec basculement.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- Planifier une infrastructure pour le clustering avec basculement.
- Implémenter un clustering avec basculement.
- Intégrer le clustering avec basculement avec la virtualisation de serveur.
- Planifier le clustering avec basculement multisite.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification d'une infrastructure pour le clustering avec basculement

Le clustering avec basculement est une fonctionnalité hautement disponible incluse dans Windows Server 2012. Si vous le configurez correctement, le clustering avec basculement permet à une application ou à un service qui s'exécute sur un nœud de cluster de basculer vers un autre nœud de cluster. Cependant, un cluster de basculement mal configuré peut connaître des pertes de données et des problèmes de performances en cas de défaillance d'un nœud de cluster. Par conséquent, pour vous assurer que votre cluster de basculement ne rencontre pas de problèmes de performances, vous devez comprendre comment planifier et concevoir le stockage partagé, la capacité matérielle et le quorum.

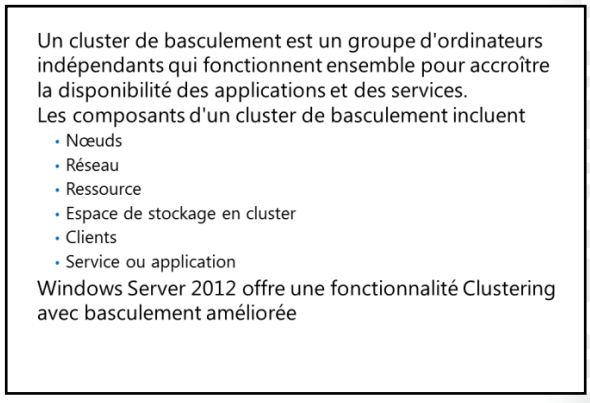
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire le clustering avec basculement.
- Décrire les éléments à prendre en compte pour les charges de travail de serveurs sur les clusters de basculement.
- Déterminer le type et la quantité de composants matériels à utiliser pour le clustering avec basculement.
- Planifier les composants réseau.
- Planifier les composants de stockage.
- Planifier le quorum du cluster.
- Décrire les éléments à prendre en compte pour les applications.

Vue d'ensemble du clustering avec basculement

Un cluster de basculement est un groupe d'ordinateurs indépendants qui fonctionnent ensemble afin d'augmenter la disponibilité des applications et des services. Si un cluster de serveur, ou un *nœud*, subit une défaillance, un autre nœud commence à assurer les services. Il s'agit du *basculement*, ce qui entraîne peu ou pas d'interruptions de service pour les utilisateurs.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Une solution de clustering avec basculement se compose de plusieurs composants, dont :

- Des nœuds, qui sont des ordinateurs membres d'un cluster de basculement. Ces ordinateurs exécutent un service de cluster, ainsi que des ressources et applications associées au cluster.
- Un réseau, sur lequel les nœuds de cluster peuvent communiquer entre eux et avec les clients. Il existe trois types de réseaux que vous pouvez utiliser dans un cluster : public, privé et public-et-privé.
- Une *ressource*, qui est une entité hébergée par un nœud. Elle est gérée par le service de cluster et vous pouvez la démarrer, l'arrêter ou la déplacer vers un autre nœud.
- Un espace de stockage en cluster, qui est un système de stockage qui, en général, est partagé par les nœuds de cluster. Dans certains cas, notamment lorsque des clusters de serveurs exécutent Microsoft® Exchange Server, aucun stockage partagé n'est requis.
- Des clients, qui sont des ordinateurs (ou utilisateurs) qui utilisent le service de cluster.
- Un service ou une application, qui est une entité logicielle que le cluster présente aux clients pour qu'ils puissent l'utiliser.

Dans un cluster de basculement, chaque nœud du cluster :

- Dispose d'une connectivité et d'une communication complète avec les autres nœuds du cluster.
- Est informé lorsqu'un autre nœud rejoint ou quitte le cluster. Par ailleurs, chaque nœud tient compte de l'échec d'un nœud ou d'une ressource et a la capacité d'assurer ces services.
- Se connecte à un réseau à travers lequel les ordinateurs clients peuvent accéder au cluster.
- Se connecte via un bus partagé ou une connexion iSCSI (Internet Small Computer System Interface) au stockage partagé.
- Connaît les services ou applications qui s'exécutent localement, et les ressources qui s'exécutent sur tous les autres nœuds du cluster.

L'espace de stockage en cluster fait généralement référence aux unités logiques, en général des disques durs ou numéros d'unités logiques auxquels tous les nœuds de cluster sont connectés via un bus partagé. Ce bus est distinct du bus qui contient le système et les disques de démarrage. Les disques partagés stockent des ressources, telles que les applications et les partages de fichiers, que le cluster gérera.

Alors que la plupart des fonctionnalités du clustering avec basculement et des techniques d'administration de Windows Server® 2008 R2 sont présentes dans Windows Server 2012, certaines nouvelles fonctionnalités et technologies de Windows Server 2012 augmentent l'extensibilité et la disponibilité de l'espace de stockage en cluster. Ces fonctionnalités fournissent également une gestion améliorée et simplifiée, ainsi qu'un basculement plus rapide.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les nouvelles fonctionnalités importantes du clustering avec basculement dans Windows Server 2012 sont les suivantes :

- Évolutivité améliorée. Dans Windows Server 2012, un cluster de basculement peut avoir 64 nœuds physiques et peut exécuter 4 000 ordinateurs virtuels sur chaque cluster. C'est une amélioration considérable par rapport à Windows Server 2008 R2, qui ne prend en charge que 16 nœuds physiques et 1 000 ordinateurs virtuels par cluster. Le Gestionnaire de serveur dans Windows Server 2012 peut découvrir et gérer tous les clusters que vous créez dans un domaine des services de domaine Active Directory® (AD DS). Si vous déployez le cluster dans un scénario multisite, l'administrateur peut désormais contrôler quels nœuds d'un cluster ont des votes pour établir le quorum. Windows Server 2012 améliore également l'extensibilité du clustering avec basculement pour les ordinateurs virtuels qui s'exécutent sur des clusters.
- CSV améliorés. Windows Server 2008 R2 a introduit cette technologie, qui est devenue très populaire pour fournir l'espace de stockage de l'ordinateur virtuel. Dans Windows Server 2012, les volumes partagés de cluster (CSV) apparaissent comme des systèmes de fichiers CSV. Ils prennent en charge le stockage SMB (Server Message Block) version 3.0 pour le rôle Hyper-V® dans Windows Server 2012 et d'autres applications. En outre, CSV peut utiliser les fonctionnalités SMB multicanal et SMB Direct pour permettre au trafic de circuler sur plusieurs réseaux dans un cluster. Vous pouvez également implémenter les serveurs de fichiers sur les volumes CSV, en mode avec montée en puissance parallèle. Pour une sécurité renforcée, vous pouvez utiliser le chiffrement de lecteur Windows BitLocker® pour des disques CSV, et vous pouvez également rendre le stockage CSV visible uniquement à un sous-ensemble de nœuds d'un cluster. À des fins de fiabilité, vous pouvez analyser et réparer les volumes CSV sans temps hors connexion.
- Mise à jour adaptée aux clusters. Dans les versions antérieures de Windows Server, la mise à jour des nœuds de cluster nécessitait une longue période de préparation et de planification, afin de réduire ou d'éviter le temps mort. Par ailleurs, la procédure de mise à jour des nœuds de cluster était généralement une procédure manuelle, ce qui entraînait des tâches administratives supplémentaires. Cependant, Windows Server 2012 présente la mise à jour adaptée aux clusters, une nouvelle technologie à cet effet. Cette technologie met automatiquement à jour les nœuds de cluster avec le correctif logiciel Windows Update, en maintenant le cluster en ligne et en réduisant le temps mort. Une section ultérieure de ce module présente cette technologie plus en détails.
- Amélioration de l'intégration AD DS. Dans Windows Server 2008, le clustering avec basculement est intégré dans AD DS. Dans Windows Server 2012, cette intégration a été améliorée. Les administrateurs peuvent maintenant créer des objets ordinateurs de cluster dans des unités d'organisation ciblées, ou par défaut dans les mêmes unités d'organisation que les nœuds de cluster. Cette conception fait coïncider les dépendances de cluster de basculement sur AD DS avec le modèle d'administration de domaine délégué qui est utilisé dans de nombreuses organisations informatiques. En outre, vous pouvez à présent déployer les clusters de basculement avec un accès uniquement aux contrôleurs de domaine en lecture seule.
- Améliorations de la gestion. Bien que le clustering avec basculement dans Windows Server 2012 utilise toujours quasiment la même console de gestion et les mêmes techniques administratives, Windows Server 2012 comprend plusieurs améliorations importantes en matière de gestion. L'Assistant Validation est amélioré, la vitesse de validation pour de grands clusters de basculement est optimisée et de nouveaux tests pour CSV, le rôle Hyper-V et des ordinateurs virtuels ont été ajoutés. Par ailleurs, de nouveaux applets de commande Windows PowerShell® sont par ailleurs disponibles pour gérer les clusters, les espaces de stockage et les numéros d'unités logiques, surveiller les applications d'ordinateur virtuel en cluster et créer des cibles iSCSI à haut niveau de disponibilité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

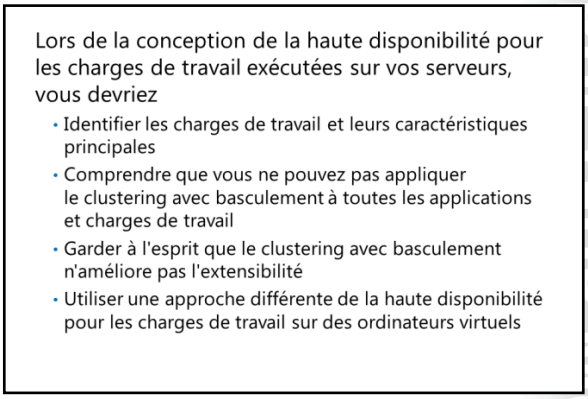
Fonctionnalités supprimées et déconseillées

Dans le clustering Windows Server 2012, certaines des fonctionnalités des versions de clustering avec basculement antérieures sont supprimées ou déconseillées. Si vous effectuez une mise à niveau à partir d'une version antérieure, vous devez être conscient des changements, notamment :

- L'outil de ligne de commande Cluster.exe est déconseillé. Cependant, vous pouvez éventuellement l'installer avec les outils de clustering avec basculement, tels que les applets de commande Windows PowerShell, qui fournissent une fonctionnalité généralement identique aux commandes **cluster.exe**.
- L'interface Component Object Model (COM) du Serveur Automation de cluster de basculement (MSClus) est déconseillée, mais vous pouvez éventuellement l'installer avec les outils de clustering avec basculement.
- La prise en charge des DLL de ressource de cluster 32 bits est déconseillée, mais des DLL 32 bits peuvent éventuellement être installées. Cependant, vous devez mettre à jour vos DLL de ressource de cluster sur 64 bits.
- L'Assistant Haute disponibilité ne contient plus le rôle Serveur d'impression et vous ne pouvez pas le configurer dans le Gestionnaire du cluster de basculement.
- L'applet de commande **Add-ClusterPrintServerRole** est déconseillée et elle n'est pas prise en charge dans Windows Server 2012.

Éléments à prendre en compte pour les charges de travail de serveurs sur les clusters de basculement

Avant d'implémenter le clustering avec basculement, vous devez identifier les services et applications que vous souhaitez rendre à haut niveau de disponibilité. En d'autres termes, vous devez identifier les charges de travail et leurs caractéristiques principales avant de décider si vous devez implémenter une solution hautement disponible. Vous ne pouvez pas appliquer le clustering avec basculement à toutes les applications. De plus, les applications disposent parfois de leurs propres mécanismes de redondance, lesquels ne sont pas compatibles avec la technologie hautement disponible que vous souhaitez implémenter.



En outre, vous devez garder à l'esprit que le clustering avec basculement n'améliore par l'extensibilité par l'ajout de nœuds. Une extensibilité accrue est obtenue par une extension verticale et au moyen de matériel puissant pour les différents nœuds. Par conséquent, vous devez utiliser le clustering avec basculement si votre objectif est la haute disponibilité, et non pas l'extensibilité. Dans Windows Server 2012, il y a une exception à ceci : si vous implémentez des services de fichiers avec montée en puissance parallèle sur des volumes partagés de cluster, vous pouvez également atteindre un niveau d'extensibilité, tout en bénéficiant toujours de la haute disponibilité.

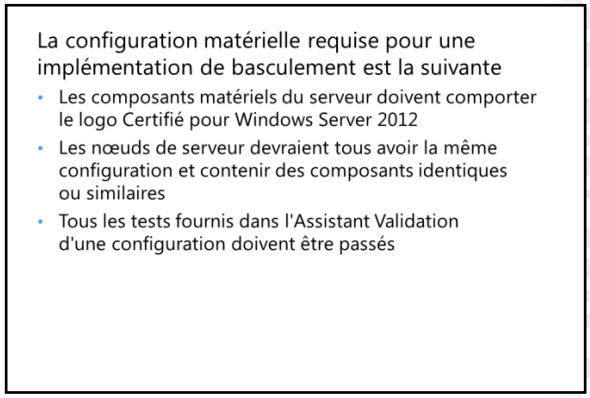
Il est très important que vous analysiez les charges de travail qui s'exécutent sur vos serveurs, avant de les rendre hautement disponibles. Cela est d'autant plus important si les charges de travail s'exécutent sur les ordinateurs virtuels. Dans ce cas, vous devez déterminer si vous allez implémenter la haute disponibilité au niveau d'un ordinateur virtuel ou au niveau du service. Une section ultérieure de ce module fournit plus de détails sur la haute disponibilité pour les charges de travail virtuelles.

Lors de l'analyse et de la planification des charges de travail du serveur pour la haute disponibilité, prenez en compte les éléments suivants :

- Pour chaque charge de travail, déterminez si elle requiert l'évolutivité, la redondance, ou les deux.
- Pour chaque charge de travail, déterminez les ressources matérielles nécessaires pour assurer la redondance.
- Lorsque vous planifiez la redondance, prenez toujours en compte la croissance. Il est recommandé d'utiliser des outils, tels que les planificateurs de charge de travail et de capacité, pour des services spécifiques, notamment Microsoft SQL Server® et Microsoft® SharePoint.
- Répartissez les applications à haut niveau de disponibilité d'un nœud défaillant. Quand tous les nœuds d'un cluster de basculement sont actifs, répartissez les services ou applications à haut niveau de disponibilité d'un nœud défaillant sur tous les nœuds restants. Ceci permet d'empêcher qu'un seul nœud ne soit surchargé.

Sélection des composants matériels pour les nœuds de cluster

Les clusters de basculement doivent répondre à plusieurs critères pour satisfaire aux conditions requises de disponibilité et de support, vous devez donc sélectionner votre matériel de nœud de cluster soigneusement, notamment :



- Vous devez sélectionner du matériel de cluster de basculement qui répond aux exigences du logo « Certifié pour Windows Server 2012 ». Le matériel sur lequel ce logo est apposé a été testé de manière indépendante pour répondre aux normes techniques les plus élevées en matière de fiabilité, de disponibilité, de stabilité, de sécurité et de compatibilité de plateforme. En outre, cela signifie qu'en cas de dysfonctionnements ou autres problèmes, vous avez accès à des options de support officiel.
- Vous devez installer le même matériel ou du matériel similaire sur chaque nœud de cluster de basculement. Par exemple, si vous choisissez un modèle spécifique de carte réseau pour un nœud, vous devez installer cette carte sur tous les nœuds.
- Vous devez vous assurer que si vous utilisez des connexions de stockage SAS (Serial Attached SCSI) ou Fibre Channel, les contrôleurs de périphérique de stockage de masse dédiés au stockage en cluster sont identiques sur tous les serveurs en cluster. Ils doivent également utiliser la même version du microprogramme.
- Vous devez vous assurer que si vous utilisez des connexions de stockage iSCSI, chaque serveur en cluster dispose d'une ou de plusieurs cartes réseau ou adaptateurs de bus hôte dédiés au stockage en cluster. En outre, vous ne pouvez pas utiliser le réseau que vous utilisez pour les connexions de stockage iSCSI pour les communications réseau. Sur tous les serveurs en cluster, les cartes réseau qui vous permettent de vous connecter à la cible de stockage iSCSI doivent être identiques (il est recommandé d'utiliser Gigabit Ethernet ou version supérieure).

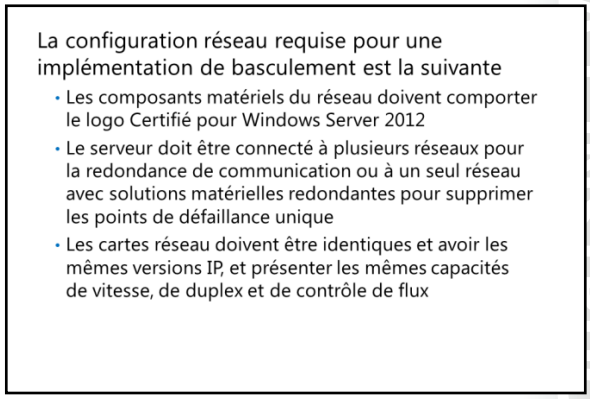
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Assurez-vous qu'après avoir configuré les serveurs avec le matériel, tous les serveurs en cluster passent tous les tests de l'Assistant Validation d'une configuration. Sinon, Microsoft ne prend pas en charge la configuration du cluster.
- Planifiez les composants matériels, en vous assurant que la capacité des nœuds est suffisante pour héberger les charges de travail d'autres nœuds susceptibles de connaître une défaillance.

Vous devez également examiner tous les composants de configuration du cluster pour identifier les points de défaillance uniques. Vous pouvez résoudre de nombreux points de défaillance uniques grâce à des solutions simples, telles que l'ajout de contrôleurs de stockage permettant de séparer des disques et de répartir leurs données, ou l'association de cartes réseau, et l'utilisation de logiciel de gestion multivoie. Ces solutions réduisent le risque que la défaillance d'un périphérique unique n'entraîne un échec dans le cluster. En général, le matériel informatique de classe serveur propose des options de redondance d'alimentation pour des alimentations multiples et pour créer des ensembles RAID (Redondant Array of Independent Disks) pour la redondance de données du disque.

Planification des composants réseau

Les composants réseau de cluster de basculement doivent avoir le logo « Certifié pour Windows Server 2012 » et passer les tests de l'Assistant Validation d'une configuration. De plus :

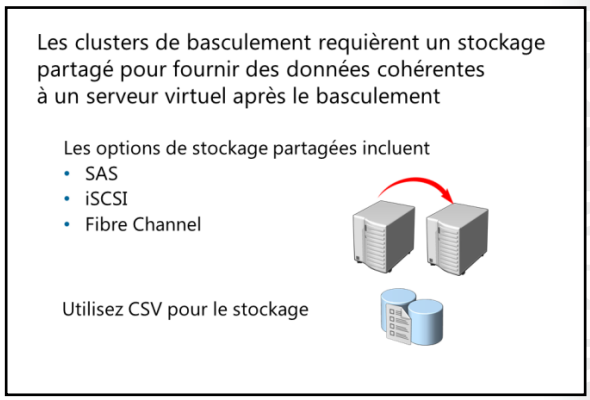


- Les cartes réseau dans chaque nœud doivent être identiques et avoir la même version IP, et présenter les mêmes capacités de vitesse, de duplex et de contrôle de flux.
- Les réseaux et l'équipement réseau auxquels vous connectez les nœuds doivent être redondants. Cela garantit que les nœuds continuent à communiquer même si un point de défaillance unique survient. Vous pouvez utiliser l'association de cartes réseau pour fournir une redondance unique de réseau. Nous vous recommandons d'utiliser plusieurs réseaux afin de fournir plusieurs chemins d'accès entre les nœuds pour la communication entre ces derniers. Dans le cas contraire, Windows génère un message d'avertissement pendant le processus de validation.
- Les cartes réseau dans un réseau de clusters doivent utiliser la même méthode d'attribution d'adresses IP, ce qui signifie qu'elles utilisent toutes des adresses IP statiques ou qu'elles utilisent toutes le protocole DHCP (Dynamic Host Configuration Protocol).

Remarque : Si vous connectez les nœuds de cluster à un réseau unique, celui-ci passera avec succès le test de redondance de l'Assistant Validation d'une configuration. Toutefois, le rapport généré par l'Assistant inclura un avertissement indiquant que le réseau ne doit pas présenter de point unique de défaillance.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification des composants de stockage



La plupart des scénarios de clustering avec basculement requièrent un stockage partagé, qui fournit des données cohérentes à un service ou à une application à haut niveau de disponibilité après le basculement. Un cluster de basculement peut utiliser l'une des trois options de stockage partagé :

- L'interface SAS partagée, qui est l'option la moins coûteuse. Cependant, l'option SAS (Serial Attached SCSI) partagée n'est pas très flexible pour le déploiement car les deux nœuds de cluster doivent être physiquement proches l'un de l'autre. En outre, les dispositifs de stockage partagé qui prennent en charge les interfaces SAS (Serial Attached SCSI) partagées ont un nombre limité de connexions pour les nœuds de cluster.
- iSCSI. iSCSI est un type de réseau de zone de stockage (SAN) qui transmet des commandes SCSI sur des réseaux IP. Les performances sont acceptables dans la plupart des scénarios lorsqu'un réseau Ethernet entre un gigabit par seconde (Gbps) et 10 Gbps est utilisé comme support physique pour la transmission des données. Ce type de réseau SAN est généralement peu coûteux à implémenter car il ne requiert aucun matériel réseau spécialisé. Dans Windows Server 2012, vous pouvez implémenter le logiciel cible iSCSI sur n'importe quel serveur, et présenter le stockage local sur l'interface iSCSI aux clients.
- Fibre Channel. Les réseaux SAN Fibre Channel présentent en général de meilleures performances que les réseaux SAN iSCSI, mais sont plus onéreux. L'implémentation de réseaux SAN Fibre Channel requiert des connaissances et du matériel Fibre Channel spécialisés.

Remarque : Microsoft iSCSI Software Target est désormais une fonctionnalité intégrée dans Windows Server 2012. Elle peut fournir le stockage d'un serveur sur un réseau TCP/IP, y compris le stockage partagé pour des applications hébergées dans un cluster de basculement. En outre, dans Windows Server 2012, vous pouvez configurer un serveur cible iSCSI à haut niveau de disponibilité comme rôle en cluster à l'aide du Gestionnaire du cluster de basculement ou de Windows PowerShell.

Configuration requise pour le stockage

Avant de choisir la solution de stockage, vous devez également être informé de la configuration requise pour le stockage :

- Vous pouvez utiliser la prise en charge native de disque incluse dans le clustering avec basculement à l'aide de disques de base et non de disques dynamiques.
- Vous devez formater les partitions avec le système de fichiers NTFS. Pour le témoin de disque, la partition doit être un système de fichiers NTFS, car Windows Server 2012 ne prend pas en charge le système de fichiers FAT.
- Vous pouvez utiliser le secteur de démarrage principal (MBR, Master Boot Record) ou la table de partition globale de l'identificateur unique universel (GUID, Globally Unique IDentifier) (GPT, GUID Partition Table) comme style de partition du disque.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Le stockage doit se conformer à la norme appelée SPC-3 (SCSI Primary Commands-3), car les améliorations apportées au clustering avec basculement nécessitent que le stockage réponde correctement à des commandes SCSI spécifiques. Plus particulièrement, le stockage doit prendre en charge les réservations persistantes, tel qu'indiqué dans la norme SPC-3.
- Vous devez sélectionner un pilote miniport pour le stockage, compatible avec le pilote de stockage Storport. Storport offre une architecture plus performante et une meilleure compatibilité Fibre Channel dans des systèmes d'exploitation Windows.
- Vous devez isoler les périphériques de stockage (un cluster par périphérique). Vous ne devriez pas permettre aux serveurs qui appartiennent à différents clusters d'accéder aux mêmes périphériques de stockage. Vous pouvez accomplir ceci à l'aide du numéro d'unité logique masquant ou zone. Ceci empêche les numéros d'unités logiques utilisés sur un cluster d'être vus sur un autre cluster. Utilisez un logiciel MPIO (Multipath I/O). Les nœuds de cluster utilisent généralement plusieurs adaptateurs de bus hôte pour accéder au stockage, qui permet de bénéficier d'une haute disponibilité supplémentaire. Néanmoins, pour utiliser plusieurs adaptateurs de bus hôte, vous devez utiliser le logiciel multivoie. Pour Windows Server 2012, vous devez baser votre solution multivoie sur MPIO. Votre fabricant de matériel fournit habituellement un module MPIO spécifique au périphérique (DSM) pour votre matériel, bien que Windows Server 2012 comprenne un ou plusieurs DSM dans le cadre du système d'exploitation.

Volumes partagés de cluster

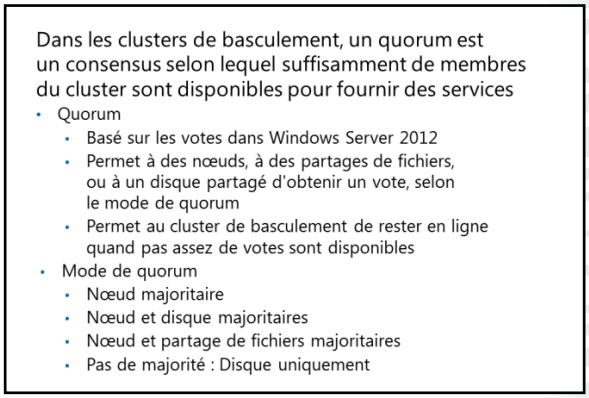
Lorsque vous planifiez le stockage en cluster, vous devez également connaître le concept de volume partagé de cluster (CSV). Dans un déploiement classique de cluster de basculement, un seul nœud contrôle un numéro d'unité logique sur le stockage partagé. Cela signifie qu'un autre nœud ne peut pas voir le stockage partagé, jusqu'à ce qu'il devienne un nœud actif. CSV est une technologie introduite dans Windows Server 2008 R2, qui permet à plusieurs nœuds de partager simultanément un numéro d'unité logique unique. Chaque nœud obtient l'accès exclusif aux fichiers individuels sur le numéro d'unité logique plutôt qu'à l'ensemble du numéro d'unité logique. En d'autres termes, les CSV fournissent une solution distribuée d'accès aux fichiers de sorte que plusieurs nœuds dans le cluster peuvent simultanément accéder au même système de fichiers NTFS.

Dans la première version de Windows Server 2008 R2, le CSV hébergeait uniquement sur les ordinateurs virtuels s'exécutant sur un serveur Hyper-V dans un cluster de basculement. Cette configuration permettait aux administrateurs d'avoir un numéro d'unité logique unique hébergeant plusieurs ordinateurs virtuels dans un cluster de basculement. Plusieurs nœuds de cluster avaient accès au numéro d'unité logique, mais chaque ordinateur virtuel ne pouvait s'exécuter que sur un seul nœud à la fois. Si le nœud sur lequel un ordinateur virtuel s'exécute échouait, le CSV laissait l'ordinateur virtuel redémarrer sur un nœud différent dans le cluster de basculement. En outre, cela simplifiait la gestion des disques pour l'hébergement des ordinateurs virtuels, car chaque ordinateur ne requiert pas de numéro d'unité logique distinct.

Dans Windows Server 2012, le CSV bénéficie d'améliorations supplémentaires. Vous pouvez maintenant utiliser des CSV pour d'autres rôles, et pas seulement Hyper-V. Par exemple, dans un scénario de serveur de fichiers avec montée en puissance parallèle, vous pouvez configurer le rôle de serveur de fichiers dans un cluster de basculement. Le serveur de fichiers avec montée en puissance parallèle fournit des partages de fichiers avec montée en puissance parallèle disponibles en permanence pour le stockage d'applications serveur basées sur des fichiers. Les partages de fichiers avec montée en puissance parallèle vous permettent de partager le même dossier sur plusieurs nœuds du même cluster. Dans ce contexte, les CSV dans Windows Server 2012 introduisent la prise en charge d'un cache de lecture, ce qui peut améliorer les performances dans certains scénarios. En outre, un système de fichier CSV peut exécuter Chkdsk.exe sans affecter les applications possédant des handles ouverts sur le système de fichiers.

Planification du quorum de cluster

Le quorum est le nombre d'éléments en ligne nécessaires pour qu'un cluster continue de s'exécuter. Chaque élément peut voter pour déterminer si le cluster continue de s'exécuter, et chaque nœud de cluster est un élément. En présence d'un nombre pair de nœuds, Windows attribue un élément supplémentaire, ou *témoin*, au cluster. L'élément témoin peut être un disque ou un partage de fichiers. Chaque élément de vote comprend une copie de la configuration du cluster et le service de cluster veille à maintenir toutes les copies synchronisées à tout moment.



Le cluster cessera d'assurer la protection du basculement si la plupart des nœuds échouent, ou s'il y a un problème de communication entre les nœuds de cluster. Sans mécanisme de quorum, chaque ensemble de nœuds peut continuer à fonctionner en tant que cluster de basculement, ce qui peut entraîner une partition du cluster. Le quorum empêche deux ou plusieurs nœuds d'exécuter une ressource du cluster de basculement simultanément. Si les membres de nœud n'atteignent pas une majorité absolue, le vote du témoin devient crucial pour maintenir la validité du cluster. L'opération simultanée peut se produire lorsque des problèmes réseau empêchent un ensemble de nœuds de communiquer avec un autre ensemble de nœuds. Cela peut entraîner des problèmes d'accès aux ressources. Par exemple, une situation peut se produire dans laquelle plusieurs nœuds tentent de contrôler l'accès à une ressource. Par exemple, si cette ressource est une application de base de données, la situation peut provoquer des dommages considérables. Imaginez que deux instances ou plus de la même base de données soient rendues disponibles sur le réseau, ou que plusieurs sources accèdent simultanément à des données et les écrivent sur une cible : les conséquences peuvent être graves. Même si l'application n'est pas endommagée, les données peuvent facilement être corrompues.

Un cluster donné a un ensemble de nœuds et une configuration de quorum spécifique, le cluster peut donc calculer le nombre de votes nécessaires pour qu'il puisse continuer à assurer la protection de basculement. Si le nombre de votes baisse en dessous de la majorité, le cluster cesse de s'exécuter, et n'assure pas la protection de basculement en cas de défaillance de nœud. Les nœuds écouteront la présence d'autres nœuds, au cas où un autre nœud apparaîtrait de nouveau sur le réseau. Cependant, les nœuds ne fonctionneront pas comme un cluster sauf s'ils obtiennent un consensus de majorité ou qu'un quorum est obtenu.

Remarque : Le fonctionnement optimal d'un cluster ne dépend pas seulement du quorum, mais également de la capacité de chaque nœud à prendre en charge les services et les applications qui basculent vers ce nœud. Par exemple, un cluster comprenant cinq nœuds peut encore avoir un quorum après la défaillance de deux nœuds, mais chaque nœud de cluster restant continuera à servir des clients, uniquement si sa capacité est suffisante pour prendre en charge les services et les applications qui ont basculé dessus. Cette capacité inclut la quantité d'espace disque disponible, de puissance de traitement, de bande passante réseau et de mémoire RAM. Une partie importante du processus de conception consiste à planifier la capacité de basculement de chaque nœud. Un nœud de basculement doit pouvoir exécuter sa propre charge et la charge des ressources supplémentaires qui pourraient être basculées vers lui.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Windows Server 2012 prend en charge quatre modes de quorum :

- Nœud majoritaire. Chaque nœud disponible et en communication peut voter. Le cluster s'exécute uniquement avec une majorité des votes, autrement dit plus de la moitié. Ce modèle est préférable quand le cluster comporte un nombre impair de nœuds de serveur et qu'aucun témoin n'est nécessaire pour maintenir ou atteindre le quorum.
- Nœud et disque majoritaires. Chaque nœud, ainsi qu'un disque désigné dans le stockage en cluster et le témoin de disque, peuvent voter chaque fois qu'ils sont disponibles et en communication. Le cluster s'exécute uniquement avec une majorité des votes. Ce modèle suppose qu'un nombre pair de nœuds de serveur peuvent communiquer entre eux et avec le témoin de disque.
- Nœud et partage de fichiers majoritaires. Tous les nœuds et un partage de fichiers désigné créé par l'administrateur, appelé témoin du partage de fichiers, peuvent voter chaque fois qu'ils sont disponibles et en communication. Le cluster s'exécute uniquement avec une majorité des votes, Ce modèle est basé sur un nombre pair de nœuds de serveur pouvant communiquer entre eux et avec le témoin de partage de fichiers.
- Pas de majorité : Disque uniquement. Le cluster a le quorum si un nœud est disponible et en communication avec un disque spécifique du stockage en cluster. Seuls les nœuds également en communication avec ce disque peuvent joindre le cluster.
- À l'exception du mode Pas de majorité -- Disque uniquement, tous les modes de quorum dans les clusters de basculement Windows Server 2012 sont basés sur un modèle simple de vote majoritaire. Tant qu'une majorité des votes est disponible, le cluster continue de fonctionner. Par exemple, si un cluster a cinq votes, il continue de fonctionner tant qu'au moins trois votes sont disponibles. La source des votes n'est pas pertinente. Le vote peut être un nœud, un témoin de disque ou un témoin de partage de fichiers. Le cluster cessera de fonctionner si une majorité des votes est indisponible.
- Dans le mode Pas de majorité -- Disque uniquement, le disque quorum partagé peut opposer son véto sur tous les autres votes possibles. Dans ce mode, le cluster continuera de fonctionner tant que le disque quorum partagé et au moins un nœud sont disponibles. Ce type de quorum empêche également que plus d'un nœud n'assume le rôle principal.

 **Remarque :** Si le disque quorum partagé n'est pas disponible, le cluster cessera de fonctionner, même si tous les nœuds sont encore disponibles. Dans ce mode, le disque quorum partagé est un point de défaillance unique, c'est pourquoi ce mode n'est pas recommandé.

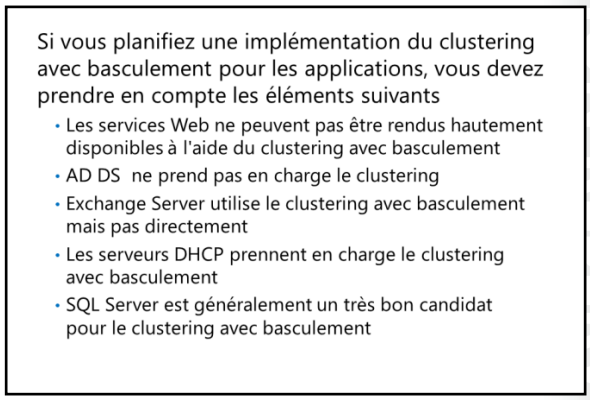
Lorsque vous configurez un cluster de basculement dans Windows Server 2012, l'Assistant Installation sélectionne automatiquement une des deux configurations par défaut. Par défaut, le clustering avec basculement sélectionne :

- Nœud majoritaire, s'il y a un numéro impair de nœuds dans le cluster.
- Nœud et disque majoritaires, s'il y a un numéro pair de nœuds dans le cluster.

Modifiez ce paramètre uniquement si vous estimez que la modification est appropriée pour votre cluster et assurez-vous de bien comprendre les implications de cette modification. Outre la planification du mode de quorum, vous devez également prendre en compte la capacité des nœuds dans votre cluster, et leur capacité à prendre en charge les services et applications qui peuvent basculer vers ce nœud. Par exemple, un cluster comprenant quatre nœuds et un témoin de disque aura toujours le quorum après la défaillance de deux nœuds. Cependant, si vous déployez plusieurs applications ou services sur le cluster, il est possible que chaque nœud de cluster restant n'ait pas la capacité requise pas assurer les services.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour les applications



Le clustering avec basculement ne peut pas protéger toutes les applications, il est donc très important d'analyser les applications et services qui doivent être hautement disponibles avant d'implémenter une technologie à haut niveau de disponibilité. Vous pouvez rendre certaines applications ou services hautement disponibles simplement en déployant plusieurs serveurs hébergeant cette application, sans devoir implémenter une technologie hautement disponible spécifique. D'autre part, certaines applications ne peuvent pas bénéficier d'un cluster de basculement, car elles n'utilisent aucune donnée partagée.

Si vous planifiez une implémentation du clustering avec basculement pour les applications, vous devez prendre en compte les éléments suivants :

- Si vous souhaitez rendre des services Web hautement disponibles, vous devez utiliser l'équilibrage de la charge réseau (NLB) plutôt que le clustering avec basculement.
- Si vous souhaitez rendre AD DS hautement disponible, vous ne devez pas inclure de contrôleurs de domaine dans le cluster. Vous ne pouvez pas déployer plusieurs contrôleurs de domaine AD DS. Un scénario similaire s'applique aux serveurs DNS.
- Si vous souhaitez implémenter Exchange Server avec un haut niveau de disponibilité, vous ne devez pas configurer la haute disponibilité à l'aide des outils Windows. Exchange Server 2010 et les versions plus récentes disposent de leurs propres mécanismes de haute disponibilité, qui utilisent le clustering avec basculement et l'équilibrage de la charge réseau.
- Si vous souhaitez rendre les serveurs DHCP hautement disponibles, vous pouvez implémenter un cluster DHCP, ou vous pouvez implémenter le basculement DHCP. Cette technologie est propre à Windows Server 2012.
- Microsoft SQL Server est généralement un très bon candidat pour le clustering avec basculement.

Lors de la planification de la haute disponibilité des applications, nous vous recommandons d'analyser toutes les possibilités et solutions alternatives avant d'implémenter une quelconque technologie de haute disponibilité. Dans certains cas, les applications sont dotées de leur propre technologie de haute disponibilité ; en général, il s'agit de la meilleure solution.

Le clustering avec basculement est plus adapté aux applications avec état qui sont limitées à un ensemble unique de données. Une base de données est un exemple d'une telle application. Les données sont enregistrées dans un emplacement unique et peuvent être utilisées uniquement par une instance de base de données. Vous pouvez également utiliser le clustering avec basculement pour des ordinateurs virtuels Hyper-V. Les meilleurs résultats pour le clustering avec basculement sont obtenus lorsque le client peut se reconnecter à l'application automatiquement après le basculement. Si le client ne se reconnecte pas automatiquement, alors l'utilisateur doit redémarrer l'application cliente.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Implémentation du clustering avec basculement

Nous recommandons certaines configurations matérielles et logicielles spécifiques pour les clusters de basculement Windows Server 2012, qui permettent à Microsoft de prendre en charge le cluster. Les clusters de basculement fournissent un niveau de service supérieur aux serveurs autonomes. Par conséquent, les configurations matérielles de cluster sont généralement plus strictes que les configurations requises pour les serveurs autonomes.

Dans cette leçon, vous allez apprendre comment vous préparer à l'implémentation d'un cluster et discuter des configurations requises en matière de matériel, de réseau, de stockage, d'infrastructure et de logiciels, pour des clusters de basculement Windows Server 2012. Enfin, cette leçon présente les étapes d'utilisation de l'Assistant Validation d'une configuration afin de garantir une configuration correcte du cluster, ainsi que la procédure de migration des clusters de basculement.

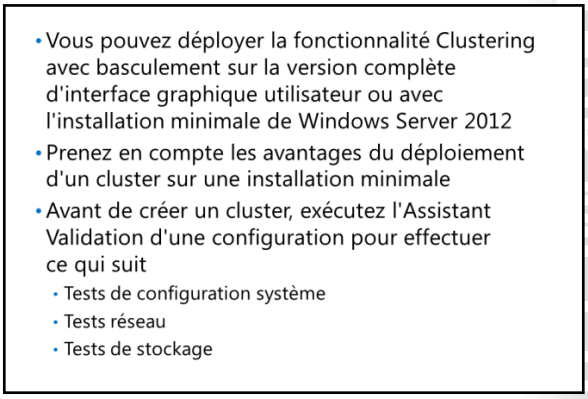
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Déployer un cluster de basculement.
- Déployer des rôles serveur sur un cluster de basculement.
- Configurer les paramètres de cluster de basculement.
- Configurer les paramètres d'applications et de ressources.
- Décrire un serveur de fichiers avec montée en puissance dans Windows Server 2012.
- Configurer un serveur de fichiers avec montée en puissance parallèle.

Déploiement et validation d'un cluster de basculement

Pour utiliser le clustering avec basculement, vous devez tout d'abord installer cette fonctionnalité sur tous les nœuds que vous utiliserez dans un cluster. Vous pouvez installer facilement la fonctionnalité Clustering avec basculement sur l'installation complète de Windows Server 2012 à l'aide de l'Assistant Ajout de rôles et de fonctionnalités du Gestionnaire de serveur, ou sur une installation minimale à l'aide de l'interface Windows PowerShell.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Une installation minimale installe uniquement les éléments essentiels, ainsi, un cluster de basculement sur une installation minimale de serveur offre plusieurs avantages clés, y compris l'installation minimale :

- Surface de vulnérabilité réduite ouverte aux attaques et nombre réduit de mises à jour requises à installer.
- Moins de composants à gérer et moins d'espace disque requis pour l'installation.
- Réduction de la surcharge des ressources, ce qui permet aux instances en cluster de disposer de plus de ressources.

Vous pouvez utiliser l'Assistant Création d'un cluster dans la console Gestionnaire du cluster de basculement pour créer un cluster. Cependant, avant de réellement créer un cluster, il est fortement recommandé de vérifier la configuration logicielle et matérielle actuelle des nœuds de cluster. Vous pouvez valider votre configuration à l'aide de l'Assistant Validation d'un cluster dans la console Gestionnaire du cluster de basculement.

L'Assistant Validation d'une configuration exécute des tests visant à déterminer si le matériel et les paramètres logiciels sont compatibles avec le clustering avec basculement. À l'aide de l'Assistant, vous pouvez exécuter l'ensemble ou une partie seulement des tests de configuration. Il est recommandé d'exécuter les tests sur des serveurs et périphériques de stockage avant de configurer un cluster de basculement, puis de les réexécuter après que des modifications importantes ont été apportées sur le cluster. Vous pouvez accéder aux résultats des tests après l'exécution de l'Assistant, ou en accédant au fichier de rapport dans le répertoire %windir%\cluster\Reports.

Les tests de l'Assistant incluent des simulations spécifiques d'actions au niveau du cluster, qui se classent en plusieurs catégories :

- Tests de configuration système**.** Ces tests déterminent si les serveurs sélectionnés répondent à des exigences spécifiques. Par exemple, vous pouvez vérifier que vous vous conformez à la condition requise selon laquelle vos serveurs exécutent la même version du système d'exploitation et les mêmes mises à jour logicielles.
- Tests réseau. Ces tests déterminent si les réseaux de clusters planifiés répondent à des exigences spécifiques. Par exemple, vous pouvez tester si vous respectez les exigences de redondance de réseau.
- Tests de stockage. Ces tests déterminent si votre stockage répond à la configuration requise. Par exemple, vous pouvez tester si votre stockage prend en charge les commandes SCSI nécessaires et s'il traite convenablement les actions de cluster simulées.

Le rapport de l'Assistant Validation d'une configuration enregistre l'un des éléments suivants pour chacun des éléments testés. C'est-à-dire :

- Respecte la configuration requise pour un cluster de basculement.
- Peut répondre à la configuration requise, mais une mise en garde s'affiche qui suggère que vous examiniez les paramètres matériels et logiciels pour vérifier que les meilleures pratiques sont respectées.
- Ne respecte pas la configuration suivante.

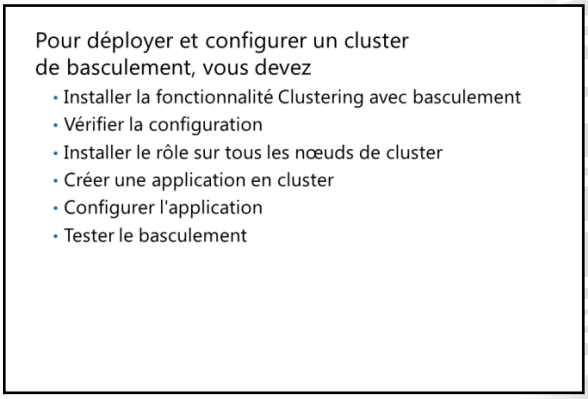
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

En outre, le rapport peut indiquer que le test n'a pas pu être exécuté. Par exemple, vous pouvez recevoir ce résultat si vous testez un seul nœud, car certains tests ne sont pas exécutés.

Le rapport de l'Assistant Validation d'une configuration contient des détails sur les tests qui ont été exécutés et les résultats. Le rapport fournit également des informations sur les motifs des éventuelles défaillances. Si vous ne pouvez pas résoudre les problèmes après avoir lu le rapport, contactez le fournisseur pour obtenir de l'aide pour la configuration ou pour connaître les modifications de compatibilité des versions logicielles. Dans certains cas, un fournisseur peut recommander un pilote ou une version de microprogramme spécifique qui est connu comme étant stable dans un environnement en cluster.

Déploiement des rôles serveur sur un cluster de basculement

Le clustering avec basculement prend en charge le clustering de plusieurs rôles Windows Server, notamment Services de fichiers, DHCP et Hyper-V. Pour implémenter le clustering pour un rôle de serveur ou pour des applications externes telles que Microsoft SQL Server ou Exchange Server, exécutez la procédure suivante :

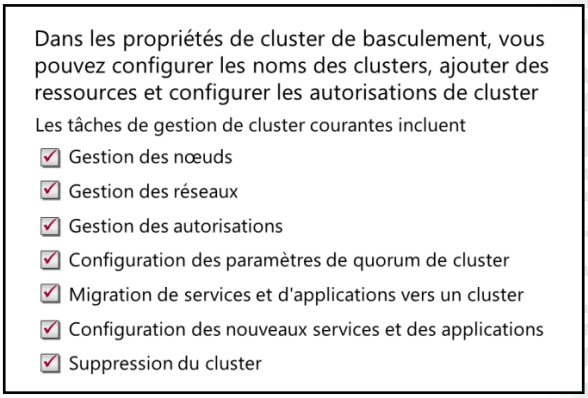


1. Installez la fonctionnalité Clustering avec basculement. Utilisez le Gestionnaire de serveur, le fichier dism.exe ou Windows PowerShell pour installer la fonctionnalité Clustering avec basculement sur tous les ordinateurs qui seront des membres du cluster. Dans Windows Server 2012, vous pouvez installer des rôles et des fonctionnalités sur plusieurs serveurs simultanément à partir d'une seule console de Gestionnaire de serveur.
2. Vérifiez la configuration et créez un cluster. Avec les nœuds appropriés, utilisez le composant logiciel enfichable Gestionnaire du cluster de basculement pour valider une configuration, puis créez un cluster avec les nœuds sélectionnés.
3. Installez le rôle sur tous les nœuds de cluster. Utilisez le Gestionnaire de serveurs, le fichier dism.exe ou Windows PowerShell pour installer le rôle de serveur que vous souhaitez utiliser dans le cluster.
4. Créez une application en cluster à l'aide du composant logiciel enfichable Gestionnaire du cluster de basculement.
5. Configurez l'application en configurant des options sur l'application utilisées dans le cluster.
6. Testez le basculement à l'aide du composant logiciel enfichable Gestion du cluster de basculement pour déplacer le service intentionnellement d'un nœud vers un autre.

Une fois le cluster créé, vous pouvez surveiller son état à l'aide de la console Gestion du cluster de basculement pour gérer les options disponibles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des paramètres d'un cluster avec basculement



Une fois que vous créez un cluster, il offre de nombreuses propriétés que vous pouvez configurer.

Lorsque vous ouvrez Propriétés du cluster, vous pouvez configurer ou modifier un nom de cluster, vous pouvez ajouter divers types de ressources telles qu'une adresse IP et un nom de réseau au cluster, et vous pouvez également configurer des autorisations de cluster. En configurant les autorisations du cluster, vous déterminez qui a le contrôle total sur ce contrôle spécifique et qui peut juste lire la configuration du cluster. En outre, vous pouvez effectuer des tâches de gestion standard sur chaque cluster périodiquement, ou à la demande. Ces tâches incluent l'ajout et la suppression de nœuds de cluster, la modification des paramètres de quorum, et peuvent également inclure :

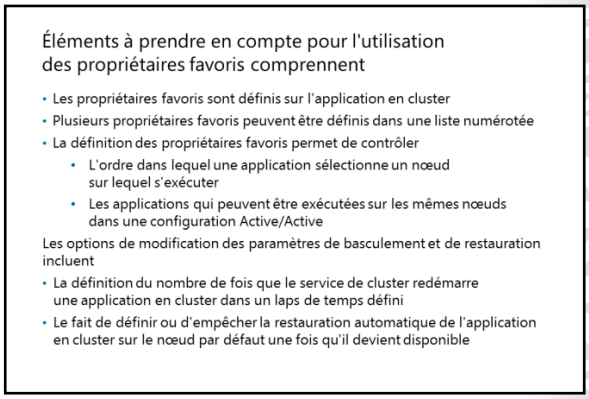
- La gestion des nœuds de cluster. Pour chaque nœud d'un cluster, vous pouvez arrêter temporairement le service de cluster, le suspendre, initialiser le bureau à distance sur le nœud ou exclure un nœud du cluster.
- La gestion des réseaux de cluster. Vous pouvez ajouter ou supprimer des réseaux de cluster, et configurer des réseaux que vous souhaitez dédier à la communication entre les clusters.
- La gestion des autorisations**.** En gérant les autorisations, vous pouvez déléguer les droits d'administration d'un cluster.
- La configuration des paramètres de quorum de cluster. En configurant des paramètres de quorum, vous déterminez comment le quorum est atteint et qui peut voter dans un cluster.
- La migration de services et d'applications vers un cluster. Vous pouvez implémenter des services existants sur le cluster et les rendre à haut niveau de disponibilité.
- La configuration de nouveaux services et applications en vue de les utiliser dans un cluster. Vous pouvez implémenter de nouveaux services dans le cluster.
- La suppression d'un cluster. Vous pouvez supprimer un cluster si vous décidez de cesser d'utiliser le clustering, ou si vous souhaitez déplacer le cluster vers un autre ensemble de nœuds.

Vous pouvez effectuer la plupart de ces tâches d'administration à l'aide de la console Gestion du cluster de basculement, ou à l'aide de Windows PowerShell. Cependant, Windows Server 2012 ne prend plus en charge Cluster.exe, qui servait pour certaines de ces tâches dans les versions précédentes du système d'exploitation Windows Server et ne fait pas partie de l'installation par défaut. Windows PowerShell 2012 introduit les applets de commande Windows PowerShell pour la gestion du cluster.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des paramètres d'applications et de ressources

Vous pouvez régler les paramètres de basculement, y compris les propriétaires favoris et les paramètres de restauration automatique, afin de contrôler la manière dont le cluster répond en cas d'échec de l'application ou du service. Vous pouvez également configurer ces paramètres dans la feuille de propriétés du service ou de l'application en cluster (dans l'onglet **Général** ou dans l'onglet **Basculement**). Le tableau suivant fournit des exemples illustrant le fonctionnement de ces paramètres.

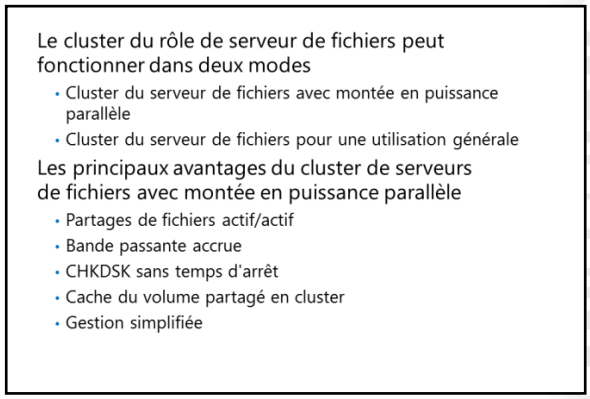


Paramètre	Résultat
Exemple 1 : Onglet **Général**, **Propriétaire favori** : **Node1** Onglet **Basculement**, paramètre **Restauration automatique** : **Autoriser la restauration automatique (Immédiatement)**	Si le service ou l'application bascule du Node1 vers le Node2, dès que le Node1 est à nouveau disponible, le service ou l'application rebascule vers le Node1.
Exemple 2 : Onglet **Basculement**, **Nombre maximal d'échecs dans la période spécifiée** : **2** Onglet **Basculement**, **Période (heures)** : **6**	Dans une période de six heures, si l'application ou le service n'échoue pas plus de deux fois, elle ou il sera redémarré ou basculé chaque fois. Si l'application ou le service échoue une troisième fois durant cette période de six heures, elle ou il sera laissé dans un état défaillant. La valeur par défaut pour le nombre maximal de défaillances est n-1, où *n* correspond au nombre de nœuds. Si vous choisissez de modifier la valeur, il est recommandé d'utiliser une valeur relativement basse. En effet, si plusieurs nœuds échouent, l'application ou le service n'est pas déplacé indéfiniment entre les nœuds.

Vous n'êtes pas obligé de configurer ces paramètres si vos nœuds de cluster sont identiques et que vous n'avez pas de préférence concernant le nœud qui hébergera principalement les services en cluster. Cependant, si vous préférez qu'un nœud soit actif la plupart du temps, et qu'un ou plusieurs autres nœuds servent d'hôtes de remplacement, vous devez configurer les paramètres de basculement et de restauration automatique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Utilisation d'un serveur de fichiers avec montée en puissance parallèle dans Windows Server 2012



Contrairement aux autres rôles dont le comportement dans le cluster est en grande partie le même que dans les versions précédentes de Windows Server, certaines modifications importantes ont été apportées au cluster du rôle Serveur de fichiers dans Windows Server 2012.

Dans Windows Server 2008 R2 et les versions antérieures, vous pouvez déployer le rôle Serveur de fichiers dans le cluster de sorte à rendre les partages de dossiers hautement disponibles. Tous les partages hautement disponibles sont accessibles sur un nœud de cluster à la fois, et si ce nœud connaît une défaillance, un autre nœud en prend la propriété et commence à héberger le partage de dossiers. En outre, nous déconseillons de stocker les fichiers tels que les ordinateurs virtuels ou les bases de données sur des serveurs de fichiers dans le cluster.

Dans Windows Server 2012, vous pouvez déployer le rôle Serveur de fichiers en cluster dans deux modes :

- Serveur de fichiers avec montée en puissance parallèle pour les données des applications (serveurs de fichiers avec montée en puissance parallèle). Windows Server 2012 introduit le mode Serveur de fichiers en cluster et permet de stocker des données d'applications serveur, telles que les fichiers d'ordinateur virtuel Hyper-V sur les partages de fichiers. De plus, il fournit un niveau similaire de fiabilité, de disponibilité, de facilité de gestion et de hautes performances que vous pouvez attendre d'un réseau SAN. Ces avantages sont dus au fait que les partages de fichiers sont en ligne sur tous les nœuds simultanément, ce qui fournit l'évolutivité généralement absente des scénarios de cluster de basculement. C'est ce que nous appelons parfois un cluster actif/actif.
- Serveur de fichiers pour une utilisation générale. Il s'agit du même clustering de serveur de fichiers que celui des versions précédentes de Windows Server. Tous les partages associés au serveur de fichiers en cluster sont en ligne sur un nœud à la fois, comme un *cluster actif/passif*. Les partages de fichiers associés à ce type de serveur de fichiers en cluster sont les *partages de fichiers en cluster*.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La modification d'extensibilité la plus importante est le serveur de fichiers avec montée en puissance parallèle, par rapport aux serveurs de fichiers en cluster dans les versions précédentes de Windows. La plupart des autres rôles de serveur en cluster s'exécutent sur un nœud de cluster à la fois. Le serveur de fichiers avec montée en puissance parallèle est une exception. Il permet de fournir une réponse rapide à l'augmentation des demandes sur vos serveurs de fichiers en ajoutant des serveurs au cluster sans interruption de service. Pour ce faire, vous pouvez tirer profit des nouvelles fonctionnalités Clustering avec basculement Windows Server et des nouvelles fonctions dans la nouvelle version du protocole de serveurs de fichiers de Windows, SMB 3.0. Chaque fois que vous ajoutez un nœud à un cluster de serveurs de fichiers avec montée en puissance parallèle, vous augmentez la bande passante totale disponible permettant d'accéder aux partages. Vous pouvez à présent effectuer des réparations de système de fichiers plus facilement, et Chkdsk.exe fonctionne sans interruption de service. Un système de fichier CSV peut exécuter Chkdsk.exe sans affecter les applications possédant des handles ouverts sur le système de fichiers. Les CSV dans Windows Server 2012 prennent également en charge la mise en cache de lecture, ce qui améliore également les performances, plus particulièrement dans des scénarios spécifiques tels que l'infrastructure de bureau virtuel (VDI). En fin de compte, la gestion du cluster de serveurs de fichiers est beaucoup plus simple, car vous n'avez pas besoin de créer plusieurs serveurs de fichiers en cluster, avec des disques de cluster distincts, puis de développer les stratégies de placement pour garantir l'activité sur chaque nœud de cluster.

Démonstration : Configuration du serveur de fichiers avec montée en puissance parallèle

Procédure de démonstration

1. Sur LON-SVR1, vérifiez que **Service de rôle Serveur de fichiers** est installé, puis installez la fonctionnalité **Clustering avec basculement** à l'aide du Gestionnaire de serveur.
2. Sur LON-SVR2, vérifiez que **Service de rôle Serveur de fichiers** est installé, puis installez la fonctionnalité **Clustering avec basculement** à l'aide du Gestionnaire de serveur.
3. Sur LON-SVR1, démarrez l'**initiateur iSCSI**.
4. Utilisez l'adresse **172.16.0.10** pour découvrir la **cible iSCSI** et vous y connecter.
5. Sur LON-SVR2, démarrez l'**initiateur iSCSI**.
6. Utilisez l'adresse **172.16.0.10** pour découvrir la **cible iSCSI** et vous y connecter.
7. Sur LON-SVR2, ouvrez la **Gestion des disques**, puis initialisez et mettez en ligne **Disque 2 et Disque 3**. Formatez ces lecteurs.
8. Sur LON-SVR1, ouvrez la **Gestion des disques**, puis mettez en ligne **Disque 3 et Disque 4**.
9. Ouvrez la console Gestionnaire du cluster de basculement sur LON-SVR1.
10. Créez un cluster avec les nœuds LON-SVR1 et LON-SVR2. N'exécutez pas la validation à ce stade.
11. Indiquez **FSCluster** comme valeur pour le **Point d'accès pour l'administration du cluster**.
12. **Spécifiez 172.16.0.127** comme Adresse IP pour le cluster.
13. Ajoutez **Disque du cluster 1** et **Disque du cluster 2** au **Stockage du cluster**, puis attribuez **Disque du cluster 1** sur un **CSV**.
14. Configurez **Paramètres de quorum** sur **Par défaut** (paramètres recommandés), puis lancez un Assistant pour configurer le rôle en cluster.

15. Ajoutez un nouveau rôle de cluster, sélectionnez **Serveur de fichiers**, puis choisissez de **configurer un serveur de fichiers avec montée en puissance parallèle pour les données d'application**.
16. Indiquez **AdatumFS** comme **Point d'accès client**, puis ajoutez un partage de fichiers au rôle de cluster ADatumFS existant.
17. Dans l'Assistant Nouveau partage, sélectionnez **Partage SMB - Applications**, puis cliquez sur **Sélectionner par le volume**.
18. Attribuez le nom **TestShare** au partage.

 **Remarque :** si vous prévoyez de faire l'atelier pratique, vous devez rétablir les ordinateurs virtuels utilisés dans cette démonstration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Intégration du clustering avec basculement avec la virtualisation de serveur

L'implémentation d'ordinateurs virtuels à haut niveau de disponibilité est quelque peu différente de l'implémentation d'autres rôles dans un cluster de basculement. Le clustering avec basculement dans Windows Server 2012 fournit de nombreuses fonctionnalités pour le clustering Hyper-V et plusieurs outils pour gérer des ordinateurs virtuels hautement disponibles. Dans cette leçon, vous apprendrez à intégrer le clustering avec basculement sur la plateforme de virtualisation du serveur Hyper-V.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les options permettant de rendre les charges de travail d'ordinateurs virtuels hautement disponibles.
- Décrire le fonctionnement d'un cluster de basculement avec Hyper-V.
- Décrire la configuration d'infrastructure requise pour l'implémentation du clustering avec basculement pour Hyper-V.
- Décrire comment implémenter la migration du stockage.
- Décrire comment implémenter la migration dynamique.
- Décrire comment implémenter la fonction Réplica Hyper-V.
- Décrire les éléments à prendre en compte pour l'implémentation de la disponibilité des ordinateurs virtuels.

Options permettant de rendre les charges de travail d'ordinateurs virtuels hautement disponibles

Pour la plupart des organisations, certaines applications sont cruciales et doivent être à haut niveau de disponibilité. Pour rendre une application à haut niveau de disponibilité, vous devez la déployer dans un environnement fournissant une redondance pour tous les composants requis par l'application. Pour que les ordinateurs virtuels soient à haut niveau de disponibilité, vous avez le choix entre plusieurs options :

Options de haute disponibilité	Description
Clustering d'hôtes	• Rend des ordinateurs virtuels hautement disponibles • Ne requiert pas de système d'exploitation ni d'application de l'ordinateur virtuel pour prendre en charge les clusters
Clustering d'invités	• Fait basculer les ordinateurs virtuels vers les nœuds de cluster • Les applications d'ordinateurs virtuels doivent prendre en charge les clusters • Requiert une interface iSCSI ou Fibre Channel virtuel pour les connexions au stockage partagé
NLB	• Transforme les ordinateurs virtuels en nœuds de cluster d'équilibrage de la charge réseau • Utilisé pour les applications Web

- Clustering d'hôtes avec lequel vous implémentez des hôtes de virtualisation en tant que rôle en cluster.
- Clustering d'invité avec lequel vous implémentez le clustering à l'intérieur des ordinateurs virtuels.
- Équilibrage de la charge réseau, que vous implémentez dans les ordinateurs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Clustering d'hôtes

Le clustering d'hôtes vous permet de configurer un cluster de basculement en utilisant des serveurs hôtes Hyper-V. Lorsque vous configurez le clustering hôte pour Hyper-V, vous configurez l'ordinateur virtuel comme ressource hautement disponible, intégrant la protection de basculement au niveau du serveur hôte. Autrement dit, le système d'exploitation invité et les applications exécutées sur l'ordinateur virtuel ne doivent pas être configurés pour prendre en charge les clusters. Cependant, l'ordinateur virtuel conserve son haut niveau de disponibilité. Voici quelques exemples d'applications ne prenant pas en charge les clusters : les serveurs d'impression ou les applications en réseau propriétaires, telles qu'une application de comptabilité. Si le nœud hôte qui contrôle l'ordinateur virtuel devient indisponible de façon inattendue, le nœud hôte secondaire prend le contrôle et redémarre l'ordinateur virtuel aussi rapidement que possible. Vous pouvez également déplacer, de manière contrôlée, l'ordinateur virtuel d'un nœud du cluster à un autre. Par exemple, vous pourriez déplacer l'ordinateur virtuel d'un nœud à l'autre tout en corrigeant le système d'exploitation d'hôtes. Les applications ou services exécutés sur l'ordinateur virtuel n'ont pas besoin d'être compatibles avec le clustering avec basculement, ni de savoir que l'ordinateur virtuel est mis en cluster. Le basculement se situe au niveau de l'ordinateur virtuel, par conséquent, cela ne dépend pas du logiciel que vous installez sur l'ordinateur virtuel.

Clustering d'invités

Vous configurez le clustering d'invités avec basculement de manière très similaire au clustering avec basculement sur un serveur physique, à l'exception près que les nœuds de cluster comprennent plusieurs ordinateurs virtuels. Dans ce scénario, vous créez au moins deux ordinateurs virtuels, puis activez le clustering avec basculement dans le système d'exploitation invité. Ensuite, vous activez l'application ou le service pour une haute disponibilité entre les ordinateurs virtuels à l'aide du clustering avec basculement dans chaque ordinateur virtuel. Vous implémentez le clustering avec basculement dans chaque système d'exploitation invité du nœud d'ordinateur virtuel, afin de pouvoir localiser les ordinateurs virtuels sur un hôte unique. Ceci peut être une configuration rapide et rentable dans un environnement de test ou de transfert.

Pour des environnements de production, toutefois, vous pouvez protéger l'application ou le service de manière plus approfondie si vous déployez les ordinateurs virtuels sur des ordinateurs hôtes distincts Hyper-V sur lesquels vous configurez le clustering avec basculement. Lorsque vous implémentez le clustering avec basculement à la fois au niveau de l'hôte et au niveau de l'ordinateur virtuel, la ressource peut être redémarrée, peu importe si le nœud qui échoue est un ordinateur virtuel ou un hôte. Cette configuration, ou *Cluster invité entre hôtes*, est considérée comme une configuration à haut niveau de disponibilité pour les ordinateurs virtuels exécutant des applications critiques dans un environnement de production.

Plusieurs facteurs doivent être pris en compte lors de l'implémentation du clustering invité :

- L'application ou le service doit prendre en charge le cluster de basculement, y compris les services Windows Server 2012 prenant en charge les clusters et les applications telles SQL Server et Microsoft Exchange Server en cluster.
- Les ordinateurs virtuels Hyper-V peuvent utiliser les connexions Fibre Channel pour partager le stockage, uniquement spécifique à Microsoft Hyper-V Server 2012. Vous pouvez également implémenter des connexions iSCSI des ordinateurs virtuels au stockage partagé.

Vous devez déployer plusieurs cartes réseau sur les ordinateurs hôtes et les ordinateurs virtuels. Dans l'idéal, lorsque vous utilisez une connexion iSCSI, vous devez consacrer une connexion réseau à la connexion iSCSI, au réseau privé entre les hôtes et à la connexion réseau utilisée par les ordinateurs clients.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Équilibrage de la charge réseau

L'équilibrage de la charge réseau fonctionne avec les ordinateurs virtuels de la même manière qu'il fonctionne avec les hôtes physiques. L'équilibrage de la charge réseau distribue le trafic IP à plusieurs instances d'un service TCP/IP, telles qu'un serveur Web en cours d'exécution sur un hôte au sein du cluster d'équilibrage de charge réseau. L'équilibrage de la charge réseau distribue de manière transparente les demandes des clients parmi les hôtes et permet aux clients d'accéder au cluster à l'aide d'un nom d'hôte virtuel ou d'adresses IP virtuelles. Du point de vue de l'ordinateur client, le cluster semble être un seul serveur répondant à ses demandes. À mesure que le trafic de l'entreprise augmente, vous pouvez ajouter un autre serveur au cluster.

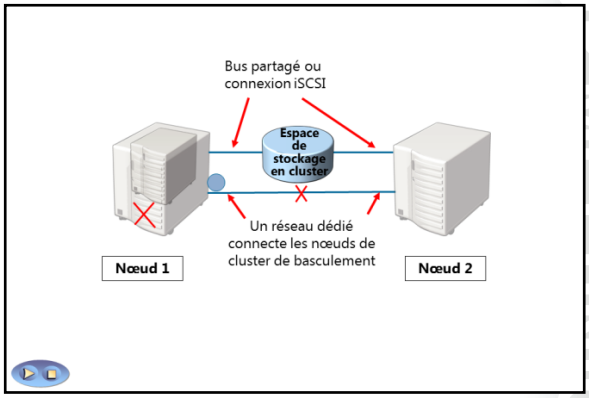
Par conséquent, l'équilibrage de la charge réseau est une solution appropriée pour les ressources qui ne doivent pas prendre en charge les demandes de lecture/écriture exclusive. Des exemples d'applications appropriées à l'équilibrage de la charge réseau s'étendent des applications Web frontales aux applications de base de données ou les serveurs d'accès au client Exchange Server.

Lorsque vous configurez un cluster d'équilibrage de la charge réseau, vous devez installer et configurer l'application sur tous les ordinateurs virtuels. Après la configuration de l'application, installez la fonctionnalité d'équilibrage de la charge réseau dans Windows Server 2012 dans chaque système d'exploitation invité de l'ordinateur virtuel (pas sur les hôtes Hyper-V). Vous devez alors configurer un cluster NLB pour l'application. Les versions antérieures de Windows Server prennent également en charge l'équilibrage de la charge réseau, ce qui signifie que le système d'exploitation invité n'est pas limité à Windows Server 2012. Comme pour un cluster invité entre hôtes, la ressource d'équilibrage de la charge tire généralement parti de l'amélioration accrue des performances d'E/S lorsque les nœuds d'ordinateur virtuel sont situés sur différents hôtes Hyper-V.

Remarque : Comme avec les versions antérieures de Windows Server, l'équilibrage de la charge réseau et le clustering avec basculement ne doivent pas être implémentés dans le même système d'exploitation invité, car les deux technologies entrent en conflit. Les deux technologies entrent en conflit.

Comment fonctionne un cluster de basculement avec Hyper-V ?

Lorsque vous implémentez le clustering avec basculement et que vous configurez les ordinateurs virtuels comme des ressources à haut niveau de disponibilité, le cluster de basculement traite les ordinateurs virtuels comme tout autre service ou toute autre application. Notamment, si un hôte est défaillant, le clustering avec basculement restaurera l'accès à l'ordinateur virtuel aussi rapidement que possible sur un autre hôte dans le cluster. Seul un nœud à la fois exécute l'ordinateur virtuel. Cependant, vous pouvez également déplacer l'ordinateur virtuel vers tout autre nœud dans le même cluster.



Le processus de basculement transfère la responsabilité de l'accès aux ressources dans un cluster d'un nœud à l'autre. Le basculement peut se produire lorsqu'un administrateur déplace des ressources vers un autre nœud à des fins de maintenance ou pour d'autres raisons, ou lorsqu'un temps mort non planifié se produit sur un nœud à la suite d'une défaillance matérielle ou pour d'autres raisons.

Le processus de basculement se déroule en plusieurs étapes :

1. Le nœud sur lequel l'ordinateur virtuel s'exécute possède l'instance en cluster de l'ordinateur virtuel, contrôle l'accès au bus partagé ou à la connexion iSCSI au stockage en cluster. Le nœud est également propriétaire de tous les disques, ou numéros d'unité logique, qui sont affectés à l'ordinateur virtuel. Tous les nœuds dans le cluster utilisent un réseau privé pour s'envoyer des signaux réguliers, connus en tant que signaux de pulsation, les uns aux autres. La pulsation signale qu'un nœud fonctionne et communique sur le réseau. La configuration de pulsation par défaut spécifie que chaque nœud envoie une pulsation par seconde (ou 1 000 millisecondes) sur le port 3343 TCP/UDP.
2. Le basculement débute lorsque le nœud hébergeant l'ordinateur virtuel n'envoie pas aux autres nœuds des signaux de pulsation réguliers sur le réseau. Par défaut, cela correspond à cinq pulsations consécutives manquées (ou 5 000 millisecondes). Le basculement peut se produire en raison d'une défaillance de nœud ou de réseau.
3. Lorsque les signaux de pulsation cessent d'être émis par le nœud défectueux, un des autres nœuds du cluster lance la récupération des ressources utilisées par les ordinateurs virtuels. Vous définissez le ou les nœuds qui pourraient continuer à fonctionner en configurant les propriétés Propriétaires possibles et favoris. Le propriétaire favori spécifie la hiérarchie de la propriété s'il y a plus d'un nœud de basculement possible pour une ressource.

   Par défaut, tous les nœuds appartiennent aux propriétaires possibles. Par conséquent, la suppression d'un nœud en tant que propriétaire possible l'empêche absolument de récupérer la ressource en cas de défaillance. Par exemple, imaginez que vous implémentez un cluster de basculement à l'aide de trois nœuds, mais que vous ne configurez que deux nœuds comme propriétaires favoris. Au cours d'un événement de basculement, le troisième nœud peut récupérer la ressource si aucun des propriétaires favoris n'est en ligne. Bien que vous ne configuriez pas le troisième nœud comme propriétaire favori, dans la mesure où il demeure un propriétaire possible, le cluster de basculement peut l'utiliser si nécessaire pour restaurer l'accès à la ressource.

   Vous devez mettre les ressources en ligne dans l'ordre de dépendance. Par exemple, si l'ordinateur virtuel fait référence à un numéro d'unité logique iSCSI, l'accès aux adaptateurs de bus hôte (HBA), réseaux et numéros d'unité logique appropriés sera enregistré dans cet ordre. Le basculement est terminé lorsque toutes les ressources sont en ligne sur le nouveau nœud. Pour les clients interagissant avec la ressource, il y a une brève interruption de service, que la plupart des utilisateurs ne remarqueront pas.
4. Vous pouvez également configurer le service de cluster pour une restauration automatique sur le nœud hors connexion une fois qu'il redevient actif. Quand le service de cluster se restaure automatiquement, il utilise les mêmes procédures auxquelles il a recours pendant le basculement. Autrement dit, le service de cluster met hors connexion toutes les ressources associées avec cette instance, déplace l'instance, puis remet toutes les ressources de l'instance en ligne.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration d'infrastructure requise pour l'implémentation du clustering avec basculement pour Hyper-V

Pour déployer Hyper-V sur un cluster de basculement, vous devez vérifier que vous répondez aux critères de configuration matérielle, logicielle, de compte et d'infrastructure réseau détaillés dans les sections suivantes.

Configuration matérielle requise pour les nœuds de cluster et le stockage	• Matériel du serveur • Cartes réseau • Adaptateurs de stockage • Stockage
Configuration logicielle requise pour les nœuds de cluster	• Windows Server 2012 Standard ou Datacenter • Mises à jour logicielles et services packs identiques • Installation complète ou minimale
Configuration requise pour l'infrastructure réseau	• Les ordinateurs virtuels sont des nœuds de cluster de basculement • Les applications d'ordinateurs virtuels doivent prendre en charge les clusters • Paramètres réseau et adresses IP • DNS • Rôle de domaine • Compte d'administrateur de domaine

Configuration matérielle et logicielle requise pour le clustering avec basculement à l'aide d'Hyper-V

La configuration matérielle requise pour les clusters Hyper-V n'est pas différente de celle des autres types de clusters. Elle est détaillée dans la leçon 1, « Planification d'une infrastructure pour le clustering avec basculement ». Si vous planifiez le matériel pour les clusters Hyper-V, les composants matériels les plus importants à prendre en considération sont le matériel et les cartes réseau, le matériel et les adaptateurs de stockage.

En outre, en ce qui concerne la configuration logicielle requise, tous les serveurs d'un cluster de basculement doivent obligatoirement exécuter l'édition Standard ou Datacenter de Windows Server 2012, et doivent être dotés des mêmes mises à jour logicielles et Service Packs.

Configuration requise pour l'infrastructure réseau

Pour implémenter l'infrastructure de clustering avec basculement, vous devez disposer d'un compte avec des autorisations administratives. De plus, l'infrastructure réseau doit respecter les caractéristiques suivantes pour un cluster de basculement :

- Les paramètres réseau et les adresses IP doivent utiliser des paramètres de communication identiques sur toutes les cartes réseau, y compris les paramètres de vitesse, de mode duplex, de contrôle de flux et de type de média. Vérifiez que l'ensemble du matériel réseau prend en charge les mêmes paramètres.
- Si vous utilisez des réseaux privés que nous ne dirigez pas vers l'ensemble de votre infrastructure réseau pour la communication entre les nœuds de cluster, vérifiez que chacun de ces réseaux privés utilise un sous-réseau unique.
- Les serveurs du cluster doivent utiliser le système DNS pour la résolution de noms. Utilisez le protocole de mise à jour dynamique DNS.
- Tous les serveurs du cluster doivent appartenir au même domaine AD DS. Il est conseillé d'affecter à tous les serveurs en cluster le même rôle de domaine, comme serveur membre ou contrôleur de domaine. Nous recommandons d'utiliser le serveur membre. Évitez d'installer des nœuds de cluster sur des contrôleurs de domaine, parce qu'AD DS possède son propre système à haut niveau de disponibilité.
- Lorsque vous créez un cluster ou que vous y ajoutez des serveurs, vous devez vous connecter au domaine à l'aide d'un compte d'administrateur sur tous les serveurs des clusters. En outre, si le compte n'est pas un compte Administrateurs du domaine, le compte doit avoir l'autorisation de création d'objets ordinateurs dans le domaine.

Implémentation de la migration du stockage

La migration du stockage vous permet de déplacer des ordinateurs virtuels et leur stockage vers un autre emplacement sans interruption. Pendant la migration

- Le disque dur de l'ordinateur virtuel est copié d'un emplacement vers un autre
- Des modifications sont écrites sur le lecteur source et le lecteur de destination
- Vous pouvez déplacer le stockage de l'ordinateur virtuel vers le même hôte, un autre hôte, ou un partage SMB
- Vous pouvez placer les configurations du stockage et de l'ordinateur virtuel à des emplacements différents

De nombreux scénarios peuvent exiger que vous déplaciez vos fichiers d'ordinateur virtuel vers un autre emplacement. Par exemple, si le disque sur lequel réside le disque dur de l'ordinateur virtuel vient à manquer d'espace, vous devez déplacer l'ordinateur virtuel vers un autre pilote ou volume. Le déplacement des ordinateurs virtuels sur d'autres hôtes est une procédure commune.

Dans Windows Server 2008 et Windows Server 2008 R2, le déplacement d'un ordinateur virtuel a entraîné un temps d'arrêt, car l'ordinateur virtuel devait être désactivé. Si vous avez déplacé un ordinateur virtuel entre deux hôtes, vous avez dû également effectuer les opérations d'exportation et d'importation pour cet ordinateur virtuel spécifique. Les opérations d'exportation peuvent être longues, selon la taille des disques durs virtuels.

Dans Windows Server 2012, la migration du stockage et de l'ordinateur virtuel permet de déplacer un ordinateur virtuel et son espace de stockage vers un autre emplacement sur le même hôte ou sur un autre ordinateur hôte sans avoir à éteindre l'ordinateur virtuel.

La migration du stockage et de l'ordinateur virtuel fonctionne comme suit :

1. Vous pouvez copier un disque dur virtuel (VHS) à l'aide de la console Hyper-V pour commencer la migration de stockage dynamique. Éventuellement, vous pouvez utiliser les applets de commande Windows PowerShell.
2. Le processus de migration crée un disque dur virtuel à l'emplacement de destination et démarre le processus de copie.
3. Au cours du processus de copie, l'ordinateur virtuel est totalement fonctionnel. Cependant, toutes les modifications qui se produisent au cours du processus de copie sont écrites à la fois dans l'emplacement source et l'emplacement de destination. Les opérations de lecture sont effectuées uniquement à partir de l'emplacement source.
4. Dès que le processus de copie de disque est terminé, Hyper-V bascule sur les ordinateurs virtuels pour s'exécuter sur le disque dur virtuel de destination. En outre, si vous déplacez l'ordinateur virtuel vers un autre hôte, Windows copie la configuration de l'ordinateur et associe l'ordinateur virtuel à l'hôte. Si une défaillance se produit du côté de la destination, il est toujours possible d'effectuer une restauration sur le répertoire source.
5. Après que l'ordinateur virtuel termine la migration, le processus supprime les disques durs virtuels source.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

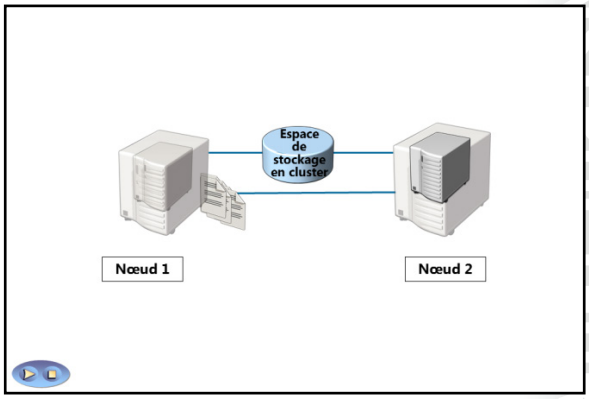
Le temps nécessaire pour déplacer un ordinateur virtuel dépend de plusieurs facteurs, dont les emplacements source et de destination, la vitesse des disques durs, du stockage ou du réseau, et la taille des disques durs virtuels. Le processus de déplacement est plus rapide si les emplacements source et de destination sont sur le stockage et que le stockage prend en charge les fichiers .odx. Au lieu d'utiliser les opérations de lecture/écriture avec mise en tampon, le fichier .odx démarre l'opération de copie avec une commande de lecture de déchargement, puis récupère un jeton qui représente les données du périphérique de stockage. Il demande ensuite le transfert du disque de source vers le disque de destination à l'aide d'une commande d'écriture de déchargement avec le jeton.

Quand vous déplacez les disques durs virtuels d'un ordinateur virtuel vers un autre emplacement, l'Assistant Déplacement des ordinateurs virtuels offre les trois options suivantes :

- Déplacer toutes les données de l'ordinateur virtuel vers un emplacement unique. Vous pouvez spécifier un emplacement cible unique, tel que le fichier de disque, la configuration, la capture instantanée et la pagination intelligente.
- Déplacer les données de l'ordinateur virtuel vers un emplacement différent. Vous pouvez spécifier des emplacements individuels pour chacun des éléments de l'ordinateur virtuel.
- Déplacer uniquement le disque dur virtuel de l'ordinateur virtuel. Vous pouvez spécifier que vous souhaitez déplacer uniquement le fichier VHD.

Implémentation de la migration dynamique

Grâce à la fonctionnalité de migration dynamique, vous pouvez déplacer des ordinateurs virtuels d'un nœud Hyper-V du cluster de basculement vers un autre nœud Hyper-V du même cluster. Avec la migration dynamique, les utilisateurs connectés à l'ordinateur virtuel ne doivent pratiquement subir aucune défaillance du serveur.



Remarque : Vous pouvez effectuer une migration dynamique d'ordinateurs virtuels à l'aide de la méthode de migration de l'ordinateur virtuel et du stockage décrite dans la rubrique précédente, vous devez savoir que la migration dynamique est basée sur le clustering avec basculement. À la différence du scénario de migration du stockage, la migration dynamique est possible uniquement si les ordinateurs virtuels sont à haut niveau de disponibilité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez lancer une migration dynamique en suivant l'une des trois méthodes suivantes :

- La console Gestionnaire du cluster de basculement.
- La console Administrateur Microsoft System Center 2012 - Virtual Machine Manager (VMM), si vous utilisez VMM pour gérer vos hôtes physiques.
- Un script WMI (Windows Management Instrumentation) ou Windows PowerShell.

Remarque : La migration dynamique vous permet de réduire considérablement la panne perçue d'un ordinateur virtuel lors d'un basculement planifié, qui correspond au lancement d'un basculement manuellement. La migration dynamique ne s'applique pas lors d'un basculement non planifié, par exemple lorsque le nœud hébergeant l'ordinateur virtuel est victime d'une défaillance.

Processus de migration dynamique

Le processus de migration dynamique se déroule en quatre étapes exécutées en arrière-plan :

1. Configuration de la migration. Lorsque vous démarrez le basculement de l'ordinateur virtuel, le nœud source crée une connexion TCP avec l'hôte physique cible. Le nœud source utilise cette connexion pour transférer les données de configuration de l'ordinateur virtuel vers l'hôte physique cible. La migration dynamique crée un ordinateur virtuel temporaire sur l'ordinateur hôte physique cible et alloue de la mémoire à l'ordinateur virtuel de destination. La préparation de la migration vérifie également si l'ordinateur virtuel peut être migré.
2. Transfert invité-mémoire. Vous transférez la mémoire invitée de façon itérative à l'hôte cible alors que l'ordinateur virtuel s'exécute toujours sur l'hôte source. Hyper-V sur l'hôte physique source analyse les pages dans la plage de travail. Quand le système modifie les pages en mémoire, il les suit et les marque comme modifiées. Au cours de cette phase de migration, l'ordinateur virtuel en cours de migration continue de s'exécuter. Hyper-V parcourt le processus de copie en mémoire plusieurs fois et copie à chaque fois un plus petit nombre de pages modifiées sur l'ordinateur physique de destination. Un processus final de copie en mémoire copie les pages en mémoire modifiées restantes vers l'hôte physique de destination. La copie s'arrête dès que le nombre de pages qui ont été modifiées dans la mémoire physique, mais pas encore réécrites sur disque (*pages de modifications*), passe en dessous d'un seuil ou à l'issue de 10 itérations.
3. Transfert de l'état. Pour migrer réellement l'ordinateur virtuel sur l'hôte cible, Hyper-V interrompt la partition source, transfère l'état de l'ordinateur virtuel (y compris les pages mémoire modifiées restantes) vers l'hôte cible, puis restaure l'ordinateur virtuel sur l'hôte cible. L'ordinateur virtuel est suspendu pendant le transfert de l'état final.
4. Procédez au nettoyage. L'étape de nettoyage termine la migration en supprimant l'ordinateur virtuel de l'hôte source, en terminant les threads de travail et en signalant l'achèvement de la migration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lors de l'implémentation de la migration dynamique, tenez compte des éléments suivants :

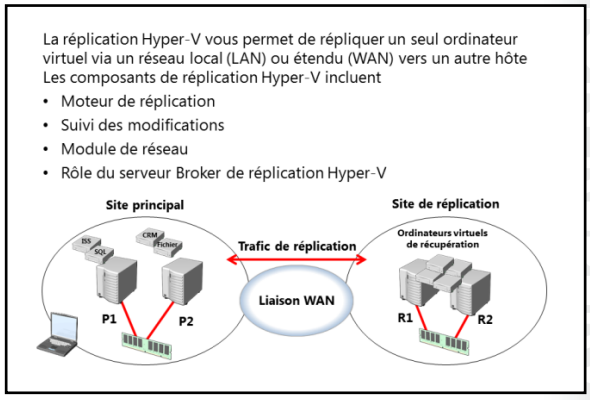
- Vérifiez les conditions de base. Avec la migration dynamique, tous les hôtes doivent faire partie d'un cluster de basculement Windows Server 2012 et les processeurs hôtes doivent présenter la même architecture. Tous les hôtes du cluster doivent avoir accès au stockage partagé, ce qui répond aux exigences de CSV.
- Configurez une carte réseau dédiée pour le réseau virtuel privé. Lorsque vous implémentez le clustering avec basculement, vous devez configurer un réseau privé pour le trafic de pulsation du cluster. Vous utilisez ce réseau pour transférer la mémoire de l'ordinateur virtuel lors du basculement. Pour optimiser cette configuration, configurez pour ce réseau une carte réseau ayant une capacité de 1 gigabit par seconde (Gbps) ou supérieure.

 **Remarque :** Lorsque vous configurez une carte réseau dédiée pour un réseau privé, vous devez activer le composant Client pour les réseaux Microsoft et Partage de fichiers et d'imprimantes pour les réseaux Microsoft pour cette carte réseau spécifique.

- Utilisez un matériel hôte similaire. À titre de recommandation, tous les nœuds de cluster de basculement doivent utiliser le même matériel pour se connecter au stockage partagé, et tous les nœuds de cluster doivent posséder des processeurs présentant la même architecture. Bien que vous puissiez activer le basculement pour les ordinateurs virtuels sur un hôte disposant de versions de processeur différentes en configurant les paramètres de compatibilité du processeur, l'expérience et les performances de basculement sont plus cohérentes si tous les serveurs sont équipés d'un matériel similaire.
- Vérifiez la configuration réseau. Tous les nœuds du cluster de basculement doivent se connecter via le même sous-réseau IP afin que l'ordinateur virtuel puisse continuer de communiquer via la même adresse IP après la migration dynamique. En outre, les adresses IP attribuées au réseau privé sur tous les nœuds doivent être sur le même sous-réseau logique. Autrement dit, les clusters multisites doivent utiliser un réseau local virtuel VLAN étiré, qui est un sous-réseau qui couvre une connexion de réseau étendu (WAN).
- Gérez les migrations dynamiques. Dans Windows Server 2008 R2, chaque nœud du cluster de basculement ne peut exécuter qu'une migration dynamique à la fois. Si vous essayez de démarrer une deuxième migration dynamique avant la fin de la première migration, la migration échoue. Cependant, dans Windows Server 2012, vous pouvez maintenant exécuter plusieurs migrations dynamiques simultanément. Par défaut, vous pouvez exécuter deux migrations dynamiques simultanément, mais vous pouvez augmenter ce nombre en fonction de la bande passante et du stockage à votre disposition.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Implémentation de la fonction Réplica Hyper-V



Dans certains cas, vous souhaiterez probablement disposer d'une copie de remplacement d'un ordinateur virtuel que vous pouvez exécuter en cas de défaillance de l'ordinateur virtuel d'origine. Cependant, lorsque vous implémentez la haute disponibilité, vous ne disposez que d'une instance d'ordinateur virtuel. La haute disponibilité n'empêche pas la corruption du logiciel qui s'exécute sur l'ordinateur virtuel. Une façon de traiter le problème de corruption consiste à copier l'ordinateur virtuel. Vous pouvez également sauvegarder l'ordinateur virtuel et son stockage. Bien que cette solution génère l'effet escompté, elle consomme beaucoup de ressources et beaucoup de temps.

Pour résoudre ce problème et permettre à des administrateurs d'avoir une copie à jour d'un ordinateur virtuel unique, Microsoft a implémenté la fonction de réplication Hyper-V dans Windows Server 2012, laquelle permet aux ordinateurs virtuels en cours d'exécution sur un site principal ou hôte d'être répliqué de manière efficace vers un site secondaire (ou emplacement ou hôte) à travers un lien WAN ou LAN. Le réplica Hyper-V permet d'avoir deux instances d'un ordinateur virtuel unique résidant sur différents hôtes : une en tant que copie principale (en ligne) et l'autre en tant que copie de réplication (hors connexion). Hyper-V synchronise ces copies et vous pouvez effectuer le basculement à tout moment. En cas de défaillance d'un site principal, vous pouvez utiliser Réplica Hyper-V pour exécuter un basculement des charges de travail de production vers des serveurs de réplication sur un emplacement secondaire en quelques minutes, entraînant ainsi un temps d'arrêt minimum.

La technologie Réplica Hyper-V se compose des éléments suivants :

- Moteur de réplication. Il gère les détails de la configuration de la réplication et gère les opérations de réplication initiale, de réplication delta, des opérations de basculement et de test de basculement. Il permet également d'effectuer un suivi des évènements de mobilité du stockage et de l'ordinateur virtuel et prend les mesures qui s'imposent, le cas échéant. Par exemple, il suspend les événements de réplication jusqu'à ce que les événements de migration se terminent, puis reprend à l'endroit où ces évènements avaient été interrompus.
- Suivi des modifications. Ce composant suit les modifications qui se produisent sur la principale copie de l'ordinateur virtuel. Il effectue le suivi des modifications peu importe où résident les fichiers .vhd de l'ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Module de réseau. Ce module réseau fournit une façon sécurisée et efficace de transférer les réplicas d'ordinateur virtuel entre les hôtes principaux et les hôtes de réplica. Il utilise la compression de données qui est activée par défaut. L'opération de transfert est sécurisée, car elle se fonde sur l'authentification basée sur des certificats et le protocole HTTPS.
- Rôle du serveur Broker de réplication Hyper-V. Il s'agit d'un nouveau rôle de serveur qui est implémenté dans Windows Server 2012 et que vous configurez pendant le clustering avec basculement. Ce rôle de serveur vous permet de bénéficier de la fonctionnalité Réplica Hyper-V même lorsque l'ordinateur virtuel que vous répliquez est à haut niveau de disponibilité et peut être déplacé entre deux nœuds de cluster. Le serveur Broker de Réplica Hyper-V redirige tous les événements propres à l'ordinateur virtuel vers le nœud de cluster de réplica approprié. Le service Broker interroge la base de données d'un cluster pour déterminer quel nœud doit traiter quels événements. Cela garantit que tous les événements sont redirigés vers le nœud de cluster approprié lorsque vous exécutez un processus de migration rapide, de migration dynamique ou de migration du stockage.

Avant d'implémenter Réplica Hyper-V, assurez-vous que votre infrastructure répond aux conditions requises :

- Le matériel serveur prend en charge le rôle Hyper-V sous Windows Server 2012. En outre, assurez-vous que le matériel serveur possède la capacité suffisante pour exécuter tous les ordinateurs virtuels sur lesquels vous effectuez les réplications.
- L'espace de stockage suffisant est disponible à la fois sur le serveur principal et sur le serveur de réplication pour héberger les fichiers qui sont utilisés par les ordinateurs virtuels répliqués.
- La connectivité réseau existe entre les emplacements hébergeant le serveur principal et le serveur de réplication. La connectivité peut être réalisée via un lien WAN ou LAN.
- Les règles du pare-feu sont correctement configurées pour permettre la réplication entre le site principal et le site de réplication. Par défaut, le trafic transite via le port TCP 80 ou 443.
- Si vous souhaitez utiliser l'authentification basée sur les certificats, assurez-vous qu'un certificat X.509v3 est disponible pour prendre en charge l'authentification réciproque avec des certificats.

Implémentation de la fonction Réplica Hyper-V

Vous n'avez pas à installer Réplica Hyper-V séparément. La réplication Hyper-V est implémentée comme faisant partie du rôle serveur Hyper-V. Vous pouvez l'utiliser sur les serveurs Hyper-V autonomes ou ceux qui font partie d'un cluster de basculement. Dans le dernier scénario, vous devez configurer le rôle serveur Broker de réplication Hyper-V. À la différence du clustering avec basculement, un rôle Hyper-V ne dépend pas d'Active Directory DS. Vous pouvez l'utiliser avec les serveurs Hyper-V autonomes ou membres de différents domaines AD DS, hormis lorsque les serveurs font partie d'un cluster de basculement.

 **Remarque :** En outre, vous ne devez pas forcer Kerberos. L'authentification doit être conviviale, et les configurations d'ordinateur virtuel doivent permettre des déploiements quel que soir le matériel, y compris le stockage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

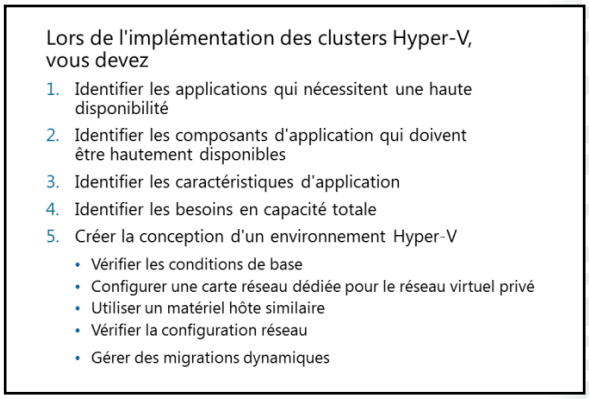
Pour activer la fonction Réplica Hyper-V, vous devez tout d'abord configurer les paramètres du serveur Hyper-V. Dans le groupe d'options **Configuration de la réplication**, activez le serveur Hyper-V en tant que serveur de réplication, puis sélectionnez les options d'authentification et de port. Vous devez également configurer les options d'autorisation. Vous pouvez choisir d'activer la réplication à partir d'un serveur quelconque qui est authentifié avec succès, ce qui est commode dans les scénarios où tous les serveurs font partie du même domaine. Vous pouvez aussi saisir les noms de domaine complets des serveurs que vous acceptez comme serveurs de réplicas. En outre, vous devez configurer l'emplacement des fichiers de réplication sur chaque serveur défini comme serveur de réplication.

Une fois les options configurées au niveau du serveur, activez la réplication sur un ordinateur virtuel. Au cours de cette configuration, vous devez spécifier à la fois le nom du serveur de réplication et les options de la connexion. Si l'ordinateur virtuel possède plusieurs disques durs virtuels, vous pouvez sélectionner les lecteurs de disque dur virtuel à répliquer. Vous pouvez également configurer l'historique de récupération et la méthode de réplication initiale. Démarrez le processus de réplication, après avoir configuré ces options.

Remarque : Les éléments à prendre en compte pour la bande passante sont essentiels. La réplication est conçue pour être utilisée sur les connexions haut débit commerciales, et ne devrait pas interrompre l'activité normale de la messagerie électronique ou du navigateur. À titre de recommandation, vous devez déterminer la quantité de modifications nécessaire sur vos ordinateurs virtuels toutes les 5 à 10 minutes. Vous obtenez ainsi une évaluation de la quantité de bande passante dont vous avez besoin.

Implémentation de la disponibilité d'ordinateurs virtuels

Lors de l'implémentation du clustering avec basculement hôte, vous pouvez rendre les ordinateurs virtuels à haut niveau de disponibilité. Toutefois, l'implémentation du clustering avec basculement de l'hôte augmente également considérablement le coût et la complexité d'un déploiement Hyper-V. Vous devez investir dans du matériel serveur supplémentaire pour fournir la redondance, et vous devez implémenter une infrastructure de stockage partagé ou avoir accès à ce type d'infrastructure.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lors de la conception de votre stratégie pour le clustering de basculement, prenez en compte les facteurs suivants pour vous assurer que votre conception répond aux besoins de votre organisation :

- Identifiez les applications ou les services qui nécessitent une haute disponibilité. Sauf si vous avez la possibilité de rendre tous les ordinateurs virtuels à haut niveau de disponibilité, vous devez développer des priorités pour lesquelles les applications seront rendues à haut niveau de disponibilité.
- Identifiez les composants qui doivent être hautement disponibles pour rendre les applications hautement disponibles. Dans certains cas, l'application peut fonctionner sur un seul serveur. Vous devez alors uniquement rendre ce serveur hautement disponible. D'autres applications peuvent requérir que plusieurs serveurs, et d'autres composants tels que le stockage ou le réseau, soient à haut niveau de disponibilité. En outre, assurez-vous que les contrôleurs de domaine sont à haut niveau de disponibilité, et que vous disposez au moins d'un contrôleur de domaine sur une infrastructure matérielle ou de virtualisation distincte.
- Identifiez les caractéristiques d'application. Vous devez comprendre plusieurs aspects à propos de l'application, notamment :
    - Est-il envisageable de virtualiser le serveur qui exécute l'application ? Un environnement virtuel ne prend pas en charge, ou n'est pas recommandé, pour certaines applications.
    - Quelles sont les options disponibles pour rendre l'application à haut niveau de disponibilité ? Vous pouvez rendre certaines applications à haut niveau de disponibilité à l'aide d'options autres que le clustering hôte. Si d'autres options sont disponibles, évaluez les avantages et les inconvénients de chaque option.
    - Quelles sont les exigences en matière de performances pour chaque application ? Collectez les informations de performance sur les serveurs qui exécutent actuellement les applications afin de bien comprendre la configuration matérielle nécessaire lors de la virtualisation du serveur.
    - Quelle est la capacité requise pour rendre les ordinateurs virtuels Hyper-V à haut niveau de disponibilité ? Dès que vous avez identifié toutes les applications que vous devez rendre hautement disponibles en utilisant le clustering hôte, vous pouvez commencer à concevoir le déploiement Hyper-V proprement dit. En identifiant les exigences en matière de performances, de réseau et de stockage pour les applications, vous pouvez définir le matériel dont vous avez besoin pour implémenter toutes les applications dans un environnement à haut niveau de disponibilité.

La migration dynamique est l'un des aspects les plus importants du clustering Hyper-V. Utilisez la fonctionnalité de migration dynamique dans Windows Server 2012 pour exécuter des migrations dynamiques des ordinateurs virtuels. Cependant, dans Windows Server 2012, vous pouvez également migrer des ordinateurs virtuels sans utiliser le clustering avec basculement. Ce processus est appelé *migration dynamique sans cluster*.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Planification d'un cluster de basculement multisite

Dans certains scénarios, vous devez déployer des nœuds de cluster sur différents sites. Cela se fait généralement lors de l'établissement de solutions de récupération d'urgence. Dans cette leçon, vous découvrirez les clusters de basculement multisites et les conditions préalables pour les implémenter. Vous découvrirez également la réplication synchrone et asynchrone, ainsi que le processus de choix d'un mode de quorum pour les clusters multisites.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les difficultés relatives à la planification des clusters multisites.
- Décrire les éléments à prendre en compte pour la réplication de données.
- Décrire les éléments à prendre en compte pour l'infrastructure réseau.
- Décrire les éléments à prendre en compte pour le mode de quorum.
- Expliquer les instructions générales pour la planification des clusters multisites.

Difficultés relatives à la planification des clusters multisites

L'implémentation de clusters multisites est plus complexe que l'implémentation de clusters sur site unique, et peut également présenter plusieurs difficultés pour l'administrateur. Le stockage et les problèmes de réseau sont les aspects les plus difficiles dans l'implémentation des clusters multisites.

Complexité du stockage	Description
Requiert une solution de réplication de données séparée ou autre que Microsoft	• Réplication basée sur le stockage du matériel (au niveau du bloc) • Réplication basée sur l'hôte des logiciels (au niveau du système de fichiers) • Réplication basée sur une application (telle que la Réplication continue en cluster d'Exchange 2007)
Elles peuvent être synchrones ou asynchrones	• Synchrones : Aucun accusé de réception des modifications de données apportées au site A jusqu'à ce que les données soient écrites sur le site B • Asynchrones : Les changements de données faites dans le site A seront par la suite écrites dans le stockage du site B

- Les communications entre les nœuds sont sensibles au temps. Vous pouvez avoir besoin de configurer ces seuils pour obtenir une latence WAN supérieure
- La réplication DNS peut avoir un impact sur les délais de reconnexion client lorsque le basculement est basé sur un nom d'hôte
- La latence de réplication Active Directory peut affecter la disponibilité des données des applications
- Certaines applications peuvent nécessiter que tous les nœuds soient dans le même site Active Directory

Dans un cluster multisite, il n'y a aucun stockage partagé. Cela signifie que chaque nœud sur chaque site doivent avoir leur propre instance de stockage. D'autre part, le clustering avec basculement n'inclut aucune fonctionnalité intégrée pour répliquer des données entre les sites. Vous disposez de trois options pour la réplication des données : la réplication de niveau bloc basée sur le matériel, la réplication de fichiers basée sur le logiciel et installée sur l'hôte, ou la réplication basée sur les applications.

La réplication de données multisite peut être synchrone ou asynchrone. La réplication synchrone ne reconnaît pas les modifications de données qui sont apportées sur le Site A par exemple, tant que les données n'ont pas été correctement copiées sur le Site B. Avec la réplication asynchrone, les modifications de données qui sont apportées sur le Site A sont ultérieurement écrites sur le Site B.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

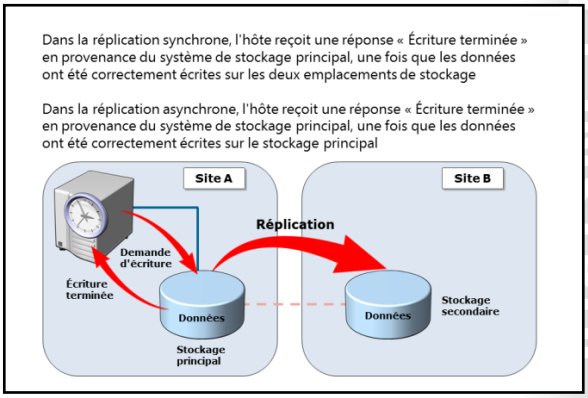
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous déployez un cluster multisite et exécutez l'Assistant Validation d'une configuration, les tests de disque ne trouveront aucun stockage partagé. Par conséquent, ils ne fonctionneront pas. Cependant, vous pouvez créer un cluster de basculement. Si vous suivez les recommandations du fabricant de matériel relatives au matériel de clustering avec basculement Windows Server, Microsoft prendra en charge la solution.

Windows Server 2012 permet l'existence de nœuds de cluster sur différents sous-réseaux IP, ce qui permet à une application ou un service en cluster de modifier son adresse IP en fonction du sous-réseau IP. Le système DNS met à jour l'enregistrement DNS de l'application en cluster de sorte que les clients puissent localiser la modification d'adresse IP. Les clients utilisent le système DNS pour rechercher un service ou une application après un basculement, vous devrez donc peut-être ajuster la **durée de vie** des enregistrements DNS et la vitesse de réplication des données DNS. En outre, lorsque des nœuds de cluster se trouvent sur plusieurs sites, la latence du réseau pourra exiger que vous modifiiez le délai de communication entre les nœuds (pulsation) et les seuils d'expiration du délai d'attente.

Planification de la réplication des données d'un cluster de basculement multisite

Il n'est pas possible qu'un cluster de basculement géographiquement dispersé utilise le stockage partagé entre des emplacements physiques. Les liaisons WAN sont trop lentes et présentent une latence trop importante pour prendre en charge le stockage partagé. Ceci signifie que vous devez avoir des instances de données distinctes. Pour avoir des copies exactes des données des deux côtés, les clusters de basculement dispersés géographiquement doivent synchroniser les données entre les emplacements à l'aide d'un matériel spécialisé.



La réplication de données multisite peut être synchrone ou asynchrone :

- Lorsque vous utilisez la réplication synchrone, l'hôte reçoit une réponse Écriture terminée en provenance du système de stockage principal, une fois que les données ont été correctement écrites sur les deux systèmes de stockage. En cas d'échec de l'écriture des données sur les deux systèmes de stockage, l'application doit tenter d'écrire sur le disque une nouvelle fois. Avec la réplication synchrone, les deux systèmes de stockage sont identiques.
- Lorsque vous utilisez la réplication asynchrone, le nœud reçoit une réponse « Écriture terminée » en provenance du système de stockage principal, une fois que les données ont été correctement écrites sur le système de stockage principal. Les données sont écrites dans le système de stockage secondaire à un autre moment, en fonction de l'implémentation du fournisseur de matériel ou de logiciels. La réplication asynchrone peut être basée sur le système de stockage, sur l'hôte, voire sur l'application. Cependant, toutes les formes de réplication asynchrone ne sont pas suffisantes pour un cluster multisite. Par exemple, le système DFS-R (Distributed File System Replication) fournit une réplication asynchrone au niveau des fichiers. Cependant, il ne prend pas en charge la réplication multisite de clustering avec basculement. C'est parce que la réplication DFS réplique de plus petits documents qui ne sont pas maintenus ouverts continuellement, et n'a pas été conçue pour la réplication haute vitesse de fichiers ouverts.

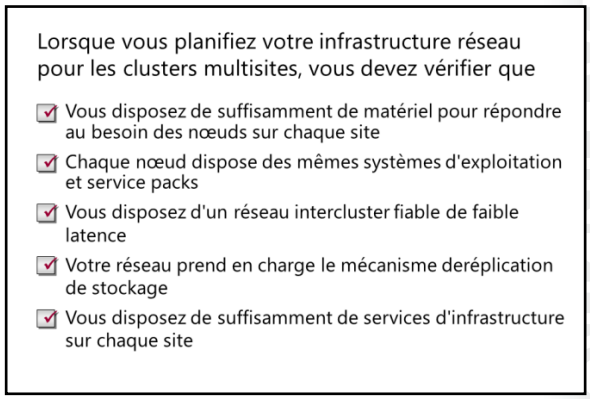
Quand utiliser la réplication synchrone ou asynchrone ?

Utilisez la réplication synchrone quand vous ne pouvez accepter aucune perte de données. Les solutions de réplication synchrone requièrent une faible latence d'écriture de disque, car l'application attend que les deux solutions de stockage reconnaissent les écritures de données. La configuration requise pour les écritures de disque à faible latence limite également la distance entre les systèmes de stockage, car une distance trop importante peut provoquer une latence plus élevée. Si la latence de disque est haute, cela peut affecter les performances et la stabilité de l'application.

La réplication asynchrone surmonte des limitations en matière de latence et de distance en reconnaissant les écritures de disque local uniquement, et en reproduisant l'écriture de disque sur le système de stockage distant dans une transaction distincte. La réplication asynchrone réalise des écritures sur le système de stockage distant après avoir écrit sur le système de stockage local, par conséquent, la possibilité de perte de données en cas de défaillance augmente.

Éléments à prendre en compte pour l'infrastructure réseau

Lors de la planification des clusters de basculement multisites, il est très important de planifier correctement l'infrastructure réseau dont vous aurez besoin. Dans les clusters de basculement ordinaires, vous n'avez besoin de concevoir qu'un seul réseau interne entre les nœuds de cluster, le stockage et les clients. Cependant, dans les clusters multisites, il est très important de planifier des liaisons réseau intersite. Lorsque vous planifiez votre infrastructure réseau pour les clusters multisites, tenez compte des recommandations suivantes :



- Vous devez fournir au moins une connexion réseau fiable et de latence faible entre les sites. Cela est important pour les pulsations de cluster. Par défaut, quelle que soit la configuration de sous-réseau, la fréquence de pulsation (également appelé le retard de sous-réseau) se produit une fois par seconde (1 000 millisecondes). La plage de la fréquence de pulsation est d'une fois toutes les 250 à 2 000 millisecondes sur un sous-réseau commun et 250 à 4 000 millisecondes sur les sous-réseaux. Par défaut, lorsqu'un nœud manque une série de 5 pulsations, un autre nœud initialise le basculement. La plage pour cette valeur, ou *seuil de sous-réseau*, est comprise entre 3 et 10 pulsations.
- Vous devez fournir un mécanisme de réplication de stockage. Le clustering avec basculement ne fournit aucun mécanisme de réplication de stockage, ainsi vous devez fournir une autre solution. Ceci requiert également que vous disposiez de plusieurs solutions de stockage, une pour chaque cluster que vous créez.
- Vous devez vous assurer que tous les autres services nécessaires pour le cluster, tel qu'AD DS et le DNS, sont également disponibles sur un deuxième site.
- Vous devez vérifier que les connexions clientes peuvent être redirigées vers un nouveau nœud de cluster lorsque le basculement se produit.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour le mode de quorum

Lors de la conception du basculement automatique pour des clusters dispersés géographiquement, vous devez

- Utiliser le mode de quorum Nœud majoritaire ou Nœud majoritaire avec partage de fichiers
- Utiliser trois emplacements pour autoriser le basculement automatique d'un seul serveur virtuel
  - Les trois emplacements doivent être liés directement entre eux
  - Un emplacement est uniquement un témoin de partage de fichiers

Chaque cluster de basculement doit avoir un mode de quorum défini, de sorte qu'un vote majoritaire puisse être facilement déterminé à tout moment. Pour les clusters géographiquement dispersés, vous ne pouvez pas utiliser de configurations de quorum qui requièrent un disque partagé, car ce type de cluster n'utilise pas de disques partagés. Les modes de quorum **Nœud et disque majoritaires** et **Pas de majorité : Disque uniquement** requièrent un disque témoin partagé qui fournit un vote déterminant pour atteindre le quorum. Utilisez ces deux modes de quorum uniquement si le fabricant du matériel prend en charge ces deux modes de quorum et recommande de les utiliser.

Pour utiliser les modes **Nœud et disque majoritaires** et **Pas de majorité : Disque uniquement** dans un cluster multisite, le disque partagé requiert que :

- vous conserviez la sémantique des commandes SCSI sur l'ensemble des sites, même en cas de panne totale de communication entre les sites ;
- vous répliquiez le disque témoin en mode synchrone dynamique sur tous les sites.

Les clusters multisites peuvent rencontrer des pannes de réseau WAN, outre les défaillances sur le réseau local et sur les nœuds, l'utilisation des modes **Nœud majoritaire** et **Nœud et partage de fichiers majoritaires** constitue une meilleure option pour les clusters multisites. En cas de défaillance du réseau WAN entraînant la perte de communication entre le site principal et les sites secondaires, une majorité doit rester disponible pour poursuivre les opérations. S'il y a un nombre impair de nœuds, utilisez le quorum **Nœud majoritaire**. S'il existe un nombre pair de nœuds, situation typique dans un cluster géographiquement dispersé, vous pouvez utiliser le mode de quorum **Nœud et partage de fichiers majoritaires**.

Si vous utilisez le mode **Nœud majoritaire** et que les sites perdent la communication, vous avez besoin d'un mécanisme pour déterminer quels sont les nœuds encore actifs et quels sont les nœuds qui ont quitté le cluster. Le deuxième site exige un autre vote pour atteindre le quorum après une défaillance. Pour obtenir un nouveau vote pour le quorum, vous devez ajouter un autre nœud au cluster ou créer un témoin de partage de fichiers. Le mode **Nœud et partage de fichiers majoritaires** peut aider à maintenir le quorum sans ajouter de nœud supplémentaire au cluster. Pour fournir une défaillance de site unique et activer le basculement automatique, il peut s'avérer nécessaire que le témoin de partage de fichiers existe sur un troisième site. Dans un cluster multisite, un serveur unique peut héberger le témoin de partage de fichiers. Cependant, vous devez créer un partage de fichier distinct pour chaque cluster.

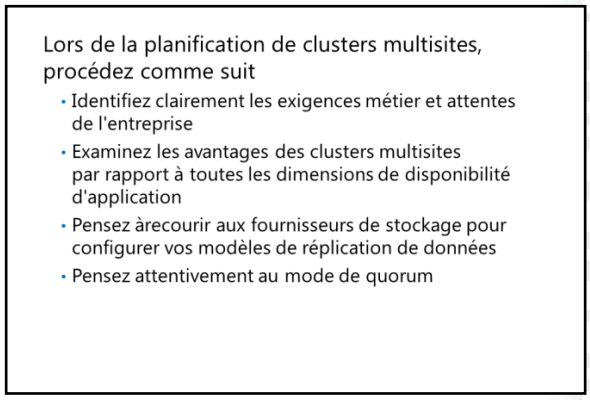
Vous devez utiliser trois emplacements pour activer le basculement automatique d'un service ou d'une application à haut niveau de disponibilité. Localisez un nœud dans l'emplacement principal qui exécute le service ou l'application à haut niveau de disponibilité. Localisez un deuxième nœud sur un site de récupération d'urgence, puis localisez le troisième nœud pour le témoin de partage de fichiers dans un autre emplacement.

Les trois emplacements doivent être directement connectés via un réseau. Ainsi, si un site devient non disponible, les deux sites restants peuvent continuer à communiquer et disposer d'un nombre suffisant de nœuds pour atteindre un quorum.

Remarque : Dans Windows Server 2008 R2, les administrateurs pouvaient configurer **le quorum pour inclure** des nœuds. Cependant, si la configuration de quorum comprenait des nœuds, tous les nœuds étaient traités de la même manière en fonction de leur vote. Dans Windows Server 2012, vous pouvez régler les paramètres de quorum du cluster de sorte que lorsque le cluster détermine s'il a le quorum, certains nœuds ont un vote et d'autres non. Ce réglage peut être utile quand des solutions sont implémentées sur plusieurs sites. Nous recommandons que lorsque vous recherchez le nombre de nœuds et les configurations de quorum correspondantes, vous effectuiez la recherche avec un nombre pair de nœuds pour le quorum.

Instructions générales pour la planification des clusters multisites

Les clusters multisites ne sont pas adaptés à toutes les applications ou entreprises. Lorsque vous concevez une solution multisite avec un fabricant de matériel, identifiez clairement les exigences métier et attentes de l'entreprise. Tous les scénarios impliquant plus d'un emplacement ne sont pas appropriés pour le cluster multisite.



Le clustering multisite est une stratégie haute disponibilité qui se concentre principalement sur la disponibilité des plateformes matérielles. Cependant, les configurations et le déploiement d'un cluster multisite spécifique ont des implications en termes de disponibilité, notamment la capacité des utilisateurs à se connecter à l'application ou encore la qualité des performances de l'application. Le clustering multisite peut être une solution efficace pour faire face au temps mort planifié et non planifié, mais vous devez examiner ses avantages en prenant en compte de toutes les dimensions de disponibilité d'application.

Les clusters multisites requièrent plus d'attention que les clusters locaux. Au lieu d'un cluster local, dans lequel chaque nœud du cluster est connecté au périphérique de stockage de masse, chaque site d'un cluster multisite doit posséder un stockage comparable. Par ailleurs, vous devez également recourir à des fournisseurs pour configurer vos modèles de réplication de données entre les sites de cluster, éventuellement acheter une bande passante réseau supplémentaire en les sites, et développer les ressources de gestion au sein de votre entreprise pour administrer efficacement votre cluster multisite.

En outre, étudiez soigneusement le mode de quorum que vous utiliserez et l'emplacement des votes de cluster disponibles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et implémentation d'une infrastructure hautement disponible à l'aide du clustering avec basculement

Scénario

Un des principaux objectifs pour le déploiement de Windows Server 2012 chez A. Datum Corporation est que tous les services, applications et serveurs doivent être hautement disponibles. A. Datum a implémenté le stockage et les applications Web hautement disponibles, et souhaite maintenant fournir la haute disponibilité aux serveurs et applications que vous ne pouvez pas rendre hautement disponibles via l'équilibrage de la charge réseau.

A. Datum a décidé d'utiliser le clustering avec basculement pour fournir la haute disponibilité pour ces services. Vous devez planifier et implémenter une solution de clustering avec basculement qui réponde aux exigences d'A. Datum. En outre, A. Datum souhaite évaluer de nouvelles fonctionnalités hautement disponibles dans Windows Server 2012, telles que Réplica Hyper-V et le serveur de fichiers avec montée en puissance parallèle.

Étant donné que la surveillance constitue une part importante de l'infrastructure d'A. Datum, l'entreprise a implémenté System Center Operations Manager 2012 et souhaite à présent intégrer ce produit avec VMM 2012, qu'elle utilise pour gérer l'environnement virtuel et les hôtes Hyper-V.

Objectifs

- Concevoir la haute disponibilité pour les rôles serveur.
- Implémenter la fonction Réplica Hyper-V.
- Déployer un cluster de basculement.
- Implémenter un serveur de fichiers avec montée en puissance parallèle.
- Implémenter des ordinateurs virtuels hautement disponibles.
- Implémenter l'intégration d'Operations Manager et de VMM.

Configuration de l'atelier pratique

Durée approximative : 110 minutes

Ordinateur(s) virtuel(s)	Démarré sur 22414B-LON-HOST1 : 22414B-LON-DC1 22414B-LON-OM1 22414B-LON-SVR1 22414B-LON-SVR2 22414B-LON-VMM1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Afin de mener à bien cet atelier pratique, les stagiaires devront travailler par deux. Un stagiaire démarre avec LON-HOST1, et le deuxième stagiaire avec LON-HOST2. Les deux serveurs doivent être connectés l'un à l'autre, mais pas au reste de la classe.

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible.
Avant de commencer cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, sur **Accueil**, cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22414B-LON-DC1**, puis cliquez sur **Démarrer** dans le volet Actions.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 et 3 pour les ordinateurs virtuels restants.

Exercice 1 : Conception de rôles serveur hautement disponibles

Scénario

L'équipe serveurs d'A. Datum vous a présenté la liste suivante de rôles serveur et d'applications qui doivent être rendus hautement disponibles. Vous devez identifier la meilleure option d'implémentation de la haute disponibilité pour chacun des rôles serveur.

Les rôles serveur qui doivent être pris en considération sont :

- Contrôleurs de domaine AD DS
- Serveurs Web
- Serveurs DHCP
- Serveurs de fichiers
- SQL Server
- Exchange Server

Les tâches principales de cet exercice sont les suivantes :

1. Analyser des rôles serveur devant être hautement disponibles.
2. Répondre à la question et proposer une conception hautement disponible.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.

▶ Tâche 1 : Analyser des rôles serveur devant être hautement disponibles

- Analysez la liste des rôles serveur fournie dans le scénario de l'exercice. En fonction de ce que vous avez appris jusqu'à présent, pensez aux solutions hautement disponibles pour ces rôles serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Répondre à la question et proposer une conception hautement disponible

Proposez une solution de conception permettant de rendre les rôles du scénario de l'exercice hautement disponibles, en répondant aux questions suivantes :

1. Comment pouvez-vous rendre des contrôleurs de domaine AD DS hautement disponibles ? Quelle technologie à haut niveau de disponibilité utiliserez-vous ?
2. Quelle technologie ou quelles technologies devez-vous utiliser pour rendre les serveurs Web hautement disponibles ?
3. Comment pouvez-vous rendre un serveur DHCP (Dynamic Host Configuration Protocol) hautement disponible ? Y a-t-il d'autres solutions ?
4. Quelle est la solution recommandée pour rendre Microsoft® SQL Server® hautement disponible ?
5. Comment pouvez-vous rendre le serveur de fichiers hautement disponible ?
6. Comment pouvez-vous rendre Microsoft Exchange Server hautement disponible ? La même approche s'applique-t-elle à tous les rôles Exchange Server ?

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

Lisez les réponses dans la section de corrigé de l'atelier pratique, puis comparez-les avec vos réponses. Discutez avec la classe.

Résultats : À la fin de cet exercice, vous aurez terminé la conception de la haute disponibilité pour différents rôles serveur.

Exercice 2 : Implémenter la fonction Réplica Hyper-V

Scénario

Une des solutions pour fournir la haute disponibilité pour un ordinateur virtuel est de configurer la fonction Réplica Hyper-V. A. Datum a décidé d'implémenter la fonction Réplica Hyper-V pour l'un des serveurs critiques situés dans le centre de données de Toronto. Néanmoins, la fonction Réplica Hyper-V doit tout d'abord être testée, c'est pourquoi l'ordinateur virtuel 22414B-LON-CORE a été fourni comme plateforme test afin d'évaluer la fonction.

Les tâches principales de cet exercice sont les suivantes :

1. Importer un ordinateur virtuel 22414B-LON-CORE sur l'ordinateur LON-HOST1.
2. Configurer un réplica sur les deux ordinateurs hôtes.
3. Configurer une réplication pour l'ordinateur virtuel.
4. Valider un basculement planifié vers le site de réplication.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Importer un ordinateur virtuel 22414B-LON-CORE sur l'ordinateur LON-HOST1

1. Sur LON-HOST1, ouvrez le **Gestionnaire Hyper-V**, puis importez l'ordinateur virtuel **22414B-LON-CORE**.
2. Utilisez le chemin d'accès E:\Programmes\Microsoft Learning\22414\Drives\22414B-LON-CORE.
3. Acceptez les valeurs par défaut.

Remarque : La lettre de lecteur peut être différente selon le nombre de lecteurs présents sur l'ordinateur hôte physique.

▶ Tâche 2 : Configurer un réplica sur les deux ordinateurs hôtes

1. Sur LON-HOST1 et LON-HOST2, configurez chaque serveur afin qu'il soit un serveur de réplication Hyper-V.
2. Utilisez le protocole Kerberos version 5 (HTTP) pour l'authentification.
3. Activez la réplication à partir de n'importe quel serveur authentifié.
4. Créez et utilisez le dossier **E:\VMReplica** comme emplacement par défaut pour stocker les fichiers de réplication. (Remarque : la lettre du lecteur peut changer en fonction de votre configuration matérielle hôte).
5. Activez la règle de pare-feu nommée **Écouteur HTTP de réplica Hyper-V (Tcp-In)** sur les deux hôtes.

▶ Tâche 3 : Configurer une réplication pour l'ordinateur virtuel

1. Sur LON-HOST1, activez la réplication pour l'ordinateur virtuel **22414B-LON-CORE**.
2. Utilisez Kerberos (HTTP).
3. Effectuez la sélection de sorte que seul le point de récupération le plus récent soit disponible.
4. Lancez immédiatement la réplication.
5. Patientez jusqu'à la fin de la réplication initiale et vérifiez que l'ordinateur virtuel 22414B-LON-CORE s'affiche correctement dans la console Gestionnaire Hyper-V sur LON-HOST2.

▶ Tâche 4 : Valider un basculement planifié vers le site de réplication

1. Sur LON-HOST2, affichez l'intégrité de la réplication pour **22414B-LON-CORE**.
2. Sur LON-HOST1, effectuez le basculement planifié vers LON-HOST2. Vérifiez que 22414B-LON-CORE est exécuté sur LON-HOST2.
3. Sur LON-HOST1, supprimez la réplication pour 22414B-LON-CORE.
4. Sur LON-HOST2, arrêtez 22414B-LON-CORE.

Résultats : À l'issue de cet exercice, les étudiants auront implémenté un réplica Hyper-V.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Déployer un cluster de basculement

Scénario

La première étape du processus d'implémentation du clustering avec basculement pour des applications et des ordinateurs virtuels est le déploiement du cluster de basculement. Vous devez configurer un cluster de basculement à deux nœuds. A. Datum dispose d'un stockage iSCSI que vous utiliserez pour les clusters. En outre, vous avez deux hôtes physiques que vous pouvez utiliser comme hôtes Hyper-V. Utilisez ces hôtes pour créer un cluster.

Les tâches principales de cet exercice sont les suivantes :

1. Se connecter à des cibles iSCSI à partir des deux ordinateurs hôtes.
2. Installer et configurer un clustering avec basculement sur les deux ordinateurs hôtes.
3. Configurer le cluster.
4. Valider le groupe.

▶ Tâche 1 : Se connecter à des cibles iSCSI à partir des deux ordinateurs hôtes

1. Sur LON-HOST1, démarrez l'**initiateur iSCSI**.
2. Utilisez l'adresse de 172.16.0.10 pour découvrir et vous connecter à la cible iSCSI.
3. Sur LON-HOST2, démarrez l'**initiateur iSCSI**.
4. Utilisez l'adresse de 172.16.0.10 pour découvrir et vous connecter à la cible iSCSI.
5. Sur LON-HOST2, ouvrez la **Gestion des disques**, puis initialisez et mettez en ligne le premier iSCSI (Disque 2). Formatez-le, puis nommez-le **ClusterDisk**.
6. Sur LON-HOST1, ouvrez la **Gestion des disques**, puis actualisez le Disque 2.

▶ Tâche 2 : Installer et configurer un clustering avec basculement sur les deux ordinateurs hôtes

1. Installez la fonctionnalité de clustering avec basculement sur LON-HOST1 et LON-HOST2.
2. Ouvrez le Gestionnaire du cluster de basculement sur LON-HOST1, puis créez un cluster avec LON-HOST1 et LON-HOST2 en tant que nœuds. Nommez le cluster **VMCluster**, puis donnez-lui l'adresse IP **172.16.0.126**.
3. N'ajoutez pas le stockage au cluster.

▶ Tâche 3 : Configurer le cluster

1. Dans la console du Gestionnaire du cluster de basculement sur LON-HOST1, ajoutez Disque du cluster 1 au cluster.
2. Vérifiez que le disque iSCSI est disponible pour le stockage en cluster.
3. À partir du nœud **VMCluster.adatum.com**, sélectionnez **Autres actions**, puis configurez les paramètres du quorum de cluster pour utiliser les paramètres standard.

▶ Tâche 4 : Valider le groupe

1. Sur l'ordinateur LON-HOST2, ouvrez la console Gestionnaire du cluster de basculement.
2. Démarrez l'Assistant Validation et installation de cluster.
3. Choisissez d'exécuter tous les tests.
4. Choisissez de tester le Disque du cluster 1.
5. Examinez le rapport. (Remarque : certains avertissements peuvent s'afficher, mais aucune erreur).

Résultats : À la fin de cet exercice, vous aurez déployé un cluster de basculement.

Exercice 4 : Implémenter un serveur de fichiers avec montée en puissance parallèle

Scénario

A. Datum a terminé le projet ayant pour objectif de fournir un stockage à haute disponibilité pour le rôle Services de fichiers. L'organisation souhaite également fournir la haute disponibilité pour les serveurs de fichiers en configurant les serveurs en tant que membres d'un serveur de fichiers avec montée en puissance parallèle, que vous pouvez ensuite utiliser comme stockage pour des ordinateurs virtuels Hyper-V.

Les tâches principales de cet exercice sont les suivantes :

1. Installation du rôle de serveur de fichiers et du clustering avec basculement sur LON-SVR1 et LON-SVR2.
2. Se connecter à la cible iSCSI des deux nœuds de cluster du serveur de fichiers.
3. Configurer le serveur de fichiers avec montée en puissance parallèle.
4. Créer un partage de fichiers disponible en permanence.

▶ Tâche 1 : Installation du rôle de serveur de fichiers et du clustering avec basculement sur LON-SVR1 et LON-SVR2

1. Sur LON-SVR1, vérifiez que service de rôle Serveur de fichiers est installé, puis ajoutez la fonctionnalité Clustering avec basculement à l'aide du Gestionnaire de serveur.
2. Sur LON-SVR2, vérifiez que service de rôle Serveur de fichiers est installé, puis ajoutez la fonctionnalité Clustering avec basculement à l'aide du Gestionnaire de serveur.

▶ Tâche 2 : Se connecter à la cible iSCSI des deux nœuds de cluster du serveur de fichiers

1. Sur LON-SVR1,démarrez l'**initiateur iSCSI**.
2. Utilisez l'adresse 172.16.0.10 pour découvrir et vous connecter à la cible iSCSI.
3. Sur LON-SVR2, démarrez l'**initiateur iSCSI**.
4. Utilisez l'adresse 172.16.0.10 pour découvrir et vous connecter à la cible iSCSI.
5. Sur LON-SVR2, ouvrez **Gestion des disques**, puis initialisez et mettez en ligne les disques 2 et 3 (ne sélectionnez pas le disque 1). Formatez ces lecteurs.
6. Sur LON-SVR1, **ouvrez Gestion des disques**, puis mettez en ligne les disques 3 et 4 (ne sélectionnez pas le disque 2).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer le serveur de fichiers avec montée en puissance parallèle

1. Ouvrez la console Gestionnaire du cluster de basculement sur LON-SVR1.
2. Créez un cluster avec les nœuds LON-SVR1 et LON-SVR2.
3. N'exécutez pas la validation à ce stade.
4. Indiquez **FSCluster** comme valeur pour le **Point d'accès pour l'administration du cluster**.
5. Spécifiez **172.16.0.127** comme **Adresse IP** pour le cluster.
6. Ajoutez le Disque du cluster 1 et le Disque du cluster 2 à **Stockage du cluster**.
7. Attribuez le Disque du cluster 1 à un **volume partagé de cluster**.
8. Configurez les paramètres de quorum sur **Par défaut** (recommandé).
9. Démarrez l'Assistant Haute disponibilité pour configurer le rôle en cluster.
10. Sélectionnez **Serveur de fichiers**, puis choisissez de configurer un **serveur de fichiers avec montée en puissance parallèle** pour les données d'application.
11. Indiquez **AdatumFS** en tant que **point d'accès client**.

▶ Tâche 4 : Créer un partage de fichiers disponible en permanence

1. Sur LON-SVR1, utilisez la console Gestionnaire du cluster de basculement pour ajouter un partage de fichiers à un rôle de cluster ADatumFS existant. (Si vous recevez un message indiquant que le point d'accès client n'est pas prêt, effectuez ces étapes sur LON-SVR2.)
2. Dans l'Assistant Nouveau partage, choisissez d'utiliser **Partage SMB - Applications.**
3. Choisissez de configurer un partage **par volume**, puis nommez le partage **VMachines**.
4. Configurez les autorisations pour le partage **VMachines** afin que les ordinateurs LON-HOST1 et LON-HOST2 disposent d'un accès complet.

Résultats : À la fin de cet exercice, vous aurez configuré un serveur de fichiers à haut niveau de disponibilité.

Exercice 5 : Implémenter des ordinateurs virtuels hautement disponibles

Scénario

Certains rôles serveur peuvent être rendus hautement disponibles uniquement en déployant les ordinateurs virtuels hautement disponibles qui exécutent le rôle serveur. Vous devez configurer et valider les ordinateurs virtuels hautement disponibles sur le cluster de basculement :

Les tâches principales de cet exercice sont les suivantes :

1. Déplacer un fichier .vhd sur le stockage hautement disponible.
2. Configurer les nœuds Hyper-V de sorte qu'ils utilisent le cluster de serveurs de fichiers avec montée en puissance parallèle.
3. Configurer l'ordinateur virtuel en tant qu'ordinateur à haut niveau de disponibilité.
4. Exécuter une migration dynamique pour l'ordinateur virtuel.
5. Valider la haute disponibilité en cas de défaillance du stockage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Déplacer un fichier .vhd sur le stockage hautement disponible

1. Ouvrez l'Explorateur de fichiers sur l'ordinateur LON-HOST1.
2. Copiez le fichier 22414B-LON-CORE.vhd d'**E:\Programmes\Microsoft Learning\22414\Drives\22414B-LON-CORE\Virtual Hard Disks** vers le dossier **\\AdatumFS\VMachines\LON-CORE**. (Remarque : Vous devez créer le dossier 22414B-LON-CORE manuellement.)

▶ Tâche 2 : Configurer les nœuds Hyper-V de sorte qu'ils utilisent le cluster de serveurs de fichiers avec montée en puissance parallèle

1. Sur LON-HOST1, dans la console du Gestionnaire Hyper-V, ouvrez les **Paramètres Hyper-V**.
2. Configurez des emplacements pour que les ordinateurs virtuels et les disques durs virtuels correspondent à **\\adatumfs\VMachines**.
3. Répétez la même procédure sur LON-HOST2.

▶ Tâche 3 : Configurer l'ordinateur virtuel en tant qu'ordinateur à haut niveau de disponibilité

1. Sur LON-HOST1, ouvrez la console Gestionnaire du cluster de basculement.
2. Développez **VMCluster.Adatum.com**, puis cliquez avec le bouton droit sur **Rôles**.
3. Sélectionnez **Ordinateurs virtuels**, puis cliquez sur **Nouvel ordinateur virtuel**.
4. Dans la fenêtre Nouvel ordinateur virtuel, sélectionnez **LON-HOST1**, puis cliquez sur **OK**.
5. Dans l'Assistant Nouvel ordinateur virtuel, dans la page **Avant de commencer**, cliquez sur **Suivant**.
6. Dans la page **Spécifier le nom et l'emplacement**, tapez **22414B-LON-CORE** pour le nom et cliquez sur **Stocker l'ordinateur virtuel à un autre emplacement**. Tapez **\\AdatumFS\VMachines\22414B-LON-CORE**, puis cliquez sur **Suivant**.
7. Dans la page **Affecter la mémoire**, saisissez **768** dans la zone **Mémoire de démarrage**, puis cliquez sur **Suivant**.
8. Dans la page **Configurer la mise en réseau**, sélectionnez **Réseau externe** dans la zone de liste déroulante, puis cliquez sur **Suivant**.
9. Dans la page **Connecter un disque dur virtuel**, cliquez sur **Utiliser un disque dur virtuel existant**, puis sur **Parcourir**. Dans la zone **Nom du fichier**, tapez **\\ADatumFS\VMachines\22414B-LON-CORE**, puis appuyez sur Entrée.
10. Sélectionnez le fichier **22414B-LON-CORE.vhd**, puis cliquez sur **Ouvrir**.
11. Cliquez sur **Suivant**.
12. Dans la page **Fin de l'Assistant Nouvel ordinateur virtuel**, cliquez sur **Terminer**.
13. Dans la **Page de résumé**, vérifiez que le processus indique **Réussite**, puis cliquez sur **Terminer**.
14. Dans le **Gestionnaire de cluster de basculement**, cliquez sur **Rôles**, cliquez avec le bouton droit sur **22414B-LON-CORE**, puis sélectionnez **Redémarrer**. Assurez-vous que l'ordinateur virtuel démarre.
15. Une fois que l'ordinateur démarre, cliquez dessus avec le bouton droit, puis sélectionnez **Connecter**.
16. Dans la fenêtre Connexion à un ordinateur virtuel, cliquez sur le bouton **Ctrl+Alt+Suppr**, puis connectez-vous en tant qu' **Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Exécuter une migration dynamique pour l'ordinateur virtuel

1. Sur LON-HOST2, ouvrez Windows PowerShell®.
2. Dans la fenêtre Windows PowerShell, tapez **ping lon-core -t**, appuyez sur Entrée, puis vérifiez que vous recevez les réponses.
3. Dans le Gestionnaire du cluster de basculement sur LON-HOST2, exécutez une migration dynamique de l'ordinateur virtuel 22414B-LON-CORE, puis déplacez-le vers LON-HOST2.
4. Basculez vers la fenêtre Windows PowerShell, et surveillez les paquets ICMP (Internet Control Message Protocol). Vous ne devez perdre qu'un minimum de paquets (1 ou 2) voire aucun.

▶ Tâche 5 : Valider la haute disponibilité en cas de défaillance du stockage

1. Sur LON-SVR1, dans le Gestionnaire du cluster de basculement, identifiez le propriétaire d'AdatumFS.
2. Dans le Gestionnaire Hyper-V sur LON-HOST1, déconnectez le réseau de l'ordinateur propriétaire d'ADatumFS.
3. Revenez au Gestionnaire du cluster de basculement sur le propriétaire actuel d'AdatumFS, puis vérifiez que le nœud propriétaire a été remplacé par AdatumFS.
4. Basculez vers la fenêtre Windows PowerShell sur LON-HOST2, puis vérifiez qu'aucun paquet n'a été perdu.
5. Reconnectez le réseau à l'ordinateur virtuel que vous avez déconnecté.
6. Sur LON-HOST1, dans le Gestionnaire du cluster de basculement, cliquez avec le bouton droit sur 22414B-LON-CORE, puis cliquez sur **Arrêter**.
7. Sur LON-HOST1 et LON-HOST2, fermez le Gestionnaire du cluster de basculement.

Exercice 6 : Implémenter l'intégration d'Operations Manager et de VMM

Scénario

A. Datum a déployé Operations Manager et VMM et souhaite à présent configurer l'intégration d'Operations Manager et de VMM, et implémenter l'optimisation des performances et des ressources (PRO). Vous allez configurer cette intégration, puis valider l'implémentation PRO.

Les tâches principales de cet exercice sont les suivantes :

1. Importer des packs d'administration.
2. Activer l'intégration de Microsoft System Center 2012 - Virtual Machine Manager (VMM) avec Operations Manager.
3. Valider l'intégration de la fonctionnalité PRO.

▶ Tâche 1 : Importer des packs d'administration

1. Ouvrez Operations Console sur **LON-OM1**, puis accédez au nœud **Packs d'administration**.
2. Importez tous les packs d'administration depuis l'emplacement **\\LON-VMM1\C$\Programmes\Microsoft System Center 2012\Virtual Machine Manager\Management Packs**.

▶ Tâche 2 : Activer l'intégration de Microsoft System Center 2012 - Virtual Machine Manager (VMM) avec Operations Manager

1. Sur **LON-VMM1**, ouvrez la console Virtual Machine Manager, accédez à **Paramètres->Paramètres de System Center**, puis ouvrez **Serveur Operations Manager**. (Remarque : Si la console VMM ne démarre pas, ouvrez les Services à partir des Outils d'administration et vérifiez que tous les services VMM définis pour démarrer automatiquement sont exécutés.)
2. Ajoutez le serveur **Operations Manager lon-om1.adatum.com** à l'aide du compte d'identification **Administrateur**.
3. Surveillez les détails dans la fenêtre Travaux pour vous assurer que le serveur a été correctement ajouté. Si le travail ne s'achève pas correctement, redémarrez LON-OM1 et LON-VMM1 et refaites les étapes 1-2.

▶ Tâche 3 : Valider l'intégration de la fonctionnalité PRO

1. Sur **LON-OM1**, dans l'espace de travail **Analyse**, développez **Analyse** et **PRO**, puis cliquez sur **État de l'objet PRO**.
2. Vérifiez que l'état de LON-VMM1 est Intègre.
3. Sur LON-VMM1, dans la console VMM Manager, ouvrez **Paramètres de System Center**.
4. Dans la fenêtre Paramètres de Operations Manager, cliquez sur **PRO de test**.
5. Dans la fenêtre Travaux, recherchez un travail appelé **Diagnostic PRO**. Sélectionnez-le, puis cliquez sur **Détails**.
6. Assurez-vous que toutes les tâches dans ce travail se sont terminées correctement.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-SVR2**, **22414B-LON-VMM1** et **22414B-LON-OM1**.
5. Sur LON-HOST1, dans la console Gestionnaire de serveur, supprimez la fonctionnalité Clustering avec basculement.
6. Redémarrez LON-HOST1. Lorsque le serveur démarre, choisissez LON-HOST1 dans le menu de démarrage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

1. Évitez d'utiliser un modèle de quorum qui dépend d'un seul disque.
2. Utilisez les CSV pour la haute disponibilité Hyper-V ou le serveur de fichiers avec montée en puissance parallèle.
3. Assurez-vous qu'en cas de défaillance du nœud, d'autres nœuds peuvent gérer la charge.
4. Planifiez soigneusement les clusters multisites.
5. Développez les configurations standard avant d'implémenter les ordinateurs virtuels à haut niveau de disponibilité. Vous devez configurer les ordinateurs hôtes d'une façon aussi similaire que possible. Afin de vous assurer que vous avez une plateforme Hyper-V cohérente, vous devez configurer des noms réseau standard, et utiliser des normes d'affectation de noms cohérentes pour les volumes CSV.
6. Implémentez la protection VMM. VMM fournit une couche de gestion sur Hyper-V et la Gestion du cluster de basculement pouvant vous empêcher de réaliser des erreurs de gestion des ordinateurs virtuels à haut niveau de disponibilité. Par exemple, cela vous empêche de créer des ordinateurs virtuels sur un stockage qui n'est pas accessible à partir de tous les nœuds du cluster.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Le basculement d'ordinateur virtuel échoue une fois que j'implémente CSV et migre le stockage partagé sur CSV.	
Quatre heures après le redémarrage d'un hôte Hyper-V membre d'un cluster hôte, aucun ordinateur virtuel ne s'exécute encore sur l'hôte.	

Questions de contrôle des acquis

Question : Que sont les principaux avantages du serveur de fichiers avec montée en puissance parallèle ?

Question : La migration dynamique requiert-elle l'implémentation d'un cluster ?

Question : Comment répliquez-vous les données dans le stockage dans un cluster multisite ?

Outils

Outils	Utilisation	Emplacement
Gestionnaire du cluster de basculement	À utiliser pour gérer les clusters	Accès à partir des outils d'administration
Windows PowerShell	À utiliser pour la gestion des lignes de commande de Windows Server	Accès à partir des outils d'administration

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Outils	Utilisation	Emplacement
Virtual Machine Manager	À utiliser pour la gestion de l'environnement virtuel	Accès à partir du menu Démarrer
Gestionnaire Hyper-V	À utiliser pour la gestion des ordinateurs virtuels	Accès à partir des outils d'administration

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 9

Planification et implémentation d'une infrastructure de mise à jour de serveur

Table des matières :

Vue d'ensemble du module **9-1**

Leçon 1 : Planification et implémentation d'un déploiement WSUS **9-2**

Leçon 2 : Planification des mises à jour logicielles avec System Center 2012 Configuration Manager **9-12**

Leçon 3 : Planification et implémentation des mises à jour dans une infrastructure de virtualisation de serveur **9-25**

Atelier pratique : Planification et implémentation d'une infrastructure de correction de serveur **9-33**

Contrôle des acquis et éléments à retenir **9-42**

Vue d'ensemble du module

La gestion des mises à jour est une part très importante de toute infrastructure informatique. Il est important d'avoir un système de mise à jour fonctionnel et fiable, de sorte que le client et les serveurs soient à jour et protégés des vulnérabilités. Vous pouvez implémenter l'infrastructure de mise à jour à l'aide de Windows® Server Update Service (WSUS) ou de Microsoft® System Center 2012 Configuration Manager. Vous devez également tenir compte de certaines techniques spéciales pour mettre à jour les environnements virtuels. Dans ce module, vous découvrirez comment planifier et implémenter une infrastructure de mise à jour de serveur à l'aide de WSUS, de Configuration Manager et Microsoft System Center 2012 - Virtual Machine Manager (VMM).

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- planifier et implémenter un déploiement WSUS ;
- planifier des mises à jour logicielles avec Configuration Manager ;
- planifier et implémenter des mises à jour dans une infrastructure de virtualisation de serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification et implémentation d'un déploiement WSUS

Les systèmes d'exploitation et les applications requièrent des mises à jour régulières, et vous devez concevoir l'infrastructure réseau pour déployer ces mises à jour avec le même soin et la même attention que pour déployer ses autres composants. Un manque de conception appropriée de votre stratégie WSUS et de la gestion des mises à jour peut augmenter le risque que le réseau et les ordinateurs de votre organisation soient exposés à des menaces de sécurité externes.

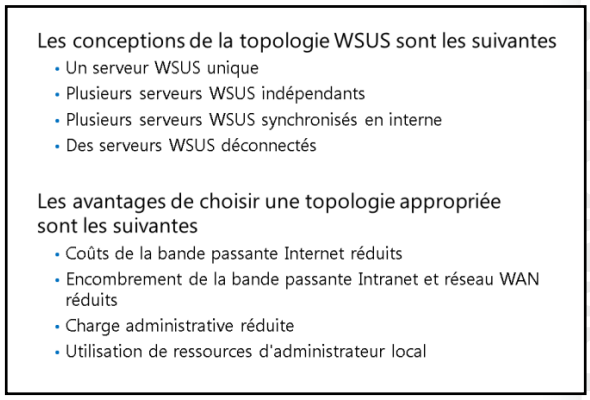
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options de topologie WSUS ;
- décrire les instructions de conception d'une infrastructure WSUS ;
- décrire les éléments à prendre en compte pour configurer des réplicas WSUS ;
- déployer WSUS sur des réseaux isolés ;
- choisir une base de données pour WSUS ;
- sélectionner un emplacement de stockage de mise à jour ;
- planifier la configuration du serveur WSUS ;
- décrire les éléments à prendre en compte pour la gestion du déploiement de la mise à jour.

Options de topologie WSUS

WSUS a un rôle serveur sur des ordinateurs qui exécutent Windows Server 2012. Cependant, il est toujours important de le déployer en utilisant une stratégie de conception appropriée. Si vous utilisez une infrastructure efficace pour déployer les mises à jour logicielles en temps utile, vous pouvez améliorer la fiabilité de vos ordinateurs, et aider à protéger des menaces de sécurité du réseau. Votre conception de WSUS doit comprendre non seulement le placement des serveurs WSUS, mais également la bande passante réseau interne et externe. En outre, vous devez tenir compte de la disponibilité du personnel d'administration de systèmes qui va gérer le processus de déploiement des mises à jour logicielles.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si vous sélectionnez une topologie WSUS appropriée, vous pouvez réduire les coûts en réduisant la quantité de données à télécharger des serveurs Microsoft Update sur Internet. Un administrateur a également moins besoin d'intervenir pour déployer les mises à jour.

La conception et l'implémentation d'une topologie appropriée WSUS fournit les avantages suivants :

- Coût de la bande passante Internet réduit. Si une organisation ne déploie pas WSUS, chaque ordinateur doit récupérer séparément des mises à jour à partir des serveurs Microsoft Update sur Internet. Par exemple, si une organisation a cent ordinateurs ou plus, et que la taille moyenne des mises à jour est de 50 à 100 mégaoctets (Mo) par mois, si chaque ordinateur doit télécharger des mises à jour, la consommation de bande passante est importante. WSUS vous permet de télécharger toutes les mises à jour en une fois sur le réseau interne, puis de les distribuer à partir du stockage de mise à jour serveur WSUS.
- Il réduit l'encombrement de bande passante intranet et réseau étendu (WAN). WSUS peut utiliser le Service de transfert intelligent en arrière-plan (BITS) pour optimiser le transfert de mise à jour vers les clients sur le réseau interne. Le placement d'un serveur WSUS sur chaque site permet aux clients d'obtenir des mises à jour d'une source locale, plutôt que de les récupérer sur une liaison WAN ou de serveurs Microsoft Update sur Internet.
- Il réduit la charge administrative. Vous pouvez déployer des serveurs WSUS en tant que réplicas, quand cela permet à Windows d'approuver une mise à jour en une fois, sur le serveur WSUS principal, pendant que le serveur de réplication télécharge automatiquement des approbations. Cela vous permet de déployer des mises à jour sur tous les ordinateurs de votre organisation, ou sur un groupe d'ordinateurs, à l'aide des groupes d'ordinateurs WSUS. Vous pouvez configurer WSUS pour utiliser des règles d'approbation automatique, ce qui garantit que les mises à jour répondent à des critères spécifiques avant de recevoir l'approbation automatique pour la distribution.
- Il utilise des ressources d'administrateur local. Vous pouvez déployer WSUS dans une configuration autonome ou de réplication. Ces options vous donnent la possibilité d'attribuer aux administrateurs d'un site spécifique la responsabilité d'approuver les mises à jour, ou vous pouvez demander à des administrateurs d'un autre site d'endosser cette responsabilité.

Conceptions de la topologie WSUS

Vous pouvez concevoir votre topologie WSUS et l'adapter à de nombreux scénarios :

- Un seul serveur WSUS. Dans le cas d'un seul serveur WSUS, il faut installer un serveur exécutant WSUS à l'intérieur du pare-feu de l'entreprise. WSUS synchronise le contenu directement avec Microsoft Update, puis distribue des mises à jour aux ordinateurs clients. C'est la topologie la plus simple pour WSUS, et les petites et moyennes entreprises l'utilisent généralement.
- Plusieurs serveurs WSUS indépendants. Dans ce scénario, vous devez déployer plusieurs serveurs pour gérer chaque serveur de manière indépendante, et chaque serveur synchronise son contenu à partir de Microsoft Update. Cette méthode peut être appropriée pour les filiales dans lesquelles vous gérez différents réseaux locaux (LAN) ou segments WAN en tant qu'entités distinctes, ou lorsque vous configurez chaque serveur exécutant WSUS pour déployer des mises à jour uniquement sur les ordinateurs clients qui exécutent un certain système d'exploitation. Toutefois, dans cette topologie, les serveurs WSUS indépendants téléchargeront leur contenu à partir de Microsoft Update séparément.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Plusieurs serveurs WSUS synchronisés en interne. Dans ce scénario, vous devez déployer plusieurs serveurs qui exécutent WSUS et synchroniser tout leur contenu dans l'intranet de leur organisation. Dans ce scénario, vous devez exposer un seul serveur à Internet pour télécharger des mises à jour à partir de Microsoft Update et le configurer en tant que serveur en amont. Il fait donc office de source avec laquelle le serveur en aval se synchronise. Le cas échéant, vous pouvez localiser les serveurs dans tout un réseau géographiquement dispersé pour fournir une meilleure connectivité à tous les ordinateurs clients. Les serveurs WSUS synchronisés en interne peuvent également fonctionner en mode de réplication, dans ce cas les serveurs de réplication synchronisent également des approbations de mise à jour du serveur en amont.
- Serveurs WSUS déconnectés. Ce scénario comprend un serveur interne qui exécute WSUS et ne se connecte pas au réseau, sauf au départ quand il se connecte à Internet pour télécharger les mises à jour. Après le téléchargement, les tests et l'approbation des mises à jour sur ce serveur, un administrateur peut exporter ensuite les métadonnées et le contenu des mises à jour vers le support approprié. Puis, depuis ce support il peut ensuite importer les métadonnées et le contenu des mises à jour sur des serveurs WSUS au sein de l'intranet. Cette méthode, que vous pouvez adapter à toute taille de déploiement, est excellente pour des sociétés ayant des stratégies strictes ou d'autres conditions qui limitent l'accès d'un ordinateur à Internet.

Instructions pour la conception d'une infrastructure WSUS

Lors de la détermination du nombre de serveurs et de leur emplacement
- Connecter un serveur WSUS à Internet
- Chaîner les serveurs WSUS
- Placer les serveurs à proximité des ordinateurs clients

Lors de la détermination de la configuration de serveurs
- Téléchargez les mises à jour dans les langues requises uniquement
- Téléchargez les mises à jour uniquement pour les produits que vous utilisez
- Utilisez une solution de stockage local, ou utilisez Microsoft Update
- Créez un plan de synchronisation pour les téléchargements

Pour simplifier la sécurité, vous pouvez placer un seul serveur WSUS dans un réseau de périmètre, que vous pouvez ensuite utiliser pour fournir des mises à jour à d'autres serveurs WSUS. Lorsque vous configurez le serveur de cette façon, WSUS partage uniquement les mises à jour et les métadonnées avec ses serveurs en aval pendant la synchronisation, et il ne partage pas les informations sur les groupes d'ordinateurs ou les mises à jour qui sont approuvées. Vous pouvez utiliser cette méthode pour télécharger des mises à jour en une fois à partir d'Internet, puis les diffuser aux filiales ayant des serveurs en aval. Cela permet d'économiser de la bande passante Internet.

En règle générale, vous devez placer des serveurs WSUS près des ordinateurs clients, afin de réduire le trafic réseau qui se produit. Par exemple, vous pouvez placer un serveur WSUS dans une filiale. Les mises à jour s'appliquent ensuite sur tous les ordinateurs de la filiale, mais la mise à jour est fournie via la liaison WAN une fois seulement au serveur WSUS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous configurez la synchronisation, téléchargez uniquement les langues requises. Les mises à jour sont disponibles dans plusieurs langues, et le fait de limiter le nombre de téléchargements réduit la bande passante Internet et l'espace de stockage sur le serveur WSUS. En outre, vous devez limiter le nombre de produits que vous mettez à jour. Vous devez sélectionner seulement des systèmes d'exploitation et des applications que vous utilisez dans votre environnement.

Remarque : WSUS télécharge et stocke en général les mises à jour sur un serveur WSUS local. Cependant, si vous spécifiez que vous voulez enregistrer des mises à jour sur Microsoft Update, WSUS agit uniquement en tant que mécanisme qui approuve les mises à jour.

La planification de la synchronisation détermine à quelle fréquence WSUS télécharge des mises à jour. Pour vous assurer d'obtenir des mises à jour critiques aussi rapidement que possible, vous devez configurer WSUS pour synchroniser quotidiennement. Lorsque vous configurez un nouveau serveur WSUS, vous pouvez accélérer la synchronisation initiale en copiant des mises à jour directement entre les serveurs WSUS.

Éléments à prendre en compte pour la configuration des réplicas WSUS

Lorsque vous déployez des serveurs WSUS qui se synchronisent en interne, ils peuvent travailler de manière indépendante ou en mode de réplication. Le serveur de réplication de WSUS hérite des approbations, et peut récupérer des fichiers de mise à jour des serveurs WSUS en amont. Cela réduit la charge administrative en permettant à un ensemble d'approbations d'être diffusée entre tous vos serveurs WSUS.

Vous devez déployer un réplica WSUS lorsque vous souhaitez qu'un serveur hérite des approbations de mise à jour d'un serveur central

En déployant le réplica WSUS tenez compte de ce qui suit

- Le réplica va-t-il obtenir des approbations uniquement à partir du serveur en amont ou obtenir des approbations et des fichiers de mise à jour ?
- Le réplica stocke-t-il les mises à jour localement ?
- Pouvez-vous déployer BranchCache à la place ?

Raisons pour lesquelles déployer un réplica

Vous devez déployer un réplica sur un site si vous souhaitez qu'un serveur hérite des approbations de mise à jour d'un serveur central. Si vous souhaitez que les administrateurs locaux contrôlent le déploiement des mises à jour, vous devez déployer un serveur autonome.

Si votre site local comprend des ordinateurs qui exécutent uniquement des systèmes d'exploitation Windows® 8 Entreprise, Windows® 7 Entreprise, Windows 7 Édition Intégrale, Windows Server® 2008 R2 ou Windows Server® 2012, vous pouvez choisir de déployer Windows BranchCache® au lieu d'un serveur WSUS local. Lorsque vous déployez BranchCache, les clients WSUS peuvent mettre en cache et partager des données de mise à jour récupérées à partir de serveurs WSUS sur des réseaux distants, et vous pouvez réduire le trafic de mise à jour qui transmet sur les liaisons WAN, sans déployer de serveur WSUS de la filiale local.

Remarque : Cette solution n'est pas appropriée si les ordinateurs des filiales exécutent Windows® Vista, Windows® XP, Windows Server® 2003 ou Windows Server 2008.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour le réplica

En configurant un réplica, il y a plusieurs facteurs que vous devez prendre en compte, notamment ce qui suit :

- Le réplica obtiendra des approbations uniquement à partir du serveur en amont ou si vous souhaitez l'activer pour obtenir des approbations et des fichiers de mise à jour. Vous pouvez configurer un réplica pour obtenir des fichiers de mise à jour directement à partir de Microsoft Update plutôt que du serveur en amont.
- Les téléchargements à partir de Microsoft Update se produisent lorsque les liaisons WAN ont une latence élevée ou sont congestionnées.
- Les téléchargements se produisent à partir d'un réplica quand il y a une bonne connectivité entre les sites.
- Le réplica stocke alors les mises à jour localement. Vous pouvez configurer des réplicas de sorte que les clients qui les utilisent pour les approbations obtiennent les mises à jour des serveurs Microsoft Update. Il s'agit d'une configuration courante pour les clients qui accèdent au réseau à distance (come les ordinateurs qui utilisent Windows 8 DirectAccess, par exemple).

Déterminer combien de serveurs WSUS un site requiert

En général, un seul serveur WSUS doit être déployé sur un site. Lorsque vous utilisez des services BITS, un seul serveur WSUS déployé sur Windows Server 2012 ou Windows Server 2008 R2 peut prendre en charge jusqu'à 25 000 clients.

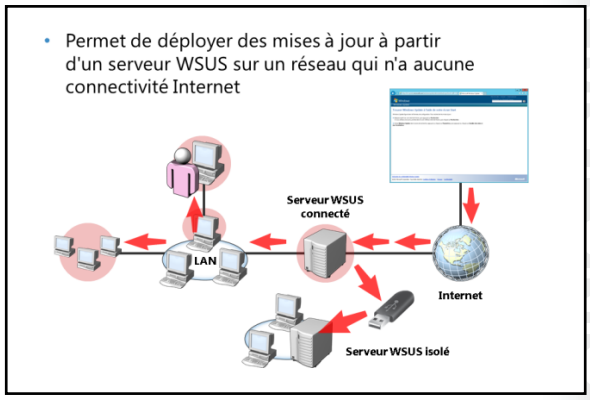
Cependant, dans certains cas, il peut être nécessaire de déployer plusieurs serveurs WSUS sur un site. Par exemple, dans certaines organisations, il est nécessaire d'avoir des infrastructures WSUS distinctes qui permettent à différents groupes de déployer des mises à jour sur les ordinateurs.

Remarque : WSUS 3.0 Service Pack 2 (SP2) ne comprend pas la fonctionnalité de contrôle d'accès basé sur les rôles, ce qui signifie qu'un utilisateur qui est autorisé à approuver des mises à jour peut les approuver sur tous les ordinateurs qui sont clients du serveur WSUS.

Déploiement de WSUS sur des réseaux isolés

Si votre entreprise possède un réseau sécurisé déconnecté, vous pouvez utiliser WSUS dans la création du déploiement de mise à jour.

Remarque : Vous pouvez renforcer la sécurité à l'aide de réseaux sécurisés déconnectés pour garantir que les ordinateurs ne peuvent pas accéder à Internet directement ou aux réseaux avec l'accès à Internet.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Bien que les ordinateurs ne puissent pas accéder à Internet directement, cette opération ne le rend pas moins vulnérables à une attaque. Bien qu'il soit impossible d'offrir une protection contre toute attaque réseau, vous pouvez atténuer le risque de ces attaques potentielles en vérifiant que les ordinateurs de réseaux déconnectés soient mis à jour via WSUS de la même manière que ceux connectés aux réseaux.

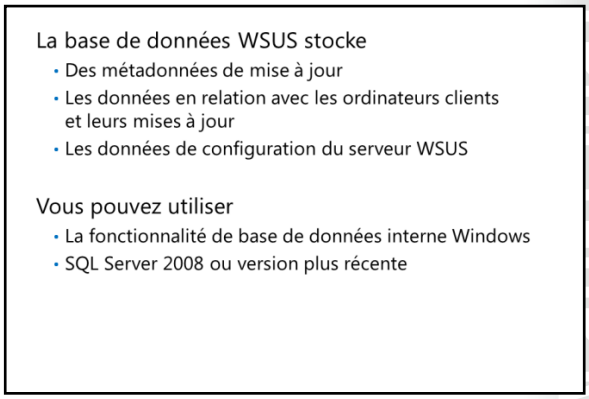
Pour configurer WSUS pour utiliser un réseau déconnecté, vous devez créer et implémenter la procédure suivante :

1. Placez un serveur WSUS sur un réseau connecté à Internet, de sorte qu'il puisse récupérer des mises à jour des serveurs Microsoft Update ou d'un serveur en amont.
2. Placez un second serveur WSUS sur le réseau déconnecté.
3. Configurer les deux serveurs WSUS avec les mêmes options avancées.
4. Vérifiez que le serveur WSUS connecté enregistre les mises à jour localement.
5. Transférez les fichiers de mise à jour du système de fichiers connecté au serveur WSUS à l'aide de supports amovibles, puis copiez ces mises à jour dans le même répertoire sur le serveur WSUS déconnecté.
6. Transférez les métadonnées de la base de données du serveur WSUS connecté à l'aide du support amovible.
7. Importer les mises à jour vers le serveur WSUS sur le réseau déconnecté.

Choix d'une base de données pour un serveur WSUS

Chaque serveur WSUS que vous déployez requiert une base de données, qu'il utilise pour stocker les informations suivantes relatives à votre infrastructure de mise à jour :

- Les métadonnées qui définissent les propriétés des mises à jour.
- Les données en relation avec les ordinateurs clients et leurs mises à jour.
- Les données de configuration du serveur WSUS.



Cependant, vous n'avez pas besoin d'avoir de compétences en administration Microsoft SQL Server® pour gérer cette base de données, car vous l'administrez entièrement via l'interface de WSUS. En outre, nous déconseillons de gérer WSUS en accédant directement aux données dans la base de données. Vous devez gérer WSUS manuellement à l'aide de la console WSUS ou par programme en appelant des interfaces de programmation d'applications (API) de WSUS.

Chaque serveur WSUS a besoin de sa propre base de données. Si vous déployez plusieurs serveurs WSUS dans votre environnement, vous devez avoir une base de données WSUS pour chaque serveur. En outre, nous ne prenons pas en charge le fait d'avoir plusieurs bases de données WSUS sur une instance unique SQL Server. La seule exception est le cas du cluster réseau dont la charge est équilibrée qui utilise un cluster de basculement SQL Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez utiliser n'importe quelle base de données compatible SQL Server pour prendre en charge cette exigence, mais seulement deux bases de données ont subi une série étendue de tests avec WSUS :

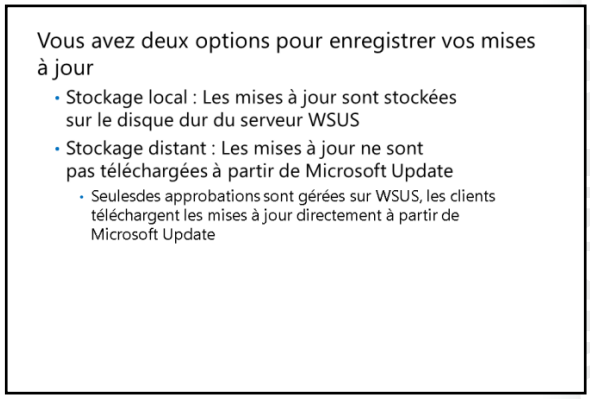
- Base de données interne Windows. Cette base de données fait partie du système d'exploitation Windows, et fournit une solution rentable de base de données pour les petits déploiements de WSUS.
- SQL Server 2008 ou version plus récente. Cette solution de base de données complète offre une meilleure fiabilité et de meilleures performances par rapport à la base de données interne de Windows. En outre, elle est mieux orientée vers de plus grands déploiements de WSUS.

Pour un plus petit déploiement de WSUS, elle est suffisante pour déployer la base de données interne de Windows, qui se déploie avec WSUS. Vous n'avez donc pas à l'installer séparément. Pour les déploiements dans des environnements d'entreprise, ou des déploiements où vous souhaitez avoir de la haute disponibilité, vous devriez utiliser SQL Server.

Sélection d'un emplacement de stockage de mise à jour

Les mises à jour se composent de deux éléments : les métadonnées qui décrivent la mise à jour et les fichiers de mise à jour réels. Bien que les bases de données stockent les métadonnées de mise à jour, le système de fichiers stocke les fichiers de mise à jour.

Quand vous déterminez comment vous souhaitez stocker les mises à jour, vous avez deux options. Vous pouvez utiliser le stockage local qui est connecté au serveur WSUS, ou vous pouvez utiliser le stockage distant.



Stockage local

Pour utiliser le stockage local, vous devez posséder un stockage local suffisant pour stocker toutes les mises à jour requises. Nous recommandons 30 gigaoctets (GB) ou plus à cet effet.

Stockage distant

Dans ce cas, le serveur WSUS stocke uniquement les métadonnées relatives aux mises à jour, alors que celles-ci restent sur le serveur Microsoft Update. Les clients utilisent le serveur WSUS pour obtenir des métadonnées de mise à jour et recevoir les instructions quant aux mises à jour à obtenir. Cependant, ils obtiennent ces mises à jour à partir du serveur Microsoft Update directement.

Selon votre scénario d'utilisation, vous devrez décider quelle solution de stockage à choisir. Chaque approche présente ses avantages et ses inconvénients. Si vous choisissez d'utiliser le stockage local pour les mises à jour, le plus grand avantage est que les ordinateurs clients téléchargeront les mises à jour d'un serveur local, et non d'Internet. Cependant, vous devez consacrer le stockage pour des mises à jour sur le serveur WSUS et vous assurer que tous les clients ont une bonne connexion au serveur WSUS.

Si vous choisissez d'utiliser le stockage distant, tous les clients téléchargeront les mises à jour que vous approuvez sur WSUS, à partir de Microsoft Update, et non du serveur WSUS local. Cela peut ajouter beaucoup de trafic sur votre lien Internet. Cependant, si vous distribuez largement vos clients et que vous n'avez pas les bonnes connexions entre les sites, cela peut être solution acceptable.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification de la configuration et de la gestion de serveur WSUS

Lorsque vous planifiez votre déploiement de serveur WSUS, vous devez organiser la configuration matérielle et logicielle pour l'ordinateur serveur qui hébergera le service WSUS. WSUS est un service très exigeant, et les conditions requises pour le déploiement peuvent varier selon les mises à jour que vous prévoyez de distribuer.

La configuration matérielle minimale requise pour le déploiement WSUS est la suivante
- Processeur : Processeur x64 de 1,4 GHz (2 GHz ou plus recommandé)
- Mémoire : Au moins 2 Go de mémoire RAM
- Espace disque disponible : 10 GB (40 GB ou plus recommandé)
- Carte réseau : 100 Mbits/s ou plus

Vous devez planifier l'espace de disque-dur selon la structure des mises à jour que vous déployez

Vous pouvez gérer WSUS à l'aide de Server Manager ou de Windows PowerShell

La configuration minimale prise en charge pour un déploiement de WSUS est :

- Processeur : 1,4 gigahertz (GHz) (x64). Nous recommandons 2 GHz ou plus.
- Mémoire : au moins 2 Go de mémoire RAM.
- Espace disque disponible : 10 Go. Nous recommandons 40 Go ou plus.
- Carte réseau : 100 mégabits par seconde (Mbits/s) ou plus.

L'espace disque est la ressource matérielle la plus importante que vous devez prévoir, et les conditions requises pour l'espace disque varient considérablement selon la structure des mises à jour que vous prévoyez de distribuer. Par exemple, vous pouvez choisir de déployer uniquement la mise à jour du système d'exploitation dans une seule langue. Dans ce scénario, vos besoins en espace disque ne seront pas plus élevés que la configuration recommandée dans la section précédente. Inversement, si vous souhaitez déployer la mise à jour pour plusieurs produits, dans plusieurs langues, vos besoins d'espace disque augmentent considérablement.

WSUS est maintenant un rôle dans Windows Server 2012, vous ne devez donc pas le télécharger séparément du Centre de téléchargement Microsoft. Par conséquent, toutes les conditions requises sont installées par le Gestionnaire de serveurs pendant l'installation de WSUS. En outre, WSUS requiert que vous installiez Internet Information Services (IIS) et la base de données interne Windows, si vous choisissez de ne pas utiliser SQL Server comme moteur de base de données.

En outre, vous pouvez gérer WSUS à l'aide de la console Gestionnaire de serveur, et dans Windows Server 2012, Microsoft fournit les applets de commande Windows PowerShell® que vous pouvez utiliser pour gérer les 10 tâches d'administration de WSUS les plus importantes. En outre, une amélioration de la sécurité WSUS dans Windows Server 2012 est l'ajout de la fonction de hachage SHA256.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour la gestion du déploiement de la mise à jour

Il est très important de concevoir votre plan de déploiement de mise à jour correctement, et chaque plan de déploiement de mise à jour doit impliquer quatre grandes phases :

Un plan de déploiement doit comprendre les activités suivantes

1. Spécification des mises à jour à déployer
2. Tests des mises à jour avant le déploiement
3. Tests des mises à jour avant le déploiement
4. Vérification du déploiement d'une mise à jour

Assurez-vous que le groupe de tests représente fidèlements votre environnement de production

Planifierdes approbations automatiques pour les mises à jour soigneusement

- Détermination des mises à jour que vous devez déployer. Microsoft publie régulièrement des bulletins de sécurité que vous pouvez consulter pour déterminer l'étendue et l'impact de toutes les nouvelles mises à jour.
- Tests des mises à jour avant le déploiement. Les organisations doivent développer une infrastructure de test qui représente les configurations logicielles diverses actuelles sur leurs ordinateurs. Il est nécessaire de déterminer si vous allez tester l'infrastructure dans un environnement virtuel, ou si vous allez tester des mises à jour à l'aide de déploiements limités à des ordinateurs dynamiques.
- Déploiement des mises à jour à tous les ordinateurs concernés. Votre plan de gestion des mises à jour doit déterminer la manière dont vous déploierez les mises à jour sur les ordinateurs concernés. La méthode de déploiement doit réduire les efforts, tout en garantissant que les mises à jour sont déployées de manière fiable. Vous devez avoir un plan qui comprend du temps alloué aux administrateurs pour déployer les mises à jour que Microsoft publie régulièrement le deuxième mardi de chaque mois. En outre, vous devez avoir des plans d'urgence pour le déploiement rapide des mises à jour hors plage, que Microsoft publie avant la diffusion planifiée classique des mises à jour.
- Vérification du déploiement d'une mise à jour. Votre plan de gestion des mises à jour doit impliquer une procédure de vérification post-déploiement, afin de pouvoir vérifier que les mises à jour ont été déployées sur les ordinateurs nécessaires. En outre, votre stratégie de vérification doit comprendre l'utilisation d'une technologie appropriée qui peut vérifier l'installation des mises à jour, et d'une planification pour savoir à quel moment vérifier les ordinateurs de votre réseau pour déterminer s'ils ont les mises à jour critiques manquantes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

En tant qu'administrateur réseau, vous devez veiller à déployer à la fois des mises à jour qui atténuent les risques de sécurité et veiller à ce qu'elles ne provoquent pas de conflits avec des fonctionnalités existantes. En développant votre stratégie de mise à jour et de déploiement pour prendre en charge cette exigence, tenez compte des facteurs suivants :

- Comprendre à quoi s'adresse la mise à jour et son impact. Microsoft publie des bulletins de notification avant la version finale des mises à jour, ils comprennent également des informations détaillées sur leur contenu. Les administrateurs doivent prendre le temps d'étudier ces bulletins de mise à jour et de déterminer quel impact elles auront sur la configuration existante dans leur organisation. Ces informations incluent l'estimation de la gravité de la mise à jour (critique ou importante), et les logiciels que la mise à jour affectera.

 **Remarque :** Il est important de savoir qu'une mise à jour que vous déployez sur vos ordinateurs peut provoquer des conséquences inattendues. Soyez très prudent lorsque vous envisagez de déployer des mises à jour sur les serveurs. Si un ordinateur serveur devient non disponible en raison de problèmes provenant des mises à jour, l'incidence sur votre infrastructure réseau peut être plus importante qu'elle le serait sur un ordinateur client unique.

- Testez les mises à jour avant le déploiement global. Vos administrateurs doivent créer un groupe de tests des ordinateurs ou des serveurs sur lesquels tester les mises à jour, et ces tests doivent :
    - Inclure des groupes qui sont représentatifs de la configuration de votre organisation dans son ensemble.
    - S'effectuer assez longtemps pour garantir qu'aucun problème critique ne se produise. Cependant, la durée d'un test ne doit pas être trop longue et retarder considérablement le déploiement d'une mise à jour.
    - Ne retardez pas trop le déploiement des mises à jour critiques. En moyenne, il faut environ 6 à 10 jours entre la sortie d'une mise à jour pour une vulnérabilité non divulguée et l'exploitation du code libéré qui cible cette vulnérabilité.
- Créez des règles de déploiement automatique. Vous pouvez utiliser des règles d'approbation automatique pour automatiser le déploiement de mises à jour spécifiques. Lorsque vous planifiez l'utilisation de règles d'approbation automatique, vous devez tenir compte de ce qui suit :
    - WSUS peut approuver automatiquement certaines mises à jour, telles que des mises à jour des définitions de programmes malveillants.
    - La configuration des règles d'approbation automatique convient pour les groupes de tests, car cela leur garantit de recevoir de nouvelles mises à jour dès que possible.
    - Les paramètres WSUS par défaut approuvent automatiquement les mises à jour sur WSUS et sur les produits qui sont approuvés. Vous devez désactiver ces options si vous êtes préoccupé par le déploiement de mises à jour que vous n'avez pas testées rigoureusement sur des configurations logicielles utilisées par votre organisation.
    - Vous devez faire attention quand vous utilisez des règles d'approbation automatiques pour déployer des mises à jour sur tous les ordinateurs de votre organisation, sans avoir au préalable testé ces mises à jour. Vous ne découvrirez aucun conflit tant que la mise à jour n'est pas déployée dans toute votre organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2

Planification des mises à jour logicielles avec System Center 2012 Configuration Manager

À l'aide de la fonctionnalité de mise à jour logicielle de Configuration Manager 2012, vous pouvez implémenter un processus de bout en bout pour gérer la tâche complexe du suivi et de l'application des mises à jour logicielles sur vos clients Configuration Manager. Configuration Manager 2012 utilise la fonctionnalité WSUS pour synchroniser, surveiller, et déployer des mises à jour logicielles sur les clients Configuration Manager dans un environnement réseau. Pour gérer et dépanner le processus de mise à jour logicielle efficacement, il est important de comprendre comment s'effectue l'intégration entre Configuration Manager 2012 et WSUS.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les mises à jour logicielles ;
- décrire les conditions préalables pour implémenter la fonctionnalité de mise à jour logicielle ;
- décrire le déploiement de la fonctionnalité de mise à jour logicielle ;
- décrire comment fonctionne la fonctionnalité de mise à jour logicielle ;
- configurer le point de mise à jour logicielle ;
- configurer le déploiement de mise à jour logicielle ;
- sélectionner une technologie de gestion des mises à jour.

Vue d'ensemble de la fonctionnalité de mise à jour logicielle dans Configuration Manager

Les organisations utilisent souvent WSUS comme principale solution pour rester à jour et gérer les sorties fréquentes des mises à jour de sécurité, des mises à jour de logiciel, et de Service Packs. Configuration Manager incorpore le moteur WSUS, qui fournit une base pour une solution complète de mise à jour pour des périphériques client Configuration Manager.

La fonctionnalité de mise à jour logicielle dans Configuration Manager analyse, puis déploie des mises à jour logicielles sur les ordinateurs clients

Le mode de mise à jour de Configuration Manager prend en charge ce qui suit

- Un déploiement de mise à jour transparent et flexible
- Des règles de déploiement automatique
- Une surveillance et des rapports améliorés
- La prise en charge de la gestion de l'alimentation et de Wake-on-LAN
- Une gestion cliente basée sur Internet
- La prise en charge des connexions NAP
- Un éditeur de mises à jour de System Center

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

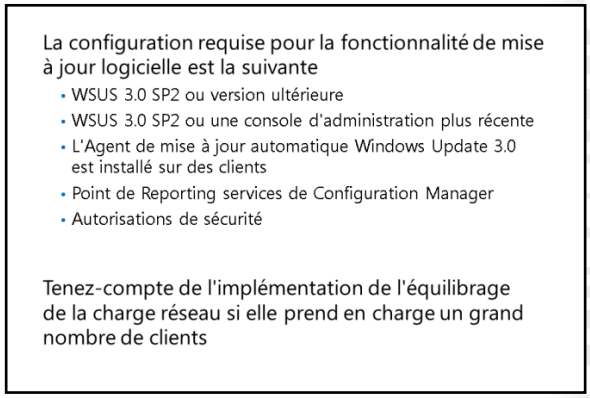
L'intégration de WSUS avec Configuration Manager 2012 fournit de nombreux avantages, notamment :

- Un déploiement de mise à jour transparent et flexible. La fonctionnalité de mise à jour logicielle fournit des fonctionnalités pour rechercher des mises à jour requises, analyser des résultats, et déployer des mises à jour sur des ordinateurs clients. En outre, vous pouvez également intégrer la fonctionnalité de mise à jour logicielle avec d'autres fonctionnalités de Configuration Manager, telles que les bases de référence de conformité et dans des séquences de tâches de déploiement du système d'exploitation. Les fenêtres de maintenance basées sur les collections permettent de s'assurer que les mises à jour sont appliquées uniquement au cours des périodes de maintenance approuvées, pour répondre aux contrats de niveau de service de l'organisation.
- Règles de déploiement automatique. Configuration Manager prend en charge l'approbation et le déploiement automatiques des mises à jour logicielles selon des règles de déploiement automatique. Cela garantit que les mises à jour qui répondent à des critères spécifiques sont déployées aussi rapidement que possible vers les ordinateurs clients, avec un effort administratif minimal.
- Surveillance et rapports améliorés. Configuration Manager offre des fonctions étendues d'analyse, telles que les messages d'état détaillés, les mises à jour d'état, et les alertes pour les principaux problèmes de mise à jour logicielle. Un nombre étendu de rapports est fourni pour afficher l'état du déploiement et les statistiques de conformité des mises à jour dans toute l'organisation.
- Prise en charge de la gestion de l'alimentation et de Wake-on-LAN. Configuration Manager inclut la prise en charge de la technologie Wake-on-LAN. Cette fonctionnalité permet de déployer des mises à jour logicielles après les heures de bureau sans avoir à laisser les ordinateurs allumés et consommer du courant inutilement. La gestion de l'alimentation permet également d'utiliser des modes de gestion qui comprennent des spécifications de mise en veille et de sortie de veille.
- Gestion cliente basée sur Internet. Vous pouvez déployer des mises à jour logicielles sur des clients basés sur Internet et l'intranet. Cela évite aux utilisateurs d'avoir à se connecter au réseau d'entreprise interne pour obtenir les dernières mises à jour approuvées. Cependant, la gestion cliente basée sur Internet nécessite des conditions préalables supplémentaires d'infrastructure, telles que la configuration HTTPS, ainsi qu'une infrastructure à clé publique (PKI).
- Prise en charge de la protection d'accès réseau (NAP). Avec l'intégration de NAP Windows Server 2012 et du rôle de système de site de point du programme de validation d'intégrité système, vous pouvez définir quelles mises à jour logicielles sont requises pour que les ordinateurs se connectent et communiquent avec les ressources réseau. Les mises à jour logicielles de Configuration Manager peuvent fournir des services WSUS aux ordinateurs qui ne respectent pas les stratégies NAP et ne fournissent pas les mises à jour logicielles nécessaires pour assurer la conformité du client.
- Éditeur de mises à jour de System Center. L'éditeur de mises à jour de System Center est un outil autonome que vous pouvez utiliser pour importer des fichiers de catalogue de mise à jour logicielle fournis par des éditeurs de logiciels indépendants. Vous pouvez ensuite importer des catalogues pour publier des mises à jour spécifiques au fournisseur sur les ordinateurs clients.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Conditions préalables à l'implémentation de la fonctionnalité de mise à jour logicielle

Vous devrez peut-être installer et configurer plusieurs éléments prérequis avant d'utiliser la fonctionnalité de mise à jour logicielle de Configuration Manager, notamment :



- WSUS 3.0 SP2 ou version ultérieure.
  Les mises à jour logicielles nécessitent WSUS 3.0 SP2 ou version ultérieure pour la synchronisation du catalogue et pour l'analyse de l'évaluation de conformité aux mises à jour logicielles sur les clients. Vous devez installer WSUS et les éléments prérequis appropriés sur un système avant de le configurer en tant que rôle de système de site de point de mise à jour logicielle Configuration Manager. WSUS 3.0 SP2 peut prendre en charge jusqu'à 100 000 clients sur l'ordinateur de point de mise à jour logicielle lorsqu'il ne coexiste pas avec un autre rôle de système de site.
- WSUS 3.0 SP2 ou une console d'administration plus récente. Si vous installez WSUS sur un serveur autre que le serveur de site, vous devez également installer la console d'administration WSUS sur le serveur du site Configuration Manager. Vous devez le faire pour permettre au serveur de site et au serveur WSUS de communiquer.
- L'Agent de mise à jour automatique Windows Update 3.0 est installé sur des clients.
  Le client Agent de mise à jour automatique Windows Update est requis sur les clients, et il se connecte au serveur WSUS 3.0 pour récupérer la liste des mises à jour logicielles. L'installation du client Configuration Manager met automatiquement l'Agent de mise à jour automatique Windows Update à niveau, si nécessaire. Toutefois, si cette mise à niveau échoue, vous devez utiliser une autre méthode, telle que la gestion des applications, pour mettre l'Agent de mise à jour automatique Windows Update à niveau sur le client. Vous devez vérifier que les ordinateurs clients ont la version requise pour l'Agent de mise à jour automatique Windows Update.
- Équilibrage de la charge réseau. Bien que ceci ne soit pas une connaissance préalable ou obligatoire, si votre point de mise à jour logicielle prend en charge plus de 100 000 ordinateurs clients, vous devez configurer WSUS sur plusieurs ordinateurs dans un cluster d'équilibrage de la charge réseau, puis configurer ce cluster comme point de mise à jour logicielle actif.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Point de Reporting services de Configuration Manager. Bien que ceci ne fasse pas partie des principales connaissances préalables, avant de pouvoir utiliser des rapports de mises à jour logicielles, vous devez configurer un système de site de point Reporting services. Cependant, comme d'autres fonctionnalités de Configuration Manager requièrent ce point de Reporting services, il sera probablement déjà déployé dans votre infrastructure.
- Des autorisations de sécurité. Pour configurer le rôle de système de site de point de mise à jour logicielle, vous devez avoir le rôle de sécurité intégral d'administrateur. Pour déléguer la gestion des mises à jour logicielles, vous devez associer les utilisateurs administratifs avec le rôle de sécurité Gestionnaire des mises à jour logicielles. Le rôle de sécurité Gestionnaire des mises à jour logicielles permet de définir et de déployer des mises à jour logicielles aux clients. Ce rôle de sécurité fournit également des autorisations pour créer et modifier des packages de mise à jour logicielle, des groupes de mise à jour logicielle, des modèles de déploiement, et la possibilité d'activer les mises à jour logicielles pour la protection d'accès réseau.

Vue d'ensemble du déploiement de la fonctionnalité de mise à jour logicielle

La fonctionnalité de mise à jour logicielle se compose de deux composants principaux que vous devez installer et configurer : WSUS 3.0 SP2 et le point de mise à jour logicielle actif.

- Activez la fonctionnalité de mises à jour logicielles en installant et en configurant WSUS 3.0 SP2 ou une version plus récente, et un point actif de mise à jour logicielle
- Tenez compte des configurations spéciales en déployant WSUS pour Configuration Manager
- Assurez-vous de sécuriser le point de mise à jour logicielle

WSUS 3.0 SP2

Vous devez installer WSUS 3.0 SP2 sur tous les systèmes du site que vous configurerez avec le rôle de système de site de point de mise à jour logicielle. Si vous avez un serveur WSUS existant, vous pouvez l'utiliser. Cependant, notez que Configuration Manager n'utilisera ni des groupes d'ordinateurs WSUS existants, ni les mises à jour qui ont été approuvées dans WSUS pour être déployées automatiquement dans Configuration Manager.

Vous devriez tenir compte des points supplémentaires suivants en installant WSUS pour Configuration Manager :

- Si le point de mise à jour logicielle n'est pas installé sur le système de serveur de site, vous devez alors y installer la console d'administration WSUS. Cela permet d'établir la communication requise entre le serveur de site et les composants WSUS sur le serveur WSUS distant.
- Pendant la procédure d'installation de WSUS, vous devez choisir d'enregistrer des mises à jour localement. Lorsque vous sélectionnez cette option, les termes du contrat de licence associés aux mises à jour logicielles sont téléchargés sur le partage de contenu WSUS pendant la synchronisation. Lorsque des clients recherchent des mises à jour applicables, ils ont besoin d'accéder à tous les termes du contrat de licence qui peuvent être associés à ces mises à jour.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- WSUS nécessite l'utilisation d'une base de données, telle que la base de données interne Windows ou SQL Server. Si vous avez besoin d'utiliser NLB, vous devez utiliser SQL Server comme base de données.
- Pendant l'installation de WSUS, vous êtes invité à choisir entre utiliser le site Web par défaut ou laisser l'installation créer un site Web WSUS 3.0 personnalisé. Vous devez choisir de créer un site Web personnalisé pour WSUS si un autre site Web existe déjà sur le serveur. Si vous choisissez ce paramètre, les numéros de port par défaut sont le port 8530 pour HTTP et 8531 pour HTTPs (HTTP/Secure). Vous devez fournir ces nouveaux numéros de port lorsque vous configurez le point de mise à jour logicielle actif.

Le rôle système pour le site de point de mise à jour logicielle

Après avoir installé WSUS 3.0 SP2, vous pouvez ensuite installer et configurer le rôle système de point de mise à jour logicielle actif pour le site.

Tenez-compte des facteurs suivants lorsque vous installez et configurez le rôle système de site de point de mise à jour logicielle :

- Selon l'emplacement où vous installez WSUS, vous devez ajouter et configurer un nouveau serveur de système de site ou ajouter le rôle serveur de point de mise à jour logicielle à un serveur existant de système de site.
- Si le serveur requiert des paramètres de proxy pour se connecter à Internet, vous pouvez indiquer le nom du serveur proxy, le port, et les informations d'identification requises pendant la tâche d'installation du point de mise à jour logicielle.
- Si vous configurez WSUS pour utiliser un site Web personnalisé, veillez à spécifier les numéros de port appropriés lorsque vous configurez le point de mise à jour logicielle actif.
- Déterminez si vous allez configurer la source de synchronisation, la planification de synchronisation, les classifications, les produits, les paramètres de remplacement et les paramètres de langues pendant l'installation du point de mise à jour logicielle ou à partir des paramètres de configuration du composant du point de mise à jour logicielle après la première installation. Notez que vous pouvez uniquement configurer ces paramètres sur le point actif de la mise à jour logicielle du site.

Vous trouverez des informations concernant l'installation du point de mise à jour logicielle dans le fichier SUPSetup.log dans <ConfigurationManagerInstallationPath>\logs dans le système de site de point de mise à jour logicielle.

Après avoir installé le point de mise à jour logicielle, vous pouvez examiner et modifier les paramètres en effectuant les tâches suivantes :

1. Dans la console **System Center 2012 Configuration Manager**, cliquez sur l'espace de travail **Administration**.
2. Dans le volet de navigation, développez **Configuration du site**, puis cliquez sur **Sites**. Dans le volet des résultats, cliquez avec le bouton droit sur un site, placez la souris sur **Configurer les composants de site**, puis cliquez sur **Point de mise à jour logicielle**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

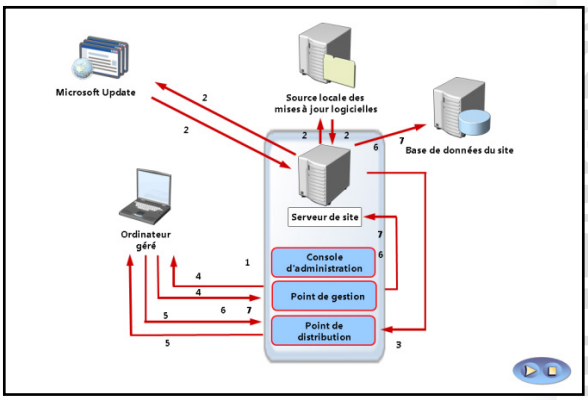
Sécurisation du rôle système pour le site de point de mise à jour logicielle

Si vous devez fournir une communication protégée au point de mise à jour logicielle, vous devez tenir compte de plusieurs choses, notamment ce qui suit :

- Vous devez attribuer un certificat de signature de serveur Web au site Web que WSUS utilise.
- Vous devez configurer plusieurs répertoires virtuels Internet Information Services (IIS) pour utiliser Secure Sockets Layer (SSL). Ces répertoires comprennent APIRemoting30, ClientWebService, DSSAuthWebService, ServerSyncWebService, et SimpleAuthWebService.
- Vous devez utiliser l'outil WSUSUtil pour configurer WSUS pour utiliser SSL. Sur le serveur WSUS, exécutez ce qui suit :
  - WSUSUtil.exe configuressl <FQDN intranet du système de site de point de mise à jour logicielle>
- Les ordinateurs clients doivent approuver le certificat de site Web de WSUS, qui doit se trouver dans le magasin local Autorités de certification racines de confiance.
- Vous devez sécuriser la communication entre le serveur de site et le point de mise à jour logicielle en sélectionnant l'option **Activer les communications SSL pour le serveur WSUS** sur l'onglet **Général** de la boîte de dialogue **Propriétés du composant du point de mise à jour logicielle**.

Fonctionnement de la fonctionnalité de mise à jour logicielle

Lorsque vous déployez des mises à jour logicielles sur les ordinateurs clients, les informations de déploiement de mises à jour logicielles sont ajoutées à la stratégie de l'ordinateur Configuration Manager. L'ordinateur client reconnaît le déploiement lors du prochain cycle de récupération et d'évaluation de stratégie d'ordinateur. Le paramètre par défaut du cycle est fixé toutes les 60 minutes.



Pour déployer les mises à jour logicielles sur les ordinateurs clients, vous devez d'abord créer un package de déploiement. Vous pouvez créer un package de déploiement en exécutant l'Assistant Déploiement des mises à jour logicielles, que vous pouvez invoquer en sélectionnant des mises à jour spécifiques, ou en sélectionnant un groupe de mises à jour logicielles, puis en cliquant sur **Déployer** dans le ruban.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le processus de déploiement de mises à jour logicielles comprend ce qui suit :

1. Dans la console System Center 2012 Configuration Manager, vous devez utiliser l'Assistant Déploiement des mises à jour logicielles pour créer un package de déploiement. Le package de déploiement définit de nombreux paramètres, notamment :
   - Des mises à jour logicielles ou des groupes de mises à jour logicielles compris dans le déploiement.
   - Une collection visée par ce déploiement.
   - Des paramètres de déploiement, par exemple si les mises à jour sont requises ou disponibles ou pas, et si la fonction Wake-on-LAN doit être utilisée.
   - La planification du déploiement qui indique quand le logiciel est disponible ainsi que la date butoir d'installation.
   - L'expérience utilisateur, comme le comportement de redémarrage et les notifications.
   - Des paramètres d'alerte.
   - Des paramètres pour le téléchargement et l'installation dans les réseaux lents.
   - Un emplacement et des points de distribution pour les sources de package.
   - Déterminer si le téléchargement des mises à jour logicielles doit s'effectuer à partir d'Internet ou d'un emplacement réseau.
   - La sélection de la langue pour les mises à jour.
2. Le serveur de site demande les binaires de mises à jour logicielles à partir du site de téléchargement que vous définissez dans le déploiement. Ces binaires peuvent provenir de Microsoft Update ou d'une source locale.
3. Le serveur de site copie les binaires de mises à jour logicielles dans la bibliothèque de contenu sur le point de distribution. Le serveur de site ajoute également le nouveau déploiement des mises à jour logicielles à la stratégie d'ordinateur.
4. Au moment de l'interrogation de la stratégie du client, celui-ci récupère la stratégie d'ordinateur à partir du point de gestion, et reçoit les nouvelles informations de déploiement.
5. Si le catalogue de mises à jour logicielles a changé, le client analyse alors chaque mise à jour pour vérifier si elle est encore requise. Si le type de déploiement de mise à jour logicielle est configuré comme Requis, le client demande les binaires du point de distribution pour chaque mise à jour requise, puis les enregistre dans le cache local. Si le type de déploiement est configuré comme Disponible, les mises à jour sont téléchargées lorsque l'utilisateur invoque l'installation.

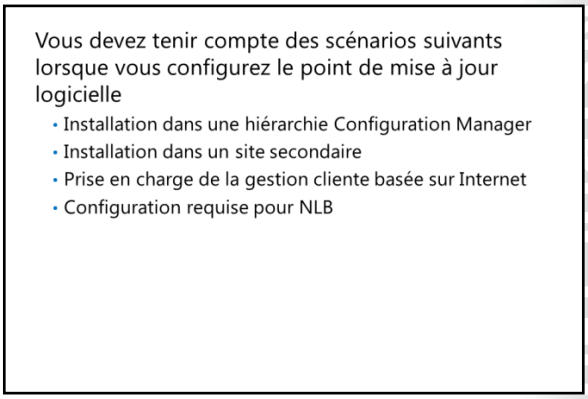
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Le client envoie un message d'état au point de gestion et indique que la mise à jour logicielle a été téléchargée. Le point de gestion transfère le message d'état au serveur de site, qui entre ensuite le message dans la base de données.
7. Lorsque la date butoir de l'installation des mises à jour logicielles est atteinte ou quand vous initialisez l'installation des mises à jour manuellement, le client analyse chaque mise à jour logicielle pour vérifier si elles sont encore requises. Le client installe la mise à jour logicielle, exécute une autre analyse sur le client pour s'assurer que la mise à jour n'est plus requise, puis envoie un message d'état au point de gestion qui indique que la mise à jour a été installée. Si un redémarrage est nécessaire, le message d'état indique que l'ordinateur client est en attente d'un redémarrage. Après le redémarrage, une analyse est initialisée pour vérifier que la mise à jour logicielle n'est plus requise et pour créer un message d'état pour indiquer que la mise à jour a été installée. Pour chaque échec d'installation de mise à jour logicielle, un message d'état d'erreur est envoyé au point de gestion. Le point de gestion transfère ensuite ce message au serveur de site, qui l'insère dans la base de données.

Les ordinateurs clients lancent un cycle de réévaluation du déploiement tous les sept jours, par défaut. Pendant ce processus d'évaluation, l'ordinateur client analyse les mises à jour logicielles précédemment déployées et installées. Si certaines sont manquantes, WSUS les réinstalle.

Configuration du point de mise à jour logicielle

Le point de mise à jour logicielle est un rôle de système de site Configuration Manager qui intègre WSUS avec l'infrastructure de Configuration Manager pour fournir la gestion des mises à jour logicielles. Vous pouvez configurer un point de mise à jour logicielle actif pour le site et il synchronisera les mises à jour à partir de Microsoft Update ou d'un point de mise à jour logicielle en amont. Les clients Configuration Manager utilisent ensuite le point de mise à jour logicielle actif pour faciliter l'évaluation de la conformité des mises à jour logicielles et l'analyse d'évaluation.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

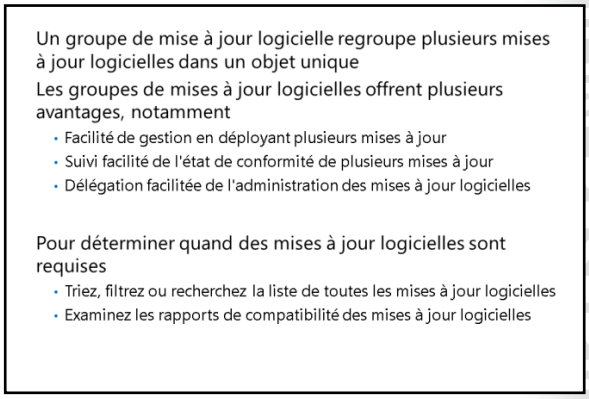
Selon vos exigences en matière de mise à jour et d'implémentation, vous avez plusieurs scénarios à prendre en compte quand vous configurez un point de mise à jour logicielle, notamment :

- Installation dans une hiérarchie Configuration Manager. Une hiérarchie Configuration Manager contient un site d'administration centrale et un ou plusieurs sites principaux. Dans ce type d'implémentation, chaque site contient un point de mise à jour logicielle actif. Le point de mise à jour logicielle situé dans le site d'administration centrale est configuré pour synchroniser des mises à jour à partir de Microsoft Update. Les points de mise à jour logicielle de chaque site principal sont configurés pour synchroniser des mises à jour à partir du serveur de mise à jour en amont situé dans le site d'administration central. Cependant, vous pouvez gérer les packages de déploiement utilisés pour déployer les mises à jour à partir de chaque site principal, si nécessaire.
- Installation dans un site secondaire. Pour les sites secondaires, un point de mise à jour logicielle est facultatif. Cependant, vous pouvez choisir de configurer un point de mise à jour logicielle actif dans un site secondaire lorsque la bande passante réseau est limitée entre les ordinateurs clients et les systèmes de site dans le site principal. Lorsque vous configurez un point de mise à jour logicielle dans un site secondaire, l'installation de WSUS est configurée comme un réplica de l'instance WSUS située dans le site principal. Vous devez configurer des clients situés dans les limites du site secondaire pour communiquer avec le point de mise à jour logicielle local dans le site secondaire. Cependant, vous devez gérer toutes les configurations de déploiement à partir du site principal.
- Prise en charge de la gestion cliente basée sur Internet. La gestion cliente basée sur Internet prend en charge l'utilisation d'un point de mise à jour logicielle placé dans le réseau de périmètre. Pour prendre en charge un point de mise à jour logicielle basé sur Internet, vous devez configurer le point de mise à jour logicielle actif dans le site principal pour autoriser uniquement les connexions clientes intranet. Vous devez également configurer le point de mise à jour logicielle basé sur Internet pour prendre en charge l'intranet et les connexions Internet. Vous devez ensuite synchroniser le point de mise à jour logicielle basé sur Internet avec le point de mise à jour logicielle actif dans le même site. Pour prendre en charge les clients basés sur Internet, vous devez installer le rôle de site sur un système de site distant situé dans un réseau de périmètre. Ce système de site doit être accessible depuis Internet et vous devez le configurer pour utiliser SSL pour la communication sécurisée HTTPS.
- Configuration requise pour NLB. Lorsque le nombre de clients pris en charge sur un site atteint les limites de capacité pour le point actif de mise à jour logicielle, vous pouvez implémenter un cluster NLB. Vous devez configurer chaque point individuel de mise à jour logicielle dans le cluster NLB comme point inactif de mise à jour de logiciels. Cependant, vous devez configurer le composant de point de mise à jour logicielle pour utiliser le cluster NLB comme point actif de mise à jour logicielle.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des déploiements de mise à jour logicielle

Avant de déployer des mises à jour logicielles, vous devez déterminer celles dont vos périphériques clients ont besoin. Dans la console Configuration Manager, le nœud Toutes les mises à jour logicielles peut afficher des milliers de mises à jour logicielles. Cependant, vos périphériques clients peuvent requérir seulement certaines de ces mises à jour. Les deux méthodes principales pour déterminer quelles mises à jour logicielles doivent être déployées comprennent :



- L'affichage des informations diffusées dans le volet de résultats du nœud Toutes les mises à jour logicielles.
- L'exécution des rapports de conformité pour les mises à jour logicielles.

La console Configuration Manager fournit plusieurs méthodes pour trier, filtrer et rechercher des mises à jour logicielles. Vous pouvez utiliser ces méthodes pour organiser et afficher la liste des mises à jour pour déterminer les exigences en matière de déploiement. Pour afficher la liste des mises à jour logicielles synchronisées, cliquez sur l'espace de travail **Bibliothèque de logiciels**, développez **Mises à jour logicielles**, puis cliquez sur **Toutes les mises à jour logicielles**.

Après avoir déterminé les mises à jour que vous souhaitez déployer sur les systèmes clients, vous pouvez utiliser un groupe de mises à jour logicielles pour aider au déploiement de chaque mise à jour séparément, ou vous pouvez utiliser un groupe de mises à jour logicielles pour gérer le déploiement de plusieurs mises à jour.

L'utilisation d'un groupe de mises à jour logicielles fournit de nombreux avantages, notamment :

- Facilité de gestion en déployant plusieurs mises à jour. Vous pouvez utiliser un groupe de mises à jour logicielles pour organiser plusieurs mises à jour logicielles en un objet unique qui peut être ensuite référencé dans un package de déploiement pour des regroupements ciblés. Vous pouvez exécuter l'Assistant Téléchargement des mises à jour logicielles basé sur un groupe de mise à jour logicielle. Vous devez utiliser cet Assistant pour créer un package de déploiement, qui référence des fichiers d'installation spécifiques de mise à jour logicielle, et diffuser des fichiers aux points de distribution. Vous pouvez également utiliser l'Assistant Déploiement des mises à jour logicielles pour un groupe de mises à jour logicielles pour déployer des mises à jour au sein de ce groupe sur un ensemble ciblé.
- Suivi facilité de l'état de conformité de plusieurs mises à jour. Un groupe de mises à jour logicielles inclut uniquement celles que vous ajoutez spécifiquement à la liste. Vous pouvez utiliser le groupe de mises à jour logicielles pour surveiller la conformité de l'état pour les systèmes cibles. En outre, si vous utilisez des groupes de mises à jour logicielles pour créer des packages de déploiement, vous pouvez utiliser des rapports tels que Conformité 1 – Conformité générale et Conformité 3 – Groupe des mises à jour (par mise à jour) pour obtenir les états pour chaque mise à jour logicielle dans le groupe.
- Délégation facilitée de l'administration des mises à jour logicielles. L'utilisation d'un groupe de mises à jour logicielles offre également la possibilité de déléguer l'administration des mises à jour logicielles. Quand vous ajoutez un utilisateur administrateur avec le rôle de sécurité Gestionnaire des mises à jour logicielles associé, vous pouvez définir une étendue de sécurité pour chaque groupe de mises à jour logicielles que vous référencerez.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le processus de déploiement de mises à jour logicielles implique de créer un package de déploiement, de télécharger les fichiers de mise à jour logicielle, et de les acheminer aux points de distribution. Vous avez aussi la possibilité de vérifier que le contenu est disponible sur les points de distribution avant de déployer les mises à jour logicielles sur les clients (même si cela est facultatif).

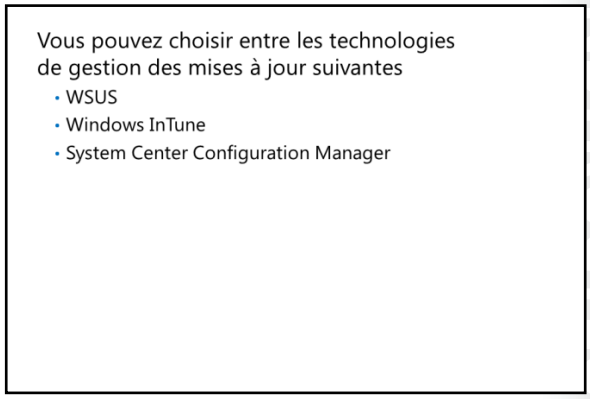
Vous pouvez utiliser l'Assistant Téléchargement des mises à jour logicielles pour créer le package de déploiement, définir les points de distribution et spécifier l'emplacement de téléchargement des fichiers de mise à jour. Vous pouvez démarrer l'Assistant en sélectionnant une mise à jour logicielle ou un groupe de mises à jour logicielles, puis en cliquant sur le bouton **Télécharger** dans le ruban.

Après avoir créé le package de déploiement, vous pouvez modifier les paramètres du package ou surveiller l'état du point de distribution en sélectionnant le nœud Packages de déploiement.

Comme avec d'autres types de contenu, la sélection d'un package de déploiement dans le volet des résultats fournit des options courantes comme la création de fichier de contenu de préconfiguration, la gestion des comptes d'accès, la distribution de contenu, la mise à jour des points de distribution et la définition des étendues de sécurité.

Le volet de visualisation fournit un résumé de l'état de point de distribution. notamment un lien vers le nœud de contenu d'état accessible sur l'espace de travail de surveillance.

Sélection d'une technologie de gestion des mises à jour



WSUS est le produit de gestion des mises à jour d'entrée de gamme disponible auprès de Microsoft. Ce produit peut être utile pour les petits et moyens réseaux, mais si vous gérez des déploiements de mise à jour sur des réseaux plus grands, vous devez envisager d'utiliser un produit disposant de plus de fonctionnalités. Microsoft fournit deux produits supplémentaires : Microsoft System Center Essentials et System Center Configuration Manager, qui fournit des fonctionnalités de gestion des mises à jour avancées. Ces produits peuvent être plus appropriés que WSUS pour les environnements réseaux spécifiques. Nous allons présenter ici les différences entre ces trois technologies de gestion des mises à jour.

WSUS

WSUS 3.0 Service Pack 2 (SP2) est une solution de gestion des mises à jour qui convient aux petites ou moyennes entreprises qui n'ont pas d'exigences de mise à jour logicielles complexes. WSUS 3.0 SP2 présente les caractéristiques suivantes :

- Elle convient si vous prenez en charge uniquement le déploiement des mises à jour des applications et des systèmes d'exploitation Microsoft. Elle ne prend pas en charge le déploiement des mises à jour d'applications non-Microsoft.
- Il n'y a aucune limite quant au nombre de serveurs WSUS que vous pouvez déployer dans un domaine. Vous pouvez déployer WSUS dans une configuration autonome ou de réplication dans les filiales et le siège social.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Elle peut prendre en charge jusqu'à 25 000 clients avec un seul serveur unique, si vous activez également le service BITS.
- Elle doit être déployée sur un ordinateur qui exécute le système d'exploitation serveur, y compris l'un des suivants : Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 ou Windows Server 2012. Il est impossible de déployer WSUS sur un ordinateur exécutant un système d'exploitation client.

Windows Intune

Windows Intune™ est un service de cloud computing Microsoft qui vous permet de gérer, de contrôler et de déployer des mises à jour, ainsi que des applications logicielles vers des ordinateurs clients. Vous payez un forfait mensuel pour ce service, qui ne requiert pas d'implémenter d'infrastructure dans votre environnement. Il dispose d'une console d'administration basée sur le Web, mais fournit la plupart des fonctionnalités WSUS et certaines fonctionnalités sur System Center Configuration Manager. Pour plus d'informations sur ce service, rendez-vous dans la page d'accueil de Windows InTune.

System Center Configuration Manager

System Center Configuration Manager est le produit de gestion de la configuration avancé de Microsoft. Il convient aux grandes entreprises dans lesquelles il faut vérifier que les ordinateurs ont des configurations qui répondent à des exigences strictes. Configuration Manager offre les fonctionnalités suivantes :

- Il autorise plusieurs serveurs Configuration Manager par domaine. Configuration Manager s'adapte bien aux grandes entreprises et permet aux administrateurs de déployer plusieurs points de gestion et de déploiement dans une infrastructure Configuration Manager. Si une filiale n'a pas de serveur local, vous pouvez même placer des points de déploiement Configuration Manager sur les stations de travail de la filiale qui exécutent Windows 7, Windows Vista, ou Windows XP. Vous devez déployer WSUS sur un serveur qui exécute un système d'exploitation serveur.
- Il prend en charge les collections dynamiques. WSUS et System Center Essentials utilisent des groupes d'ordinateurs dans lesquels un ordinateur peut être membre d'un seul groupe uniquement. Configuration Manager utilise des collections, il s'agit d'un ensemble d'ordinateurs ou d'utilisateurs qui ont une propriété commune. Par exemple, vous pouvez créer une collection qui comprend tous les ordinateurs qui n'exécutent pas la version la plus récente d'une application autre que Microsoft particulière.
- Il prend en charge la gestion des mises à jour à la fois pour les applications de Microsoft et autres que Microsoft. Vous pouvez utiliser Configuration Manager pour déployer des mises à jour sur des applications autres que Microsoft. Configuration Manager vous permet de cibler des mises à jour sur des collections. Cela signifie que vous pouvez spécifiquement cibler une mise à jour, plutôt que de la déployer sur des ordinateurs qui ne sont pas concernés.
- Le déploiement de mise à jour planifié est pris en charge. Vous pouvez utiliser Configuration Manager pour planifier une mise à jour avant le déploiement à une heure spécifique. Vous pouvez également personnaliser les messages d'avertissement au cas où l'ordinateur ait besoin de redémarrer pour déployer la mise à jour.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- La fonction Wake on LAN est prise en charge pour le déploiement des mises à jour. La fonction Wake on LAN garantit que les ordinateurs spécifiquement configurés sortent de veille en mode d'alimentation minimale de sorte que les installations de mise à jour logicielle se produisent. La fonction Wake on LAN vous permet de déployer des mises à jour et des logiciels au moment qui convient et lorsque le personnel n'utilise pas les ordinateurs.
- Les fonctions de création de rapport intégrées sont prises en charge. Configuration Manager prend en charge des fonctions de création de rapport intégrées avancées, et la possibilité de créer des rapports avec le Concepteur de rapports dans Microsoft SQL Server Business Intelligence Design Studio. Vous pouvez également planifier les rapports à exécuter, puis les transférer par courrier électronique pour vous assurer que les administrateurs sachent qu'un déploiement de mise à jour a été effectué avec succès.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Planification et implémentation des mises à jour dans une infrastructure de virtualisation de serveur

La gestion de l'infrastructure de Virtual Machine Manager (VMM) dans Microsoft System Center 2012 comprend des tâches comme l'ajout de nouveaux serveurs hôtes Windows Server 2012 Hyper-V® et la garantie que les composants de l'infrastructure contiennent les dernières mises à jour logicielles approuvées.

VMM s'intègre également une fonctionnalité fournie par WSUS pour vérifier que tous les serveurs sont en conformité avec les dernières exigences de base de référence de mise à jour.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire la mise à jour adaptée aux clusters ;
- décrire les éléments à prendre en compte pour la configuration de la mise à jour adaptée aux clusters ;
- décrire la gestion des mises à jour dans VMM ;
- configurer la gestion des mises à jour dans VMM ;
- décrire les éléments à prendre en compte pour planifier une base de référence de mise à jour ;
- décrire les éléments à prendre en compte pour le déploiement des mises à jour logicielles ;

Qu'est-ce que la mise à jour adaptée aux clusters ?

L'application de mises à jour de système d'exploitation sur les nœuds d'un cluster requiert une attention particulière. Si vous souhaitez garantir un temps mort nul pour un rôle en cluster, vous devez manuellement mettre à jour les nœuds de cluster l'un après l'autre, puis déplacer manuellement des ressources du nœud en cours de mise à jour vers un autre nœud. Cette procédure peut être fastidieuse. Dans Windows Server 2012, Microsoft a une nouvelle fonctionnalité pour la mise à jour automatique des nœuds de cluster.

La mise à jour adaptée aux clusters est une fonctionnalité automatisée spécifique à Windows Server 2012 qui met à jour des nœuds de cluster avec un temps d'arrêt minimal voire nul

Elle peut fonctionner selon deux modes

- Le mode de mise à jour à distance
- Le mode de mise à jour automatique

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La mise à jour adaptée aux clusters est une fonctionnalité qui permet aux administrateurs de mettre à jour automatiquement des nœuds de cluster, tout en entraînant peu ou pas de perte de disponibilité pendant le processus de mise à jour. Pendant une procédure de mise à jour, la mise à jour adaptée aux clusters place chaque nœud de cluster hors connexion de manière transparente, installe les mises à jour et les mises à jour dépendantes, exécute un redémarrage si nécessaire, replace le nœud en ligne et procède à la mise à jour du nœud suivant.

Pour de nombreux rôles en cluster, ce processus de mise à jour automatique déclenche un basculement planifié et il peut provoquer une interruption passagère de service pour les clients connectés. Cependant, pour des charges de travail disponibles en permanence dans Windows Server 2012, notamment Hyper-V avec la migration dynamique ou le serveur de fichiers avec le basculement transparent SMB, la mise à jour adaptée aux clusters peut orchestrer des mises à jour de cluster sans impact sur la disponibilité des services.

Modes de mise à jour de cluster

La mise à jour adaptée aux clusters peut orchestrer l'opération complète de mise à jour de cluster dans deux modes :

- Mode de mise à jour à distance. Dans ce mode, un ordinateur qui exécute Windows Server 2012 ou Windows 8 est appelé orchestrateur et configuré tel quel. Pour configurer un ordinateur en tant qu'orchestrateur de mise à jour adaptée aux clusters, vous devez y installer des outils d'administration de clustering avec basculement. L'ordinateur orchestrateur n'est pas un membre du cluster qui fait l'objet de la mise à jour. À partir de l'ordinateur orchestrateur, l'administrateur déclenche une mise à jour à la demande en utilisant un profil d'Exécution de mise à jour par défaut ou personnalisé. Le mode de mise à jour à distance est utile pour surveiller la progression en temps réel de l'exécution de mise à jour et pour les clusters qui s'exécutent sur des installations minimales de Windows Server 2012.
- Mode de mise à jour automatique. Dans ce mode, vous devez configurer le rôle en cluster de mise à jour adaptée aux clusters comme charge de travail sur le cluster de basculement que vous voulez mettre à jour, puis définir une planification de mise à jour associée. Dans ce scénario, la mise à jour adaptée aux clusters n'a pas d'ordinateur orchestrateur dédié. Le cluster se met à jour aux heures planifiées à l'aide d'un profil d'exécution de mise à jour par défaut ou personnalisé. Pendant l'exécution de la mise à jour, le processus orchestrateur de mise à jour adaptée aux clusters démarre sur le nœud qui possède actuellement le rôle en cluster de mise à jour adaptée aux clusters, et le processus réalise des mises à jour sur chaque nœud de cluster de manière séquentielle. En mode de mise à jour automatique, la mise à jour adaptée aux clusters peut mettre à jour le cluster de basculement à l'aide d'un processus de mise à jour entièrement automatisé et de bout en bout. Dans ce mode, un administrateur peut également déclencher des mises à jour à la demande ou utiliser l'approche de mise à jour à distance. En mode de mise à jour automatique, un administrateur peut accéder à des informations résumées sur une exécution de mise à jour en cours en se connectant au cluster et en exécutant l'applet de commande Windows PowerShell Get-CauRun.

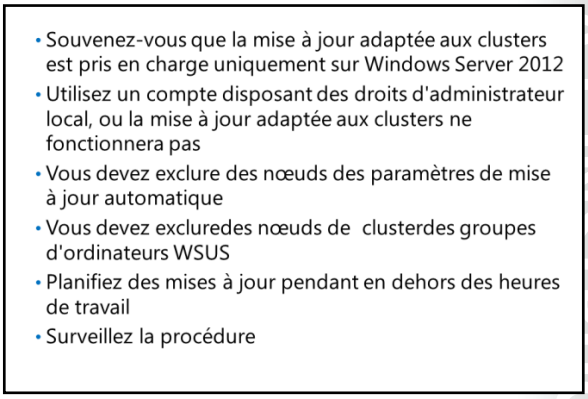
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour utiliser la mise à jour adaptée aux clusters, vous devez installer la fonctionnalité Clustering avec basculement dans Windows Server 2012 et créer un cluster de basculement. Les composants qui prennent en charge la fonctionnalité de mise à jour adaptée aux clusters sont automatiquement installés sur chaque nœud de cluster.

Vous devez installer les outils de mise à jour adaptée aux clusters. Ils sont inclus dans les outils de clustering avec basculement (qui font également partie des outils d'administration de serveur distant (RSAT, Remote Server Administration Tools)). Les outils de mise à jour adaptée aux clusters comprennent l'interface utilisateur de mise à jour adaptée aux clusters et les applets de commande Windows PowerShell de mise à jour adaptée aux clusters. Lorsque vous installez la fonctionnalité de clustering avec basculement, les outils de clustering avec basculement sont installés par défaut sur chaque nœud de cluster. Vous pouvez aussi installer ces outils sur un ordinateur local ou distant qui exécute Windows Server 2012 ou Windows 8 et qui est connecté au cluster de basculement.

Éléments à prendre en compte pour la configuration de la mise à jour adaptée aux clusters

Bien que la mise à jour adaptée aux clusters fournisse plusieurs avantages et réduise le travail administratif pour gérer les mises à jour sur des nœuds de cluster, il y a quelques éléments à prendre en compte quand vous déployez cette fonctionnalité, notamment ce qui suit :



- Seul Windows Server 2012 prend en charge la mise à jour adaptée aux clusters, et il requiert l'installation de la fonctionnalité et des outils de clustering avec basculement.
- Si vous souhaitez lancer des actions dans la console de mise à jour adaptée aux clusters, vous devez utiliser le compte disposant des droits d'administrateur local sur les nœuds de cluster que vous mettez à jour.
- Si vous implémentez la fonctionnalité de mise à jour adaptée aux clusters sur des nœuds de cluster, il est recommandé d'exclure ces nœuds des paramètres de mises à jour automatiques que vous déployez dans la stratégie de groupe ou de les configurer localement dans le Panneau de configuration. Cela élimine la possibilité que des déploiements inutiles de mise à jour se produisent en dehors du calendrier de mise à jour adapté aux clusters. En outre, l'installation de mises à jour automatiques sur les nœuds de cluster peut interférer avec l'installation des mises à jour adaptées aux clusters et peut provoquer des défaillances de ces dernières.
- Si vous déployez WSUS, excluez les nœuds de cluster qui utilisent la mise à jour adaptée aux clusters des groupes d'ordinateurs WSUS.
- Si vous utilisez un système de gestion de configuration pour appliquer des mises à jour logicielles à vos ordinateurs du réseau (Configuration Manager, par exemple), excluez les nœuds de cluster de toutes les mises à jour automatiques ou obligatoires.

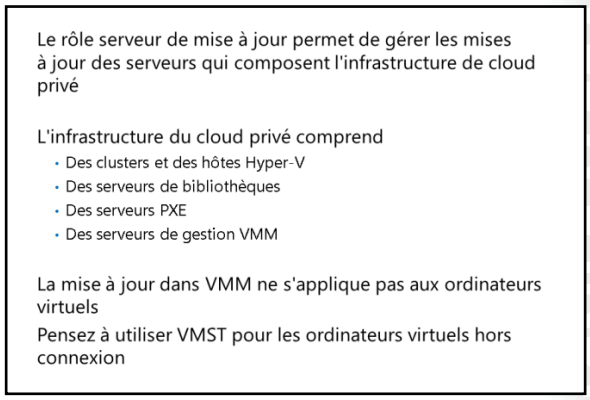
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Vous devez planifier les mises à jour que la mise à jour adaptée aux clusters gère pour le déploiement pendant les heures de fermeture, lorsque cela affecte le moins le personnel de votre organisation.
- Vous ne pouvez pas utiliser Configuration Manager pour extraire les mises à jour. Vous devez installer un serveur en aval pour la mise à jour adaptée aux clusters ou le WSUS principal, si vous avez plusieurs serveurs WSUS, vous pouvez synchroniser des mises à jour avec Windows PowerShell pour conserver les mêmes informations sur vos autres serveurs.

Bien que la mise à jour adaptée aux clusters soit une fonctionnalité automatique qui ne requiert aucune intervention administrative, vous devez surveiller le processus et vérifier si les mises à jour sont déployées correctement sur les nœuds de cluster.

Vue d'ensemble de la gestion des mises à jour dans VMM

Microsoft fournit un certain nombre de solutions pour déployer les mises à jour logicielles et analyser la conformité des ordinateurs. Cependant, certains clients réseau, tels que les nœuds de serveur basés sur un cluster ou d'autres rôles serveurs hautement disponibles, présentent généralement des complexités qui peuvent rendre difficile et long le maintien d'un processus standard de gestion des mises à jour.



VMM s'intègre avec WSUS pour fournir une analyse de conformité à la demande et la mise à jour des serveurs qui composent une infrastructure, notamment les hôtes Hyper V, les serveurs de bibliothèque, les serveurs PXE, et le serveur de gestion VMM.

L'intégration de WSUS dans VMM fournit également la possibilité d'effectuer des mises à jour orchestrées

des clusters hôtes Hyper-V. Lorsque vous mettez à jour un cluster hôte, VMM place un seul nœud de cluster à la fois en mode de maintenance, puis installe les mises à jour approuvées. Pour les clusters qui prennent en charge la migration dynamique, le placement intelligent écarte les ordinateurs virtuels du nœud de cluster que vous mettez à jour. Si un cluster ne prend pas en charge la migration dynamique, VMM enregistre alors l'état des ordinateurs virtuels avant de mettre le nœud de cluster à jour.

Remarque : Vous devez avoir Windows Server 2008 R2 ou Windows Server 2012 installé sur un nœud de cluster Hyper-V, pour prendre en charge la migration dynamique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez utiliser le rôle serveur de mise à jour dans VMM pour gérer les tâches plus complexes de mise à jour pour les serveurs qui composent votre infrastructure de cloud privé. Ces serveurs incluent les suivants :

- Hôtes Hyper-V
- Clusters Hyper-V
- Serveurs de bibliothèques VMM
- Serveurs PXE
- Serveurs de gestion VMM

Remarque : Vous devez utiliser uniquement le rôle serveur de mise à jour pour la mise à jour des serveurs qui composent l'infrastructure VMM. Vous ne pouvez pas utiliser cette solution pour mettre à jour les ordinateurs virtuels gérés par VMM. Pour mettre des ordinateurs virtuels à jour, vous devez utiliser une solution (telle que WSUS ou Configuration Manager) détaillée dans les premières sections de ce module.

Pour tous les rôles serveur de l'infrastructure VMM, vous devez effectuer une recherche sur une base de référence des mises à jour approuvées pour déterminer l'état de conformité. Pour les serveurs qui ne sont pas conformes, vous pouvez effectuer des tâches de mise à jour pour installer celles manquantes et redémarrer les serveurs, si nécessaire.

Virtual Machine Servicing Tool 2012

Dans l'environnement de cloud public, il existe des scénarios où un ou plusieurs ordinateurs virtuels sont autorisés hors connexion (désactivés) pendant de longues périodes. Vous pouvez par exemple arrêter les ordinateurs virtuels que vous utilisez moins fréquemment afin d'économiser les ressources physiques. Lorsqu'ils sont arrêtés, ces ordinateurs virtuels ne peuvent pas forcément recevoir les mises à jour du système d'exploitation ou d'applications. Ceci représente un risque pour tout l'environnement informatique une fois que vous mettez en marche ces ordinateurs virtuels. Pour cette raison, vous devez prévoir comment mettre ces ordinateurs virtuels à jour et les maintenir conformes à votre stratégie de sécurité actuelle. Une solution consiste à mettre en marche ces ordinateurs au moment où les mises à jour planifiées sont déployées sur le reste de votre infrastructure. Toutefois, cette opération peut s'avérer très longue si vous avez un grand nombre d'ordinateurs virtuels hors connexion.

À cet effet, Microsoft fournit l'outil de maintenance de l'ordinateur virtuel (version 2012) pour vous aider à maintenir les ordinateurs virtuels hors connexion à jour. L'outil de maintenance des ordinateurs virtuels fonctionne avec System Center Virtual Machine Manager pour activer la maintenance des éléments suivants :

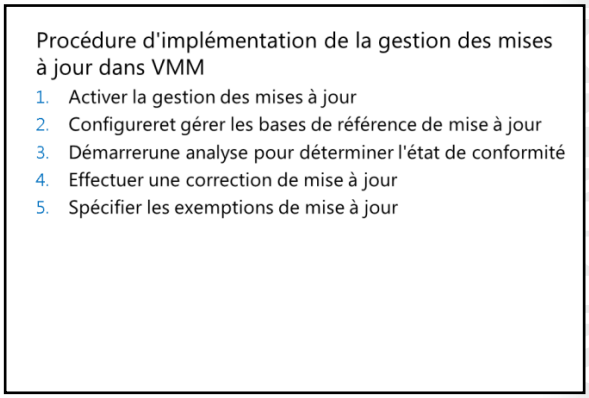
- Ordinateurs virtuels hors ligne dans une bibliothèque VMM.
- Ordinateurs virtuels dans un état sauvegardé et arrêtés sur un hôte.
- Modèles d'ordinateurs virtuels.
- Disques durs virtuels hors connexion dans une bibliothèque VMM, en injectant des mises à jour.

Pour utiliser VMST, vous devez déployer un système de gestion des mises à jour, tel que WSUS ou Configuration Manager, dans votre infrastructure. L'outil de maintenance de l'ordinateur virtuel est gratuit, et vous pouvez le télécharger à partir du Centre de téléchargement Microsoft.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de la gestion des mises à jour dans VMM

Le processus d'implémentation de la gestion des mises à jour dans votre environnement VMM consiste à :



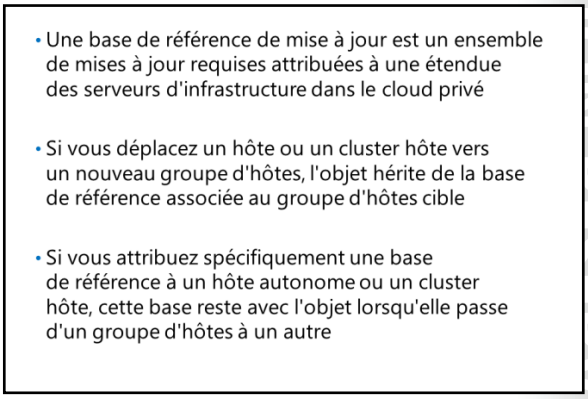
1. Utiliser VMM pour gérer les mises à jour en commençant par activer la gestion des mises à jour. Vous devez activer la gestion des mises à jour en ajoutant un serveur WSUS existant à VMM, ou vous pouvez installer un serveur WSUS dédié, puis ajouter le nouveau serveur de mise à jour à VMM.
2. Configurer et gérer les bases de référence de mise à jour, qui définissent un ensemble de mises à jour à déployer sur un groupe d'hôtes, un hôte autonome, un cluster hôte, ou un serveur VMM. La rubrique suivante détaille les bases de référence de mise à jour. Une fois que vous ajoutez un serveur de mise à jour, vous pouvez effectuer les tâches suivantes dans la console VMM :
   - Exécuter la synchronisation à la demande de WSUS avec Windows Update.
   - Configurer le nom de serveur proxy et des paramètres de port, qui sont requis pour se connecter à Internet pour des synchronisations de WSUS.
   - Spécification des classifications de mise à jour à synchroniser.
   - Spécification des produits à synchroniser.
   - Spécification des langues prises en charge à synchroniser.
3. Démarrez une analyse pour déterminer l'état de conformité, une fois que vous attribuez une base de référence de mise à jour. Pendant une analyse de conformité, WSUS vérifie chaque mise à jour dans la base de référence de mise à jour attribuée pour déterminer si elle est applicable et installée sur le serveur cible. Le serveur cible enregistre alors l'état de conformité pour chaque mise à jour.
4. Procédez à une correction de mise à jour pour mettre un serveur géré ou un cluster hôte Hyper-V en conformité. Vous pouvez choisir de corriger toutes les bases de référence de mise à jour attribuées à un ordinateur, toutes les mises à jour non conformes dans une base de référence spécifique de mise à jour, ou une seule mise à jour, selon les besoins.
5. Spécifiez quelles exemptions de mise à jour empêcheront une mise à jour spécifique d'être installée sur un serveur. L'ordinateur restera responsable de la base de référence attribuée, même si vous excluez une mise à jour spécifique de l'installation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification d'une base de référence de mise à jour

Une fois que vous avez ajouté un serveur WSUS à VMM pour effectuer le rôle serveur de mise à jour, l'étape suivante consiste à déterminer quelles mises à jour installer sur chaque serveur dans l'infrastructure du cloud privé. VMM ajoute les mises à jour que vous sélectionnez dans une base de référence de mise à jour, sur laquelle chaque serveur effectue une analyse. VMM corrige ensuite tous les serveurs non conformes à la base de référence, pour installer immédiatement les mises à jour manquantes.



Une fois que vous avez déterminé quelles mises à jour sont requises pour vos serveurs d'infrastructure VMM, vous devez ensuite créer une liste pour VMM et l'utiliser comme base de référence à partir de laquelle effectuer des analyses et des corrections. VMM utilise la base de référence de mise à jour en tant que liste, et vous pouvez ajouter ou supprimer des mises à jour, selon les besoins.

Qu'est-ce qu'une base de référence de mise à jour ?

Toutes les mises à jour d'un produit spécifique et d'une catégorie s'affichent dans la console VMM lorsque vous synchronisez avec WSUS. Pour spécifier uniquement les mises à jour nécessaires selon vos besoins, vous devez créer une base de référence de mise à jour. Il s'agit d'un ensemble de mises à jour requises qui sont attribuées à une étendue de serveurs d'infrastructure dans le cloud privé. Vous pouvez attribuer une base de référence de mise à jour à ce qui suit :

- Tous les hôtes au sein de tous les groupes d'hôtes
- Des groupes d'hôtes spécifiques
- Un serveur autonome spécifique au sein d'un groupe d'hôtes
- Un cluster hôte spécifique au sein d'un groupe d'hôtes
- Des serveurs de bibliothèques
- Serveurs PXE
- Le serveur VMM
- Le serveur de mise à jour

Planification des bases de référence de mise à jour

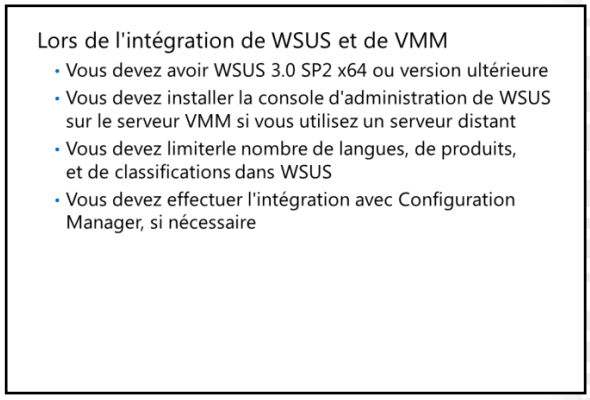
Vous devez tenir compte des facteurs suivants lorsque vous planifiez des bases de référence de mise à jour :

- Si vous attribuez une base de référence à un groupe d'hôtes, tous les hôtes ou le cluster d'hôtes au sein de ce groupe seront affectés à cette base. Si vous déplacez un hôte vers un nouveau groupe d'hôtes, WSUS supprime la base de référence d'origine, et l'hôte héritera de la base de référence associée au nouveau groupe d'hôtes.
- Si vous attribuez spécifiquement une base de référence à un hôte autonome ou un cluster hôte, cette base reste avec l'objet lorsqu'elle passe d'un groupe d'hôtes à un autre.

- Quand vous ajoutez d'abord le serveur de mise à jour, deux bases de référence de mise à jour intégrées sont fournies. La base de référence témoin pour les mises à jour critiques contient toutes les mises à jour critiques qui se synchronisent initialement, et la base de référence témoin pour les mises à jour de sécurité contient toutes les mises à jour de sécurité qui se synchronisent initialement. Si vous prévoyez d'utiliser ces bases de référence de mise à jour intégrées, vous devez conserver les mises à jour lorsque vous effectuez des tâches de synchronisation ultérieures. Vous devez également affecter des ordinateurs à la base de référence avant de pouvoir l'utiliser pour l'analyse et la mise à jour de conformité.
- Vous pouvez créer une nouvelle base de référence de mise à jour qui contient les mises à jour nécessaires, ainsi que celles que vous attribuez aux serveurs pour lesquels vous souhaitez assurer la conformité des mises à jour.

Éléments à prendre en compte pour l'intégration de WSUS et de VMM

Vous devez examiner les facteurs suivants avec attention lorsque vous intégrez WSUS dans l'infrastructure VMM :



- Si WSUS est installé sur un serveur distant, vous devez installer la console d'administration de WSUS sur le serveur de gestion VMM. Si le serveur de gestion VMM fait partie d'un cluster, vous devez installer la console d'administration WSUS sur chacun des nœuds de cluster.
- Si vous utilisez un serveur WSUS dédié, vous devez limiter le nombre de langues, de produits, et de classifications uniquement à ceux requis par les serveurs qui composent l'infrastructure VMM.
- Si vous utilisez un serveur WSUS qui est partagé avec un environnement Configuration Manager :
    - Vous devez apporter des modifications de configuration WSUS uniquement à l'aide de Configuration Manager.
    - Vous devez noter que pour l'environnement VMM, la planification de synchronisation est toujours à la demande.
    - Vous devez créer une collection dans Configuration Manager de tous les serveurs pour lesquels VMM gèrera les mises à jour. Vous devez exclure cet ensemble de tous les déploiements de mise à jour logicielle que Configuration Manager déploie.
- Si vous ajoutez le serveur WSUS à VMM, vérifiez que vous désactivez la case à cocher Autoriser les modifications de configuration du serveur de mise à jour. Vous allez configurer ce paramètre dans la console VMM, dans la fenêtre des propriétés du serveur de mise à jour.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et implémentation d'une infrastructure de correction de serveur

Scénario

La direction informatique d'A. Datum souhaite vérifier que toutes les mises à jour Windows Server requises sont bien appliquées sur les serveurs. La direction voudrait évaluer les outils Windows Server 2012 et System Center 2012 pour mettre des ordinateurs hôtes Hyper-V ainsi que les serveurs qui sont membres du cluster à jour. Elle souhaite implémenter un environnement WSUS pour déployer des mises à jour sur tous les autres serveurs Windows.

Vous devez valider la fonctionnalité fournie par la mise à jour hôte dans VMM et par CAU dans Windows Server 2012. Vous devez ensuite planifier et implémenter un déploiement de WSUS pour l'organisation.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- Implémenter la mise à jour hôte dans VMM.
- Configurer CAU.
- Planifier un déploiement de WSUS.
- Déployer un WSUS réplica.
- Configurer et valider un déploiement WSUS.

Configuration de l'atelier pratique

Durée approximative : 75 minutes

Ordinateurs virtuels	22414B-LON-DC1 22414B-LON-WSUS 22414B-LON-SVR1 22414B-LON-SVR2 22414B-LON-VMM1 22414B-TOR-SVR1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible. Avant de commencer cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, sur **Accueil**, cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22414B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   a. Nom d'utilisateur : **ADATUM\Administrateur**
   b. Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour tous les ordinateurs virtuels.

Exercice 1 : Implémenter la mise à jour hôte dans VMM

Scénario

A. Datum a déployé VMM pour gérer les ordinateurs hôtes Hyper-V dans son centre de données de Londres. Il envisage d'utiliser VMM pour gérer les mises à jour qui doivent être appliquées aux hôtes Hyper-V. Puisque les hôtes Hyper-V contrôleront plusieurs ressources importantes dans les ordinateurs virtuels, il est essentiel qu'elles soient à jour avec tous les correctifs de sécurité et de fonctionnalité.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer l'intégration de VMM avec WSUS.
2. Configurer une base de référence de mise à jour logicielle dans VMM.
3. Vérifier la conformité de la base de référence.

▶ Tâche 1 : Configurer l'intégration de VMM avec WSUS

1. Sur LON-VMM1, ouvrez la **Console Virtual Machine Manager**, cliquez sur **Connecter**, puis cliquez sur l'espace de travail **Ensemble fibre optique**.
2. Dans le volet de navigation, développez le nœud **Serveurs** et cliquez sur **Serveur de mise à jour**.
3. Ajoutez un serveur de mise à jour avec la configuration suivante :
   - Nom de l'ordinateur : **LON-WSUS**
   - Port TCP/IP : **8530**
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
4. Dans la fenêtre Travaux, sélectionnez le travail **Ajouter un serveur de mise à jour**. Sur les onglets **Résumé** et **Détails**, surveillez le statut de la tâche de configuration.
5. Une fois le travail affiché en tant que **Terminé avec des informations**, fermez la fenêtre Travaux.

▶ Tâche 2 : Configurer une base de référence de mise à jour logicielle dans VMM

1. Sur LON-VMM1, dans la console **Virtual Machine Manager**, cliquez sur l'espace de travail **Bibliothèque**.
2. Dans le volet de navigation, développez **Mettre à jour le catalogue et les lignes de base**, puis cliquez sur **Mettre à jour le catalogue**.
3. Vérifiez que les diverses mises à jour s'affichent.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Créez une mise à jour de la ligne de base avec les paramètres suivants :
   - Nom : **Serveur base de référence**
   - Mises à jour :
     - **Mise à jour pour Windows Server 2012 (KB2751352)**
   - Étendue de l'affectation :
     - Serveurs de bibliothèque : **LON-VMM1.Adatum.com**
     - Serveur de mise à jour : **LON-WSUS.Adatum.com**
     - Serveur VMM : **LON-VMM1.Adatum.com**
5. Vérifiez que la tâche Créer une nouvelle ligne de base été accomplie avec succès.

▶ Tâche 3 : Vérifier la conformité de la base de référence

1. Sur LON-VMM1, cliquez sur l'espace de travail **Ensemble fibre optique**.
2. Dans le volet de navigation, développez **Serveurs**, et cliquez sur **Serveurs de bibliothèque**.
3. Dans le ruban, cliquez sur le bouton **Compatibilité**.
4. Dans le volet des résultats, notez la conformité et l'état opérationnel de **LON-VMM1.Adatum.com**.
5. Analysez **LON-VMM1.Adatum.com**, et vérifiez son état de conformité. **Remarque :** il doit être conforme. Remarque : si l'état de conformité est indiqué comme étant **Non compatible**, cliquez avec le bouton droit sur LON-VMM1.Adatum.com, et sélectionnez **Corriger** dans la fenêtre Correction de mise à jour. En outre, activez la case à cocher **Ne pas redémarrer les serveurs après correction**, puis cliquez sur le bouton **Corriger**. Après une minute environ, l'**État de conformité** doit devenir Conforme.
6. Rétablissez 22414B-LON-VMM1.

Résultats : Après avoir terminé cet exercice, vous aurez configuré la mise à jour hôte VMM.

Exercice 2 : Configuration du clustering avec basculement et de la mise à jour adaptée aux clusters

Scénario

A. Datum envisage également d'utiliser la fonctionnalité de mise à jour adaptée aux clusters pour mettre tous les hôtes à jour dans un cluster de basculement. L'entreprise a eu auparavant plusieurs problèmes avec la mise à jour des nœuds de cluster. Comme chaque cluster héberge des ressources importantes, les administrateurs mettaient ces nœuds à jour manuellement, au milieu de la nuit, pour réduire le temps d'interruption du service. A. Datum cherche une solution pour rendre ce processus automatique et moins gourmand en main-d'œuvre.

Vous devez d'abord installer et configurer le cluster de basculement, puis configurer et valider la fonctionnalité de mise à jour adaptée aux clusters pour mettre les ordinateurs hôtes de Windows Server 2012 à jour.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Implémenter un clustering avec basculement.
2. Configurer la cible iSCSI.
3. Configurer le cluster.
4. Configurer CAU.
5. Mettre à jour le cluster de basculement.

▶ Tâche 1 : Implémenter un clustering avec basculement

1. Sur LON-SVR1, ajoutez la fonctionnalité **Clustering avec basculement** à l'aide du Gestionnaire de serveur.
2. Sur LON-SVR2, ajoutez la fonctionnalité **Clustering avec basculement** à l'aide du Gestionnaire de serveur.

▶ Tâche 2 : Configurer la cible iSCSI

1. Sur LON-SVR1, démarrez l'**initiateur iSCSI**.
2. Utilisez l'adresse 172.16.0.10 pour découvrir et vous connecter à la cible iSCSI.
3. Sur LON-SVR2, démarrez l'**initiateur iSCSI**.
4. Utilisez l'adresse 172.16.0.10 pour découvrir et vous connecter à la cible iSCSI.
5. Sur LON-SVR2, ouvrez Gestion des disques, initialisez et mettez les disques 2 et 3 en ligne (ne sélectionnez pas le disque 1). Formatez ces lecteurs.
6. Sur LON-SVR1, ouvrez Gestion des disques et mettez les disques 3 et 4 en ligne (ne sélectionnez pas le disque 2).

▶ Tâche 3 : Configurer le cluster

1. Ouvrez le **Gestionnaire du cluster de basculement** sur LON-SVR1.
2. Créez un cluster avec les nœuds LON-SVR1 et LON-SVR2.
3. N'exécutez pas la validation à ce stade.
4. Indiquez **FSCluster** comme Nom du cluster.
5. Spécifiez **172.16.0.127** comme **Adresse IP** pour le cluster.
6. Ajoutez le Disque de cluster 1 et le Disque de cluster 2 à **Stockage du cluster**.
7. Attribuez le Disque de cluster 1 à un **volume partagé de cluster**.
8. Configurez les paramètres de quorum sur **Par défaut** (recommandé).
9. Dans le Gestionnaire du cluster de basculement, ajoutez un nouveau rôle **Serveur de fichiers** et choisissez de configurer **Serveur de fichiers avec montée en puissance parallèle pour les données d'application**.
10. Configurez **AdatumFS** en tant que nom du point d'accès client.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer CAU

1. Sur LON-DC1, installez la fonctionnalité Clustering avec basculement à l'aide de la console Gestionnaire de serveur.
2. Sur LON-SVR1, ouvrez la console **Pare-feu Windows avec fonctions avancées de sécurité**, puis activez les deux règles de trafic entrant appelées **Règle entrante pour l'arrêt à distance (RPC-EP entrant)** et **Règle entrante pour l'arrêt à distance (TCP entrant)**. Répétez ce processus pour LON-SVR2.
3. Basculez vers l'ordinateur LON-WSUS et ouvrez la console Windows Server Update Services.
4. Accédez au nœud Toutes les mises à jour et approuvez **Mise à jour pour Windows Server 2012 (KB2771431)** et **Mise à jour pour Windows Server 2012 (KB2772501)** pour l'installation sur les ordinateurs non attribués.
5. Sur LON-DC1, dans le Gestionnaire de serveur, ouvrez la mise à jour adaptée aux clusters.
6. Connectez-vous à **FSCluster**.
7. Générez la liste des aperçus de mises à jour pour les nœuds dans **FSCluster**.

▶ Tâche 5 : Mettre à jour le cluster de basculement

1. Sur LON-DC1, démarrez le processus de mise à jour pour FSCluster, en sélectionnant **Appliquer les mises à jour à ce cluster**.
2. Dans l'Assistant de mise à jour, acceptez les valeurs par défaut.
3. Attendez que le processus de mise à jour soit terminé, c'est-à-dire lorsque dans les deux nœuds la valeur **Opération réussie** apparaît dans la colonne État de la dernière exécution.
4. Ouvrez une session sur LON-SVR1 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
5. Sur LON-SVR1, ouvrez Mise à jour adaptée aux clusters, puis connectez-vous au FSCLUSTER.
6. Sélectionnez l'option **Configurer les options de mise à jour automatique du cluster**.
7. Choisissez Ajouter le rôle en cluster de la mise à jour adaptée aux clusters, avec le mode de mise à jour automatique activé, à ce cluster.
8. Configurez une mise à jour automatique **Chaque semaine**, le **dimanche** à **04:00.**
9. Fermez l'Assistant à la fin de son exécution.

Résultats : Après avoir terminé cet exercice, vous aurez installé la fonctionnalité de cluster de basculement et configuré la mise à jour adaptée aux clusters.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Planification d'un déploiement WSUS

Scénario

A. Datum a déployé un serveur WSUS dans le centre de données central à Londres. Le déploiement de WSUS fonctionne bien dans le bureau principal, mais pas aussi bien dans les filiales de Toronto et de Sydney. La direction informatique d'A. Datum a fourni les conditions requises suivantes pour mettre à jour le déploiement de WSUS :

- L'infrastructure de mise à jour doit réduire l'utilisation de la bande passante entre le bureau de Londres et celui de Sydney.
- L'infrastructure de mise à jour doit réduire l'utilisation de bande passante sur la connexion Internet à Toronto.
- Un seul serveur WSUS doit être déployé sur chaque site.
- Chaque bureau doit avoir un ensemble d'ordinateurs de test qui testera tous les déploiements du bureau.
- Les mises à jour doivent être distribuées selon les services dans chaque bureau.
- Les administrateurs WSUS de Londres doivent approuver toutes les mises à jour attribuées aux ordinateurs de Toronto, et les administrateurs WSUS de Sydney peuvent approuver les mises à jour sur le serveur local.

Les tâches principales de cet exercice sont les suivantes :

1. Lisez et analysez le scénario de l'exercice.
2. Selon les exigences du scénario de l'exercice, proposez une conception de déploiement WSUS.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.

▶ Tâche 1 : Lisez et analysez le scénario de l'exercice

1. Utilisez le manuel du stagiaire pour lire le scénario de l'exercice.

▶ Tâche 2 : Selon les exigences du scénario de l'exercice, proposez une conception de déploiement WSUS

Proposez une topologie WSUS appropriée pour répondre aux exigences du scénario de l'atelier pratique. Utilisez les questions suivantes pour vous aider :

1. Combien de serveurs WSUS A. Datum a-t-il en tout ?
2. Quel type de configuration de serveur WSUS allez-vous déployer à Sydney ?
3. Quel type de configuration de serveur WSUS allez-vous déployer à Toronto ?
4. Comment allez-vous répondre aux exigences pour déployer les mises à jour par service ?
5. Comment répondre aux exigences pour stocker la bande passante entre Londres et Sydney ?
6. Comment répondre aux exigences pour stocker la bande passante entre Toronto et Internet ?
7. Comment allez-vous configurer les groupes de tests ?
8. Y a-t-il d'autres solutions ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

1. Utilisez le corrigé de l'atelier pratique pour comparer votre solution avec celle fournie.
2. Comparez votre solution avec celle de la classe et de l'instructeur.

Résultats : À la fin de cet exercice, vous aurez planifié une scénario de déploiement WSUS.

Exercice 4 : Déploiement d'un serveur WSUS en mode Réplication

Scénario

A. Datum a accepté votre conception pour le déploiement WSUS. Elle souhaite implémenter les modifications à l'infrastructure existante dès que possible. Étant donné qu'il est urgent de réduire le trafic Internet pour WSUS dans le bureau de Toronto, vous avez décidé d'implémenter un serveur de réplication WSUS d'abord à Toronto. Les administrateurs d'A. Datum de Toronto vous ont fourni l'ordinateur TOR-SVR1. Vous devez déployer WSUS sur TOR-SVR1, le configurer comme réplica sur le serveur central de LON-WSUS, puis recréer l'objet de stratégie de groupe approprié (GPO).

Les tâches principales de cet exercice sont les suivantes :

1. Installer et configurer un serveur de réplication sur TOR-SVR1.
2. Vérifier la réplication à partir du serveur en amont.
3. Configurer un objet de stratégie de groupe pour WSUS.

▶ Tâche 1 : Installer et configurer un serveur de réplication sur TOR-SVR1

1. Lancez l'**Assistant Ajout de rôles et de fonctionnalités** sur l'ordinateur TOR-SVR1.
2. Ajoutez le rôle **Services WSUS (Windows Server Update Services)**. Acceptez les valeurs par défaut de l'Assistant, puis configurez l'emplacement de mise à jour sur **C:\Mises à jour**.
3. Une fois l'installation terminée, cliquez sur le nœud WSUS, et lancez les tâches de post-configuration dans la console du Gestionnaire de serveur. Attendez que les tâches soient effectuées.
4. Ouvrez la console Windows Server Update Services.
5. Lancez la configuration initiale.
6. Choisissez d'implémenter WSUS en mode de réplica, puis de le répliquer de LON-WSUS.adatum.com.
7. Choisissez de synchroniser manuellement.

▶ Tâche 2 : Vérifier la réplication à partir du serveur en amont

1. Sur TOR-SVR1, commencez la synchronisation par le serveur en amont.
2. Sur LON-WSUS, ouvrez la console WSUS, accédez à **Mises à jour critiques**, puis sélectionnez d'afficher **Toutes** les mises à jour.
3. Activez la mise à jour appelée **Mise à jour pour Windows 8 pour ordinateurs à processeur x64 (KB2751352)**, puis approuvez-la pour l'installer sur tous les ordinateurs.
4. Basculez vers TOR-SVR1, ouvrez la console WSUS, accédez aux mises à jour critiques, puis assurez-vous que la mise à jour **Mise à jour pour Windows 8 pour ordinateurs à processeur x64 (KB2751352)** n'est pas approuvée pour l'installation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Synchronisez manuellement TOR-SVR1 avec LON-WSUS.
6. Basculez vers TOR-SVR1 et dans la console WSUS, accédez à **Mises à jour critiques**, et choisissez d'afficher les mises à jour **Approuvées**.
7. Vérifiez que **Mise à jour pour Windows 8 pour ordinateurs à processeur x64 (KB2751352)** est approuvée.

▶ Tâche 3 : Configurer un objet de stratégie de groupe pour WSUS

1. Sur LON-DC1, ouvrez la console Gestion de stratégie de groupe.
2. Créez un nouvel objet de stratégie de groupe (GPO) appelé **WSUS**.
3. Ouvrez l'Éditeur de gestion des stratégies de groupe pour modifier l'objet de stratégie de groupe WSUS.
4. Accédez au nœud **Configuration ordinateur**, développez **Stratégies**, puis **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local**, puis **Composants Windows**, et cliquez sur **Windows Update**.
5. Activez le paramètre des mises à jour automatiques, puis choisissez de télécharger automatiquement et de planifier l'installation chaque dimanche.
6. Ouvrez et activez le paramètre **Spécifier l'emplacement intranet du service de mise à jour Microsoft**.
7. Saisissez **http://TOR-SVR1.adatum.com** dans les deux champs.
8. Fermez l'Éditeur de gestion des stratégies de groupe.

Résultats : À la fin de cet exercice, vous aurez déployé un serveur de réplication WSUS.

Exercice 5 : Configurer les options de mise à jour du client

Scénario

Maintenant que le déploiement du serveur WSUS est terminé, l'étape finale est la configuration des groupes d'ordinateurs WSUS, les mises à jour et les paramètres de mise à jour automatique. En raison de différentes planifications de mise à jour, vous devez créer des groupes distincts pour les clients et serveurs. En outre, pour vous adapter aux exigences de la stratégie de mise à jour, vous devez configurer des options supplémentaires dans un objet GPO pour WSUS.

Les tâches principales de cet exercice sont les suivantes :

1. Créer les groupes d'ordinateurs requis.
2. Configurer des mises à jour automatiques.
3. Valider la configuration de la mise à jour.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Créer les groupes d'ordinateurs requis

- Sur LON-WSUS, dans la console WSUS, créez deux groupes d'ordinateurs. Nommez le premier groupe **Clients ADatum** et le deuxième groupe **Serveurs ADatum**.

▶ Tâche 2 : Configurer des mises à jour automatiques

1. Sur LON-DC1, dans la console Gestion de stratégie de groupe, modifiez l'objet de stratégie de groupe **WSUS**.
2. Configurez la fréquence de détection des mises à jour automatiques sur 1 heure.
3. Activez les options suivantes : **Autoriser l'installation immédiate des mises à jour automatiques** et **Activer les mises à jour automatiques recommandées via le service Mises à jour automatiques**.
4. Fermez l'Éditeur de gestion des stratégies de groupe.
5. Liez l'objet de stratégie de groupe au domaine Adatum.com.

▶ Tâche 3 : Valider la configuration de la mise à jour

1. Sur LON-DC1, ouvrez Windows PowerShell et exécutez **gpupdate /force**.
2. Sur LON-DC1, ouvrez le **Panneau de configuration**.
3. Ouvrez l'élément **Windows Update**.
4. Cliquez sur **Modifier les paramètres**.
5. Vérifiez que vous ne pouvez pas modifier de paramètres concernant la façon d'installer les mises à jour importantes.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-SVR2**, **22414B-LON-WSUS**, et **22414B-TOR-SVR1**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré le serveur WSUS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
WSUS n'a pas pu se synchroniser avec Microsoft Update.	
Les ordinateurs clients figurent dans les groupes incorrects.	

Questions de contrôle des acquis

Question : Quelle est la différence entre la gestion des mises à jour avec Configuration Manager et avec VMM ?

Outils

- Console de gestion WSUS
- Console VMM
- Console de mise à jour adaptée aux clusters
- Console de gestion des stratégies de groupe

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 10

Planification et implémentation d'une stratégie de continuité des activités de l'entreprise

Table des matières :

Vue d'ensemble du module **10-1**

Leçon 1 : Vue d'ensemble de la planification de la continuité des activités de l'entreprise **10-2**

Leçon 2 : Planification et implémentation des stratégies de sauvegarde **10-13**

Leçon 3 : Planification et implémentation de la récupération **10-22**

Leçon 4 : Planification et implémentation de la sauvegarde et de la récupération des ordinateurs virtuels **10-32**

Atelier pratique : Implémentation d'une stratégie de sauvegarde d'ordinateurs virtuels avec DPM **10-40**

Contrôle des acquis et éléments à retenir **10-47**

Vue d'ensemble du module

Une stratégie de continuité des activités représente un ensemble de normes, de procédures, d'instructions et de stratégies qu'une entreprise crée pour s'assurer de pouvoir conserver ses fonctions métier stratégiques. Cette stratégie expose les activités que vous devez effectuer quotidiennement pour maintenir le service, la cohérence et la capacité de récupération.

Dans ce module, vous apprendrez comment planifier et implémenter une stratégie de continuité des activités pour votre organisation, et comment planifier et implémenter des stratégies de sauvegarde et de récupération, y compris la sauvegarde et la récupération des ordinateurs virtuels.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- comprendre l'importance de la planification de la continuité des activités de l'entreprise ;
- planifier et implémenter des stratégies de sauvegarde ;
- planifier et implémenter la récupération ;
- planifier et implémenter la sauvegarde et la récupération des ordinateurs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1

Vue d'ensemble de la planification de la continuité des activités de l'entreprise

Les objectifs principaux de la planification de la continuité des activités de l'entreprise consistent à reconnaître et à identifier les risques et les opérations critiques, ainsi qu'à permettre une prévention et une récupération efficaces dans l'éventualité d'un événement susceptible d'impacter les activités quotidiennes de votre organisation, tel que la suppression de données essentielles, la défaillance d'un disque ou une panne de serveur.

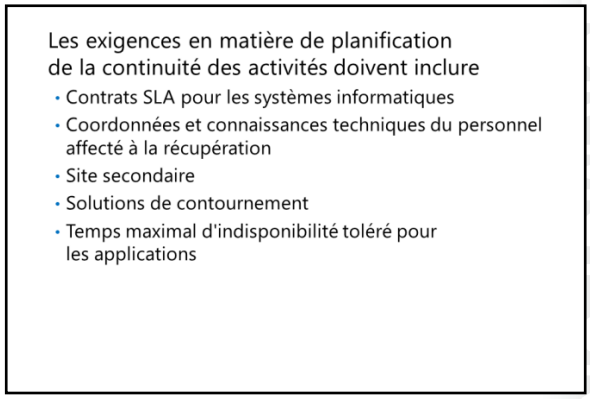
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- identifier les conditions requises pour la planification de la continuité des activités ;
- créer des stratégies pour implémenter la continuité des activités ;
- comprendre les contrats de niveau de service (SLA) ;
- décrire les composants d'une stratégie de sauvegarde ;
- décrire les composants d'une stratégie de restauration ;
- définir les éléments à prendre en compte pour utiliser la sauvegarde Windows Server® 2012 ;
- définir les éléments à prendre en compte pour utiliser Microsoft® System Center 2012 - Data Protection Manager (DPM) ;
- définir les éléments à prendre en compte pour utiliser Windows Azure™ Online Backup.

Collecte des exigences en matière de planification de la continuité des activités

Vous collectez les exigences en matière de planification de la continuité des activités au cours d'une phase d'analyse initiale et utilisez les résultats pour créer votre infrastructure entière. Les exigences en matière de planification des activités diffèrent selon la structure organisationnelle de l'entreprise.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Voici plusieurs exigences à prendre en compte pour élaborer votre plan de continuité des activités :

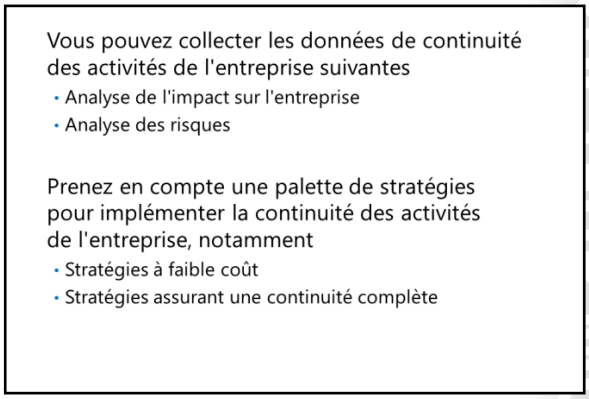
- les contrats SLA relatifs à vos systèmes informatiques, à la fois pour le matériel et les logiciels ;
- les informations de contact et les détails techniques de vos administrateurs de sauvegarde ;
- un site secondaire à partir duquel vous pouvez accéder aux applications critiques et aux données d'application des fonctions métier stratégiques ;
- des solutions de contournement ;
- le temps maximal d'indisponibilité toléré pour vos applications.

La création d'une liste concrète d'exigences ne doit pas seulement impliquer les employés du service informatique, mais aussi les responsables de l'entreprise et d'autres décideurs de haut niveau. Les responsables de l'entreprise doivent connaître le processus lié aux risques et comprendre comment une défaillance peut avoir un impact sur l'activité de l'entreprise. Les responsables doivent également déterminer quelles applications sont essentielles pour leur activité et il est probable qu'ils seront chargés de définir les délais de récupération nécessaires pour définir la stratégie appropriée de sauvegarde et de restauration.

Remarque : Les organisations présentent des exigences différentes selon leur infrastructure métier et leurs objectifs. Les exigences en matière de planification de la continuité des activités ne doivent pas être statiques. Vous devez les évaluer et les mettre à jour régulièrement et vous devez réévaluer régulièrement votre planification au bout de quelques mois.

Stratégies d'implémentation de la continuité des activités

Vous pouvez concevoir vos stratégies d'implémentation de la continuité des activités en recueillant les données suivantes :



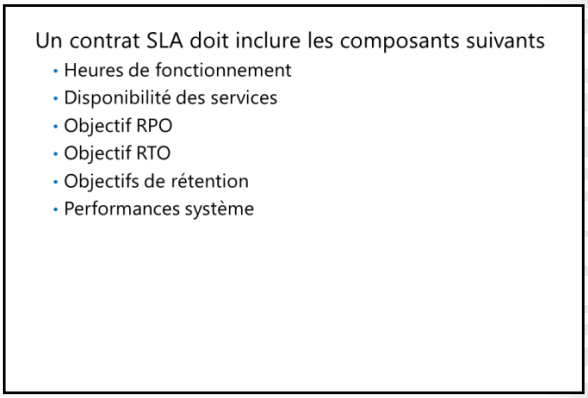
- Analyse de l'impact sur l'entreprise. L'analyse de l'impact sur l'entreprise détermine les processus métier critiques d'une organisation, ainsi que les dommages et les pertes potentiels qui peuvent résulter d'une interruption ou d'une défaillance de ces processus.
- Analyse des risques. L'analyse des risques identifie les risques qui peuvent se produire et leur probabilité. L'analyse des risques identifie également les points de défaillance uniques, tels que les lecteurs de disques, les commutateurs réseau, le stockage ou l'alimentation électrique d'une organisation.

Il existe une palette de stratégies pour implémenter la continuité des activités, qui vont d'une stratégie à bas coût jusqu'à une stratégie assurant la continuité complète. La stratégie à bas coût fournit une protection dans des situations où les impacts sont minimaux et où le risque est acceptable. La stratégie assurant une continuité complète présente un coût élevé, mais elle est nécessaire lorsque les impacts sont élevés et que les risques sont supérieurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrats de niveau de service

Un contrat SLA est un document qui décrit les responsabilités et les objectifs spécifiques d'un service, d'une organisation ou d'un autre fournisseur. Plus particulièrement, le contrat SLA d'un service informatique ou d'un prestataire de services informatiques couvre généralement la protection des données et spécifie généralement les parties précises qu'une organisation doit protéger en ce qui concerne son infrastructure informatique et ses données. De plus, un tel contrat SLA spécifierait probablement le délai dans lequel les services doivent être rétablis après une défaillance.



Certaines organisations disposent de contrats SLA formels, et d'autres non. Les performances d'un service informatique sont mesurées généralement par rapport aux objectifs définis par un contrat SLA. Ces mesures font partie de l'évaluation des performances du service informatique et ont une influence directe sur des éléments, tels que les budgets et les salaires. Pour les services gérés ou les fournisseurs de services cloud, les contrats SLA sont essentiels pour la facturation. Dans d'autres organisations, les contrats SLA correspondent à des directives moins formelles. Il est important de concevoir un contrat SLA qui soit réaliste et réalisable, plutôt que d'établir un standard irréalisable.

Un contrat SLA peut inclure les éléments suivants :

- Heures de fonctionnement. Ce paramètre définit le nombre d'heures durant lesquelles les données et les services sont disponibles pour les utilisateurs, ainsi que le temps d'interruption planifié pour la maintenance du système.
- Disponibilité des services. Il s'agit d'un pourcentage de temps annuel durant lequel les données et les services sont disponibles pour les utilisateurs. Par exemple, une disponibilité des services de 99,9 % par an signifie que les données et les services ne peuvent pas présenter un temps d'interruption non planifié supérieur à 0,1 % de l'année, soit 8,75 heures par an sur la base d'un fonctionnement 24 heures/24 et 7 jours/7.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Objectif de point de récupération (RPO, Recovery point objective). Un objectif RPO fixe une limite quant à la quantité des données pouvant être perdues en cas de défaillance, mesurée en tant qu'unité de temps. Par exemple, si une organisation définit un objectif RPO de six heures, il est nécessaire d'effectuer une sauvegarde toutes les six heures ou de créer une copie de réplication à différents emplacements, toutes les six heures. En cas de défaillance, une organisation utilisera la sauvegarde la plus récente, qui, dans le scénario le plus grave, en supposant que la défaillance s'est produite juste avant (ou pendant) la sauvegarde suivante, remonterait à six heures.

  Vous pouvez configurer le logiciel de sauvegarde pour effectuer des sauvegardes toutes les heures et fournir un objectif RPO théorique de 60 minutes, ce qui signifie que si une perte de données se produit 60 minutes après la dernière sauvegarde, seules les nouvelles données créées au cours de cet intervalle d'une heure ne seront pas restaurées. Toutes les autres données créées auparavant, avant la sauvegarde, sont restaurées à partir du support de sauvegarde. Lorsque vous calculez un objectif RPO, il est important de prendre en considération le temps nécessaire à l'exécution d'une sauvegarde. Par exemple, supposons qu'une sauvegarde prenne 15 minutes et que vous effectuiez une sauvegarde toutes les heures. Si une défaillance se produit pendant le processus de sauvegarde, votre meilleur objectif RPO possible sera de 1 heure et 15 minutes. Un objectif RPO réaliste doit toujours équilibrer le temps de récupération que vous souhaitez avec les réalités propres à votre infrastructure réseau. Vous ne devez pas viser un objectif RPO de deux heures si la sauvegarde dure trois heures.

  Un objectif RPO dépend également de la technologie du logiciel de sauvegarde que vous utilisez. Par exemple, si vous utilisez la fonctionnalité de capture instantanée disponible dans Sauvegarde Windows Server ou un autre logiciel de sauvegarde qui utilise le service VSS (service de cliché instantané des volumes), vous effectuez une sauvegarde jusqu'à l'instant où la sauvegarde a commencé.

- Objectif RTO (Recovery Time Objective). Un objectif RTO détermine la durée de récupération après une défaillance. L'objectif RTO varie en fonction du type de défaillance. La perte d'une carte mère sur un serveur critique présente un objectif RTO différent de la perte d'un disque sur un serveur critique, parce que le remplacement d'une carte mère demande sensiblement plus de temps que celui d'un disque.

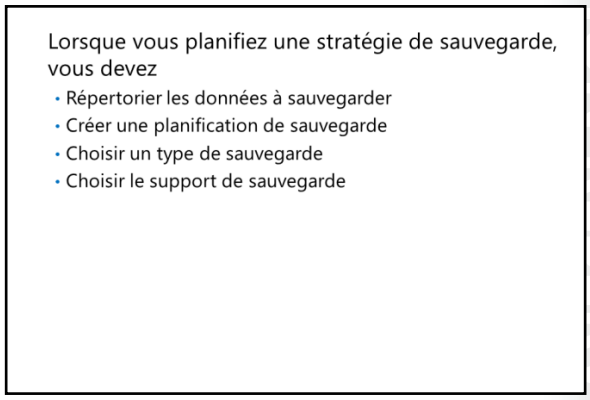
- Objectifs de rétention. Les objectifs de rétention constituent une mesure du temps nécessaire au stockage des données sauvegardées. Par exemple, vous pouvez avoir besoin de récupérer rapidement des données de moins d'un mois, mais devez stocker les données, sous une forme quelconque, pour plusieurs années. La vitesse à laquelle vous acceptez de récupérer les données dans votre contrat SLA dépend de l'âge des données et doit également prendre en compte la vitesse à laquelle les données sont récupérables ou si elles doivent être récupérées dans vos archives.

- Performances système. Les performances système sont un composant important du contrat SLA, bien qu'en général elles ne soient pas liées directement à la récupération d'urgence. Les applications figurant dans un contrat SLA doivent être disponibles et doivent avoir des temps de réponse acceptables aux demandes des utilisateurs. Si les performances système sont lentes, les exigences métier ne seront pas satisfaites.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Composants d'une stratégie de sauvegarde

La création d'une stratégie de sauvegarde complète et correcte est l'une des étapes les plus importantes que vous entreprendrez lorsque vous planifierez des sauvegardes.



Lors de la planification d'une stratégie de sauvegarde, vous devez :

- Répertorier les données à sauvegarder. Vous devez identifier toutes les données qui exigent une sauvegarde afin de pouvoir restaurer vos données et vos systèmes en cas d'incident. Vous devez identifier la quantité de données, ainsi que les fichiers et les dossiers, et les volumes du système d'exploitation Windows Server 2012 à sauvegarder. Cela vous permet de choisir un support de stockage approprié et d'identifier le temps qui sera nécessaire à une opération de sauvegarde ou de restauration.
- Créer une planification de sauvegarde. Vous devez programmer à quelle fréquence et à quelles heures les serveurs devront effectuer les tâches de sauvegarde automatisées. La plupart des organisations effectuent au moins des sauvegardes quotidiennes.
- Choisir un type de sauvegarde. Vous devez choisir un type de sauvegarde en fonction de la fréquence souhaitée pour les opérations de sauvegarde et de restauration et du temps que ces opérations nécessitent. Vous pouvez également être amené à sélectionner un type de sauvegarde particulier. Votre logiciel de sauvegarde vous permet de choisir parmi les types de sauvegarde suivants :
    - Complète ou normale. Une sauvegarde complète est un réplica au niveau de tous les blocs de tous les volumes du serveur. La Sauvegarde Windows Server effectue des sauvegardes complètes par défaut.
    - Incrémentielle. Une sauvegarde incrémentielle est une copie renfermant uniquement les blocs qui ont été modifiés depuis la dernière sauvegarde complète ou incrémentielle.
    - Différentielle. Une sauvegarde différentielle est une copie renfermant uniquement les blocs qui ont changé depuis la dernière sauvegarde complète. La Sauvegarde Windows Server ne prend pas en charge les sauvegardes différentielles.
    - Sauvegarde en ligne. Windows Server 2012 a introduit pour la première fois cette fonctionnalité appelée Windows Azure Online Backup.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Choisir un support de sauvegarde en fonction de votre logiciel de sauvegarde, de la taille des sauvegardes et du temps qui vous est donné pour restaurer les données. Les supports de sauvegarde suivants sont possibles :
    - Bande
    - Disque dur : fixe ou amovible, USB (Universal Serial Bus)
    - DVD
    - Dossier partagé
    - Service cloud en ligne

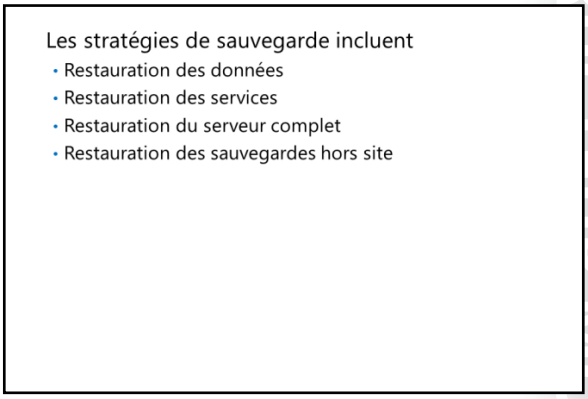
La bande est disponible dans différents formats et prend en charge divers débits de données et capacités de stockage. Si vous effectuez des sauvegardes sur bande, assurez-vous que le format de bande employé convient pour la quantité de données à sauvegarder.

La fonctionnalité de sauvegarde de Windows Server 2012 ne prend pas en charge la sauvegarde sur bande. Les volumes et les dossiers partagés sont les seuls supports de stockage pris en charge. Considérez la durée pendant laquelle vous devez conserver les sauvegardes. Serez-vous en mesure de restaurer les données datant d'un mois, de six mois, d'un an ou plus ?

Vous devez également tenir compte de l'emplacement de stockage de vos supports de sauvegarde. Les bandes sont sensibles aux champs magnétiques et à la chaleur. Vous devez donc les stocker à l'écart de tels facteurs environnementaux. De plus, vous devez stocker les supports de sauvegarde hors site, dans l'éventualité d'un incident, tel qu'un incendie ou une inondation, dans les bureaux de votre organisation.

Composants d'une stratégie de restauration

Lors de la planification de la stratégie de sauvegarde de votre entreprise, vous devez développer des stratégies pour restaurer les données, les services, les serveurs et les sites. Vous devez également prendre des dispositions pour une sauvegarde hors site.



Stratégies de restauration des données

Les données correspondent à l'élément le plus couramment récupéré dans un environnement d'entreprise. En effet, la suppression accidentelle de fichiers par les utilisateurs est plus probable que la défaillance du matériel serveur ou l'endommagement des données par les applications. Dans le cadre des stratégies de restauration des données, la sauvegarde n'est pas la seule technologie de récupération des données. Vous pouvez prendre en charge de nombreux scénarios de récupération de fichiers et dossiers en implémentant les versions précédentes de la fonctionnalité de fichier sur les partages de fichiers. Vous pouvez également répliquer des données dans différents emplacements physiques, sur un cloud public ou privé, ou en utilisant DPM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Stratégies de restauration des services

Les fonctionnalités d'un réseau dépendent de la disponibilité de certains services réseau critiques. Bien que les réseaux bien conçus établissent une redondance dans les services de noyau tels que DNS (Domain Name System) et AD DS (Active Directory® Domain Services), même ces services peuvent rencontrer des problèmes. Par exemple, un défaut majeur requérant une restauration à partir d'une sauvegarde peut être répliqué. En outre, une solution de sauvegarde d'entreprise doit assurer la restauration en temps utile de services tels que le protocole DHCP (Dynamic Host Configuration Protocol) et AD CS (services de certificats Active Directory), ainsi que de ressources importantes, telles que les partages de fichiers.

Stratégies de restauration de serveur complète

Développer une stratégie de récupération de serveur complète implique que vous déterminiez les serveurs concernés par la récupération, y compris les objectifs RPO et RTO pour les serveurs critiques. Par exemple, supposez que vous disposez d'un site avec deux ordinateurs fonctionnant comme contrôleurs de domaine. Lors du développement de votre stratégie de sauvegarde, posez-vous les questions suivantes :

- Devez-vous envisager d'avoir deux serveurs capables d'effectuer une récupération de serveur complète avec un objectif RPO de 15 minutes ?
- Est-il vraiment nécessaire de récupérer rapidement un serveur en cas de défaillance, vu que l'un ou l'autre des serveurs pourra fournir le même service réseau et assurer la continuité des activités ?

Lorsque vous développez le composant de récupération de serveur complète du plan de sauvegarde d'entreprise de votre organisation, déterminez quels serveurs sont requis pour garantir la continuité des activités. Veillez à ce que votre plan inclut des sauvegardes régulières de ces serveurs.

Stratégies de restauration de site

La plupart des grandes entreprises possèdent des filiales. Bien qu'il puisse être souhaitable de sauvegarder tous les ordinateurs à ces emplacements, cela peut ne pas être économiquement possible. Le développement d'une stratégie de récupération de site implique de déterminer les données, les services et les serveurs d'un site spécifique qui doivent être récupérables pour garantir la continuité des activités.

Stratégies de restauration des sauvegardes hors site

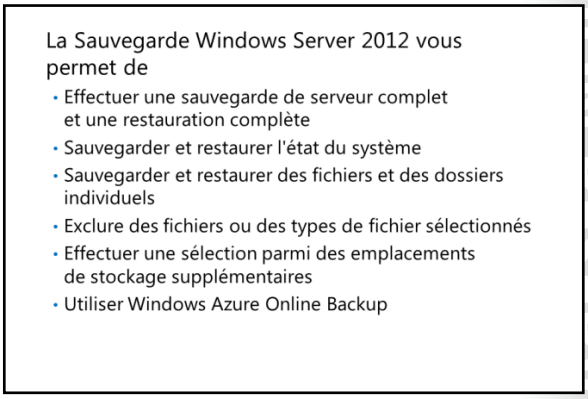
De nombreuses organisations ne stockant pas les sauvegardes hors site n'ont pas pu récupérer leurs données après un incident sur le site principal. Si le siège social de votre organisation est exposé à un incendie, une inondation majeure, un cyclone ou une tornade, peu importe les stratégies de sauvegarde mises en place si vous stockez ces sauvegardes à l'emplacement ravagé par le sinistre.

Une stratégie de protection complète des données de l'entreprise implique le déplacement des données sauvegardées vers un emplacement hors site sécurisé, afin que vous puissiez les récupérer, quel que soit le sinistre subi. Cette opération n'a pas besoin d'être effectuée chaque jour. L'objectif RPO pour la récupération des données stockées dans l'emplacement hors site (souvent appelé site de récupération d'urgence) est habituellement différent de l'objectif RPO sur le site principal.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Avantages liés à l'utilisation de la Sauvegarde Windows Server

La fonctionnalité Sauvegarde Windows Server dans Windows Server 2012 se compose d'un composant logiciel enfichable MMC, de la commande **wbadmin** et des commandes Windows PowerShell®. Vous pouvez utiliser des assistants dans le cadre de la fonctionnalité Sauvegarde Windows Server pour qu'ils vous guident dans l'exécution des sauvegardes et des récupérations.



Vous pouvez utiliser la fonctionnalité de sauvegarde de Windows Server 2012 pour sauvegarder :

- un serveur entier (tous les volumes) ;
- des volumes sélectionnés ;
- des éléments spécifiques sélectionnés pour la sauvegarde, tels que des dossiers spécifiques ou l'état du système.

En outre, la fonctionnalité de sauvegarde de Windows Server 2012 vous permet d'effectuer les opérations suivantes :

- Réaliser une restauration complète. Une sauvegarde complète contient au moins tous les volumes critiques et vous permet d'effectuer une restauration sans avoir à installer au préalable un système d'exploitation. Pour cela, utilisez le support d'installation sur DVD ou clé USB, et l'Environnement de récupération Windows (Windows RE, Windows Recovery Environment). Vous pouvez utiliser ce type de sauvegarde, ainsi que Windows RE, pour récupérer après une défaillance de disque dur, ou si vous devez récupérer l'image entière d'un ordinateur sur un nouveau matériel.
- Utiliser l'état du système. La sauvegarde contient toutes les informations pour restaurer un serveur à un moment spécifique. Cependant, vous devez installer un système d'exploitation avant de récupérer l'état du système.
- Récupérer chaque fichier, dossier ou volume. L'option relative aux fichiers et dossiers individuels vous permet de choisir de sauvegarder et de restaurer des fichiers, des dossiers ou des volumes spécifiques, ou encore d'ajouter des fichiers, des dossiers ou des volumes spécifiques à votre sauvegarde lorsque vous utilisez une option telle que le volume critique ou l'état du système.
- Exclure des fichiers ou des types de fichier sélectionnés. Par exemple, vous pouvez exclure des fichiers temporaires de la sauvegarde.

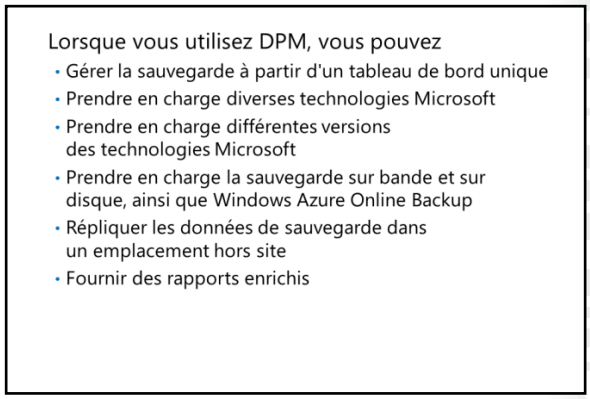
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Effectuer une sélection parmi des emplacements de stockage supplémentaires. Vous pouvez stocker des sauvegardes dans des partages distants ou sur des volumes non dédiés.
- Utiliser Windows Azure™ Online Backup. Windows Azure™ Online Backup est une solution de sauvegarde basée sur le cloud pour Windows Server 2012, qui vous permet de sauvegarder et de récupérer des fichiers et dossiers hors site, à partir du cloud public ou privé.

En cas d'incident, tel qu'une défaillance de disque dur, vous pouvez effectuer la récupération du système à l'aide d'une sauvegarde de serveur complète et de Windows RE. Ceci restaurera votre système entier sur un nouveau disque dur.

Avantages de l'utilisation de System Center 2012 DPM

DPM fait partie de System Center 2012 et est un logiciel qui permet d'utiliser les fonctionnalités de sauvegarde et de restauration d'entreprise pour différents produits et technologies Microsoft. Les moyennes et grandes entreprises peuvent préférer utiliser DPM plutôt que la Sauvegarde Windows Server, car DPM vous permet d'effectuer les opérations suivantes :



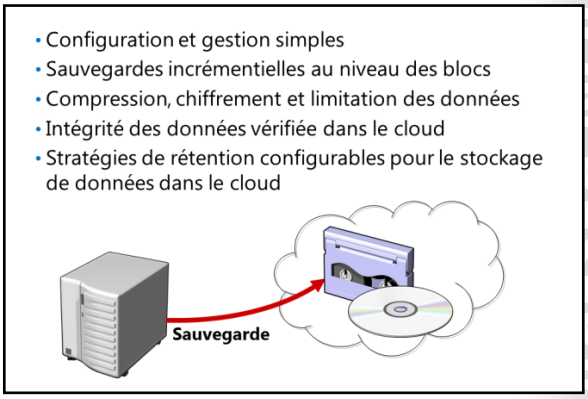
- Gérer les travaux de sauvegarde et de restauration à partir d'un tableau de bord unique. Vous pouvez également définir des paramètres de configuration et des rapports pour plusieurs serveurs.
- Prendre en charge plusieurs technologies Microsoft, telles que Windows Server, Active Directory, Microsoft Exchange Server, Microsoft SQL Server® et Microsoft SharePoint® Server, y compris les serveurs virtuels et les systèmes d'exploitation clients Microsoft.
- Prendre en charge plusieurs versions des technologies Microsoft, telles que Windows Server 2012, Windows Server 2008 R2, Exchange Server 2010, Exchange Server 2007, etc.
- Prendre en charge la sauvegarde sur bande et sur disque, ainsi que Windows Azure Online Backup.
- Répliquer des données de sauvegarde dans un emplacement hors site, dans un site de récupération d'urgence.
- Créer des rapports enrichis sur les travaux de sauvegarde et de restauration, l'utilisation des supports de sauvegarde et les tendances de protection des données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour utiliser Windows Azure Online Backup

Windows Azure Online Backup est une solution de sauvegarde basée sur le cloud pour Windows Server 2012 qui est gérée par Microsoft. Vous pouvez utiliser ce service pour sauvegarder des fichiers et dossiers, et les récupérer à partir du cloud public ou privé. Cela vous permet de fournir une protection hors site contre toute perte de données causée par des incidents et vous pouvez utiliser Windows Azure Online Backup pour sauvegarder et protéger des données essentielles à partir de n'importe quel emplacement.



Windows Azure Online Backup est basé sur la plate-forme Windows Azure et utilise le stockage des objets BLOB de Windows Azure pour conserver les données client. Windows Server 2012 utilise l'agent Windows Azure Online Backup pour transférer des données de fichiers et dossiers de manière sécurisée vers Windows Azure Online Backup. Cet agent peut être téléchargé. Une fois l'agent Windows Azure Online Backup installé, il intègre ses fonctionnalités dans l'interface de sauvegarde Windows Server.

Fonctionnalités clés

Les fonctionnalités clés fournies par Windows Server 2012 par l'intermédiaire de Windows Azure Online Backup comprennent :

- Configuration et gestion simples. L'intégration à l'outil Sauvegarde Windows Server fournit une expérience transparente de sauvegarde et de restauration sur un disque local ou vers une plateforme de cloud. Autres fonctionnalités :
  - interface utilisateur simple pour configurer et surveiller les sauvegardes ;
  - expérience de récupération intégrée pour récupérer des fichiers et dossiers à partir d'un disque local ou d'une plateforme de cloud ;
  - récupération aisée des données sauvegardées sur un serveur quelconque ;
  - capacité d'écriture de scripts fournie par l'interface de ligne de commande Windows PowerShell.
- Sauvegardes incrémentielles au niveau des blocs. L'agent Windows Azure Online Backup effectue des sauvegardes incrémentielles en effectuant le suivi des modifications au niveau des fichiers et des blocs, et transfère uniquement les blocs modifiés, ce qui réduit le stockage et l'utilisation de bande passante. Les différentes versions des sauvegardes, enregistrées à des moments différents, utilisent efficacement le stockage en stockant uniquement les blocs qui ont été modifiés entre ces versions.

- Compression, chiffrement et limitation des données. L'agent Windows Azure Online Backup garantit la compression et le chiffrement des données sur le serveur avant leur envoi au composant Windows Azure Online Backup sur le réseau. Par conséquent, Windows Azure Online Backup stocke uniquement les données chiffrées dans le stockage dans le cloud. Le service Windows Azure Online Backup ne dispose pas de la phrase secrète de chiffrement. Par conséquent, les données ne sont jamais déchiffrées dans le cloud. De plus, les utilisateurs peuvent configurer la limitation et la manière dont Windows Azure Online Backup utilise la bande passante réseau lors de la sauvegarde ou de la restauration des informations.
- Vérification de l'intégrité des données dans le cloud. Outre les sauvegardes sécurisées, l'intégrité des données sauvegardées est automatiquement vérifiée à la fin de la sauvegarde. Par conséquent, vous pouvez identifier tout endommagement susceptible de se produire pendant le transfert des données et la Sauvegarde de Windows Azure les résoudra automatiquement lors de la sauvegarde suivante.
- Stratégies de rétention configurables pour le stockage de données dans le cloud. Le service Windows Azure Online Backup accepte et implémente des stratégies de rétention pour recycler des sauvegardes qui dépassent la plage de rétention souhaitée, répondant ainsi aux stratégies de l'entreprise et permettant la gestion des coûts de sauvegarde.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Planification et implémentation des stratégies de sauvegarde

Cette leçon examine les éléments de planification nécessaires qui constituent un processus de sauvegarde abouti, gérable et sécurisé. Vous pouvez appliquer ces éléments à prendre en compte lorsque vous planifiez la sauvegarde de différents types de données sur votre réseau. En règle générale, vous devez distribuer les tâches de sauvegarde entre les différents serveurs et employés de votre environnement.

Objectifs de la leçon

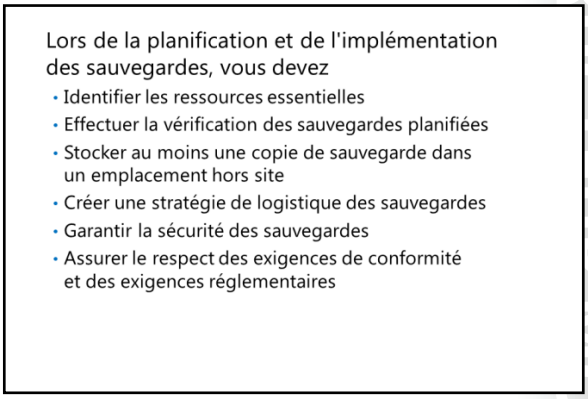
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire le processus de planification de la sauvegarde des serveurs ;
- définir les options de sauvegarde AD DS ;
- sauvegarder les rôles Windows Server 2012 ;
- sauvegarder le stockage des fichiers ;
- sauvegarder les serveurs Windows ;
- sauvegarder les serveurs Windows à l'aide de DPM ;
- planifier votre stratégie de sauvegarde.

Options de planification des sauvegardes des serveurs

Lors de la planification des sauvegardes dans l'ensemble de votre organisation, vous devez veiller à protéger les ressources que vous considérez essentielles en :

- identifiant les ressources essentielles ;
- effectuant la vérification des sauvegardes planifiées ;
- stockant les sauvegardes dans un emplacement hors site ;
- créant une stratégie de logistique des sauvegardes ;
- garantissant la sécurité des sauvegardes ;
- garantissant le respect des exigences de conformité et des exigences réglementaires.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Détermination des ressources essentielles à sauvegarder

Dans un scénario idéal, vous sauvegarderiez tout, puis restaureriez instantanément les données telles qu'elles existaient à un moment quelconque au cours des dernières années. Toutefois, dans la réalité, ce type de stratégie de sauvegarde serait onéreux et consommerait d'importantes ressources de stockage. Par conséquent, la première étape de la planification de la sauvegarde au sein de votre entreprise consiste à déterminer les données qu'il vous faut sauvegarder.

Par exemple, vous devez déterminer si vous devez sauvegarder chaque contrôleur de domaine, vu que les informations AD DS seront répliquées en retour sur un contrôleur de domaine de remplacement dès sa promotion. Vous devez également déterminer s'il est nécessaire de sauvegarder chaque serveur de fichiers dans tous les partages de fichiers si chaque fichier est répliqué sur plusieurs serveurs par l'intermédiaire d'un système de fichiers distribués.

Vous devez également distinguer les raisons techniques et les raisons réglementaires liées à la sauvegarde des données. En raison d'obligations légales, vous pouvez être amené à récupérer des données vitales pour l'entreprise âgées de plus de 10 ans.

Lorsque vous déterminez les données à sauvegarder, vous devez prendre en compte si :

- les données sont stockées dans un seul emplacement : dans ce cas, assurez-vous que cet emplacement fait l'objet d'une sauvegarde ;
- les données sont répliquées : dans ce cas, il n'est peut être pas nécessaire de sauvegarder chaque réplica ; toutefois, vous devez sauvegarder au moins un emplacement pour vous assurer de pouvoir restaurer la sauvegarde ;
- le serveur ou les données sont des composants essentiels : si tel est le cas, vous devez les sauvegarder ;
- des étapes spécifiques doivent être exécutées pour récupérer un serveur ou un disque défaillant ou pour récupérer des données endommagées.

De nombreuses organisations assurent la disponibilité des services et des données essentielles par redondance. Par exemple, Exchange Server 2010 et 2013 assurent la réplication continue des bases de données de boîtes aux lettres sur les autres serveurs à l'aide des groupes de disponibilité de base de données, et certaines organisations peuvent choisir de ne pas exécuter de sauvegarde et d'utiliser les fonctionnalités de protection des données natives Exchange. Toutefois, l'utilisation des groupes de disponibilité de base de données ne signifie pas qu'aucune organisation ne doit sauvegarder ses serveurs de boîtes aux lettres Exchange Server. Cela change la manière dont une organisation doit sauvegarder ses serveurs de boîtes aux lettres ou planifier ses stratégies de sauvegarde.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vérification de vos sauvegardes

Vous pouvez effectuer une sauvegarde ou vous assurer que la sauvegarde contient tout ce dont vous avez besoin. Vous devez mettre en place une méthode pour vérifier que chaque sauvegarde est un succès et vous devez également savoir quand une sauvegarde échoue. Au minimum, ceci signifie que vous devez vérifier les journaux de chaque serveur pour déterminer si un échec s'est produit. Par exemple, si vous avez configuré des sauvegardes sur chaque serveur toutes les six heures, vous devez déterminer la fréquence à laquelle vous devez vérifier les journaux. Vous pouvez utiliser un mécanisme d'alerte disponible dans Microsoft System Center 2012 - Operations Manager (Operations Manager) pour être averti de l'échec d'une sauvegarde. La meilleure pratique consiste à être averti des échecs des sauvegardes dès qu'ils se produisent. De cette manière, vous ne découvrirez pas que vos sauvegardes d'un serveur particulier ont échoué au moment même où vous aurez besoin de ces sauvegardes pour une récupération.

Une manière de vérifier les sauvegardes consiste à effectuer un test régulier de vos procédures de récupération, dans lesquelles vous simulez un échec particulier. Ceci vous permet de vérifier l'intégrité des données que vous utilisez pour effectuer une récupération, mais aussi que vos procédures de récupération résolvent efficacement une défaillance. Il vaut mieux découvrir que vous devez ajouter des étapes à votre procédure de récupération lors d'un test, plutôt que lors d'une défaillance réelle.

Stockage des sauvegardes dans un emplacement hors site

Les organisations doivent conserver au moins deux copies des supports de sauvegarde. Les organisations doivent stocker une copie dans leur centre de données et stocker l'autre copie dans un emplacement hors site. Vous pouvez déterminer votre emplacement de stockage hors site en fonction de votre type d'organisation (banque, institution gouvernementale) ou en fonction des obligations légales en vigueur dans le pays spécifique où se situe votre organisation. Vous pouvez également décider que des employés transporteront les copies de vos supports de sauvegarde vers votre emplacement hors site ou vous pouvez les copier dans l'emplacement hors site par l'intermédiaire du réseau privé de votre organisation. Certaines organisations répliquent leurs données critiques, puis effectuent des sauvegardes à la fois dans l'emplacement central et dans l'emplacement hors site.

Création d'une logistique des sauvegardes

Les procédures de sauvegarde stockent les données sur différents types de support. Ces supports doivent être stockés dans un emplacement de stockage protégé contre les inondations et les incendies. Chaque support de sauvegarde doit être étiqueté avec des informations telles que la date de la sauvegarde, le type de sauvegarde (complète, incrémentielle) et les données qui sont stockées (par exemple, la base de données Exchange Server des responsables ou la base de données SQL Server des données financières). Les organisations doivent également décider si elles utiliseront un nouveau support de sauvegarde pour chaque nouvelle sauvegarde qu'elles effectueront, ou si elles implémenteront un schéma de rotation dans lequel un ancien support de sauvegarde sera supprimé et réutilisé. Par exemple, une organisation peut effectuer une sauvegarde quotidienne et utiliser un nouveau support chaque jour, du lundi au vendredi. Le support de la sauvegarde du vendredi sera stocké à part et remplacé par un nouveau support, alors que tous les autres supports de sauvegarde de la semaine précédente seront remplacés du lundi au jeudi. Le support de sauvegarde du vendredi suivant sera de nouveau stocké à part et remplacé par un nouveau support. À la fin de l'année, l'organisation aura des copies des données de chaque semaine de l'année. Ces supports de sauvegarde pourront également être réutilisés quelques années plus tard, s'ils ne sont plus requis.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Confirmation de la sécurisation des sauvegardes

Par définition, un bon jeu de sauvegardes contient toutes les données essentielles de votre organisation que vous devez protéger contre tout accès non autorisé. Bien que vous puissiez protéger vos données à l'aide d'autorisations et de contrôles d'accès alors qu'elles sont hébergées sur des serveurs dans un environnement de production, toute personne ayant accès au support qui héberge ces données de sauvegarde peut les restaurer. Par exemple, certains produits, tels que la Sauvegarde Windows Server, ne permettent pas aux administrateurs de chiffrer les données de sauvegarde. Cela signifie que la sécurité physique est la seule manière de s'assurer que ces données essentielles ne tombent pas aux mains d'utilisateurs non autorisés.

En développant une stratégie de sauvegarde d'entreprise, assurez-vous de stocker vos données de sauvegarde en lieu sûr.

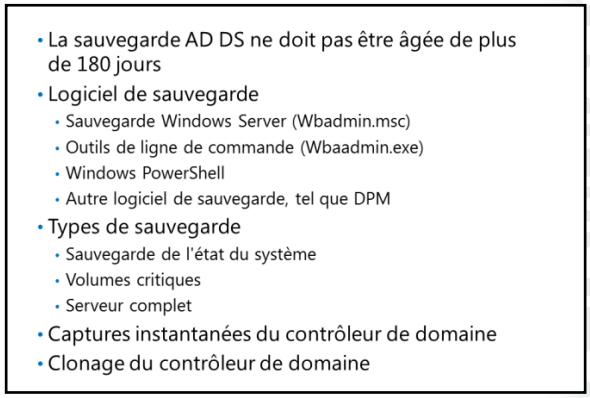
Vous devez également envisager d'utiliser un logiciel de sauvegarde vous permettant de fractionner les rôles de sauvegarde et de restauration, de sorte que les utilisateurs dotés d'autorisations de sauvegarde des données ne disposent pas d'autorisations pour restaurer ces données, et inversement, que les utilisateurs dotés d'autorisations de restauration des données ne disposent pas d'autorisations pour les sauvegarder.

Vérification de la conformité et du respect des responsabilités réglementaires

Les administrateurs système doivent être conscients des responsabilités réglementaires et de conformité de l'organisation en matière d'archivage des données. Par exemple, la politique de certaines organisations requiert que les données des messages électroniques relatives à l'entreprise soient conservées pendant sept ans. Malheureusement, les exigences réglementaires varient d'un pays à l'autre, et même d'une région à une autre. En développant la stratégie de protection des données de votre organisation, vous devez prévoir une réunion avec l'équipe juridique de votre organisation pour déterminer avec précision les données qui doivent être stockées et la durée de stockage requise.

Options de sauvegarde AD DS

La sauvegarde du rôle AD DS est une procédure très importante et doit faire partie de tout processus ou stratégie de sauvegarde et de récupération.



En sauvegardant AD DS, vous devez prendre en compte :

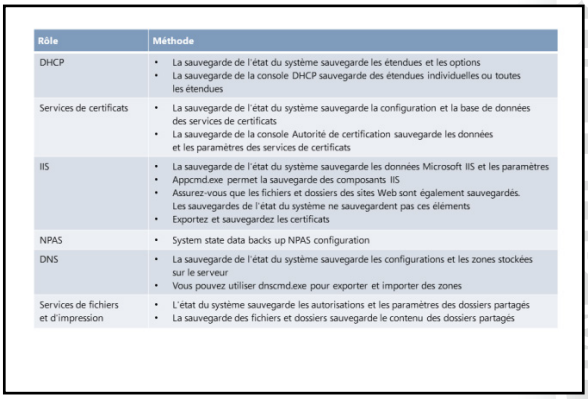
- Votre planification de sauvegarde. Il est primordial que vous planifiiez vos sauvegardes AD DS, parce que vous ne pouvez pas restaurer une sauvegarde de plus de 180 jours. En effet, lorsqu'un annuaire Active Directory est supprimé, les informations sur cette suppression sont conservées pendant 180 jours. Si vous possédez une sauvegarde qui n'est pas antérieure à 180 jours, vous pourrez restaurer l'objet supprimé. Si votre sauvegarde est antérieure à 180 jours, la procédure de restauration ne répliquera pas l'objet restauré sur un autre contrôleur de domaine, ce qui se traduira par un état incohérent des données AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Les outils de sauvegarde disponibles pour AD DS. Vous avez le choix entre quatre options :
  - Sauvegarde Windows Server (Wbadmin.msc)
  - Interface de ligne de commande (Wbaadmin.exe)
  - Windows PowerShell
  - Logiciel de sauvegarde, tel que DPM
- Les types de sauvegarde. Il existe différents types de sauvegarde, notamment :
  - *Sauvegarde de l'état du système*. Seules les données système sont sauvegardées et les données qui sont sauvegardées dépendent des rôles que vous installez sur le serveur.
  - *Volumes critiques*. Cela permet la sauvegarde des volumes sur lesquels vous enregistrez les fichiers d'état du système.
  - *Serveur complet*. Cela permet de sauvegarder le serveur entier, y compris tous les volumes sur le serveur ciblé.
- Des captures instantanées du contrôleur de domaine. Si le contrôleur de domaine s'exécute en tant qu'ordinateur virtuel, vous pouvez envisager de créer une capture instantanée, afin d'enregistrer l'état de votre contrôleur de domaine sain et opérationnel.
- Le clonage du contrôleur de domaine. Si le contrôleur de domaine s'exécute en tant qu'ordinateur virtuel, vous pouvez envisager de créer un clone, que vous pouvez utiliser pendant le déploiement rapide d'autres contrôleurs de domaine et à des fins de restauration.

Options de sauvegarde des rôles Windows Server 2012

Vous pouvez sauvegarder quasiment tous les services sur des ordinateurs exécutant Windows Server 2012 en effectuant une sauvegarde de l'état du système. Certains services permettent également la sauvegarde de la configuration et des données à partir de leurs consoles de gestion respectives.



Rôle	Méthode
DHCP	• La sauvegarde de l'état du système sauvegarde les étendues et les options • La sauvegarde de la console DHCP sauvegarde des étendues individuelles ou toutes les étendues
Services de certificats	• La sauvegarde de l'état du système sauvegarde la configuration et la base de données des services de certificats • La sauvegarde de la console Autorité de certification sauvegarde les données et les paramètres des services de certificats
IIS	• La sauvegarde de l'état du système sauvegarde les données Microsoft IIS et les paramètres • Appcmd.exe permet la sauvegarde des composants IIS • Assurez-vous que les fichiers et dossiers des sites Web sont également sauvegardés. Les sauvegardes de l'état du système ne sauvegardent pas ces éléments • Exportez et sauvegardez les certificats
NPAS	• System state data backs up NPAS configuration
DNS	• La sauvegarde de l'état du système sauvegarde les configurations et les zones stockées sur le serveur • Vous pouvez utiliser dnscmd.exe pour exporter et importer des zones
Services de fichiers et d'impression	• L'état du système sauvegarde les autorisations et les paramètres des dossiers partagés • La sauvegarde des fichiers et dossiers sauvegarde le contenu des dossiers partagés

Sauvegarde des rôles

Le tableau ci-dessous répertorie les méthodes que vous pouvez utiliser pour sauvegarder des rôles spécifiques sur des ordinateurs exécutant Windows Server 2012.

Rôle	Méthode
DHCP	• La sauvegarde de l'état du système sauvegarde les étendues et les options. • La sauvegarde de la console DHCP sauvegarde des étendues individuelles ou toutes les étendues.
Services de certificats	• La sauvegarde de l'état du système sauvegarde la configuration et la base de données des services de certificats. • La sauvegarde de la console Autorité de certification sauvegarde les données et les paramètres des services de certificats.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Rôle	Méthode
IIS	• La sauvegarde de l'état du système sauvegarde les données Microsoft Internet Information Services (IIS) et les paramètres. • Appcmd.exe permet la sauvegarde des composants IIS. • Assurez-vous que les fichiers et dossiers des sites Web sont également sauvegardés. Les sauvegardes de l'état du système ne sauvegardent pas ces éléments. • Exportez et sauvegardez les certificats.
Services de stratégie et d'accès réseau (NPAS)	• Les données de l'état du système sauvegardent la configuration NPAS.
DNS	• La sauvegarde de l'état du système sauvegarde les configurations et les zones stockées sur le serveur. • Vous pouvez utiliser dnscmd.exe pour exporter et importer des zones.
Services de fichiers et d'impression	• L'état du système sauvegarde les autorisations et les paramètres des dossiers partagés. • La sauvegarde des fichiers et dossiers sauvegarde le contenu des dossiers partagés.

Remarque : Certaines applications serveur, telles qu'Exchange Server et SQL Server, s'inscrivent avec la Sauvegarde Windows Server. Cela permet à la Sauvegarde Windows Server de sauvegarder et restaurer ces applications, selon les besoins. En général, vous devez vérifier la documentation d'un fournisseur pour rechercher des recommandations spécifiques concernant la façon de garantir la sauvegarde réussie d'une application spécifique.

Options de sauvegarde du stockage de fichiers

Dans de nombreuses organisations, les technologies et solutions de stockage de fichiers jouent un rôle essentiel et vous devez soigneusement planifier les scénarios de sauvegarde et de restauration.

Les solutions de stockage de fichiers incluent
- Serveurs de fichiers
- DFSEspaces de stockage
- CSV

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

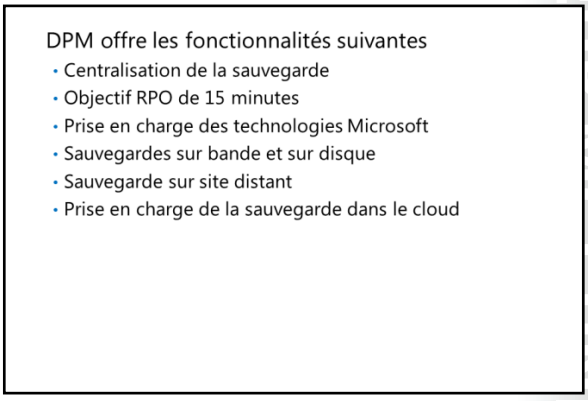
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les solutions de stockage de fichiers incluent :

- Serveurs de fichiers. En fonction de l'importance des données, vous devez développer différentes stratégies de sauvegarde et de restauration pour chaque serveur de fichiers. En outre, vous devez vous assurer que vos serveurs de fichiers sont protégés par des procédures de sauvegarde sur les dossiers partagés contenant les données.
- Système de fichiers distribués (DFS). Avant de sauvegarder les données qui se trouvent dans le système DFS, consultez la documentation de votre logiciel de sauvegarde. De nombreuses solutions logicielles de sauvegarde reconnaissent le système DFS, si bien que vous pouvez configurer la sauvegarde en sélectionnant l'espace de noms DFS approprié. Vous devez également sauvegarder vos serveurs répliqués, ainsi que l'état du système sur le serveur racine DFS pour pouvoir sauvegarder les données de configuration DFS.
- Espaces de stockage. Si vous organisez vos serveurs de fichiers pour utiliser des espaces de stockage, vous devez sauvegarder les données sur des volumes logiques que les espaces de stockage créeront. Certaines organisations peuvent considérer les espaces de stockage comme une solution pour la protection des données, puisqu'ils peuvent assurer la redondance des données. Toutefois, vous devez être conscient que si vous supprimez des fichiers, la seule manière de les restaurer consiste à les extraire de votre sauvegarde.
- Volumes partagés de cluster (CSV). Windows Server 2012 permet une interopérabilité améliorée avec différentes solutions logicielles de sauvegarde lors de l'implémentation de vos procédures de sauvegarde et de restauration sur les volumes de partage en cluster. Ceci tient au fait que le logiciel de sauvegarde ne doit pas nécessairement prendre en charge les volumes CSV. Pendant la sauvegarde, Windows crée une capture instantanée distribuée conforme à une application. En outre, la procédure de sauvegarde n'a pas besoin de l'appartenance aux volumes CSV, ce qui signifie que des sauvegardes parallèles peuvent être effectuées sur des volumes CSV ou des nœuds en cluster identiques ou différents. Dans Windows Server 2012, les performances d'E/S pendant le processus de sauvegarde sont améliorées par rapport aux versions précédentes de Windows Server.

Réalisation de sauvegardes Windows Server à l'aide de DPM

Lorsque vous planifiez la sauvegarde d'ordinateurs Windows Server, tenez compte des avantages suivants de DPM :

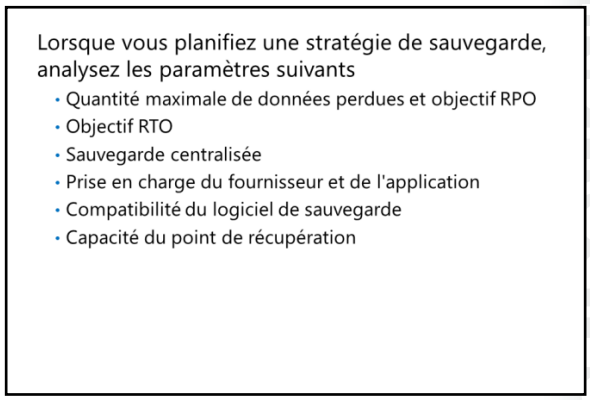


- Centralisation de la sauvegarde. DPM utilise une architecture client/serveur, dans laquelle le logiciel client est installé sur tous les ordinateurs que vous sauvegardez. Ces clients diffusent en continu les données de sauvegarde sur le serveur DPM, ce qui permet à chaque serveur DPM de prendre en charge des petites ou moyennes entreprises complètes. Vous pouvez également gérer plusieurs serveurs DPM à partir d'une même console DPM centralisée.
- Objectif RPO de 15 minutes. DPM permet des captures instantanées toutes les 15 minutes des données protégées, telles que des fichiers, des dossiers, des bases de données Exchange Server, des bases de données SQL Server ou des ordinateurs virtuels Hyper-V®.

- Prise en charge des charges de travail Microsoft. DPM a été conçu spécifiquement par Microsoft pour prendre en charge des applications Microsoft telles qu'Exchange Server, SQL Server et Hyper-V. Toutefois, DPM n'a pas été conçu pour prendre en charge les applications serveur non-Microsoft qui ne possèdent pas des états de disque cohérents ou qui ne prennent pas en charge VSS.
- Sauvegarde sur disque. Vous pouvez configurer DPM pour effectuer des sauvegardes planifiées sur des baies de disque et des réseaux SAN, et pour exporter des données de sauvegarde spécifiques sur bande pour des tâches de conservation et de conformité.
- Sauvegarde sur site distant. DPM utilise une architecture qui lui permet de sauvegarder des clients dans des sites distants. Cela signifie qu'un serveur DPM situé dans les locaux du siège social peut effectuer des sauvegardes des serveurs et des clients par l'intermédiaire de liaisons WAN (réseau étendu).
- Prise en charge des stratégies de sauvegarde dans le cloud. DPM prend en charge la sauvegarde des serveurs DPM, ce qui signifie que vous pouvez utiliser un serveur DPM d'une installation d'hébergement en cloud pour sauvegarder le contenu du serveur DPM d'un autre bureau. Pour bénéficier d'une redondance en cas d'incident, vous pouvez également configurer les serveurs DPM pour une sauvegarde mutuelle.

Planification d'une stratégie de sauvegarde

Lorsque vous planifiez une stratégie de sauvegarde pour votre organisation, vous devez prendre en compte les éléments suivants :



- La quantité maximale de données que vous pouvez vous permettre de perdre. Quel est le RPO théorique du produit ? Les produits qui offrent la restauration la plus proche du point de défaillance sont susceptibles de coûter plus que les produits qui offrent des RPO de 15 ou 30 minutes. Vous devez déterminer les besoins de votre organisation. Votre organisation a-t-elle besoin de récupérer les données jusqu'à la dernière transaction SQL Server ou une fenêtre de récupération de 15 minutes constitue-t-elle un compromis acceptable ?
- Temps de récupération. Vous devez prendre en compte le temps nécessaire entre la défaillance et la restauration des fonctionnalités. La restauration des données jusqu'à la dernière transaction SQL Server constitue la solution optimale. Si deux jours sont nécessaires pour récupérer les données jusqu'à ce point, la solution ne fonctionne pas dans votre entreprise.
- Solutions de sauvegarde centralisées. Vous devez savoir comment le produit vous permet de centraliser votre solution de sauvegarde sur un seul serveur, ou vous devez prendre en compte la manière dont les sauvegardes s'effectuent directement sur chaque serveur de votre organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Prise en charge du fournisseur. Vous ne devez pas utiliser d'interfaces de programmation d'applications (API) non documentées pour sauvegarder et récupérer des produits spécifiques, ou pour sauvegarder des fichiers sans vérifier si le service est dans un état cohérent.
- Compatibilité de l'application. Vous pouvez être amené à déployer une mise à jour produit qui rendra la solution de sauvegarde incompatible. Contactez le fournisseur de l'application pour déterminer si cette dernière prend en charge la solution de sauvegarde en vigueur dans votre entreprise.
- Capacité du point de récupération. Vous devez déterminer la capacité de votre point de récupération. Vous devez également prendre en compte le nombre de points de restauration qu'offre la solution de protection des données de votre entreprise et si ce nombre est approprié aux besoins de votre organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Planification et implémentation de la récupération

La récupération d'urgence est une méthodologie qui décrit les étapes nécessaires à la résolution d'un incident une fois qu'il s'est produit, pour faire en sorte que les données, les services et les serveurs redeviennent opérationnels. Un plan de récupération d'urgence efficace satisfait les besoins de l'organisation sans fournir un niveau de couverture inutile. Bien qu'une protection absolue puisse paraître souhaitable, il est peu probable qu'elle soit économiquement viable. En créant un plan de récupération d'urgence, vous devez équilibrer le coût d'un incident particulier pour l'organisation avec le coût que la protection contre cet incident représente pour l'organisation.

Objectifs de la leçon

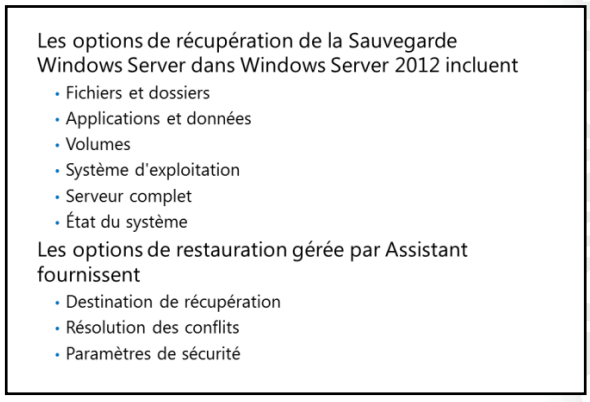
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- planifier la récupération des serveurs ;
- planifier et restaurer AD DS ;
- restaurer les rôles Windows Server 2012 ;
- restaurer les fichiers et les données ;
- restaurer les serveurs Windows ;
- effectuer les restaurations Windows Server à l'aide de DPM ;
- envisager et planifier une stratégie de récupération ;
- implémenter un site de récupération d'urgence.

Options de planification de la récupération des serveurs

La Sauvegarde Windows Server dans Windows Server 2012 fournit les options de récupération suivantes :

- Fichiers et dossiers. Vous pouvez sauvegarder individuellement les fichiers ou les dossiers si la sauvegarde se trouve sur un volume distinct ou dans un dossier partagé distant.
- Applications et données. Vous pouvez récupérer des applications et des données si l'application a un enregistreur VSS et est inscrite pour la Sauvegarde Windows Server.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

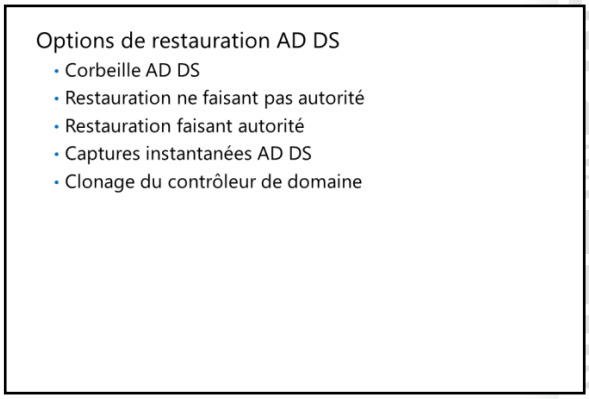
- Volumes. La restauration d'un volume restaure toujours tout son contenu. Lorsque vous choisissez de restaurer un volume, vous ne pouvez pas restaurer des fichiers ou des dossiers spécifiques.
- Système d'exploitation. Vous pouvez récupérer le système d'exploitation via Windows RE, le DVD du produit ou un lecteur flash USB.
- Serveur complet. Vous pouvez récupérer le serveur complet à l'aide de Windows RE.
- État du système. *L*'état du système crée une sauvegarde à un moment donné, que vous pouvez utiliser pour restaurer un serveur à un état de fonctionnement précédent.

L'Assistant Récupération dans la Sauvegarde Windows Server propose plusieurs options pour gérer la récupération des fichiers et des dossiers, dont notamment :

- Destination de récupération. Dans l'option Destination de récupération, vous pouvez sélectionner l'une quelconque des options suivantes :
  - Emplacement d'origine. Restaure les données à l'emplacement de la sauvegarde initiale.
  - Autre emplacement. Restaure les données à un emplacement différent.
- Résolution des conflits. La restauration de données à partir d'une sauvegarde crée fréquemment des conflits avec les versions existantes des données. L'option Résolution de conflit vous permet de déterminer comment gérer ces conflits. Lorsque de tels conflits se produisent, les options suivantes s'offrent à vous :
  - créer des copies et conserver les deux versions ;
  - remplacer la version existante par la version récupérée ;
  - ne pas récupérer les éléments s'ils existent déjà dans l'emplacement de récupération.
- Paramètres de sécurité. Utilisez cette option pour restaurer les autorisations sur les données en cours de récupération.

Options de restauration AD DS

AD DS est le service le plus important dans toute organisation. Chaque contrôleur de domaine stocke une copie des données AD DS, de sorte que la planification soignée de votre stratégie de sauvegarde et de restauration AD DS est une priorité pour tout service informatique. Il est très important de garder à l'esprit que vous pouvez restaurer uniquement des sauvegardes de moins de 180 jours.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous planifiez vos stratégies de restauration Active Directory, les options suivantes s'offrent à vous :

- Corbeille Active Directory. Vous utiliserez la Corbeille Active Directory dans un scénario où un objet est supprimé d'AD DS. Vous pouvez alors utiliser la console GUI du Centre d'administration Active Directory pour restaurer l'objet. Si votre organisation possède un niveau fonctionnel de forêt AD DS correspondant à Windows Server 2008 R2 ou à une version plus récente, vous devez activer la Corbeille Active Directory dans Windows PowerShell ou à l'aide de l'outil ldp.exe avant de pouvoir utiliser cette fonctionnalité. Une fois que vous avez activé la Corbeille Active Directory, vous ne pouvez plus la désactiver.
- Restauration ne faisant pas autorité. Lorsque vous restaurez et mettez en ligne un contrôleur de domaine défaillant, il établira la communication avec les autres contrôleurs de domaine. Le moment où vous avez effectué la sauvegarde est antérieur à la date de restauration, si bien que les autres contrôleurs de domaine répliqueront leurs données AD DS actuelles sur le contrôleur de domaine restauré. Ainsi, lorsque le processus de restauration sera terminé, les données du contrôleur de domaine restauré seront à jour. Ceci est dû au fait que le réplication AD DS utilise un horodateur, si bien que les attributs plus récents de l'objet AD DS sont toujours répliqués vers les attributs plus anciens de l'objet AD DS. Vous devez utiliser la restauration ne faisant pas autorité dans un scénario où un contrôleur de domaine est détruit suite à une défaillance matérielle. Pour effectuer une restauration ne faisant pas autorité, vous devez démarrer le contrôleur de domaine en mode de réparation des services d'annuaire.

 **Remarque :** Ce type de restauration n'est pas approprié lorsqu'un compte d'utilisateur est supprimé. Si vous essayez de restaurer un compte d'utilisateur supprimé à l'aide d'une restauration ne faisant pas autorité, le processus de réplication à partir des autres contrôleurs de domaine supprimera de nouveau le compte d'utilisateur. Ceci se produit car les données restaurées à partir de la sauvegarde ont un horodateur plus ancien que le processus qui a supprimé le compte d'utilisateur.

- Restauration faisant autorité. La restauration faisant autorité répond à un scénario dans lequel la procédure de restauration se produit et où l'objet ou l'attribut supprimé restauré est supprimé de nouveau au cours du processus de réplication. Dans une restauration faisant autorité, une fois que vous effectuez une restauration, l'objet ou l'attribut sélectionné est modifié. Cela signifie que l'horodateur est remplacé par une valeur supérieure par rapport aux horodateurs des réplicas sur les autres contrôleurs de domaine. Cette modification survient avant qu'un contrôleur de domaine puisse communiquer avec les autres contrôleurs de domaine du réseau. Par conséquent, dans ce scénario, l'objet ou l'attribut AD DS est restauré, marqué comme faisant autorité, puis répliqué sur les autres contrôleurs de domaine, en raison d'une valeur d'horodateur supérieure. Pour effectuer une restauration faisant autorité, vous devez démarrer le contrôleur de domaine en mode de réparation des services d'annuaire et utiliser l'outil **ntdsutil**.

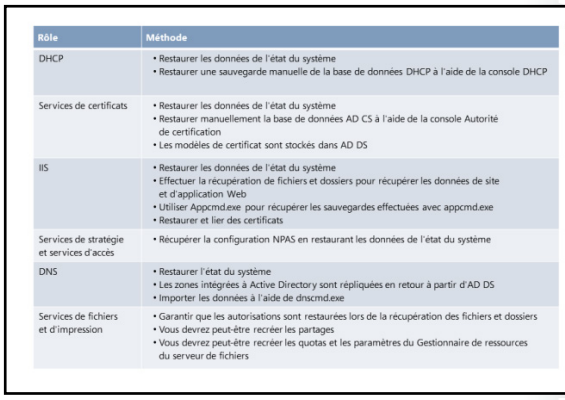
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Captures instantanées AD DS. Si Windows Server 2012 s'exécute dans un environnement virtuel, vous pouvez restaurer un contrôleur de domaine à l'aide des captures instantanées des ordinateurs virtuels. Une fois que vous aurez restauré un contrôleur de domaine, il exécutera une restauration ne faisant pas autorité. Cela fonctionne bien si un contrôleur de domaine présente un dysfonctionnement. Vous pouvez alors utiliser la capture instantanée pour rétablir l'état du contrôleur de domaine à l'état qu'il présentait au moment de la capture instantanée.
- Le clonage du contrôleur de domaine. Si Windows Server 2012 s'exécute dans un environnement virtuel, vous pouvez utiliser un contrôleur de domaine clone. Ce type de restauration est utile si un contrôleur de domaine présente une défaillance matérielle majeure, car vous pouvez déployer une nouvelle copie du contrôleur de domaine dans un délai très court.

Restauration des rôles Windows Server 2012

Vous pouvez récupérer la configuration de la majorité des composants de Windows Server 2012 en effectuant la récupération de l'état du système. Il est également possible, avec certains composants, d'exécuter une récupération en utilisant les outils disponibles dans la console de gestion associée au rôle.

Le tableau ci-dessous répertorie les méthodes que vous pouvez utiliser pour récupérer les rôles spécifiques Windows Server 2012 et les données associées.



Rôle	Méthode
DHCP	• Restaurer les données de l'état du système • Restaurer une sauvegarde manuelle de la base de données DHCP à l'aide de la console DHCP
Services de certificats	• Restaurer les données de l'état du système • Restaurer manuellement la base de données AD CS à l'aide de la console Autorité de certification • Les modèles de certificat sont stockés dans AD DS
IIS	• Restaurer les données de l'état du système • Effectuer la récupération de fichiers et dossiers pour récupérer les données de site et d'application Web • Utiliser Appcmd.exe pour récupérer les sauvegardes effectuées avec appcmd.exe • Restaurer et lier des certificats
Services de stratégie et services d'accès	• Récupérer la configuration NPAS en restaurant les données de l'état du système
DNS	• Restaurer l'état du système • Les zones intégrées à Active Directory sont répliquées en retour à partir d'AD DS • Importer les données à l'aide de dnscmd.exe
Services de fichiers et d'impression	• Garantir que les autorisations sont restaurées lors de la récupération des fichiers et dossiers • Vous devrez peut-être recréer les partages • Vous devrez peut-être recréer les quotas et les paramètres du Gestionnaire de ressources du serveur de fichiers

Rôle	Méthode
DHCP	• Restaurer les données de l'état du système. • Restaurer une sauvegarde manuelle d'une base de données DHCP à l'aide de la console DHCP.
Services de certificats	• Restaurer les données de l'état du système. • Restaurer une base de données AD CS manuellement à l'aide de la console Autorité de certification. • Stocker des modèles de certificats dans AD DS.
IIS	• Restaurer les données de l'état du système. • Effectuer la récupération de fichiers et dossiers pour récupérer des applications Web et des données de site. • Utiliser Appcmd.exe pour récupérer des sauvegardes effectuées avec appcmd.exe. • Restaurer et lier des certificats.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

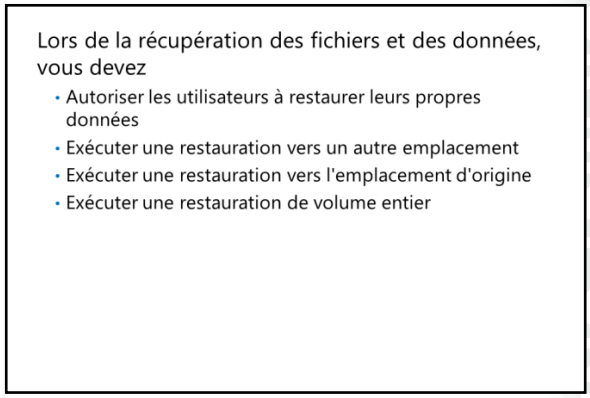
(suite)

Rôle	Méthode
Services de stratégie et services d'accès	• Récupérer la configuration de la stratégie réseau et • des services d'accès en restaurant les données de l'état du système.
DNS	• Restaurer l'état du système. • Répliquer les zones intégrées à Active Directory à partir d'AD DS. • Importer les données à l'aide de dnscmd.exe.
Services de fichiers et d'impression	• Garantir que les autorisations sont restaurées lors de la récupération des fichiers et dossiers. • Recréer les partages, si nécessaire. • Recréer les quotas et les paramètres du Gestionnaire de ressources du serveur de fichiers (FSRM), si nécessaire.

Remarque : L'inconvénient de la réalisation d'une récupération de l'état du système est qu'elle récupère tous les paramètres de l'état du système. Vous ne pouvez pas choisir de restaurer certains paramètres et pas d'autres. Par exemple, vous pouvez modifier les paramètres d'étendue DHCP de votre organisation, puis déterminer que vous devez effectuer une récupération sur la base de données d'autorité de certification d'entreprise hébergée sur le même serveur. La récupération de l'état du système réinitialise les paramètres DHCP et la base de données d'autorité de certification d'entreprise à l'état où ils étaient quand la sauvegarde a été effectuée, annulant ainsi de ce fait les modifications apportées à vos paramètres d'étendue DHCP.

Restauration des fichiers et des données

Les fichiers et les données sont les composants que vous restaurerez le plus souvent dans vos infrastructures informatiques. Ceci tient au fait que vous les récupérez en général après que les utilisateurs les ont supprimés par inadvertance. Vous pouvez utiliser les stratégies suivantes lorsque vous développez une procédure de restauration pour les fichiers et les données :



- autoriser les utilisateurs à restaurer leurs propres données ;
- exécuter une restauration vers un autre emplacement ;
- exécuter une restauration vers l'emplacement d'origine ;
- exécuter une restauration de volume entier.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Autoriser les utilisateurs à restaurer leurs fichiers et données

La forme de restauration de données la plus couramment effectuée par les services informatiques est la restauration de fichiers et dossiers que les utilisateurs ont supprimés, perdus ou endommagés d'une certaine façon. La fonctionnalité Version précédente des fichiers, qui a été introduite dans Windows Server 2003 et que vous pouvez également activer sur tous les ordinateurs exécutant Windows Server 2012, permet aux utilisateurs de restaurer leurs propres fichiers à l'aide des propriétés de fichiers ou dossiers sur leur station de travail. Une fois que vous aurez formé les utilisateurs finaux à cette procédure, votre service informatique passera moins de temps à récupérer les données des utilisateurs, ce qui permettra à votre personnel informatique de se concentrer sur des tâches plus importantes.

Du point de vue de la planification, vous devriez envisager d'augmenter la fréquence à laquelle les versions précédentes des fichiers sont générées. Cela offre aux utilisateurs davantage d'options pour restaurer leurs fichiers.

Restaurer les fichiers et les données vers un autre emplacement

Lors d'une restauration à partir d'une sauvegarde, un problème courant peut se produire : le remplacement involontaire de données importantes. Ceci peut se produire lorsque vous effectuez une restauration vers un emplacement contenant des données actives, au lieu d'un emplacement distinct où vous pouvez extraire les données requises et ignorer les données inutiles.

Lorsque vous effectuez une restauration vers un autre emplacement, assurez-vous toujours que les autorisations sont également restaurées. Il arrive couramment que des administrateurs récupèrent des données contenant des informations sensibles vers un emplacement où aucune autorisation n'est appliquée. Ceci permet alors l'accès à ces données à des utilisateurs non autorisés.

Restaurer les fichiers et les données vers leur emplacement d'origine

Lors de certaines défaillances, telles que l'endommagement ou la suppression de données, vous devez restaurer les données à leur emplacement d'origine. C'est le cas lorsque des applications ou des utilisateurs qui accèdent aux données sont préconfigurés avec des informations sur l'emplacement de ces données.

Restaurer un volume

En cas de défaillance d'un disque, la manière la plus rapide de restaurer les données peut être d'effectuer une récupération de volume, au lieu d'une restauration sélective de fichiers et dossiers. Lorsque vous effectuez une récupération de volume, vérifiez si des dossiers partagés sont configurés pour les disques et si les quotas et les stratégies de gestion du Gestionnaire de ressources du serveur de fichiers sont toujours en vigueur.

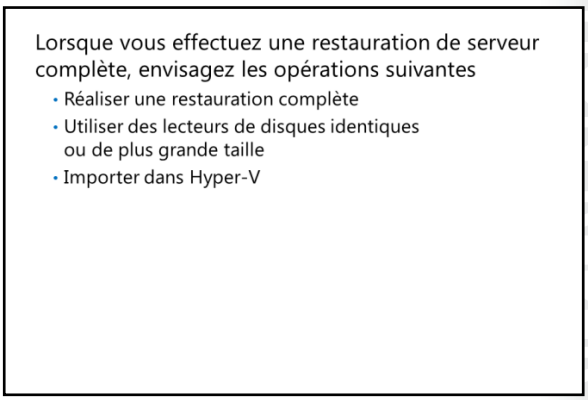


Remarque : Dans le cadre du processus de restauration, vous devriez copier les journaux des événements avant de démarrer le processus de restauration. Si vous remplacez les fichiers journaux d'événements, par une récupération système, par exemple, vous ne pourrez pas lire les informations de journal des événements antérieures au début de la restauration. Toutefois, ce journal des événements pourrait s'avérer très important en vous aidant à comprendre la cause initiale du problème.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Restauration des serveurs Windows

Vous pouvez effectuer une restauration de serveur en démarrant l'ordinateur à partir du support d'installation de Windows Server 2012, en sélectionnant l'option de réparation d'ordinateur, puis en sélectionnant l'option de restauration de serveur complète. Vous pouvez également utiliser le support d'installation sur un lecteur flash USB ou à l'aide de l'environnement de récupération Windows (Windows RE).



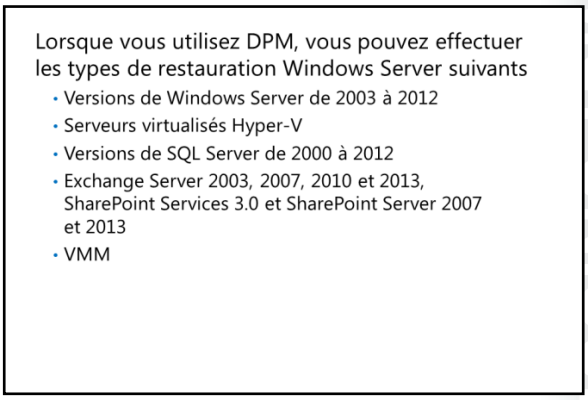
Lorsque vous effectuez une restauration de serveur complet, plusieurs options s'offrent à vous :

- Mener une restauration complète. Une restauration complète est un processus au cours duquel vous restaurez un serveur existant dans sa totalité sur un matériel neuf ou de remplacement. Quand vous effectuez une restauration complète, le serveur redémarre et devient opérationnel. Dans certains cas, il peut être nécessaire de réinitialiser le compte Active Directory de l'ordinateur parce que ces comptes peuvent parfois être désynchronisés.
- Utiliser des lecteurs de disques identiques ou de plus grande taille. Le matériel de serveur sur lequel vous restaurez doit posséder des disques durs de capacité identique ou supérieure à celle des disques du serveur hôte d'origine. Si ce n'est pas le cas, la restauration échouera. Il est possible, bien que cela ne soit pas recommandé, de restaurer sur des hôtes dotés de processeurs plus lents et d'une mémoire vive (RAM) moindre.
- Importer vers Hyper-V. Les données de sauvegarde du serveur sont écrites au format VHD (disque dur virtuel), qui est également le format utilisé pour les disques durs des ordinateurs virtuels. Si vous faites attention, vous pouvez utiliser les données de sauvegarde du serveur complet comme base pour créer un ordinateur virtuel, ce qui garantit la continuité des activités pendant la recherche du matériel de remplacement approprié.

Restaurations Windows Server à l'aide de Data Protection Manager

Vous pouvez utiliser DPM pour restaurer les éléments suivants :

- les versions de Windows Server de 2003 à 2012 au niveau de l'état du système, des volumes, des partages, des dossiers ou des fichiers ;
- des serveurs virtualisés Hyper-V au niveau des volumes, des dossiers, des fichiers ou VHD ;
- les versions de SQL Server de 2000 à 2012 au niveau des bases de données ;

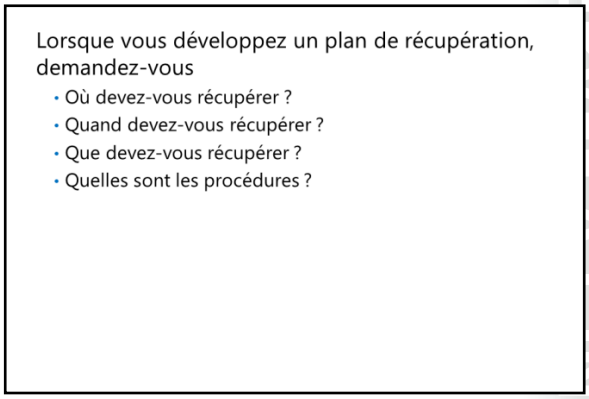


UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Exchange Server 2003 et 2007 au niveau des groupes de stockage, des bases de données ou des boîtes aux lettres, et Exchange Server 2010 et 2013 au niveau des bases de données ou des boîtes aux lettres, y compris les bases de données protégées à l'aide d'un DAG ;
- SharePoint Services 3.0 et SharePoint Server 2007, 2010 et 2013 sur une batterie, une base de données, une application Web, un fichier ou un élément de liste, la recherche SharePoint et un serveur Web frontal SharePoint ;
- Microsoft System Center 2012 Virtual Machine Manager (VMM) au niveau des bases de données.

Planification d'une stratégie de récupération

Pour vous assurer que votre organisation répond aux objectifs RTO stipulés dans vos contrats SLA, veillez à documenter toutes les procédures de récupération et assurez-vous qu'elles sont faciles à suivre. En outre, vous devez vous assurer que vous et le personnel de votre organisation n'aurez pas à déterminer comment effectuer une récupération après qu'une défaillance se sera produite.



Mise au point d'un plan de récupération

Lors du développement de votre plan de récupération, prenez en compte les questions suivantes :

- Où les données récupérées doivent-elles être placées ?
- Quand la récupération doit-elle se produire ?
- Quelles données faut-il récupérer ?

Choix d'un emplacement de récupération des données

Choisir où récupérer les données est moins compliqué si votre organisation possède du matériel de remplacement, tel qu'un lecteur de disque dur de remplacement ou un châssis de serveur complet.

Avec la croissance de la virtualisation, il est de plus en plus souvent inutile d'attendre qu'un matériel spécifique devienne disponible lorsque vous devez exécuter une récupération de serveur complète. Il est possible d'effectuer une récupération temporaire vers un hôte Hyper-V et de lui permettre d'héberger virtuellement le serveur récupéré jusqu'au moment où le matériel de remplacement sera fourni. Cela vous donne le temps nécessaire de migrer de l'ordinateur virtuel à un serveur physique.

Détermination du moment propice à la récupération des données

Si une défaillance se produit et que votre organisation n'a pas d'accord avec un fabricant de matériel pour le remplacement en 24 heures des composants, vous devrez attendre la livraison des composants. Cela peut affecter votre objectif RTO. Une autre solution consiste à effectuer une récupération partielle vers un autre emplacement. Par exemple, en cas de défaillance d'un serveur de fichiers d'une filiale distante, si les composants de remplacement ne seront pas livrés avant 72 heures, vous pouvez décider d'héberger temporairement le partage de fichiers sur un autre serveur de fichiers. Ou bien, si vous utilisez DFS avec les fichiers partagés, vous pouvez créer un nouveau réplica sur le site, puis le supprimer lorsque le fonctionnement du serveur de fichiers d'origine sera rétabli.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sélection des données à récupérer

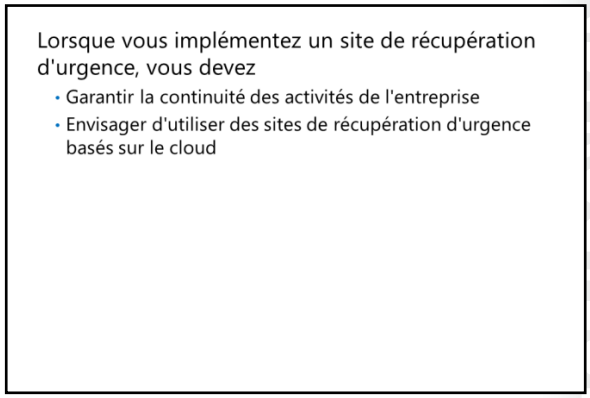
Dans la plupart des cas, vous récupérerez tout ce qui a été sauvegardé. Dans certaines circonstances, vous pouvez opter pour une simple récupération partielle afin de respecter les objectifs de continuité de l'entreprise, en remettant à plus tard la récupération complète. Cela vaut d'être considéré, notamment si une récupération complète prendrait beaucoup de temps, tandis qu'une récupération partielle permettrait à vos utilisateurs de se remettre au travail en peu de temps.

Test des procédures de récupération

Vous devez tester vos stratégies de sauvegarde et de restauration avant de les déployer dans un environnement de production. Vous devez également tester régulièrement vos stratégies de sauvegarde et de restauration en production. Les procédures de test doivent être effectuées de manière à ne pas affecter votre environnement de production. Dans le cadre des tests, vous devez utiliser un environnement isolé et non destiné à la production, ainsi qu'une copie des données de production. De cette façon, vous garantissez que si des défaillances inattendues se produisent, vous pourrez récupérer vos données, services et serveurs dans le délai défini dans le contrat SLA de votre organisation. Comme l'informatique et l'infrastructure informatique de votre organisation sont dynamiques, vous devez constamment évaluer et mettre à jour vos procédures de sauvegarde, de restauration et de test, afin d'assurer la continuité des activités de votre organisation.

Implémentation d'un site de récupération d'urgence

Des sites de récupération d'urgence doivent être mis en service en adéquation avec le matériel si vous souhaitez qu'ils soient utiles si un site est perdu lors d'un incident.



Mise en service d'un site de récupération d'urgence

Lorsque vous mettez en service un site de récupération d'urgence, vous pouvez prendre en compte la virtualisation comme une alternative à l'achat de plusieurs châssis de serveur. Un ordinateur exécutant Windows Server 2012 Datacenter Edition avec Hyper-V, mis en service avec suffisamment de ressources de disque et de RAM, peut faire office de solution de récupération d'urgence. L'édition Datacenter vous permet d'utiliser un nombre illimité d'ordinateurs virtuels. De nombreuses organisations ont consolidé leur infrastructure physique existante sur des hôtes virtuels, si bien que l'utilisation d'un hôte virtuel comme hôte de site de récupération d'urgence est déjà peut être nécessaire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Garantie de la continuité des activités de l'entreprise

La fonction d'un site de récupération d'urgence est d'assurer la continuité des activités si une installation est détruite par une inondation, un incendie ou tout autre incident. La continuité des activités de l'entreprise s'étend au-delà de la disponibilité des serveurs et inclut les ordinateurs clients. Si un site est perdu dans une catastrophe naturelle, votre organisation peut perdre plus que des serveurs critiques ou les ordinateurs clients que vous utilisez pour accéder à ces serveurs. Si vous utilisez une solution d'entreprise pour sauvegarder les clients et les serveurs, vous pouvez utiliser la virtualisation des clients pour héberger les serveurs d'opération d'ordinateur client virtuellement et autoriser l'accès des clients légers à ces serveurs jusqu'à ce que vous puissiez mettre en service du matériel de remplacement.

La garantie de la continuité des activités implique l'audit de l'infrastructure informatique de votre organisation pour déterminer les aspects de cette structure qui doivent rester disponibles pour que vous puissiez maintenir la continuité des activités. Ceci requiert des efforts de planification et de préparation. Vous devez également effectuer des exercices de simulation de la perte totale des sites pour déterminer si vos préparations de récupération d'urgence répondent à vos objectifs de récupération d'urgence. En outre, votre site de récupération d'urgence doit être maintenu aussi à jour que possible. Cela peut impliquer de conserver un contrôleur de domaine AD DS actif sur le site, de posséder des copies locales d'applications, telles que SQL Server et Microsoft Exchange Server, et de configurer la réplication pour que le basculement puisse se produire automatiquement en cas de catastrophe.

Sites de récupération d'urgence basés sur le cloud

Les sites de récupération d'urgence basés sur le cloud deviennent de plus en plus populaires. En cas de défaillance, un fournisseur basé sur le cloud peut fournir à une organisation l'infrastructure temporaire nécessaire pour assurer la continuité des activités de l'entreprise. Une fois que l'organisation a restauré son infrastructure, les services du fournisseur basé sur le cloud ne sont plus nécessaires.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4

Planification et implémentation de la sauvegarde et de la récupération des ordinateurs virtuels

Les organisations qui envisagent de déployer leurs serveurs dans un environnement virtuel doivent avoir un plan détaillé pour la sauvegarde et la récupération. Les administrateurs doivent déterminer le plan de sauvegarde et de restauration de leur organisation, que cette organisation ait déployé uniquement quelques serveurs virtuels ou possède un environnement hautement virtualisé avec un cloud privé. Un plan de sauvegarde et de restauration basé sur les exigences métier d'une organisation est l'un des documents les plus importants qu'un service informatique puisse créer.

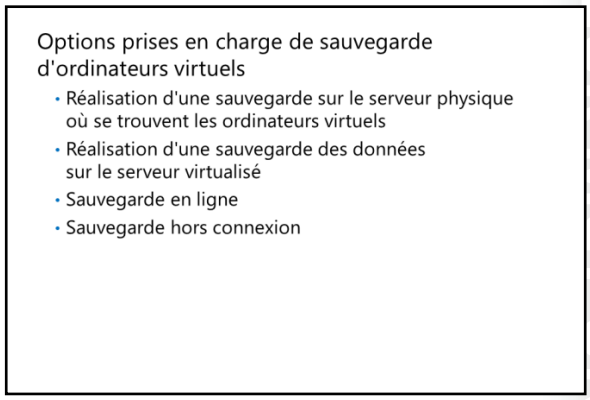
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options d'implémentation d'un plan de sauvegarde pour les ordinateurs virtuels ;
- décrire l'intégration de DPM et d'Hyper-V ;
- planifier le processus de déploiement DPM ;
- configurer les options DPM ;
- utiliser DPM pour sauvegarder les ordinateurs virtuels ;
- utiliser DPM pour restaurer les ordinateurs virtuels ;
- configurer le réplica Hyper-V ;
- décrire les éléments à prendre en compte pour implémenter la sauvegarde et la récupération des ordinateurs virtuels.

Options d'implémentation de sauvegardes pour les ordinateurs virtuels

Lorsque vous planifiez une stratégie de sauvegarde pour les ordinateurs virtuels, vous devez tenir compte de vos options de sauvegarde en ce qui concerne le produit ou les services spécifiques qui s'exécutent sur vos ordinateurs virtuels. En outre, vous devez suivre la documentation technique et les options de sauvegarde prises en charge pour chaque service ou produit qui s'exécute sur vos ordinateurs virtuels, tels qu'Active Directory, DHCP, les fichiers et les dossiers, Exchange Server et SQL Server.



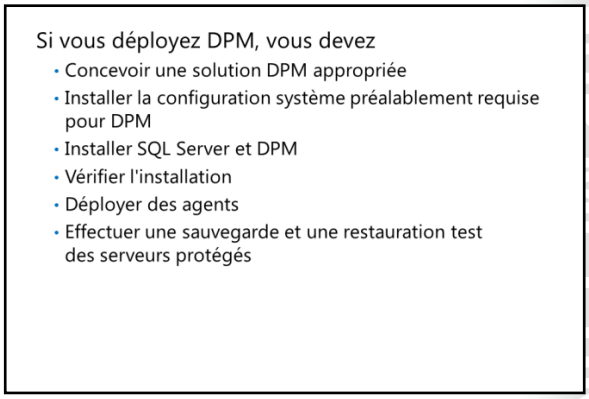
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous devez prendre en compte les options suivantes pour implémenter la sauvegarde des ordinateurs virtuels dans votre organisation :

- Effectuez des sauvegardes sur le serveur physique où se trouvent les ordinateurs virtuels. Dans ce scénario, vous sauvegardez tous les fichiers des ordinateurs virtuels. Ce type de sauvegarde est complet, car l'ensemble de la configuration et des données de vos ordinateurs virtuels est sauvegardé. Toutefois, vous devez vous assurer que ce type de sauvegarde est pris en charge pour les services ou les produits qui s'exécutent sur vos ordinateurs virtuels. Par exemple, nous vous déconseillons ce type de sauvegarde pour Microsoft Exchange Server, s'il s'exécute dans un environnement virtuel.
- Effectuez des sauvegardes des données sur le serveur virtualisé. Cette option permet d'effectuer la sauvegarde des données de la même manière que si un serveur était installé sur un ordinateur physique, ce qui signifie que seules les données sur l'ordinateur virtuel sont sauvegardées. Nous recommandons ce type de sauvegarde lorsque Microsoft Exchange Server s'exécute dans un environnement virtuel.
- Exécutez une sauvegarde en ligne. Ce type de sauvegarde garantit que les données ont été sauvegardées sans interrompre un environnement de production. Si le produit installé dans l'environnement virtualisé prend en charge ce type de sauvegarde, nous recommandons que les organisations utilisent la sauvegarde en ligne afin que leurs serveurs puissent continuer à fonctionner pendant le processus de sauvegarde.
- Exécutez une sauvegarde hors connexion. Ce type de sauvegarde requiert l'arrêt des ordinateurs virtuels jusqu'à ce que la sauvegarde soit terminée. Les ordinateurs virtuels peuvent alors reprendre leur fonctionnement. Nous ne recommandons pas ce type de sauvegarde, car il provoque un temps d'arrêt des services qui s'exécutent sur l'ordinateur virtuel. Vous pouvez envisager d'effectuer une sauvegarde hors connexion si aucun autre type de sauvegarde n'est pris en charge ni possible dans votre organisation.

Déploiement de DPM

De nombreux composants des exigences métier d'une organisation concernent la protection des données et la récupération, si bien que le déploiement de DPM peut nécessiter une certaine planification. Les exigences métier peuvent inclure les différentes technologies à protéger, les fonctionnalités DPM à utiliser, ainsi que le nombre de serveurs DPM que vous souhaitez utiliser et leur emplacement.



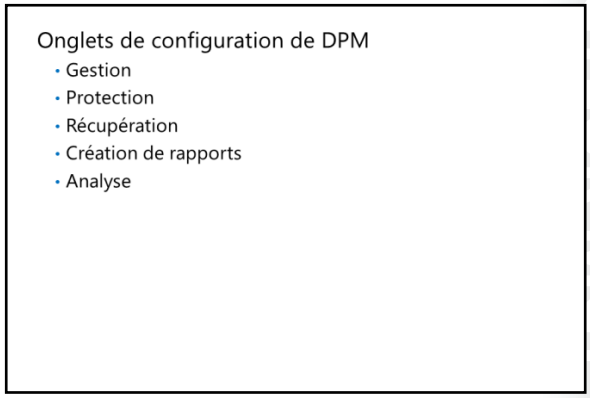
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si vous envisagez de déployer DPM, vous devez effectuer les opérations suivantes :

- Concevez une solution DPM appropriée. Les organisations doivent toujours commencer par analyser leurs données essentielles et par effectuer une évaluation des risques, générant ainsi une stratégie pour les sauvegardes et la restauration des données, et une conception de déploiement DPM.
- Installez la configuration système préalablement requise pour DPM. En fonction de la conception de déploiement DPM que vous créez, les administrateurs informatiques doivent préparer l'infrastructure de serveur appropriée et une solution de support de sauvegarde, puis installer la configuration requise appropriée.
- Installez SQL Server et DPM. Un déploiement DPM requiert une base de données SQL Server 2012 ou SQL Server 2008 R2, si bien qu'après avoir déterminé la configuration requise, vous devez installer DPM et SQL Server sur le même serveur ou sur les différents serveurs, en fonction de votre conception de déploiement.
- Vérifiez l'installation. Après l'installation du serveur DPM, vous devez vérifier si l'installation s'est terminée correctement en analysant les journaux d'événements et d'installation.
- Déployez des agents. Une fois la vérification terminée, vous devez déployer des agents sur vos ordinateurs qui nécessitent une protection, conformément à votre conception de déploiement.
- Effectuez une sauvegarde et une restauration test des serveurs protégés. Avant de placer un serveur DPM en production, vous devez effectuer une sauvegarde et une restauration test des serveurs que vous protégez. Ceci vous permet de garantir que vos procédures de sauvegarde et de restauration sont entièrement fonctionnelles. Vous devez également vous assurer que vos composants DPM, tels que le matériel de support de sauvegarde, les lecteurs de disque et les bibliothèques de bandes, sont opérationnels.

Options de configuration pour DPM

Les options de configuration DPM vous permettent de concevoir et d'implémenter aisément une solution qui peut vous aider à protéger les données essentielles et les données d'infrastructure système de votre organisation. Les paramètres de configuration dans DPM sont situés dans différentes fenêtres de console et vous pouvez basculer entre elles en sélectionnant les onglets appropriés dans la partie inférieure gauche des fenêtres de console.



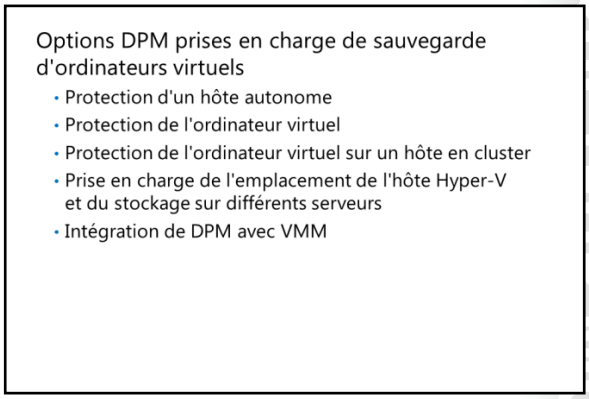
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez configurer les options DPM dans les espaces de travail suivants, dans la console DPM :

- Gestion. L'espace de travail Gestion vous permet d'installer des agents sur les ordinateurs que vous souhaitez protéger. Vous pouvez également configurer des supports différents pour le stockage des données sauvegardées, par exemple configurer des disques dans des pools de stockage, configurer des périphériques et des bibliothèques de bandes ou configurer Windows Azure Online Backup.
- Protection. L'espace de travail Protection vous permet de créer des groupes de protection, qui peuvent contenir chacun des données issues de technologies différentes que vous souhaitez protéger, telles que des dossiers de serveur de fichiers, des boîtes aux lettres Exchange Server, des bases de données SQL Server et des ordinateurs virtuels.
- Récupération. L'espace de travail Récupération vous fournit des options pour effectuer la récupération des données qui ont été protégées et vous pouvez choisir d'effectuer une restauration à partir de différents points de récupération.
- Création de rapports : L'espace de travail Création de rapports fournit des rapports sur le statut des sauvegardes qui ont lieu, sur l'utilisation des disques et des bandes, et sur les tendances d'utilisation. Vous pouvez également planifier l'exécution de rapports à différents intervalles de temps et leur envoi par courrier électronique en utilisant différents formats, tels qu'HTML, Microsoft Excel® 2010 ou PDF (Portable Document Format).
- Analyse. L'espace de travail Analyse fournit des alertes au sujet des erreurs, des avertissements et des différents types d'événements de sauvegarde et de restauration qui se produisent. Vous pouvez également surveiller l'état des travaux de protection planifiés, terminés et ayant échoué.

Utilisation de DPM pour sauvegarder les ordinateurs virtuels

Les organisations peuvent utiliser DPM comme solution de sauvegarde et de restauration pour leur environnement virtualisé Hyper-V. DPM protège les ordinateurs physiques et virtuels en installant un agent chargé de sauvegarder et restaurer les travaux. DPM s'intègre avec Hyper-V afin de fournir les éléments suivants aux ordinateurs virtuels :



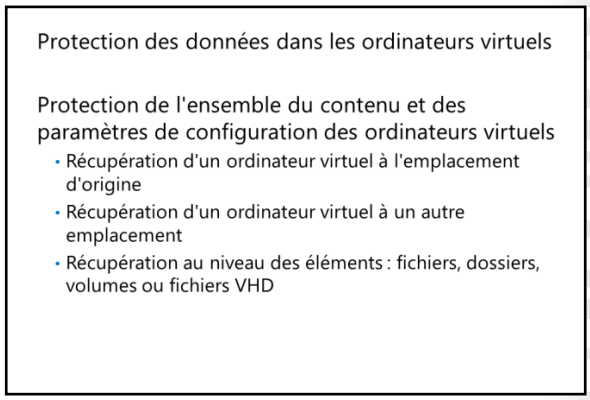
- Protection d'un hôte autonome. Dans ce scénario, vous installez l'agent de protection DPM sur l'hôte Hyper-V où plusieurs ordinateurs virtuels s'exécutent. Un travail de sauvegarde s'effectuera au niveau de l'hôte, ce qui signifie qu'il sauvegardera tous les fichiers et paramètres de configuration des ordinateurs virtuels.
- Protection de l'ordinateur virtuel. Dans ce scénario, vous installez l'agent de protection DPM sur l'ordinateur virtuel qui s'exécute sur l'hôte Hyper-V. Un travail de sauvegarde sera effectué sur l'ordinateur virtuel, de sorte que seules des données d'application spécifiques seront sauvegardées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Protection de l'ordinateur virtuel qui s'exécute sur l'hôte en cluster. Dans ce scénario, les ordinateurs virtuels s'exécutent sur un hôte Hyper-V en cluster et vous installez les agents de protection DPM sur tous les nœuds du cluster. La sauvegarde s'effectue au niveau de l'hôte.
- Hôte et stockage Hyper-V situés sur des serveurs différents. Dans ce scénario, l'hôte Hyper-V se trouve sur un serveur et les lecteurs d'ordinateur virtuel sont situés sur un serveur distinct qui héberge la solution de stockage. Vous devez installer un agent de protection DPM sur les deux serveurs et la sauvegarde aura lieu au niveau de l'hôte.
- Intégration de DPM avec VMM. Dans ce scénario, les ordinateurs virtuels se trouvent sur plusieurs hôtes physiques, que vous gérez à l'aide de VMM. DPM s'intègre à VMM pour protéger les ordinateurs virtuels sur chaque hôte physique et protège les ordinateurs virtuels même au cours du processus de migration dynamique à partir d'un hôte physique vers un autre. La protection de migration dynamique est prise en charge dans les scénarios de migration suivants : à l'intérieur du cluster, des ordinateurs autonomes vers les ordinateurs en cluster, des ordinateurs en cluster vers les ordinateurs autonomes et entre les ordinateurs autonomes. Vous devriez installer des agents de protection DPM sur chaque hôte physique où des ordinateurs virtuels s'exécutent et où la sauvegarde se produit au niveau de l'hôte. Si vous souhaitez intégrer DPM et VMM, vous devez installer la console VMM sur le serveur qui exécute DPM.

Restauration d'ordinateurs virtuels à l'aide de DPM

Pour protéger les ordinateurs virtuels à l'aide de DPM, vous pouvez :

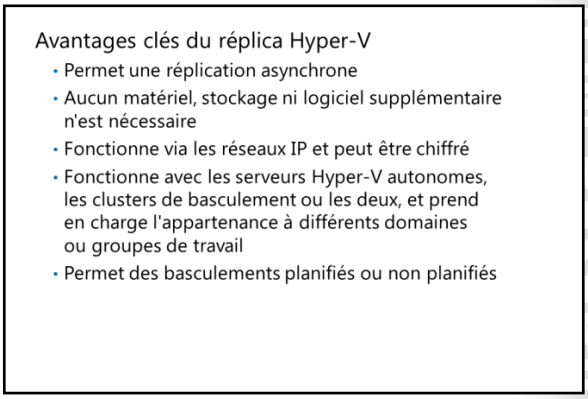


- Protéger les données sur vos ordinateurs virtuels, ce qui requiert d'installer un agent de protection sur l'ordinateur virtuel. Ce type de procédure de restauration est quasiment identique à la protection des données sur des ordinateurs physiques.
- Protéger l'ensemble du contenu et des paramètres de configuration de vos ordinateurs virtuels, ce qui exige que vous installiez la protection sur le serveur physique où se trouvent les ordinateurs virtuels. Pour ce type de restauration, plusieurs options s'offrent à vous :
    - récupérer un ordinateur virtuel à l'emplacement d'origine lorsque les fichiers VHD et de configuration d'origine sont supprimés et remplacés à partir de la sauvegarde ;
    - récupérer un ordinateur virtuel à un autre emplacement lorsque le fichier VHD et les fichiers de configuration sont restaurés vers un autre hôte ;
    - récupérer des éléments spécifiques : vous pouvez choisir de restaurer des fichiers, des dossiers, des volumes ou des fichiers VHD spécifiques.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration du réplica Hyper-V

Le réplica Hyper-V est une nouvelle fonctionnalité dans Windows Server 2012 qui permet aux organisations d'avoir un réplica de leurs ordinateurs virtuels sur un autre hôte Hyper-V à des fins de restauration ou pour prendre en charge des scénarios de récupération d'urgence.



Les avantages clés du réplica Hyper-V sont les suivants :

- La réplication est asynchrone. Lorsque vous activez le réplica Hyper-V, le processus de copie des données à partir du site principal vers le site de réplication commence. Pour préserver la bande passante entre les deux sites, vous pouvez envisager de copier les fichiers des ordinateurs virtuels sur un support externe, tel qu'un lecteur de disque dur externe, puis de les copier sur le serveur dans le site de réplication. Une fois le processus de copie initial terminé, les modifications apportées aux fichiers des ordinateurs virtuels sont répliquées dans le site de réplication à une fréquence comprise entre 5 et 15 minutes, selon votre configuration.
- Aucun matériel, système de stockage ni logiciel supplémentaire n'est nécessaire. La configuration du réplica Hyper-V requiert uniquement que vous installiez un rôle Hyper-V sur les deux hôtes de serveur principal et de réplication.
- Il fonctionne via les réseaux IP et vous pouvez le chiffrer. Le processus de réplication fonctionne via un protocole IP, mais si des pare-feu sont déployés entre les deux sites, vous devez configurer les règles appropriées pour autoriser le trafic de réplication. Si des organisations choisissent d'utiliser un chiffrement, elles doivent déployer des certificats. Vous pouvez configurer une autorité de certification interne pour qu'elle délivre des certificats auto-signés ou vous pouvez utiliser une autorité de certification commerciale.
- Il fonctionne avec des serveurs Hyper-V autonomes, des clusters de basculement, ou les deux. Les hôtes Hyper-V peuvent être dans des domaines ou des groupes de travail différents et vous pouvez configurer le réplica Hyper-V sur les serveurs Hyper-V que vous déployez dans différentes configurations, telles que des serveurs Hyper-V autonomes, des clusters de basculement, ou les deux. L'appartenance aux domaines des hôtes de serveur principal et de réplication peut également être différente, ou ils peuvent être membres d'un même groupe de travail. Vous devez lire la documentation technique relative à DPM sur la façon de configurer le réplica Hyper-V dans ces divers scénarios spécifiques.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

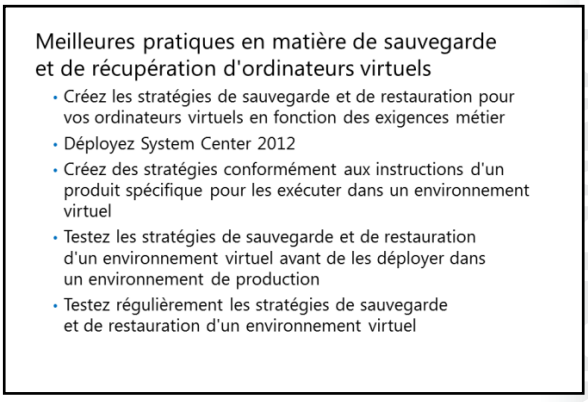
Scénarios de récupération d'urgence avec le réplica Hyper-V :

- Les organisations peuvent utiliser la technologie du réplica Hyper-V en définissant un site de récupération d'urgence qui contiendrait le réplica des ordinateurs virtuels dans le centre de données principal. Le site de récupération d'urgence peut être construit et conçu spécialement à des fins de récupération d'urgence. Les petites et moyennes entreprises peuvent définir un site de récupération d'urgence dans certaines des filiales de l'entreprise ou il peut être hébergé par un fournisseur dans un cloud.
- Les basculements dans les organisations peuvent être planifiées ou non planifiées. Les organisations doivent tester régulièrement le processus de récupération. Lorsque le basculement est initié par un administrateur, il s'agit d'un basculement planifié. Dans ce scénario, l'administrateur déplace l'exploitation de l'ordinateur virtuel du centre de données principal vers le centre de données du site de récupération d'urgence. Toutes les modifications apportées à l'ordinateur virtuel dans le centre de données principal seront répliquées dans le réplica de l'ordinateur virtuel du centre de données du site de récupération d'urgence, et aucune donnée ne sera perdue au cours de cette opération. Une fois le basculement planifié accompli, l'ordinateur virtuel du site de récupération d'urgence agira en tant qu'ordinateur principal et prendra en charge la charge de travail.
- Si le basculement est initié en raison d'une défaillance d'un centre de données principal, un basculement non planifié se produit automatiquement. Dans ce scénario, un administrateur doit ajouter le réplica de l'ordinateur virtuel dans le site de récupération d'urgence. Si un basculement non planifié se produit, aucune option n'est disponible pour répliquer les données qui n'ont pas été répliquées avant la défaillance, si bien que certaines données peuvent être perdues.

Liens de référence : Déployez le réplica Hyper-V à l'adresse http://go.microsoft.com/fwlink/?LinkID=285327.

Éléments à prendre en compte pour implémenter la sauvegarde et la récupération d'ordinateurs virtuels

Les organisations qui choisissent de déployer un environnement virtualisé et un cloud privé disposeront d'une infrastructure optimisée et maniable, ainsi que de la capacité de s'adapter aux exigences métier changeantes. Par conséquent, vous pouvez exécuter le processus de sauvegarde et de restauration au sein de cette infrastructure maniable.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous planifiez des stratégies de sauvegarde et de restauration pour des environnements virtuels, les organisations doivent tenir compte des meilleures pratiques suivantes :

- Créer des stratégies de sauvegarde et de restauration qui répondront aux exigences métier.
- Utiliser une solution logicielle pour gérer, surveiller et protéger les environnements virtuels, tels que System Center 2012.
- Lire la documentation sur chaque solution qui s'exécute dans les environnements virtuels et déterminer les recommandations pour les processus de sauvegarde et de restauration, tels qu'Exchange Server, SQL Server et SharePoint Server.
- Tester les stratégies de sauvegarde et de restauration de vos ordinateurs virtuels avant de les déployer en production.
- Tester régulièrement les stratégies de sauvegarde et de restauration de vos ordinateurs virtuels lorsqu'ils sont en production. Veillez à ne pas affecter l'environnement de production au cours des tests. Dans le cadre des tests, vous devez utiliser un environnement isolé et non destiné à la production, ainsi qu'une copie des données de production.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation d'une stratégie de sauvegarde d'ordinateurs virtuels avec DPM

Scénario

Dans le cadre de la stratégie de virtualisation, A. Datum convertit la plupart de ses serveurs physiques en ordinateurs virtuels et déploie presque tous les nouveaux serveurs sous la forme d'ordinateurs virtuels. A. Datum a besoin de développer une stratégie pour traiter les sauvegardes des ordinateurs virtuels afin de s'assurer que toutes les données stockées sur les ordinateurs virtuels sont sauvegardées. Dans certains cas, les ordinateurs virtuels doivent également être sauvegardés.

Vous devez configurer DPM pour sauvegarder les données stockées au sein d'un ordinateur virtuel, ainsi que les ordinateurs virtuels eux-mêmes.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

1. configurer Data Protection Manager ;
2. sauvegarder et restaurer les données des ordinateurs virtuels ;
3. sauvegarder et restaurer les ordinateurs virtuels.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Informations de connexion	
Ordinateurs virtuels	22414B-LON-DC1 22414B-LON-SVR1 22414B-LON-DM1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible.
Avant de débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, sur **Accueil**, cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22414B-LON-DC1**, puis, dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **Administrateur**
   - Mot de passe : **Pa$$w0rd**
   - Domaine : **ADATUM**
5. Répétez les étapes 2 à 4 pour **22414B-LON-SVR1** et **22414B-LON-DM1**.

De plus, pour cet atelier pratique, vous devez créer l'ordinateur virtuel 22414B-LON-TEST sur lequel vous effectuerez la sauvegarde et la récupération. Pour cela, procédez comme suit :

1. Dans le **Gestionnaire Hyper-V**, dans le volet Actions, cliquez sur **Nouveau**, sur **Ordinateur virtuel**, puis, dans l'Assistant Nouvel ordinateur virtuel, dans la page **Avant de commencer**, cliquez sur **Suivant**.
2. Dans la page **Spécifier le nom et l'emplacement**, dans la zone **Nom**, tapez **22414B-LON-TEST**, activez la case à cocher **Stocker l'ordinateur virtuel à un autre emplacement**, puis cliquez sur **Parcourir**.
3. Dans la page **Sélectionner un dossier**, dans le volet de navigation, accédez au dossier **E:\Programmes\Microsoft Learning\22414**, cliquez sur **Sélectionner un dossier**, puis cliquez sur **Suivant**.
4. Dans la page **Affecter la mémoire**, dans le champ **Mémoire de démarrage**, tapez **1024**, puis cliquez sur **Suivant**.
5. Dans la page **Configurer la mise en réseau**, dans la zone de liste déroulante **Connexion**, sélectionnez **Réseau externe**, puis cliquez sur **Suivant**.
6. Dans la page **Connecter un disque dur virtuel**, acceptez les paramètres par défaut, puis cliquez sur **Suivant**.
7. Dans la page **Options d'installation**, veillez à ce que la case d'option **Installer un système d'exploitation ultérieurement** soit sélectionnée, puis cliquez sur **Suivant**.
8. Dans la page **Fin de l'Assistant Nouvel ordinateur virtuel**, cliquez sur **Terminer**.
9. Attendez que l'Assistant se termine, puis, dans le Gestionnaire Hyper-V, vérifiez que l'ordinateur virtuel **22414B-LON-TEST** a été créé avec l'état **Désactivé**.

Exercice 1 : Configurer DPM

Scénario

A. Datum a déployé un serveur DPM dans son centre de données de Londres. Vous devez configurer les composants DPM requis pour sauvegarder et restaurer les données et les ordinateurs virtuels.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer un pool de stockage dans Microsoft System Center® 2012 - Data Protection Manager (DPM).
2. Déployer les agents de protection DPM.
3. Configurer des groupes de protection.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Configurer un pool de stockage dans Microsoft System Center 2012 - Data Protection Manager (DPM)

1. Basculez vers LON-DM1, puis réduisez la fenêtre du Gestionnaire de serveur.
2. Sur le Bureau, double-cliquez sur **Microsoft System Center 2012 Service Pack 1 Data Protection Manager**.
3. Dans la Console Administrateur System Center 2012 Service Pack 1 DPM, à partir de l'espace de travail **Administration**, ajoutez un nouveau disque au pool de stockage nommé **Disque 1**.
4. Vous devez voir **Disque 1 (Virtuel HD ATA Device)** (périphérique ATA HD virtuel) ajouté dans **Disques du pool de stockage DPM**, marqué d'une case à cocher verte.

▶ Tâche 2 : Déployer les agents de protection DPM

1. Basculez vers **LON-**SVR1.
2. Dans la barre des tâches, ouvrez le **Gestionnaire de serveur**, puis **Pare-feu Windows avec sécurité avancée**.
3. Dans la fenêtre Pare-feu Windows avec fonctions avancées de sécurité, dans le volet de navigation, ouvrez la boîte de dialogue **Propriétés de : Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local**.
4. Dans la fenêtre Propriétés de : Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local, dans la liste déroulante **Connexions entrantes**, sélectionnez **Autoriser**, puis cliquez sur **OK**.
5. Fermez la fenêtre Pare-feu Windows avec fonctions avancées de sécurité.
6. Basculez vers **LON-HOST1**.
7. Répétez les étapes de 1 à 5 sur **LON-HOST1**.
8. Basculez vers **LON-DM1**.

 **Remarque :** Dans l'environnement de production, vous pouvez personnaliser les paramètres de pare-feu sur les serveurs d'entreprise pour autoriser le trafic provenant des adresses IP et des ports nécessaires pour la communication avec DPM.

9. Dans la Console Administrateur DPM, cliquez sur l'espace de travail **Administration**, puis, dans la barre de navigation, cliquez sur le lien **Agents**.
10. Déployez l'agent de protection DPM sur **LON-SVR1** et **LON-HOST1** en utilisant les paramètres suivants :
    - Nom d'utilisateur et mot de passe : **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**
    - Méthode de redémarrage : **Oui.** Redémarrer les ordinateurs sélectionnés une fois les agents de protection installés (si nécessaire)
11. Dans la fenêtre Résumé, démarrez l'installation, puis patientez jusqu'à ce que l'état **Réussite** apparaisse dans la colonne **Résultats**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer des groupes de protection

Créer un groupe de protection de données

1. Sur LON-DM1, dans la Console Administrateur DPM, cliquez sur l'espace de travail **Protection**.
2. Dans le ruban, cliquez sur **Nouveau** pour démarrer l'Assistant **Créer un nouveau groupe de protection**, puis sélectionnez les options suivantes pour créer un nouveau groupe de protection :
   - Sélectionner le type de groupe de protection : **Serveurs**
   - Sélectionnez les membres du groupe : **LON-SVR1\Tous les volumes\C:\Financial Data** (Données financières)
   - Nom du groupe de protection : **Dossier des données financières du groupe de protection**
   - Méthode de protection : **Protection à court terme à l'aide de Disque**
   - Spécifier les objectifs à court terme : **paramètres par défaut**
   - Vérifier l'allocation de disque : **Paramètres par défaut**
   - Méthode de création de réplica : **Paramètres par défaut**
   - Options de vérification de cohérence : **Paramètres par défaut**
3. Dans la page **État**, vérifiez que les deux processus indiquent **Réussite** dans la colonne **Résultats**, puis cliquez sur **Fermer**.

Créer un groupe de protection d'ordinateurs virtuels

1. Sur LON-DM1, dans la Console Administrateur DPM, cliquez sur l'espace de travail **Protection**.
2. Dans le ruban, cliquez sur **Nouveau** pour démarrer l'Assistant Créer un nouveau groupe de protection, puis sélectionnez les options suivantes pour créer un nouveau groupe de protection :
   - Sélectionner le type de groupe de protection : **Serveurs**
   - Sélectionnez les membres du groupe : **LON-HOST1\Hyper-V\Backup Using Saved State\ 22414B-LON-TEST**
   - Nom du groupe de protection : **Groupe de protection VM**
   - Méthode de protection : **Protection à court terme à l'aide de Disque**
   - Spécifier les objectifs à court terme : **paramètres par défaut**
   - Vérifier l'allocation de disque : **Paramètres par défaut**
   - Méthode de création de réplica : **Paramètres par défaut**
   - Options de vérification de cohérence : **Paramètres par défaut**
3. Dans la page **État**, vérifiez que les deux processus indiquent **Réussite** dans la colonne **Résultats**, puis cliquez sur **Fermer**.

Résultats : Une fois ces tâches terminées, vous aurez : configuré un pool de stockage dans DPM ; déployé des agents de protection DPM ; configuré des groupes de protection.

Exercice 2 : Implémenter la sauvegarde et la récupération des données des ordinateurs virtuels

Scénario

Les ordinateurs virtuels chez A. Datum hébergeront une grande partie des données de l'entreprise et il est essentiel que ces données soient sauvegardées et puissent être restaurées. Par conséquent, vous devez configurer DPM pour sauvegarder et restaurer les données de fichiers et de dossiers sur un ordinateur virtuel.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer Data Protection Manager pour sauvegarder les données d'ordinateur virtuel.
2. Supprimer les données.
3. Restaurer les données supprimées.

▶ Tâche 1 : Configurer Data Protection Manager pour sauvegarder les données d'ordinateur virtuel

1. Sur LON-DM1, dans la Console Administrateur DPM, cliquez sur l'espace de travail **Protection**.
2. Dans le volet d'informations, assurez-vous que l'état du **Dossier des données financières du groupe de protection** est marqué d'une case à cocher verte.
3. Dans le volet d'informations, créez un point de récupération pour le dossier **C:\Financial Data** (Données financières).

▶ Tâche 2 : Supprimer les données

1. Basculez vers LON-SVR1.
2. Ouvrez l'Explorateur de fichiers, puis supprimez le dossier **C:\Financial Data** (Données financières).

▶ Tâche 3 : Restaurer les données supprimées

1. Basculez vers LON-DM1.
2. Dans la Console Administrateur DPM, cliquez sur l'espace de travail **Récupération**.
3. Configurez une récupération pour le dossier **Financial Data** situé sur LON-SVR1 avec les options suivantes :
   - Vérifier la récupération sélectionnée : **Financial Data**
   - Sélectionner le type de récupération : **Récupérer à l'emplacement d'origine**
   - Spécifier les options de récupération : Paramètres par défaut
4. Dans la page **Statut de la récupération**, vérifiez que Statut de la récupération est **Réussite**, puis cliquez sur **Fermer**.
5. Cliquez sur l'espace de travail **Protection**, puis cliquez sur **Tous les groupes de protection**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Effectuez une vérification de cohérence pour **C:\Financial Data** (Données financières). Quelques instants plus tard, l'**État de la protection** doit présenter une coche verte.
7. Basculez vers LON-SVR1.
8. Sur LON-SVR1, assurez-vous que le dossier **C:\Financial Data** (Données financières) a été restauré.
9. Fermez l'Explorateur de fichiers.

Résultats : Une fois ces tâches terminées, vous aurez : configuré DPM pour sauvegarder les données d'ordinateur virtuel ; supprimé les données ; restauré les données.

Exercice 3 : Implémenter la sauvegarde et la restauration des ordinateurs virtuels à l'aide de Data Protection Manager

Scénario

A. Datum a décidé d'implémenter Data Protection Manager pour sauvegarder et restaurer les ordinateurs virtuels. Vous devez configurer Data Protection Manager pour effectuer une sauvegarde d'un ordinateur virtuel. Ensuite, vous récupérerez l'ordinateur virtuel à un état précédent.

Les tâches principales de cet exercice sont les suivantes :

1. Sauvegarder un ordinateur virtuel à l'aide de Data Protection Manager.
2. Modifier une configuration sur l'ordinateur virtuel.
3. Restaurer l'ordinateur virtuel.

▶ Tâche 1 : Sauvegarder un ordinateur virtuel à l'aide de Data Protection Manager

1. Sur LON-DM1, dans la Console Administrateur DPM, cliquez sur l'espace de travail **Protection**, puis, dans le volet d'informations, cliquez sur **Groupe de protection : Groupe de protection VM**.
2. Dans le volet d'informations, assurez-vous que l'état du **Groupe de protection VM** est marqué d'une coche verte. Jusqu'à 10 minutes peuvent être nécessaires pour que l'état indique **OK**.
3. Dans le volet d'informations, créez un point de récupération pour l'ordinateur virtuel **\Backup Using Saved State\22414B-LON-TEST**.

▶ Tâche 2 : Modifier une configuration sur l'ordinateur virtuel

1. Basculez vers **LON-HOST1**.
2. Dans le Gestionnaire Hyper-V, modifiez les propriétés de **22414B-LON-TEST**, afin de configurer **256 Mo** de mémoire vive (RAM) de démarrage pour LON-TEST.

 Remarque : Cette modification perturbera le fonctionnement normal de LON-TEST en raison de la petite quantité de mémoire configurée. Dans la tâche suivante, vous restaurerez le paramètre initial de mémoire pour LON-TEST à partir de la sauvegarde.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Restaurer l'ordinateur virtuel

1. Basculez vers LON-DM1.
2. Dans la Console Administrateur DPM, cliquez sur l'espace de travail **Récupération**.
3. Dans le volet de navigation, développez **Données récupérables\Adatum.com\LON-HOST1**, puis cliquez sur **Toutes les données HyperV protégées**.
4. Dans le volet de résultats, sous **Élément récupérable**, configurez une récupération pour l'élément récupérable **Backup Using Saved State\22414B-LON-TEST** avec les options suivantes :
   - Sélectionner le type de récupération : **Récupérer sur l'instance d'origine**
   - Spécifier les options de récupération : **Paramètres par défaut**
5. Dans la page **Statut de la récupération**, vérifiez que **Statut de la récupération** est **Réussite**, puis cliquez sur **Fermer**.
6. Basculez vers LON-HOST1.
7. Dans le Gestionnaire Hyper-V, vérifiez que les paramètres pour **22414B-LON-TEST** ont été restaurés.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1** et **22414B-LON-DM1**.

Résultats : Une fois ces tâches terminées, vous aurez : sauvegardé un ordinateur virtuel à l'aide de DPM ; modifié une configuration sur l'ordinateur virtuel ; restauré l'ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée : Vous devez tester vos stratégies de sauvegarde et de restauration avant de les déployer dans un environnement de production. Vous devez également tester régulièrement vos stratégies de sauvegarde et de restauration en production. Toutefois, veillez à ne pas affecter votre environnement de production au cours des tests. Dans le cadre des tests, vous devez utiliser un environnement isolé et non destiné à la production, ainsi qu'une copie des données de production.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Échec de l'installation de l'agent de protection DPM	

Questions de contrôle des acquis

Question : Qu'est-ce qui convient le mieux aux organisations, utiliser une solution de protection centralisée comme DPM ou disposer de produits distincts pour protéger des serveurs, des données et des services différents ?

Problèmes réels et scénarios

Votre organisation a défini sa stratégie de sauvegarde et de restauration. Toutefois, après plusieurs mois d'exécution réussie des travaux de sauvegarde, votre responsable informatique souhaite tester la restauration des données situées sur un serveur de fichiers. Aucune défaillance du serveur n'a été détectée à ce stade. Au cours de la restauration, l'administrateur de sauvegarde a découvert qu'aucune données d'entreprise n'a été restaurée car un dossier incorrect du serveur de fichiers avait été configuré pour la sauvegarde. Votre organisation doit à présent mener des tests réguliers des procédures de restauration pour vérifier que les données correctes seront restaurées en cas de défaillance.

Outils

- DPM. Interface utilisateur (GUI) globale permettant de configurer et gérer DPM.
- DPM Management Shell. Windows PowerShell permettant de configurer et gérer DPM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 11

Planification et implémentation d'une infrastructure à clé publique

Table des matières :

Vue d'ensemble du module **11-1**

Leçon 1 : Planification et implémentation d'un déploiement d'autorité de certification **11-2**

Leçon 2 : Planification et implémentation de modèles de certificats **11-17**

Leçon 3 : Planification et implémentation la distribution et la révocation de certificats **11-24**

Leçon 4 : Planification et implémentation de l'archivage et de la récupération de clé **11-34**

Atelier pratique : Planification et implémentation d'une infrastructure AD CS **11-39**

Contrôle des acquis et éléments à retenir **11-48**

Vue d'ensemble du module

L'infrastructure à clé publique (PKI) de Microsoft® pour le système d'exploitation Windows Server® 2012 fournit une PKI intégré qui vous permet de sécuriser et échanger des informations de manière fortement sécurisée et avec une administration facile sur les réseaux Internet, extranets, intranets et les applications. Dans Windows Server 2012, vous pouvez générer une PKI interne pour publier et gérer des certificats au moyen des services intégrés. Dans ce module, vous allez apprendre à planifier et implémenter les divers aspects d'une PKI, et vous générerez une PKI interne à l'aide des services de certificats Active Directory® (AD CS).

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- planifier et implémenter un déploiement d'autorité de certification (AC) ;
- planifier et implémenter des modèles de certificats ;
- planifier et implémenter la distribution et la révocation de certificats ;
- planifier et implémenter l'archivage et la récupération de clé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification et implémentation d'un déploiement d'autorité de certification

Pour prendre en charge dans votre organisation des applications compatibles avec une PKI, il vous faut organiser, concevoir et implémenter une hiérarchie d'autorités de certification. Une autorité de certification est une autorité dans un réseau qui émet et gère les informations d'authentification de sécurité et les clés publiques de chiffrement. Dans cette leçon, vous découvrirez les éléments clés d'une conception d'autorité de certification réussie.

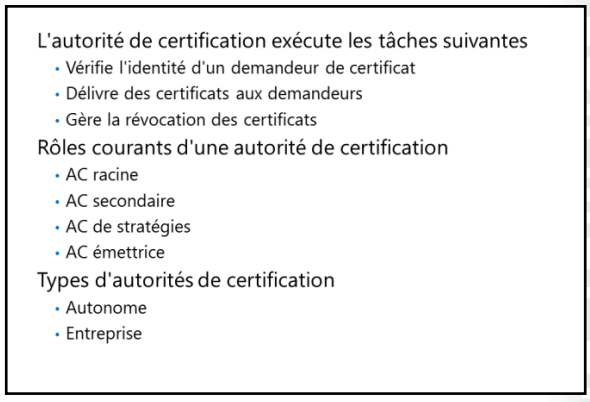
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les autorités de certification ;
- collecter des informations pour élaborer une hiérarchie des autorités de certification ;
- décrire les autorités de certification internes et publiques ;
- planifier une hiérarchie d'autorités de certification ;
- décrire les éléments à prendre en compte des autorités de certification autonomes et d'entreprise ;
- présenter les éléments à prendre en compte relatifs au déploiement d'une AC racine ;
- décrire les instructions de conception d'une hiérarchie d'autorités de certification ;
- concevoir un plan de récupération d'urgence pour une hiérarchie d'autorités de certification ;
- faire migrer et mettre à niveau les autorités de certification.

Vue d'ensemble des autorités de certification

L'autorité de certification (AC) est une composante essentielle d'une solution PKI d'entreprise. Dans un réseau Windows Server 2012, une autorité de certification est un serveur Windows Server 2012 où est installé AD CS. Une autorité de certification (AC) est un composant obligatoire dans les organisations qui souhaitent gérer leurs propres PKI. Une autorité de certification peut émettre et révoquer des certificats et peut publier l'accès aux informations de l'autorité (AIA) ainsi que les listes de révocation de certificats. Cela garantit que les utilisateurs, les services et les ordinateurs ont des certificats émis qui peuvent être validés.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Une autorité de certification a plusieurs fonctions ou rôles dans une PKI. Dans une grande PKI, il est courant de séparer les rôles de l'autorité de certification entre plusieurs serveurs. Une autorité de certification fournit plusieurs des tâches de gestion, notamment :

- la vérification de l'identité du demandeur du certificat ;
- l'émission de certificats aux utilisateurs, ordinateurs et services qui en font la demande ;
- la gestion des modèles de certificats ;
- la gestion de la révocation des certificats.

Vous attribuez un rôle à chaque autorité de certification dans une hiérarchie d'autorités de certification, et vous déterminez ces rôles en choisissant où localiser une autorité de certification dans la hiérarchie. Parmi les rôles communs dans une hiérarchie d'autorités de certification, vous pouvez trouver :

- l'autorité de certification racine. Toutes les autres autorités de certification de la hiérarchie approuvent l'AC racine. L'autorité de certification racine produit et signe son propre certificat. L'AC racine ne fournit généralement pas de certificats aux utilisateurs finaux ou aux ordinateurs, à moins que ce ne soit la seule autorité de certification dans la PKI ;
- l'autorité de certification secondaire. Une autorité de certification secondaire approuve l'autorité de certification racine, ou son autorité de certification parente. Cette approbation se produit quand un serveur secondaire reçoit un certificat de l'autorité de certification racine. L'AC secondaire émet des certificats et implémente des stratégies ;
- l'autorité de certification de stratégies. C'est une autorité de certification secondaire, qui repose directement en dessous de l'autorité de certification racine. Vous pouvez utiliser des autorités de certification de stratégies pour émettre des certificats aux autorités de certification secondaire qui sont directement en dessous d'elle dans la hiérarchie. Vous pouvez également utiliser des autorités de certification de stratégies quand les différentes divisions, secteurs ou sites de votre organisation requièrent des stratégies et procédures d'émission distinctes. En général, une autorité de certification de stratégies est déployée dans les environnements de PKI plus complexes ;
- l'autorité de certification émettrice. L'autorité de certification émettrice émet des certificats aux utilisateurs et aux ordinateurs, et est généralement en ligne en permanence. Dans de nombreuses hiérarchies d'autorités de certification, une AC émettrice est une AC secondaire, et elle authentifie les utilisateurs qui demandent des certificats, lance les demandes de révocation et participe à la récupération des clés.

Du point de vue des opérations des services de domaine Active Directory (AD DS), il existe deux types d'autorités de certification :

- les autorités de certification autonomes. Vous utilisez généralement une autorité de certification autonome pour les autorités de certification hors connexion, mais vous pouvez également l'utiliser pour une autorité de certification qui est uniformément disponible sur le réseau. Une autorité de certification hors connexion est une autorité que vous pouvez déconnecter du réseau pour empêcher de compromettre la sécurité des clés qui sont utilisées pour signer les certificats. En outre, les AC autonomes ne s'intègrent pas avec les services AD DS, de sorte qu'il est impossible de les utiliser pour l'inscription automatique ou la personnalisation de modèles de certificat ;
- les autorités de certification d'entreprise. Vous utilisez généralement une AC d'entreprise pour délivrer des certificats aux utilisateurs, aux ordinateurs et aux services, ou en tant qu'AC de stratégies. Cela requiert AD DS, et l'AC d'entreprise s'intègre toujours avec les services AD DS. Vous pouvez utiliser ce type d'AC comme base de données de configuration et d'enregistrement, et il fournit un point de publication pour les certificats délivrés aux utilisateurs et aux ordinateurs. En outre, ce type prend en charge l'inscription automatique de certificat et la personnalisation de modèle de certificat.

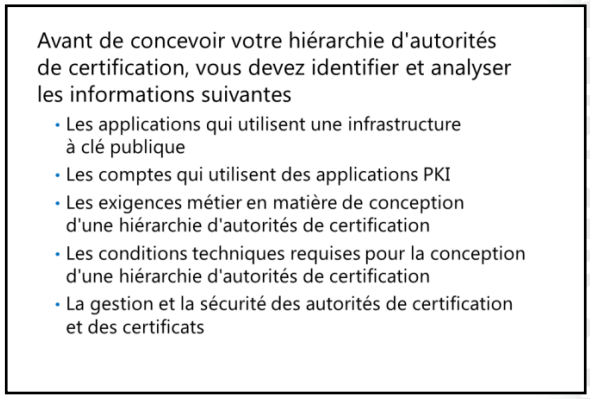
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le tableau suivant répertorie les différences principales entre une Autorité de certification autonome et une Autorité de certification d'entreprise.

Fonctionnalité	Autorité de certification d'entreprise	Autorité de certification autonome
S'intègre avec AD DS	Oui	Non
Inscription automatique	Oui	Non
Personnalisation des modèles de certificats	Oui	Non
Propagation dans le magasin racine approuvé du client	À l'aide d'une stratégie de groupe	Manuellement, sauf si elle est installée dans le domaine

Collecte d'informations pour élaborer une hiérarchie d'autorités de certification

Avant d'entamer la conception de votre hiérarchie d'autorités de certification, vous devez rassembler et analyser des informations sur la façon dont vous envisagez d'émettre et gérer des certificats et sur la façon dont vous administrerez les autorités de certification. Au cours de ce processus, vous devez rassembler les informations suivantes :



- les applications qui utilisent une infrastructure à clé publique. Vous devez collecter des informations sur les applications qui utilisent des PKI, ainsi que sur les technologies utilisées par ces applications. Une infrastructure à clé publique Windows Server prend en charge les types d'applications PKI suivants :
  - les signatures numériques. sécurisent les transactions Internet en chiffrant et en déchiffrant des messages, authentifient le compte qui envoie le message et confirment que le contenu qui est reçu est identique au contenu qui a été envoyé.
  - la connexion par carte à puce. Implémente l'authentification à deux facteurs et fournit une carte à puce et un code confidentiel (PIN) pour l'authentification réseau des informations d'identification.
  - la messagerie sécurisée. Assure la confidentialité des communications, l'intégrité des données et la non-répudiation pour les messages électroniques. Vous pouvez renforcer la sécurité des messages électroniques en utilisant des certificats pour vérifier les informations d'identification d'un expéditeur, le point d'origine d'un message et l'authenticité d'un message.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

  - la signature du code logiciel. Protège les ordinateurs contre l'installation de contrôles Microsoft ActiveX® ou d'applets de commande Java non autorisés. La technologie Authenticode permet aux éditeurs de logiciels de signer numériquement toute forme de contenu actif, y compris les archives à plusieurs fichiers.
  - la sécurité IP. Permet les communications cryptées et signées numériquement entre deux ordinateurs, ou entre un ordinateur et un routeur sur un réseau public.
  - 802.1x. Permet seulement aux utilisateurs authentifiés d'accéder à un réseau, et protège les données qui sont transmises sur un réseau. Dans une infrastructure à clé publique, la norme IEEE (Institute of Electrical and Electronics Engineers, Inc.) 802.1x assure la prise en charge de l'identification centralisée des utilisateurs, de l'authentification, de la gestion dynamique des clés et de la gestion des comptes pour authentifier les accès aux réseaux sans fil 802.11 et aux réseaux Ethernet câblés.

- la stratégie de restriction logicielle. Vous devez identifier le besoin d'implémentation d'une stratégie de restriction logicielle et l'intégrer au mode de conception de PKI. L'intégration entre une PKI et la stratégie de restriction logicielle vous permet de signer numériquement vos applications en utilisant un certificat émis par votre autorité de certification, puis de configurer une stratégie de restriction logicielle qui n'autorisera que l'exécution de ces applications.
- l'authentification Internet. Vous devez identifier la façon dont le client et le serveur sont authentifiés lors de transactions client-serveur. Par exemple, lorsque vous utilisez le protocole de cryptage SSL (Secure Sockets Layer), un client authentifie le serveur Web en validant les certificats présentés par le serveur. L'implémentation de SSL requiert une autorité de certification publique ou privée ; cette information est donc importante pour votre conception d'autorité de certification.
- l'authentification d'accès distant. Vous devez identifier les certificats que vous souhaitez utiliser pour l'authentification mutuelle. Si vos utilisateurs se connectent au réseau interne à partir d'Internet, vous utiliserez généralement des certificats. Par exemple, si vous utilisez Windows® 8 DirectAccess, vous devez implémenter les certificats. En outre, la passerelle des services Bureau à distance requiert un certificat sur le serveur RDGateway. Si vous prévoyez d'utiliser ces services, vous devez les inclure dans votre création de hiérarchie d'autorités de certification.
- le système de fichiers EFS (Encrypting File System). Vous devez identifier votre besoin d'implémenter EFS, qui chiffre les données. Pour récupérer les données chiffrées par EFS, vous pouvez implémenter une récupération de clé ou de données, ou les deux. La récupération de clé récupère la clé privée de l'utilisateur à partir d'une base de données de l'autorité de certification, et l'importe dans le magasin de certificats de n'importe quel utilisateur, permettant de ce fait le déchiffrement des fichiers chiffrés. Pour accomplir la récupération de données, vous implémentez des agents de récupération EFS qui ne peuvent pas accéder à une clé privée d'utilisateur. Ils ne peuvent accéder qu'à la clé de chiffrement générée aléatoirement. Si vous envisagez d'implémenter EFS, vous devez prendre en considération plusieurs aspects de votre conception d'autorité de certification, tels que la récupération de données et les agents de récupération de clé.

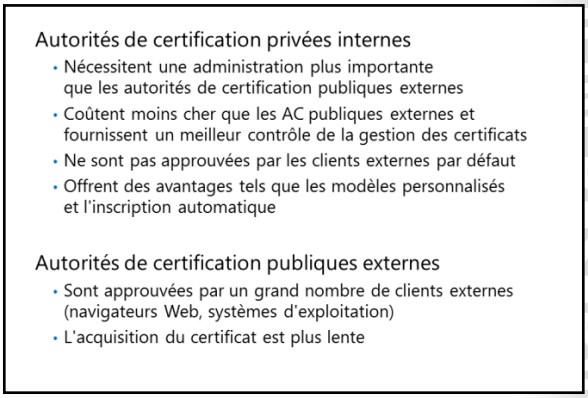
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- les comptes qui utilisent des applications PKI. Vous devez avoir des informations au sujet des comptes qui utiliseront des certificats. Plusieurs types de comptes peuvent obtenir des certificats numériques avec les services AD DS Windows Server 2012. Lorsque vous concevez la hiérarchie d'autorités de certification, n'oubliez pas que les comptes suivants sont pris en charge :
  - comptes d'utilisateur. Lorsqu'une autorité de certification délivre un certificat numérique à un utilisateur, il identifie ce dernier de manière unique auprès d'une application PKI. L'utilisateur peut obtenir un ou plusieurs certificats numériques pour remplir différents rôles sur le réseau.
  - comptes d'ordinateurs. Lorsqu'une autorité de certification délivre à un ordinateur un certificat numérique, aussi appelé certificat d'ordinateur, il identifie ce dernier de manière unique auprès d'une application PKI. Vous utilisez en général un certificat numérique pour authentifier un ordinateur auprès d'autres ordinateurs ou utilisateurs. Un ordinateur peut obtenir un certificat numérique unique activé pour remplir plusieurs fonctions, ou plusieurs certificats numériques qui auront chacun un rôle différent sur le réseau.
  - comptes de service. Lorsqu'une autorité de certification délivre un certificat numérique à un service, il identifie ce dernier de manière unique lorsque le service participe au réseau. Le certificat numérique authentifie le service auprès des ordinateurs, des utilisateurs ou des autres services, et fournit des services de cryptage si le service doit crypter les données transmises. Les autorités de certification ne délivrent pas de certificats directement aux services. Une autorité de certification fournit un certificat soit au compte d'ordinateur qui héberge le service (comme Internet Information Services, IIS), soit au compte d'utilisateur qu'utilise le service, comme l'agent de récupération EFS.
- les exigences métier en matière de conception d'une hiérarchie d'autorités de certification. Vous devez identifier les exigences métier auxquelles répond la hiérarchie d'autorités de certification que vous proposez. En outre, si vous implémentez une hiérarchie d'autorités de certification dans une société mondiale, vous devez vérifier que votre hiérarchie est conforme aux règlementations locales.
- les conditions techniques requises pour la conception d'une hiérarchie d'autorités de certification. Vous devez définir la configuration matérielle requise, allouer des ressources et assurer la disponibilité nécessaire pour votre hiérarchie d'autorités de certification. Une autorité de certification n'est pas un rôle exigeant au niveau du matériel. Cependant, si vous souhaitez garantir une haute disponibilité, vous devriez envisager d'implémenter les autorités de certification dans un cluster. Bien qu'il soit possible de déployer AD CS sur un serveur unique, plusieurs déploiements vont impliquer plusieurs serveurs que vous configurerez comme autorités de certification, ainsi que d'autres serveurs que vous configurerez comme répondeurs en ligne, et d'autres encore que vous configurerez comme portails d'inscription Web. Vous pouvez configurer les autorités de certification sur des serveurs exécutant divers systèmes d'exploitation, notamment Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, et Windows Server 2003. Cependant, tous les systèmes d'exploitation ne prennent pas en charge toutes les fonctionnalités ou conditions de la conception. Par conséquent, l'élaboration d'une conception optimale requerra une planification et des tests rigoureux avant de déployer AD CS dans un environnement de production.
- la gestion et la sécurité des autorités de certification et des certificats. N'oubliez pas que vous devrez gérer votre autorité de certification au moyen de la console de gestion d'une autorité de certification ou des outils en ligne de commande. Spécificité de Windows Server 2012, vous pouvez également gérer vos AC au moyen de Windows PowerShell®. Les serveurs d'autorités de certification doivent être fortement protégés. Lorsque vous planifiez une hiérarchie d'autorités de certification, vous devez décider d'une méthode de sécurisation des serveurs et des certificats. Vous pouvez choisir d'utiliser des modules de sécurité matérielle (HSM) ou une autre méthode telle que le chiffrement de lecteur Windows BitLocker®.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Autorités de certification internes et publiques

Quand vous prévoyez l'implémentation d'une PKI pour votre organisation, un des premiers choix que vous devez faire consiste à décider si vous voulez utiliser des autorités de certification privées ou publiques. Vous pouvez établir une PKI selon l'une de ces deux approches. Si vous décidez d'utiliser une autorité de certification privée, déployez le rôle de serveur AD CS, puis établissez une PKI interne. Si vous décidez d'utiliser une PKI externe, vous n'avez aucun service à déployer en interne.



Les deux approches ont des avantages et des inconvénients, comme le tableau suivant les indique.

Type d'AC	Avantages	Inconvénients
Autorité de certification publique externe	• À laquelle beaucoup de clients externes font confiance (navigateurs Web, systèmes d'exploitation) • Nécessite une administration minimale	• Un coût plus élevé par rapport à une autorité de certification interne • Le coût est basé sur le certificat • L'acquisition du certificat est plus lente
Autorité de certification privée interne	• Assure un contrôle supérieur de la gestion de certificat • Moins onéreux par rapport à une autorité de certification publique • Modèles personnalisés • Inscription automatique	• Par défaut, les clients externes ne lui font pas confiance (navigateurs Web, systèmes d'exploitation) • Nécessite une administration supérieure

Certaines organisations utilisent une approche hybride de leur architecture de PKI. Cette approche utilise une autorité de certification publique externe pour l'autorité de certification racine, et une hiérarchie d'autorités de certification interne pour la distribution des certificats. Les organisations ont l'avantage que les clients externes ont confiance en leurs certificats émis en interne, avec les avantages d'une autorité de certification interne. Le seul inconvénient à cette méthode est le coût. Une approche hybride est en général l'approche la plus coûteuse parce que les certificats publics sont très chers.

Vous pouvez également déployer des PKI internes avec lesquelles vous pouvez utiliser EFS et les signatures numériques. Pour les fins externes, comme la protection des serveurs Web ou de messagerie avec SSL, vous devez acheter un certificat public. Cette approche est probablement la solution la plus rentable car elle n'est en général pas très coûteuse.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification d'une hiérarchie d'autorités de certification

Lors de la planification de la hiérarchie, il existe plusieurs raisons éventuelles au déploiement de plusieurs AC, notamment

- Créer des autorités de certification spécialisées dans la génération de certains types de certificats
- Répondre aux besoins de plusieurs départements
- Améliorer les performances
- Limiter les accès administratifs
- Déployer une AC de stratégies

Quand vous décidez d'implémenter une PKI dans votre organisation, une des premières décisions que vous devez prendre concerne la conception de votre hiérarchie d'autorités de certification. Elle détermine la conception de base de votre PKI interne ainsi que l'objectif de chaque autorité de certification dans la hiérarchie. Chaque hiérarchie d'autorités de certification comporte deux autorités de certification ou plus. Seule l'autorité de certification racine est obligatoire. Par conséquent vous déployez généralement la deuxième autorité de certification, et toutes celles qui la suivent dans la hiérarchie, avec un objectif spécifique. Vous ne pouvez pas avoir une AC secondaire sans avoir une AC racine. Cependant, une AC racine peut exister sans AC secondaire. Si vous gérez un environnement de petite dimension et que la sécurité n'est pas votre principal souci, vous pouvez avoir simplement une AC racine qui fournit des certificats aux utilisateurs et aux ordinateurs.

Vous pouvez créer une hiérarchie d'autorités de certification pour accomplir les actions suivantes :

- créer des autorités de certification spécialisées dans la génération de certains types de certificats, ou de certificats ayant des objectifs spécifiques ;
- satisfaire les besoins de plusieurs divisions de votre organisation, qui peuvent rendre nécessaires des stratégies d'autorité de certification différentes ou des accès administrateur spécifiques ;
- améliorer les performances en déchargeant le processus de publication des certificats aux autorités de certification dédiées ;
- restreindre l'accès administratif en déléguant les autorisations administratives à des autorités de certification spécifiques et non à la PKI entière.

Scénarios supplémentaires d'implémentation d'une hiérarchie d'autorités de certification dans des environnements plus complexes :

- AC de stratégies. Dans ce scénario, vous utilisez les AC de stratégies comme autorité de certification secondaire, qui repose directement en dessous de l'autorité de certification racine dans la hiérarchie. Vous utilisez des autorités de certification de stratégies pour émettre des certificats aux autorités de certification secondaires situées directement en dessous. Utilisez des autorités de certification de stratégies quand les différents divisions, secteurs, ou sites de votre organisation requièrent différentes stratégies et procédures d'émission ;
- approbation de certification croisée. Dans ce scénario, deux hiérarchies d'autorités de certification indépendantes interagissent quand une autorité de certification dans une hiérarchie émet un certificat d'autorité de certification à une autorité de certification dans l'autre hiérarchie. Les approbations de certification croisée sont détaillées dans des sections ultérieures de ce module ;
- hiérarchie à deux niveaux. Dans ce scénario, il existe une autorité de certification racine et au moins une autorité de certification secondaire, pour former deux niveaux. L'autorité de certification secondaire est responsable des stratégies et de l'émission des certificats aux demandeurs.

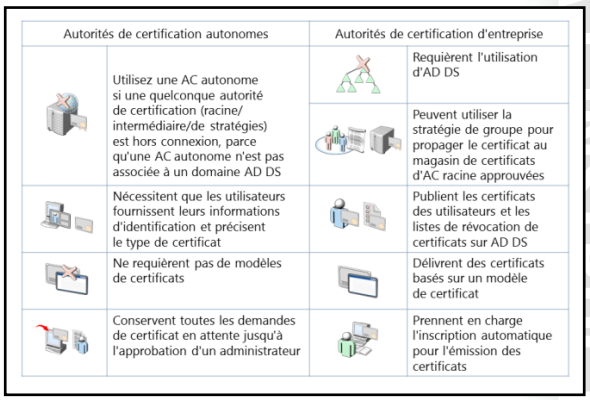
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les avantages de la création d'une hiérarchie d'autorités de certification sont entre autres :

- le renforcement de la sécurité et de l'évolutivité qui découle de l'utilisation d'autorités de certification dédiées pour des types de tâches spécifiques, telles que la gestion des cartes à puce. En outre, vous pouvez répartir l'émission de certificats sur plusieurs autorités de certification, équilibrant de ce fait la charge ;
- l'administration flexible de la hiérarchie d'autorités de certification, qui permet le contrôle d'accès basé sur les rôles (RBAC) et la décentralisation de la gestion des autorités de certification ;
- la prise en charge des autorités de certification commerciales, ce qui permet à la racine d'une hiérarchie de commencer au niveau d'une racine d'autorité de certification commerciale ;
- la prise en charge de la plupart des applications n'est pas un souci dans une hiérarchie. Cela découle du fait que les applications qui consomment les certificats d'une hiérarchie ne posent aucun problème, contrairement à ce qui se passe dans un environnement d'autorité de certification unique.

Éléments à prendre en compte des autorités de certification autonomes et d'entreprise

Sous Windows Server 2012, vous pouvez déployer deux types d'autorités de certification : autonomes et d'entreprise. La différence entre ces types d'autorités de certification est fondée sur leur fonctionnalité et leur configuration de stockage, pas sur la hiérarchie. La différence la plus importante entre ces deux types d'AC est l'intégration et la dépendance avec Active Directory. Une autorité de certification autonome peut fonctionner sans AD DS, et n'en dépend pas. Une AC d'entreprise requiert AD DS, mais présente également plusieurs avantages, comme l'inscription automatique.



Le tableau suivant répertorie les différences principales entre une autorité de certification autonome et une autorité de certification d'entreprise.

Caractéristique	Autorité de certification autonome	Autorité de certification d'entreprise
Utilisation normale	Vous utilisez généralement une autorité de certification autonome pour les autorités de certification hors connexion, mais vous pouvez également l'utiliser pour une autorité de certification qui est uniformément disponible sur le réseau.	Vous l'utilisez généralement en tant qu'autorité de certification d'entreprise pour délivrer des certificats aux utilisateurs, aux ordinateurs et aux services. Vous ne l'utilisez généralement pas comme autorité de certification hors connexion.
Dépendances à Active Directory	Une autorité de certification autonome ne dépend pas d'AD DS et peut être déployée dans des environnements non-Active Directory.	Une AC d'entreprise requiert AD DS, qui peut être utilisé comme base de données de configuration et d'inscription. Une AC d'entreprise constitue également un point de publication pour des certificats émis aux utilisateurs et aux ordinateurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

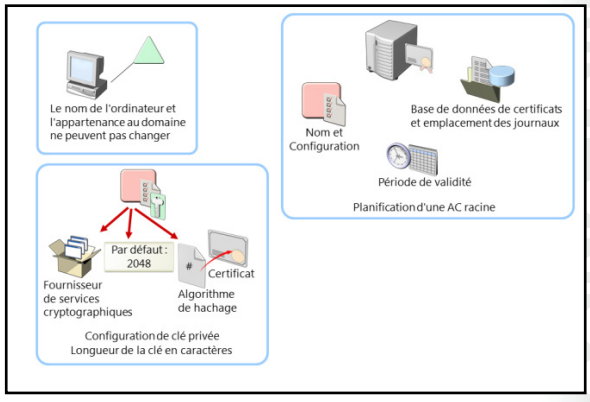
(suite)

Caractéristique	Autorité de certification autonome	Autorité de certification d'entreprise
Méthodes de demande de certificat	Les utilisateurs peuvent demander des certificats à une autorité de certification autonome uniquement à l'aide d'une inscription manuelle ou sur le Web.	Les utilisateurs peuvent demander des certificats à une AC d'entreprise comme suit : • inscription manuelle ; • inscription via le Web ; • Inscription automatique • agent d'inscription.
Méthodes d'émission de certificat	Un administrateur de certificat doit approuver manuellement toutes les demandes.	L'autorité de certification peut émettre le certificat ou refuser la demande automatiquement, selon la liste de contrôle d'accès discrétionnaire (DACL) du modèle.

La manière la plus courante de déployer une autorité de certification racine (qui est la première autorité de certification déployée) consiste à la déployer en tant qu'autorité de certification autonome. Elle peut ensuite être mise hors connexion après l'émission d'un certificat pour elle-même et pour une autorité de certification secondaire. De plus, vous déployez habituellement une autorité de certification secondaire comme une AC d'entreprise, et vous la configurez selon l'un des scénarios décrits dans la rubrique précédente.

En général, vous déployez l'autorité de certification autonome lorsque vous ne souhaitez pas effectuer l'intégration avec AD DS, et quand vous n'avez pas besoin d'automatiser le processus d'émission de certificats. Par exemple, si vous souhaitez publier des certificats pour les membres extérieurs au domaine, une AC autonome est une bonne solution. D'autre part, nous recommandons une AC d'entreprise dans les scénarios où vous voulez tirer profit d'AD DS et d'une stratégie de groupe pour automatiser la plupart des processus relatifs aux certificats.

Éléments à prendre en compte pour le déploiement d'une AC racine



Vous devez prendre plusieurs décisions avant de déployer une AC racine. Tout d'abord, vous devez décider si vous avez besoin de déployer une AC racine hors connexion. En fonction de cette décision, vous devez également déterminer si vous devez déployer une AC racine autonome ou une AC racine d'entreprise.

Le choix le plus courant consiste à opter pour une AC racine d'entreprise si vous déployez une hiérarchie d'autorités de certification à une seule couche ; en d'autres termes, vous déployez une seule autorité de certification. Toutefois, si vous déployez une hiérarchie à deux couches, le scénario le plus commun est le déploiement d'une autorité de certification racine autonome et d'une autorité de certification secondaire d'entreprise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le facteur suivant à prendre en considération est le type d'installation du système d'exploitation. AD CS prend en charge les scénarios d'installation complète et d'installation minimale. L'installation minimale offre une moindre surface d'attaque et suscite moins de traitement administratif. Par conséquent, vous avez fortement intérêt à envisager une installation minimale si vous avez un environnement d'entreprise.

Vous devez également être conscient du fait que, après le déploiement d'une autorité de certification sur un ordinateur, vous ne pouvez pas modifier les noms d'ordinateur ou les appartenances au domaine d'ordinateurs, ni modifier le nom de domaine. Par conséquent, il est important de déterminer ces attributs avant d'installer une autorité de certification.

Le tableau suivant détaille les éléments à prendre en compte supplémentaires.

Élément à prendre en compte	Description
Vous utilisez un fournisseur de services de chiffrement pour générer de nouvelles clés	• Le fournisseur de services de chiffrement par défaut est le fournisseur de services cryptographiques renforcés Microsoft. • N'importe quel fournisseur dont le nom commence par un signe de numéro (#) est un fournisseur CNG.
La longueur possible de la clé en caractères	La longueur de clé par défaut pour le fournisseur de services cryptographiques renforcés Microsoft est de 2 048 caractères. C'est la valeur minimale recommandée pour une autorité de certification racine.
L'algorithme de hachage utilisé pour signer des certificats émis par une autorité de certification	La valeur par défaut de l'algorithme de hachage est SHA-1.
La période de validité pour les certificats émis par une autorité de certification	La valeur par défaut pour les certificats est de cinq ans.
L'état du serveur racine (en ligne ou hors connexion)	Il convient de déployer le serveur racine comme une autorité de certification hors connexion. Cela améliore la sécurité et protège le certificat racine (parce qu'il n'est pas disponible pour être attaqué sur le réseau).

Spécifiquement, si vous décidez de déployer une autorité de certification racine autonome hors connexion, voici quelques facteurs spécifiques à prendre en compte :

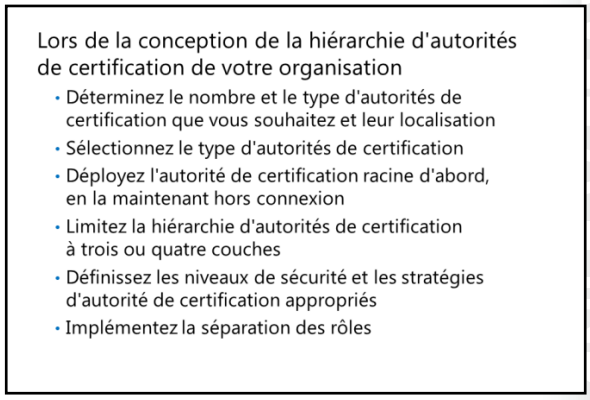
- Avant que vous n'émettiez un certificat secondaire d'autorité de certification racine, assurez-vous de fournir au moins un emplacement de distribution (CDP) de liste de révocation de certificat et un accès aux informations de l'autorité (AIA) qui sera à la disposition de tous les clients. En effet, par défaut, une autorité de certification racine autonome comprend le CDP et l'AIA. Par conséquent, quand vous mettez l'autorité de certification racine hors réseau, le test de vérification de révocation échoue car les emplacements de CDP et d'AIA sont inaccessibles. Quand vous définissez ces emplacements, vous devez copier manuellement les informations de la liste de révocation des certificats et de l'AIA à ces emplacements.
- Vous devez définir une période de validité pour les listes de révocation de certificats que l'autorité de certification racine publie pour une durée étendue, comme un an. Cela signifie que vous devez activer l'autorité de certification racine une fois par an pour publier une nouvelle liste de révocation de certificats, puis la copier vers un emplacement disponible aux clients. Si vous ne faites pas cela, après l'expiration de la liste de révocation de certificats de l'AC racine, le test de vérification de révocation pour tous les certificats échouera également.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Vous devez utiliser une stratégie de groupe pour publier le certificat d'AC racine dans un magasin AC racine de confiance sur tous les serveurs et les ordinateurs clients. Vous devez le faire manuellement, parce qu'une autorité de certification autonome ne peut pas le faire automatiquement, à la différence d'une AC d'entreprise. Vous pouvez également publier le certificat d'AC racine sur AD DS à l'aide de l'outil de ligne de commande **certutil**.
- Si vous décidez de déployer une AC racine autonome hors connexion comme ordinateur virtuel, vous devez vérifier que l'ordinateur est aussi sécurisé que possible. Nous vous recommandons de le supprimer du stockage où se trouvent d'autres ordinateurs virtuels et de limiter l'accès à l'ordinateur virtuel autorité de certification.

Instructions de conception d'une hiérarchie d'autorités de certification

Prenez en compte les instructions suivantes lors de votre conception de la hiérarchie d'AC de votre organisation :



- décidez de combien d'autorités de certification vous avez besoin, de quels types, et où les localiser. Rassemblez les éléments de configuration requise pour chaque AC ;
- sélectionnez le type d'une autorité de certification avant de la déployer. Il est impossible de convertir une autorité de certification racine en autorité de certification secondaire, ou vice-versa. Vous devez donc déterminer le type d'une autorité de certification avant de commencer son déploiement. Souvenez-vous en outre qu'il est impossible de convertir les autorités de certification autonomes en autorités de certification d'entreprise ;
- commencez par le haut et suivez la hiérarchie en descendant. Déployez l'autorité de certification racine d'abord. Si vous choisissez de déployer une AC racine privée, vérifiez qu'elle est sécurisée en la conservant hors connexion. Déployez l'autorité de certification racine dans un emplacement physiquement sécurisé. Ne faites pas de l'ordinateur un membre d'un domaine.
- Créez une hiérarchie d'autorités de certification de trois à quatre couches de profondeur. Le déploiement de plus de quatre couches introduit une complexité supplémentaire dans la hiérarchie d'autorités de certification qui peut devenir difficile à gérer. Mais une profondeur de moins de trois couches peut ne pas garantir une sécurité suffisante si votre entreprise a de fortes exigences de sécurité.
- Définissez les niveaux de sécurité et les stratégies d'autorité de certification appropriées pour chaque AC de votre hiérarchie, en fonction des exigences de la conception.
- Implémentez la séparation des rôles de sorte qu'une personne ne puisse pas compromettre la sécurité de la PKI de votre organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Conception d'un plan de récupération d'urgence pour une hiérarchie d'autorités de certification

La PKI est un service très important dans toute infrastructure réseau. Il est donc nécessaire de bien planifier la façon dont vous la récupèrerez si un incident se produit. Soyez conscient qu'une hiérarchie d'autorités de certification non fonctionnelle peut non seulement empêcher l'émission de nouveaux certificats, mais aussi empêcher l'utilisation des certificats existants.

Un plan de récupération d'urgence pour une hiérarchie d'autorités de certification doit comprendre

- La documentation sur les paramètres de la hiérarchie d'autorités de certification
- La documentation sur les modèles de certificats personnalisés
- La procédure de sauvegarde pour les composants essentiels des autorités de certification
- La procédure de restauration de la fonctionnalité AD CS sur le nouveau serveur
- Les problèmes potentiels

AD CS peut cesser de fonctionner pour de nombreuses raisons. Par exemple, si le service d'autorité de certification ne peut pas démarrer sur l'ordinateur d'AC, vous ne pourrez pas émettre de nouveaux certificats. En outre, vous ne pourrez pas traiter le contrôle de révocation sur le certificat existant. Si le matériel d'un serveur d'autorité de certification connaît une défaillance, cela peut affecter les services de certification. Les défaillances de l'infrastructure réseau peuvent également empêcher AD CS de fonctionner correctement.

Il est important de disposer d'un plan de récupération d'urgence dans le cadre de n'importe quel scénario. Il vous permettra de restaurer votre hiérarchie d'autorités de certification aussi vite que possible.

La sauvegarde est une composante très importante de tout plan de récupération d'urgence pour la PKI. Vous devez identifier clairement les composants et les paramètres de votre PKI que vous devez sauvegarder régulièrement. En outre, il est très important que vous documentiez toutes les modifications que vous exécutez sur votre hiérarchie d'autorités de certification, de sorte que vous puissiez restaurer facilement les objets si nécessaire, et notamment :

- les définitions de modèle de certificat, pour tous les modèles de certificats que vous créez manuellement ;
- la liste des modèles de certificats émis dans votre hiérarchie d'autorités de certification ;
- les autorisations des modèles de certificats ;
- les droits de gestion des autorités de certification ;
- tous les paramètres spécifiques présents dans les propriétés des autorités de certification ;
- les chemins de données pour la base de données des autorités de certification ;
- tous les emplacements personnalisés définis pour les points AIA et CDP ;
- le contenu du fichier CAPolicy.inf, si vous l'utilisez pendant le déploiement des AC ;
- Le fournisseur de services de chiffrement utilisé pour protéger la clé privée des autorités de certification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si vous avez documenté ces éléments, vous pourrez facilement restaurer la fonctionnalité des autorités de certification, même sans sauvegarde. Cependant, notez que vous n'avez pas besoin de sauvegarder la clé privée d'une autorité de certification pour restaurer sa fonctionnalité après un incident, et qu'il est beaucoup plus fiable de maintenir des sauvegardes régulières des composantes essentielles des autorités de certification.

Vous pouvez effectuer une sauvegarde de votre AC à l'aide de la Sauvegarde Windows Server. Si vous choisissez d'effectuer une sauvegarde de l'état du système, elle réalisera également la sauvegarde de l'AC avec tous les composants nécessaires.

Vous pouvez également utiliser l'outil en ligne de commande **certutil** et des applets de commande Windows PowerShell pour gérer les sauvegardes de la hiérarchie d'autorités de certification.

Par exemple, si vous souhaitez effectuer une sauvegarde d'autorité de certification, utilisez cette commande :

```
certutil -backup -p Mot de passe chemin_accès_fichier
```

Pour exporter tous les paramètres de registre d'une autorité de certification, exécutez la commande suivante :

```
reg export HKLM\System\CurrentControlSet\Services\CertSvc\Configuration chemin_accès_fichier
```

Pour exporter toutes les informations sur les modèles de certificats, exécutez la commande suivante :

```
Certutil –catemplates > chemin_accès_fichier
```

Restauration des fonctionnalités AD CS

Si vous ne pouvez pas récupérer votre autorité de certification courante en ligne après un incident, vous devez activer la fonctionnalité AD CS sur un autre serveur. Il y a plusieurs étapes à effectuer pour restaurer AD CS sur un autre serveur. Tout d'abord, vous devez vous assurer que vous avez une sauvegarde fiable et à jour de l'autorité de certification antérieure, ce qui a été exposé en détail précédemment dans cette rubrique.

Voici les étapes que vous devez réaliser pour restaurer les fonctionnalités AD CS sur un autre serveur :

- étendre la durée de vie du fichier de la liste de révocation de certificats ;
- désaffecter l'ancienne autorité de certification ;
- installer AD CS sur le nouveau serveur ;
- restaurer la configuration des autorités de certification ;
- restaurer la base de données et les modèles des autorités de certification ;

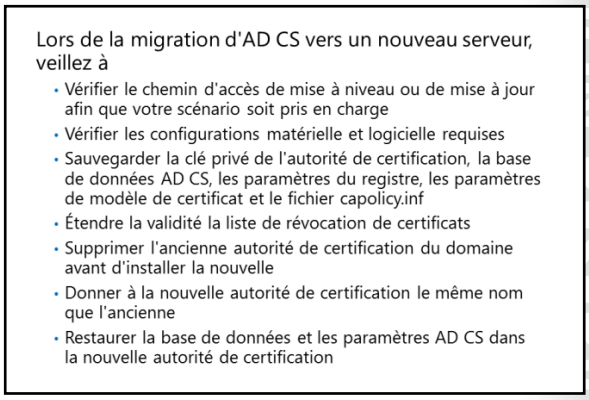
Pour restaurer les fonctionnalités AD CS sur le nouveau serveur, vous devez disposer d'une sauvegarde à jour. Vous devez de plus vérifier que l'ancienne autorité de certification ne se connectera plus jamais à votre réseau, car la nouvelle autorité de certification aura la même identité. Cela pourrait provoquer un conflit et avoir pour résultat le rejet des certificats.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Migration et mise à niveau des autorités de certification

Dans certains scénarios, vous devrez faire migrer les fonctionnalités AD CS vers un autre ordinateur, ou faire migrer votre autorité de certification vers un autre serveur. Par exemple, si votre autorité de certification actuelle s'exécute sous Windows Server 2008 R2, vous pouvez souhaiter la faire migrer vers un serveur sous Windows Server 2012.

AD CS prend en charge la migration entre plateformes ; le tableau ci-dessous décrit les scénarios possibles.



Processeur du serveur source	Système d'exploitation du serveur source	Système d'exploitation du serveur de destination	Processeur du serveur de destination
x86 ou x64	Windows Server 2003 avec Service Pack 2 (SP2)	Windows Server 2008 R2, installations complète ou minimale	x64
x86 ou x64	Windows Server 2003 R2	Windows Server 2008 R2, installations complète ou minimale	x64
x86 ou x64	Windows Server 2008	Windows Server 2008 R2 ou Windows Server 2012, installations complète ou minimale	x64
x64	Windows Server 2008 R2	Windows Server 2008 R2 ou Windows Server 2012, installations complète ou minimale	x64

Avant de faire migrer votre autorité de certification vers un nouveau serveur, vous devez effectuer plusieurs tâches de préparation :

- vérifier que le serveur de destination répond aux exigences logicielles et matérielles pour le déploiement d'AD CS ;
- sauvegarder votre serveur AD CS source, notamment :
  - la liste des modèles d'autorité de certification (requise uniquement pour les autorités de certification d'entreprise). Vous pouvez prendre note par écrit des détails de vos modèles personnalisés, ou vous pouvez le faire en tapant :

```
certutil.exe –catemplates > catemplates.txt command
```

  - enregistrer l'algorithme de signature et le fournisseur de services de chiffrement de l'autorité de certification. Pour cela, tapez la commande suivante :

```
certutil.exe –getreg ca\csp\* > csp.txt
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- publier une liste de révocation de certificats avec une période de validité étendue ;
- sauvegarder votre clé privée et la base de données de l'autorité de certification sur votre serveur source. Vous pouvez le faire à partir du composant logiciel enfichable de l'autorité de certification en cliquant avec le bouton droit sur un objet Autorité de certification, en sélectionnant **Toutes les tâches**, puis en sélectionnant **Sauvegarder l'autorité de certification**. Vous pouvez également utiliser l'outil de commande en ligne **certutil**.
- enregistrer les paramètres de Registre actuels de l'autorité de certification. Vous pouvez le faire au moyen de l'outil en ligne de commande Reg.exe ou en tapant la commande suivante :

```
reg export HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration <fichier de résultat.reg>
```

- enregistrez le fichier capolicy.inf sur votre autorité de certification actuelle (si elle existe). Ce fichier est en général situé dans le dossier C:\Windows.

Après avoir effectué toutes les étapes de préparation, vous pouvez initier le processus de migration, qui comprend plusieurs étapes :

1. Supprimer le rôle AD CS de votre autorité de certification actuelle. Il est très important d'effectuer cette étape avant de continuer, parce que votre nouvelle autorité de certification aura le même nom. Cela peut entraîner un conflit si les deux autorités de certification s'exécutent sous le même nom simultanément. Cependant, vous devez savoir que lorsque vous désinstallerez le rôle AD CS du serveur, la base de données de l'autorité de certification, la clé privée et le certificat ne seront pas supprimés du serveur source. Cela vous donne la possibilité de restaurer l'ancien serveur si la migration ne se déroule pas correctement.
2. Supprimer l'ancien serveur d'autorité de certification de votre domaine. Vous devez faire cela pour les mêmes raisons que l'étape précédente, car la nouvelle autorité de certification aura le même nom de domaine.
3. Renommer le nouveau serveur et le joindre au domaine. Une fois que votre serveur d'autorité de certification actuel a été supprimé du domaine, vous devez renommer votre nouveau serveur de sorte qu'il ait le même nom que l'ancien. Vous devez ensuite le joindre à votre domaine AD DS.
4. Ajouter le rôle AD DS au nouveau serveur. Vous pouvez faire cela au moyen de la console du Gestionnaire de serveur sur le serveur de destination.
5. Importer le certificat à partir de l'ancien serveur d'autorité de certification. Pour restaurer l'identité de votre ancien serveur d'autorité de certification, vous devez importer la clé privée de l'ancienne autorité de certification.
6. Restaurerez les données à partir de la sauvegarde. Vous devez restaurer la base de données AD CS que vous avez sauvegardée, ainsi que vos paramètres du Registre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Planification et implémentation de modèles de certificats

Les modèles de certificats définissent la manière dont il est possible de demander un certificat et l'utilisation qui peut en être faite. Les modèles sont configurés dans l'AC et sont enregistrés dans la base de données AD DS. Il existe différentes versions des modèles : l'AC d'entreprise de Windows 2000 Server prend en charge la version 1 des modèles de certificats. Windows Server 2003 Enterprise Edition prend en charge les versions 1 et 2 des modèles et Windows Server 2008 Enterprise Edition prend en charge les versions 1, 2 et 3 des modèles de certificats. Windows Server 2012 propose la version 4 des modèles, mais prend toujours en charge les trois versions précédentes.

Dans cette leçon, vous allez apprendre à planifier et implémenter des modèles de certificats.

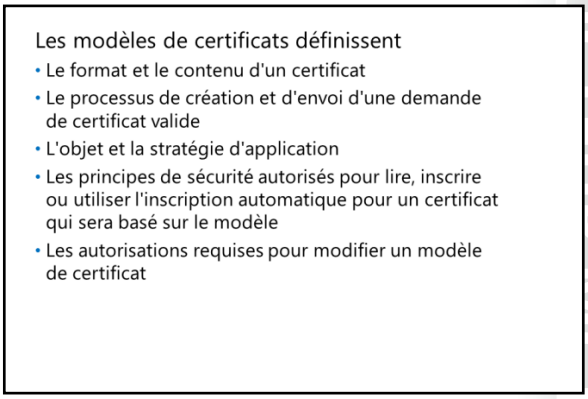
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les modèles de certificats ;
- décrire les versions des modèles de certificats ;
- décrire les méthodes de modification des modèles de certificat ;
- décrire les éléments à prendre en compte lors de la conception de la sécurité des modèles de certificats ;
- décrire les éléments à prendre en compte lors de la conception de modèles de certificats.

Que sont les modèles de certificats ?

Les modèles de certificats permettent aux administrateurs de personnaliser la méthode de distribution des certificats, de définir les objectifs des certificats et de mandater le type d'utilisation qu'autorisé un certificat. Les administrateurs peuvent facilement créer des modèles puis les déployer rapidement au niveau de l'entreprise à l'aide d'une interface graphique utilisateur ou d'outils de ligne de commande intégrés. L'autorité de certification utilise des modèles de certificats pour :



- définir le format et le contenu des certificats ;
- définir l'objectif du certificat et sa stratégie d'application ;
- spécifier les utilisateurs et les ordinateurs qui peuvent s'inscrire pour différents types de certificats ;
- définir le processus d'inscription, comme l'inscription automatique, l'inscription avec signatures autorisées uniquement et l'inscription manuelle.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La liste DACL, associée à chaque modèle de certificat, définit les principaux de sécurité qui disposent des autorisations de lecture et de configuration du modèle, ainsi que d'inscription ou d'inscription automatique de certificats en fonction du modèle. Les modèles de certificats et leurs autorisations sont définies dans AD DS et demeurent valides au sein de la forêt. Si plusieurs AC d'entreprise sont exécutées dans la forêt AD DS, les modifications d'autorisations auront un effet sur toutes les AC.

Lorsque vous définissez un modèle de certificat, cette définition doit être disponible pour toutes les AC de la forêt. Pour ce faire, enregistrez les informations sur le modèle de certificat dans le contexte de nommage de configuration, où CN=Configuration et DC=ForestRootName. La réplication de ces informations dépend du programme de réplication Active Directory. En outre, le modèle de certificat peut ne pas être disponible à toutes les AC jusqu'à la fin de la réplication. Le stockage et la réplication se produisent automatiquement.

Remarque : Avant Windows Server 2008 R2, seules les éditions Enterprise de Windows Server prenaient en charge la gestion des modèles de certificats. Sous Windows Server 2008 R2 et Windows Server 2012, vous pouvez également gérer des modèles de certificats dans les éditions Standard.

Versions des modèles de certificats

L'autorité de certification de Windows Server 2012 prend en charge quatre versions des modèles de certificats. Les versions 1, 2 et 3 des modèles de certificats sont des versions précédentes des modèles de Windows Server, alors que la version 4 est une nouveauté de Windows Server 2012.

Version 1
- Introduit dans Windows Server 2000, fournie pour la rétrocompatibilité dans les versions plus récentes
- Créé par défaut lorsqu'une AC est installée
- Ne peut pas être modifié (excepté pour les autorisations) ni supprimé, mais peut être dupliqué pour devenir modèle de version 2 ou 3 (que vous pouvez alors modifier)

Version 2
- Modèle par défaut introduit avec Windows Server 2003
- Permet la personnalisation de la plupart des paramètres du modèle
- Offre plusieurs modèles préconfigurés quand une AC est installée

Version 3
- Prend en charge les paramètres avancés de chiffrement de Suite B
- Inclut des options avancées pour le chiffrement, les signatures numériques, l'échange de clé et le hachage
- Prend en charge uniquement les serveurs Windows Server 2008 et Windows Server 2008 R2
- Prend en charge uniquement les ordinateurs clients Windows Vista et Windows 7

Version 4
- Uniquement disponible pour Windows Server 2012 et les clients Windows 8
- Prend en charge les fournisseurs de services cryptographiques (CSP) et les fournisseurs de stockage de clés (KSP)
- Prend en charge le renouvellement avec la même clé

Les versions des modèles de certificat correspondent à la version du système d'exploitation Windows Server. Windows 2000 Server, Windows Server 2003, Windows Server 2008 et Windows Server 2012 correspondent à la version 1, à la version 2, à la version 3 et à la version 4 respectivement.

En plus de correspondre aux versions du système d'exploitation Windows Server, les versions des modèles de certificat présentent également des différences fonctionnelles, notamment :

- le système d'exploitation Windows 2000 Advanced Server prend en charge la version 1 des modèles de certificats. La seule modification qu'il permet pour les modèles de version 1 est la modification des autorisations pour autoriser ou interdire l'inscription du modèle de certificat. Lorsque vous installez une autorité de certification d'entreprise, des modèles de certificats version 1 sont créés par défaut. À compter du 13 juillet 2010, Microsoft ne prend plus en charge Windows 2000 Server ;
- les systèmes d'exploitation Windows Server 2003 Enterprise Edition prennent en charge la version 1 et la version 2 des modèles. Vous pouvez personnaliser plusieurs paramètres dans les modèles de version 2. L'installation par défaut fournit quelques modèles préconfigurés de version 2. Vous pouvez ajouter des modèles de version 2 en fonction des besoins de votre organisation. Sinon, vous pouvez dupliquer un modèle de certificat de version 1 pour créer une nouvelle version 2 du modèle. Vous pouvez ensuite modifier et sécuriser le modèle de certificat de version 2 récemment créé. Lorsque de nouveaux modèles sont ajoutés à une autorité de certification d'entreprise Windows Server 2003, il s'agit par défaut de la version 2 ;

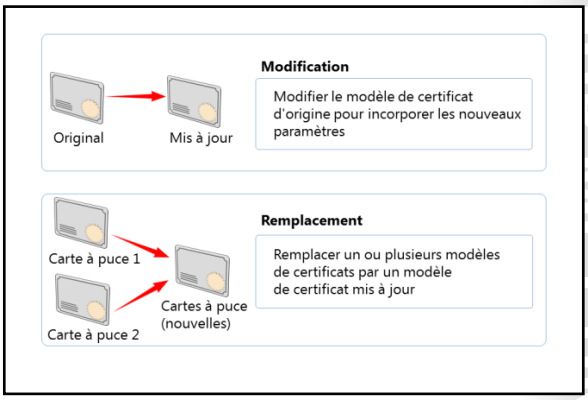
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- les systèmes d'exploitation Windows Server 2008 Enterprise prennent en charge les nouveaux modèles de certificats de version 3. De plus, ils prennent en charge les versions 1 et 2. Les modèles de certificats de version 3 prennent en charge plusieurs fonctionnalités d'une AC d'entreprise Windows Server 2008, comme CNG. CNG prend en charge des algorithmes cryptographiques de Suite B comme le chiffrement à courbe elliptique (ECC). Dans Windows Server 2008 Enterprise, vous pouvez dupliquer les modèles de versions 1 et 2 par défaut pour les enregistrer comme modèles de version 3. De plus, Windows Server 2008 propose par défaut deux nouveaux modèles de certificats : l'authentification Kerberos et la signature de réponse OCSP (Online Certificate Status Protocol). Dans Windows Server 2008 R2, la version standard prenait également en charge des modèles de certificat. Lorsque vous utilisez des modèles de certificats de version 3, vous pouvez utiliser le chiffrement CNG et des algorithmes de hachage pour les demandes de certificat, les certificats émis et la protection des clés privées pour l'échange et l'archivage des clés ;
- les systèmes d'exploitation Windows Server 2012 prennent en charge les modèles de certificats de version 4 et toutes les autres versions des éditions antérieures de Windows Server. Ces modèles de certificats sont disponibles uniquement sous Windows Server 2012 et Windows 8. Pour permettre aux administrateurs de distinguer les fonctionnalités prises en charge par une version de système d'exploitation spécifique, l'onglet Compatibilité a été ajouté à l'onglet Propriétés du modèle de certificat. Cette onglet indique certaines options comme indisponibles dans les propriétés du modèle de certificat, selon les versions du système d'exploitation sélectionné du client de certificat et de l'autorité de certification. Les modèles de certificats de version 4 prennent également en charge les fournisseurs CSP (fournisseurs de services de chiffrement) et les fournisseurs de stockage de clés. Vous pouvez les configurer pour demander le renouvellement avec la même clé.

La mise à niveau des modèles de certificats est un processus qui ne s'applique que lorsque l'AC a été mise à niveau de Windows Server 2008 ou 2008 R2 vers Windows Server 2012. Après la mise à niveau, vous pouvez mettre à niveau les modèles de certificats en démarrant la console du Gestionnaire d'autorités de certification et en cliquant sur **Oui** pour accepter l'invite de mise à jour.

Méthodes de modification des modèles de certificat

La hiérarchie d'autorités de certification de la plupart des organisations comporte un modèle de certificat pour chaque fonction. Par exemple, il peut y avoir un modèle de certificat pour le chiffrement de fichier et un autre pour la signature de code. En outre, il peut y avoir quelques modèles qui couvrent des fonctions pour la plupart des groupes ayant un objet commun.



En tant qu'administrateur informatique, il est possible que vous deviez modifier un modèle de certificat existant en raison de paramètres incorrects ou d'autres problèmes dans le modèle de certificat original. Il est également possible que vous deviez fusionner plusieurs modèles de certificats existants en un modèle d'unique.

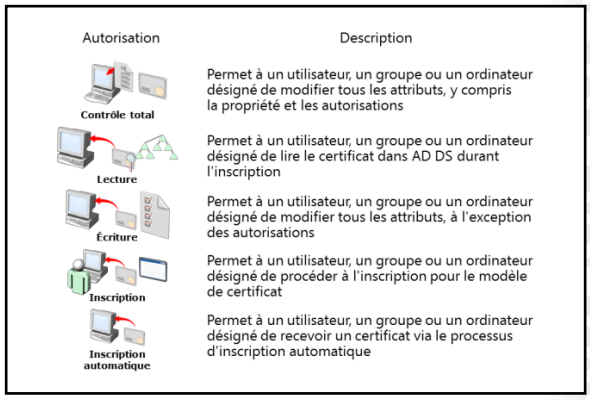
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez mettre à jour un modèle de certificat en modifiant le modèle ou en remplaçant le modèle existant :

- modification du modèle de certificat d'origine. Pour modifier un modèle de certificat de version 2, 3 ou 4, vous devez effectuer les modifications puis les appliquer à ce modèle. Cela fait, tout certificat émis par une autorité de certification et basé sur ce modèle inclura les modifications que vous avez apportées ;
- remplacement de modèles de certificats existants. La hiérarchie d'autorités de certification d'une organisation peut avoir plusieurs modèles de certificats qui proposent une fonctionnalité identique ou similaire. Dans ce cas, vous pouvez remplacer plusieurs modèles de certificats par un modèle unique. Pour cela, dans la console Modèles de certificat, vous pouvez désigner un nouveau modèle de certificat qui remplace les modèles de certificats existants.

Conception de la sécurité d'un modèle de certificat

Pour configurer les autorisations des modèles de certificat, vous devez définir la liste DACL pour chaque modèle. Les autorisations attribuées à un modèle de certificat définiront quels utilisateurs et groupes pourront lire ou modifier ce modèle ou s'y inscrire, automatiquement ou non. Vous devez configurer une liste DACL pour chaque modèle de certificat que vous utiliserez. Vous pourrez ainsi définir les tâches que les utilisateurs ou les ordinateurs sont autorisés à réaliser sur ce modèle.



Vous pouvez attribuer les autorisations suivantes aux modèles de certificats :

- Contrôle total. L'autorisation Contrôle total permet à une entité de sécurité de modifier tous les attributs d'un modèle de certificat, notamment les autorisations pour le modèle de certificat lui-même.
- Lecture. L'autorisation Lecture permet aux utilisateurs et aux ordinateurs d'afficher le modèle de certificat lors de l'inscription aux certificats. L'autorisation Lecture est requise par le serveur de certificat pour trouver les modèles de certificats dans AD DS.
- Écriture. L'autorisation Écriture permet aux utilisateurs et aux ordinateurs de modifier les attributs d'un modèle de certificat, notamment les autorisations que vous lui avez attribuées.
- Inscription. L'autorisation Inscription permet aux utilisateurs et aux ordinateurs de s'inscrire à un certificat sur la base du modèle de certificat. Toutefois, pour s'inscrire à un certificat, vous devez disposer également de l'autorisation de Lecture pour son modèle.
- Inscription automatique. L'autorisation Inscription automatique permet aux utilisateurs et aux ordinateurs de recevoir un certificat via le processus d'inscription automatique. Toutefois, l'autorisation Inscription automatique nécessite aussi que les utilisateurs et les ordinateurs disposent des autorisations de Lecture et d'Inscription pour un modèle de certificat.

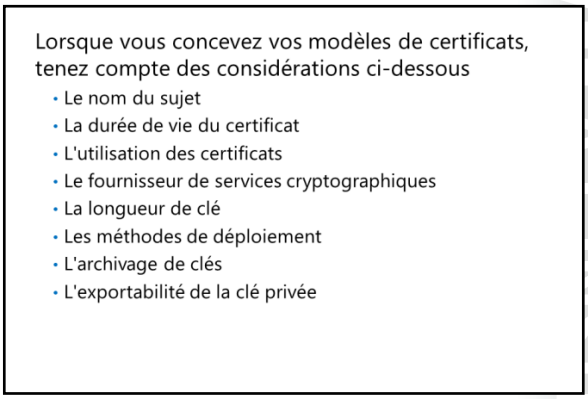
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Il vous est recommandé d'attribuer des autorisations de modèle de certificat uniquement à des groupes globaux ou universels, parce que le contexte de nommage des certificats dans AD DS stocke les objets des modèles de certificat. Vous ne pouvez pas attribuer d'autorisations à l'aide de groupes de domaine locaux présents dans un domaine AD DS, et vous ne devez jamais attribuer d'autorisations de modèle de certificat à un utilisateur individuel ou à des comptes d'ordinateurs.

Dans le cadre des meilleures pratiques, l'autorisation de Lecture doit toujours être attribuée au groupe d'utilisateurs authentifiés. Cela permet à tous les utilisateurs et ordinateurs d'afficher les modèles de certificat dans AD DS, et permet également à l'autorité de certification exécutée dans le contexte Système d'un compte d'ordinateur d'afficher les modèles lors de l'attribution de certificats.

Éléments à prendre en compte pour la conception de modèles de certificats

Lors de la conception des modèles de certificats, vous définissez les options disponibles sur la copie du modèle de certificat existant. En conséquence, vous obtenez un nouveau modèle de certificat dont les paramètres répondent à vos exigences. Lorsque vous concevez des modèles de certificats, tenez compte des considérations ci-dessous :



- le nom du sujet. Le nom du sujet du certificat est une valeur qui décrit normalement l'identité d'un utilisateur, d'un ordinateur ou d'un service qui s'inscrit à un certificat. Assurez-vous que vous saisissez le nom de sujet correct lors de l'inscription à un certificat. Cela empêche d'éventuels problèmes d'approbation du certificat. L'autorité de certification Windows Server 2012 peut également publier des certificats avec d'autres noms de sujets, ce qui vous permet d'utiliser plusieurs noms de sujets sur un seul certificat :
- la durée de vie du certificat. Chaque modèle de certificat définit la durée de vie des certificats émis par l'autorité de certification sur la base de ce modèle. Vous ne pouvez pas émettre de certificat à durée de vie illimitée. Il n'existe aucune recommandation stricte concernant la durée de vie qu'il convient de configurer pour un modèle. La durée de vie dépend des exigences de sécurité, de l'utilisation du certificat et du type de celui-ci. La durée de vie des certificats fonctionne comme un sous-ensemble de la durée de vie du certificat de l'autorité de certification. Tous les certificats, y compris des certificats de l'autorité de certification, ont des dates d'expiration après lesquelles ils ne sont plus valides. En conséquence, vous ne pouvez pas émettre de certificat dont la durée de vie dépasse celle de l'autorité de certification émettrice ;
- l'utilisation des certificats. Vous pouvez émettre de nombreux certificats, chacun avec un objectif particulier, ou un moindre nombre avec une utilisation plus large pour chacun. Cette décision dépend de votre environnement, du niveau d'administration que vous souhaitez, des effets potentiels sur les sujets et des effets de la multiplicité des certificats sur les applications qui les utiliseront. Une bonne stratégie d'administration des certificats consiste à créer un modèle pour chaque fonction, telle que le chiffrement de fichier ou la signature de code. Les sujets peuvent alors s'inscrire à chaque certificat de la manière adéquate à leur fonction. Cela permet de faire en sorte que les sujets démarrent avec peu de certificats, puis n'obtiennent que les nouveaux certificats dont ils ont besoin. L'inconvénient de cette stratégie est que le sujet peut accumuler un grand nombre de certificats et de clés privées qu'il devient difficile de gérer ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- le fournisseur de service de chiffrement que vous implémenterez. Un modèle de certificat de version 2 vous permet de définir un ou plusieurs fournisseurs de services de chiffrement (CSP) qu'il utilisera. Cela permet à l'administrateur de contrôler les types de chiffrement que les sujets pourront utiliser au sein de l'entreprise. Cela est utile lorsque la sécurité est votre priorité. Comme les sujets utilisent le CSP pour les deux aspects d'un service d'encryptage (tant le chiffrement que le déchiffrement, ou la signature que la confirmation de signature), vous devez vous assurer que tous les sujets peuvent utiliser le même fournisseur de services de chiffrement. La meilleure façon de procéder consiste à configurer chaque modèle de certificat pour identifier un fournisseur de services de chiffrement. L'administrateur doit déterminer le CSP à utiliser pour chaque modèle, selon le niveau de sécurité requis, les objectifs prévus du certificat et la présence de matériels de sécurité tels que des cartes à puce ;
- la longueur de clé. Vous pouvez définir une taille de clé minimum autorisée pour un modèle de certificat. En règle générale, pour un même algorithme, les clés longues assurent une meilleure sécurité que les clés courtes. Toutefois, les clés longues prennent plus de temps à générer et à utiliser. Vous devez choisir la taille de clé minimale qui garantit le niveau de protection nécessaire sans affecter les performances ;
- les méthodes de déploiement. Vous pouvez configurer l'émission de certificats aux sujets de plusieurs manières, y compris l'inscription manuelle, l'inscription automatique et l'inscription Web. En outre, il existes de nombreuses stratégies de certificat, notamment l'émission d'un certificat global à tous les sujets ou l'émission pour les sujets de plusieurs certificats spécifiques à des applications, selon les besoins. Devant tant de possibilités, vous devez planifier votre méthode de déploiement bien avant de déployer les certificats ;
- l'archivage de clés. Lorsque les sujets perdent leurs clés privées, ils ne peuvent pas accéder aux informations qui ont été chiffrées de manière permanente avec la clé publique correspondante. Pour éviter ce problème, l'archivage de clés vous permet de chiffrer et archiver les clés dans la base de données de l'autorité de certification lors de l'émission des certificats. Si les sujets perdent leurs clés, vous pouvez récupérer ces informations dans la base de données et les mettre à leur disposition. Cela vous permet de récupérer les informations chiffrées au lieu de les perdre ;
- si les utilisateurs ont la possibilité d'exporter la clé privée. Si vous souhaitez autoriser des utilisateurs à exporter des certificats avec leurs clés privées, vous devez configurer cette option sur le modèle de certificat. Si vous activez cette option, les utilisateurs pourront utiliser la console de gestion de certificats pour exporter leurs certificats puis les déplacer vers un autre ordinateur.

Vous pouvez personnaliser les modèles de certificats avec plusieurs extensions qui régissent leur utilisation, notamment :

- les stratégies d'émission. Une stratégie d'émission, également appelé une stratégie d'inscription ou de certificat, est un groupe de règles administratives que vous implémentez à l'émission des certificats. Un identificateur d'objet (OID) que vous définissez au niveau de l'autorité de certification représente une stratégie d'émission dans un certificat. Le certificat émis comprend l'OID, et quand un sujet présente son certificat, la cible peut l'examiner pour vérifier la stratégie d'émission, puis déterminer si ce niveau de stratégie d'émission est suffisant pour réaliser l'action demandée ;
- les stratégies d'application. Les stratégies d'application vous permettent de déterminer quels certificats peuvent être utilisés à certaines fins. Cela vous permet de délivrer des certificats en grande quantité sans vous préoccuper de leur utilisation à des fins imprévues. Les stratégies d'application sont parfois sont appelées stratégies d'utilisation avancée de la clé. Comme certaines implémentations des applications de PKI ne peuvent pas interpréter les stratégies d'application, les sections des stratégies d'application et d'utilisation avancée de la clé sont présentes dans les certificats émis par les autorités de certification basées sur Windows Server ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- l'utilisation de la clé**.** Un certificat permet au sujet d'effectuer une tâche spécifique. Afin d'empêcher l'abus des certificats, ceux-ci font automatiquement l'objet de restrictions. L'utilisation de la clé est une méthode de restriction qu'utilisent les administrateurs pour définir l'utilisation des certificats ;
- les contraintes de base. Les contraintes de base assurent que les certificats d'autorité de certification ne sont utilisés que dans certaines applications. Par exemple, une contrainte de base peut être la longueur du chemin d'accès. La longueur de chemin d'accès détermine le nombre d'autorités de certification autorisées en dessous de l'autorité de certification en cours. Cette contrainte sur la longueur du chemin garantit que les autorités de certification à son extrémité ne peuvent émettre que des certificats d'entité finale et non des certificats d'autorité de certification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Planification et implémentation la distribution et la révocation de certificats

La définition des méthodes pour la distribution et la révocation de certificats constitue l'étape suivante du déploiement d'une PKI. Il peut y avoir plusieurs raisons pour révoquer des certificats ; par exemple si une clé est compromise ou si un employé quitte l'entreprise. Vous devez vous assurer que les clients réseau peuvent déterminer quels certificats sont révoqués avant d'accepter les demandes d'authentification. Pour vérifier l'évolutivité et la haute disponibilité, vous pouvez déployer le répondeur en ligne AD CS et vous pouvez l'utiliser pour fournir l'état de révocation des certificats. Dans ce cours, vous découvrirez des méthodes de distribution et de révocation de certificats.

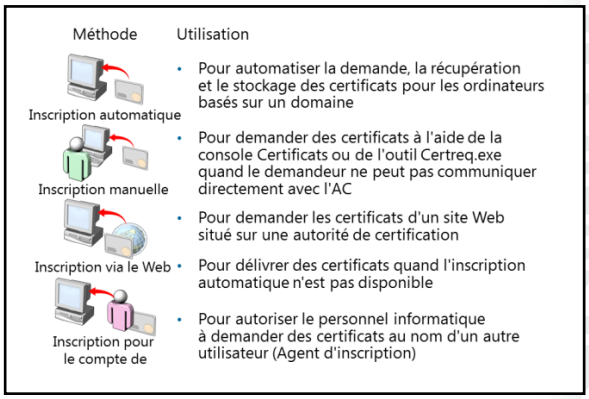
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options d'inscription et de distribution des certificats ;
- décrire le processus d'inscription automatique des certificats ;
- décrire les éléments à prendre en compte lors du choix d'une méthode d'inscription ;
- décrire les options de mise en œuvre de la révocation de certificats ;
- décrire les éléments à prendre en compte lors de la conception de la révocation de certificats ;
- déléguer une autorité de certification et la gestion des certificats.

Options d'inscription de certificat

Sous Windows Server 2012, vous pouvez utiliser plusieurs méthodes pour inscrire un ordinateur ou un utilisateur à un certificat. L'utilisation de ces méthodes varie en fonction des scénarios. Par exemple, vous utiliserez très probablement l'inscription automatique pour déployer en masse des certificats sur un grand nombre d'utilisateurs ou d'ordinateurs, alors que vous utiliserez très probablement l'inscription manuelle pour des certificats consacrés uniquement à des principaux de sécurité.



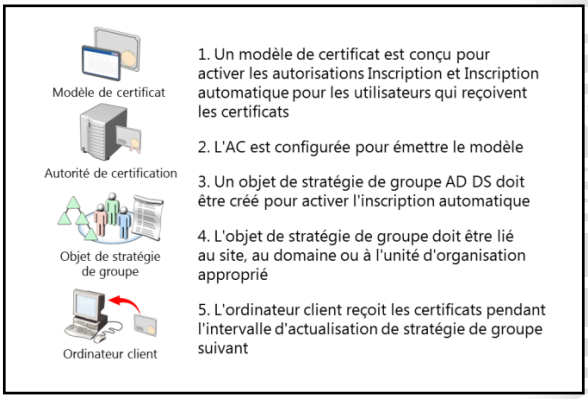
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La liste suivante décrit les différentes méthodes d'inscription, et quand les utiliser :

- Inscription automatique. L'administrateur définit les autorisations et la configuration d'un modèle de certificat. Ces définitions permettent au demandeur de demander, de récupérer et de remplacer des certificats automatiquement sans interaction de l'utilisateur final. Utilisez cette méthode pour les ordinateurs de domaine AD DS, et configurez le certificat pour l'inscription automatique au travers d'une stratégie de groupe.
- Inscription Web de l'autorité de certification. Vous pouvez activer une autorité de certification de site Web de sorte que les utilisateurs puissent obtenir des certificats. Pour utiliser l'inscription Web de l'AC, vous devez installer les services Internet (IIS) et le rôle de l'inscription Web sur l'autorité de certification AD CS. Pour obtenir un certificat, le demandeur ouvre une session sur le site Web, choisit le modèle de certificat approprié et envoie une demande. L'autorité de certification émet automatiquement le certificat si l'utilisateur a les autorisations d'inscription appropriées. Utilisez cette méthode pour délivrer des certificats quand vous ne pouvez pas utiliser l'inscription automatique, comme par exemple pour une demande de certificat avancée. Cependant, dans certains cas, l'inscription automatique peut être utilisée pour certains certificats, mais pas pour tous.
- Inscription manuelle. La clé privée et une demande de certificat sont générées sur un périphérique, tel qu'un service Web ou un ordinateur. La demande de certificat est ensuite transmise à l'autorité de certification pour générer le certificat demandé. Le certificat est ensuite rapatrié sur le périphérique en vue de son installation. Utilisez cette méthode lorsque le demandeur ne peut pas communiquer directement avec l'autorité de certification ou lorsque le périphérique ne prend pas en charge l'inscription automatique.
- Inscription au nom de (agent d'inscription). Un administrateur d'autorité de certification crée un compte d'agent d'inscription pour un utilisateur, qui peut alors s'inscrire à des certificats au nom d'autres utilisateurs. Par exemple, utilisez cette méthode si vous devez permettre à un gestionnaire de précharger les certificats de connexion de nouveaux employés sur des cartes à puce.

Processus d'inscription automatique des certificats



L'inscription automatique est l'une des méthodes les plus utilisées pour le déploiement de certificats dans un environnement Active Directory. Cette méthode automatise le déploiement de certificats aux utilisateurs et aux ordinateurs au sein d'une PKI. Vous pouvez utiliser l'inscription automatique dans des environnements qui répondent à des exigences spécifiques, comme l'utilisation des modèles de certificats et de la stratégie de groupe dans AD DS. Toutefois, il est important de noter que vous ne pouvez pas utiliser l'inscription automatique avec une autorité de certification autonome. Vous devez avoir une AC d'entreprise disponible pour utiliser l'inscription automatique.

L'inscription automatique permet de déployer automatiquement des certificats basés sur des clés publiques pour les utilisateurs et les ordinateurs d'une organisation. L'administrateur des services de certificats duplique un modèle de certificat puis configure les autorisations pour activer les autorisations Lecture, Inscription et Inscription automatique pour les utilisateurs qui recevront les certificats. Les stratégies de groupe basées sur les domaines, telles que des stratégies basées sur l'ordinateur et sur l'utilisateur, peuvent activer et gérer l'inscription automatique.

Par défaut, la stratégie de groupe est appliquée au redémarrage des ordinateurs, ou à la connexion des utilisateurs. De plus, par défaut, la stratégie de groupe est actualisée toutes les 90 minutes pour les membres du domaine. Ce paramètre de stratégie de groupe se nomme Client des services de certificats – Inscription automatique, et il se trouve sous les paramètres de sécurité du nœud Configuration ordinateur dans l'Éditeur de gestion des stratégies de groupe.

Un minuteur interne déclenche l'inscription automatique toutes les huit heures après sa dernière activation. Le modèle de certificat peut spécifier l'interaction utilisateur pour chaque demande. Pour une telle demande, une fenêtre contextuelle s'affiche approximativement 60 secondes après la connexion de l'utilisateur.

Vous pouvez distribuer de nombreux certificats sans que le client ne sache que l'inscription a lieu. Ces certificats comprennent la plupart des types de certificats publiés pour les ordinateurs et services, aussi bien que de nombreux certificats publiés pour les utilisateurs.

Pour configurer l'inscription automatique à des certificats dans un environnement de domaine, vous devez :

- être membre des administrateurs du domaine ou des administrateurs de l'entreprise, (ou équivalent), ce qui est le minimum requis pour réaliser cette procédure ;
- configurer un modèle de certificat avec les autorisations d'inscription automatique ;
- configurer une stratégie d'inscription automatique pour le domaine.

Qu'est-ce que l'itinérance des informations d'identification ?

L'itinérance des informations d'identification permet aux organisations de stocker des certificats et des clés privées AD DS séparément des informations d'état d'application ou de configuration.

L'itinérance des informations d'identification utilise des mécanismes existants de connexion et d'inscription automatique pour télécharger des certificats et des clés sur un ordinateur local lorsqu'un utilisateur se connecte et, au besoin, les supprimer lorsque l'utilisateur se déconnecte. En outre, l'itinérance des informations d'identification préserve l'intégrité de ces informations dans toutes les conditions, comme lors de la mise à jour des certificats ou lorsque les utilisateurs se connectent à plusieurs ordinateurs simultanément. Ceci évite le scénario dans lequel un utilisateur est inscrit automatiquement pour un certificat sur chaque nouvel ordinateur auquel il se connecte.

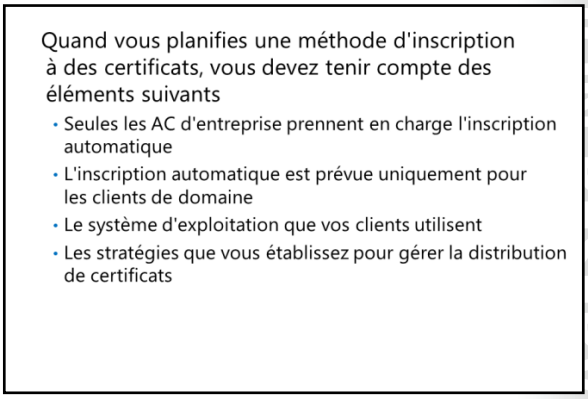
L'itinérance des informations d'identification est déclenchée quand une clé privée ou un certificat dans le magasin de certificats local de l'utilisateur change, lorsque l'utilisateur verrouille ou déverrouille l'ordinateur et chaque fois que la stratégie de groupe est actualisée.

Toute la communication liée au certificat entre les composants de l'ordinateur local et entre l'ordinateur local et AD DS est signée et chiffrée. Windows 7 et les systèmes d'exploitation Windows plus récents prennent en charge l'itinérance des informations d'identification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour le choix d'une méthode d'inscription

Au moment de choisir la méthode d'inscription appropriée pour vos clients, tenez compte des éléments suivants :



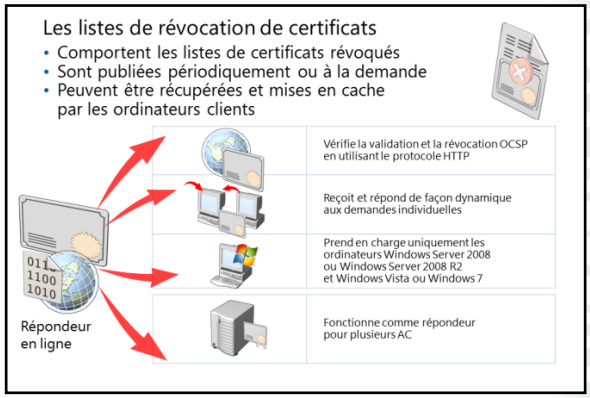
- seules les AC d'entreprise prennent en charge l'inscription automatique. Il n'est pas possible de configurer l'inscription automatique à l'aide d'une autorité de certification autonome, car cette fonctionnalité requiert AD DS ;
- seules les AC d'entreprise prennent en charge l'inscription de cartes à puces. Si vous comptez déployer des cartes à puce dans votre environnement, vous devez savoir que les AC autonomes ne prennent pas en charge l'émission des certificats de carte à puce ;
- dans Windows XP, Windows Server 2003 et toutes les versions plus récentes, l'inscription automatique est disponible pour les utilisateurs, les ordinateurs, et les cartes à puce ;
- l'inscription automatique est disponible uniquement pour les clients de domaine.

Pour sélectionner l'inscription des certificats et les processus de renouvellement appropriés à votre organisation, vous devez considérer plusieurs facteurs soigneusement, notamment :

- les utilisateurs, ordinateurs et services auxquels vous avez l'intention de fournir des services. Déterminez s'ils sont internes ou externes à l'organisation. Identifiez les systèmes d'exploitation sous lesquels ils s'exécutent, puis déterminez s'ils sont connectés à AD DS ;
- le système d'exploitation que vos clients utilisent. Les clients qui exécutent Windows Server 2003, Windows XP, Windows Vista, Windows 7 et Windows 8 peuvent utiliser l'assistant de demande de certificat, l'inscription automatique ou la station d'inscription de carte à puce. Windows 2000 Server prend en charge l'assistant de demande de certificat, mais ne prend pas en charge l'inscription automatique de carte à puce. L'inscription automatique et la station d'inscription de carte à puce requièrent également AD DS. La plupart des autres clients peuvent utiliser leurs navigateurs Web pour accéder aux services basés sur le Web d'inscription et de renouvellement ;
- les stratégies que vous établissez pour gérer la distribution de certificats. Cela comprend aussi bien les stratégies procédurales que vous établissez pour votre PKI et les paramètres de stratégie de groupe que vous utilisez pour implémenter ces stratégies ;
- le type d'autorité de certification qui émet les certificats. Par exemple, vous devez avoir une AC d'entreprise pour utiliser la station d'inscription de carte à puce. En outre, les AC autonomes prennent en charge uniquement l'inscription Web ou manuelle, tandis que les AC d'entreprise prennent en charge l'inscription Web, manuelle et automatique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options d'implémentation de la révocation de certificats



Pendant le processus de gestion de certificat, vous pouvez avoir besoin de révoquer des certificats pour plusieurs raisons. Par exemple, dans le cas où une clé se trouverait compromise ou quand un utilisateur quitterait l'organisation. Vous devez vous assurer que les clients réseau peuvent déterminer quels certificats sont révoqués avant d'accepter des demandes d'authentification.

Chaque fois que vous révoquez un certificat, vous devez en indiquer la raison. L'autorité de certification Windows Server 2012 vous permet de définir un code de raison à partir d'une liste de codes prédéfinis. Il est recommandé d'utiliser ces codes à chaque révocation de certificat, afin de garder trace de cette activité.

Lorsque vous révoquez un certificat, vous devez l'annoncer afin qu'aucun service n'utilise ou accepte ce certificat. Pour ce faire, utilisez les listes de révocation de certificats, ou configurez le service de répondeur en ligne basé sur OCSP.

Listes de révocation de certificats

Les listes de révocation de certificats répertorient les certificats révoqués. Les autorités de certification gèrent ces listes dans le cadre de la base de données de certificats. Les listes de révocation de certificats offrent aux clients un moyen de vérifier la révocation éventuelle d'un certificat avant de l'accepter et de procéder aux communications.

Les clients utilisent les points de distribution de liste de révocation de certificats comme références pour localiser les listes à jour. Chaque point de distribution de liste de révocation de certificats définit un point où les clients peuvent accéder à ces listes, comme sur un partage de fichiers, un emplacement LDAP (Lightweight Directory Access Protocol), ou un emplacement HTTP. Cependant, tous ces points peuvent ne pas être accessibles. D'autres options de configuration courantes consistent à définir si l'autorité de certification publie des listes de révocation de certificats standard ou delta vers un emplacement. Vous pouvez publier périodiquement des listes de révocation de certificats de base.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si l'autorité de certification émet et révoque de nombreux certificats, vous devrez peut-être publier une liste de révocation de certificats de base de grande taille. Une liste de révocation de certificats de base est une liste de révocation de certificats qui contient tous les certificats révoqués. Pour éviter de publier de grandes listes de révocation de certificats de base, vous pouvez publier des listes delta. Les listes de révocation des certificats delta sont des listes temporaires, plus petites et qui contiennent seulement les certificats qui ont été révoqués depuis la publication de la dernière liste de révocation des certificats de base. Cela permet aux clients de récupérer la liste de révocation des certificats delta puis d'établir rapidement la liste complète des certificats révoqués. Les listes de révocation de certificats delta se transfèrent plus rapidement que les listes de révocation de certificats de base. Vous pouvez également utiliser des listes de révocation des certificats delta pour publier des données de révocation de manière fréquente. Les ordinateurs Windows peuvent également utiliser les listes de révocation des certificats delta.

Vous pouvez configurer un paramètre de publication de liste de révocation des certificats ainsi qu'une période de publication. La période de publication de la liste de révocation des certificats définit à quel moment une autorité de certification doit publier automatiquement une liste de révocation des certificats actualisée. Lors de l'installation d'une autorité de certification, la période de publication par défaut est d'une semaine. Vous pouvez configurer la période de publication de la liste de révocation de certificats selon vos besoins.

Répondeur en ligne

Avec OCSP, un répondeur en ligne offre aux clients un moyen efficace de déterminer l'état de révocation d'un certificat. OCSP envoie des demandes d'état de certificat à l'aide du protocole HTTP.

Les clients accèdent aux listes de révocation de certificats pour déterminer l'état de révocation d'un certificat. Les listes de révocation de certificats peuvent être grandes, et les clients peuvent passer un certain temps à les examiner. Un répondeur en ligne peut examiner les listes de révocation de certificats pour le compte des clients et répondre uniquement au certificat demandé. Les répondeurs en ligne reçoivent toutes les données de révocation de certificats, au lieu des clients de confiance. Une partie de confiance envoie une demande d'état concernant un certificat individuel à un répondeur en ligne, lequel renvoie une réponse définitive, signée numériquement, qui indique l'état du seul certificat mentionné dans la demande. La quantité de données extraites par demande reste constante, quel que soit le nombre de certificats révoqués dans la base de données de certificats de l'autorité de certification.

Vous pouvez utiliser un répondeur en ligne unique pour fournir des informations d'état de la révocation concernant des certificats émis par une autorité de certification unique ou par plusieurs autorités de certification. Cependant, vous pouvez utiliser plusieurs répondeurs en ligne pour distribuer les informations de révocation d'autorité de certification.

Vous pouvez installer le répondeur en ligne sur n'importe quel ordinateur sous Windows Server 2008 Enterprise Edition, Windows Server 2008 Datacenter Edition ou Windows Server 2012. Une autorité de certification située sur un ordinateur sous Windows Server 2008, Windows Server 2003 ou une autorité de certification autre que Microsoft émet les données de révocation des certificats. Vous devez installer le répondeur en ligne et l'autorité de certification sur des ordinateurs distincts.

 **Remarque :** Vous devez configurer les paramètres des listes de révocation des certificats et d'OCSP sur l'autorité de certification avant d'émettre des certificats. L'emplacement de ces services est inclus dans chaque certificat délivré par l'autorité de certification. Les certificats émis avant la configuration d'OCSP ne contiendront pas les informations correctes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour assurer évolutivité et haute disponibilité, vous pouvez déployer le répondeur en ligne sur un ordinateur unique ou sur un cluster logiciel comportant plusieurs ordinateurs. Vous pouvez de plus configurer des réseaux de plusieurs ordinateurs reliés ensemble qui hébergent les répondeurs en ligne, puis traiter les demandes d'état de certificat. Vous pouvez surveiller et gérer chaque membre du réseau indépendamment. Pour configurer le répondeur en ligne, vous devez utiliser la console de gestion du répondeur en ligne.

Vous devez configurer les autorités de certification pour qu'elles incluent l'URL du répondeur en ligne dans l'extension AIA des certificats émis. Le client OCSP utilise cette URL pour valider l'état des certificats. Vous devez également publier le modèle de certificat de signature de réponse OCSP, de sorte que le répondeur en ligne puisse également inscrire ce certificat.

Éléments à prendre en compte lors de la conception de la révocation de certificats

Lors de la conception d'une infrastructure de révocation des certificats, vous devez tout d'abord déterminer si vous utiliserez des listes de révocation de certificats ou des répondeurs en ligne, ou les deux. Avant de choisir la technologie de révocation appropriée, vous devez connaître les différences entre les deux.

Lors de la conception de la révocation de certificats, suivez les instructions suivantes

- Évaluez les avantages potentiels de compléter les listes de révocation de certificats par l'utilisation des répondeurs en ligne
- Identifiez les emplacements où les répondeurs en ligne pourraient apporter un avantage
- Identifiez la configuration d'installation la plus adaptée à votre organisation
- Identifiez les emplacements de chaque répondeur en ligne et déterminez la manière de les gérer
- Testez le répondeur en ligne et la configuration de PKI

Les caractéristiques les plus importantes des listes de révocation des certificats sont les suivantes :

- une liste de révocation des certificats est un fichier créé et signé par une autorité de certification ;
- les listes de révocation des certificats contiennent les numéros de série des certificats émis par une autorité de certification puis révoqués par vous ;
- la liste de révocation des certificats contient également la raison de la révocation de chaque certificat et le moment où il a été révoqué ;
- par défaut, la liste de révocation des certificats est publiée dans le dossier systemroot\system32\CertSrv\CertEnroll\ ;
- si l'ordinateur est membre du domaine et a l'autorisation d'écrire dans AD DS, la liste de révocation de certificats également est publiée dans AD DS ;
- la période de publication d'une liste de révocation de certificats n'est pas identique à la période de validité d'une liste de révocation de certificats. Par défaut, la période de validité d'une liste de révocation de certificats dépasse sa période de publication de 10 % (jusqu'à un maximum de 12 heures) afin de permettre la réplication de répertoire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Parmi les difficultés potentielles de l'utilisation des listes de révocation de certificats, vous pouvez trouver :

- la taille potentiellement grande du fichier. Cela peut constituer une restriction à l'évolutivité ;
- la charge de stockage et de bande passante. Le volume élevé des fichiers sur le serveur ou sur les clients peut être un facteur défavorable ;
- la capacité de traitement de l'AC. La publication à haute fréquence peut affecter négativement les performances du serveur ;
- la latence. Il existe un délai entre le moment de révocation d'un certificat et la disponibilité de ces informations.

Les caractéristiques les plus importantes d'OCSP sont les suivantes :

- OCSP est un protocole HTTP.
- Il permet de soumettre une demande d'état de certificat à un répondeur OCSP ;
- la réponse de répondeur est signée numériquement, et indique l'état du certificat ;
- la quantité de données extraites par demande reste constante indépendamment du nombre de certificats révoqués dans l'AC.

La plupart des répondeurs OCSP reçoivent leurs données des listes de révocation des certificats publiées. Par conséquent, leur fonctionnement dépend de la fréquence de publication par l'autorité de certification. Certains répondeurs OCSP peuvent recevoir leurs données directement de la base de données d'état de l'autorité de certification, afin de fournir les états quasiment en temps réel.

AD DS déploie par défaut des listes de révocation des certificats sur chaque autorité de certification. Vous pouvez ajouter des points de distribution de liste de révocation des certificats supplémentaires, mais, si vous utilisez une AC d'entreprise, chaque autorité de certification publiera ses listes de révocation des certificats vers un dossier de partage qui y résides, et également vers AD DS.

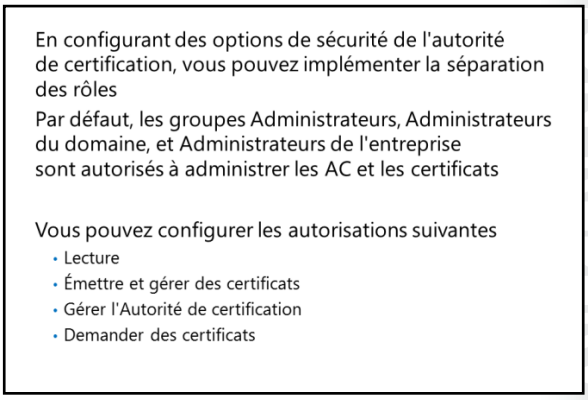
Cependant, si vous décidez de déployer un répondeur en ligne, procédez comme suit :

- évaluez les avantages potentiels que représente le fait de compléter les listes de révocation de certificats avec l'utilisation de répondeurs en ligne pour gérer le contrôle de la révocation dans votre organisation ;
- identifiez les emplacements où les répondeurs en ligne pourraient apporter un avantage ;
- identifiez la configuration de l'installation qui convient le mieux à votre organisation, en fonction du nombre d'autorités de certification et d'emplacements que vous prenez en charge, du volume des demandes de validation de certificats que vous anticipez et des conditions réseau entre vos autorités de certification et vos emplacements ;
- identifiez les emplacements de chaque répondeur en ligne et déterminez la manière de les gérer ;
- testez la configuration des répondeurs en ligne et de l'infrastructure à clé publique dans un environnement de test afin de valider la conception PKI et d'identifier les options de configuration de chaque répondeur en ligne et de la révocation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Délégation d'une autorité de certification et de la gestion des certificats

Vous pouvez déléguer la gestion de l'autorité de certification et des certificats en configurant des options de sécurité dans les propriétés de l'autorité de certification. Il est recommandé de configurer ces options de sorte à affecter le personnel à la gestion de l'autorité de certification et des certificats. Par défaut, les groupes de sécurité Administrateurs, Administrateurs du domaine et Administrateurs de l'entreprise peuvent gérer des autorités de certification et émettre et gérer des certificats, et le groupe Utilisateurs authentifiés peut demander des certificats à une autorité de certification.



Si vous souhaitez implémenter la séparation des rôles pour l'autorité de certification et la gestion de certificat, vous devez vous connecter à l'autorité de certification en tant que membre d'un groupe Administrateurs, Administrateurs du domaine ou Administrateurs de l'entreprise, et configurer les options de sécurité pour l'autorité de certification. En implémentant le la séparation des rôles, déléguez à d'autres utilisateurs qui ne sont pas membres des groupes d'administration les droits d'autorité de certification et de gestion de certificat.

Pour configurer les options de délégation pour l'autorité de certification et les certificats, cliquez avec le bouton droit sur votre serveur d'autorité de certification, puis sélectionnez **Propriétés**. Sous l'onglet de sécurité, vous pouvez configurer les autorisations suivantes :

- Lecture. Cette autorisation permet à un utilisateur ou à un groupe de sécurité de voir toutes les options d'autorité de certification, mais ne permet aucune modification des paramètres. Vous pouvez attribuer cette autorisation à une personne ou à un groupe qui effectue l'audit des paramètres d'autorité de certification.
- Émettre et gérer des certificats. Cette autorisation permet un utilisateur ou un groupe de sécurité d'approuver les inscriptions en suspens et les demandes de révocation. Ce rôle est parfois appelé gestionnaire de certificat ou agent d'administration d'autorité de certification. Un membre d'un groupe doté de cette autorisation ne peut modifier aucun paramètre d'autorité de certification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Gérer l'Autorité de certification. Cette autorisation permet à un utilisateur ou à un groupe de sécurité de configurer et maintenir l'autorité de certification. Cela comprend également la capacité d'attribuer tous les autres rôles de l'autorité de certification et de renouveler le certificat d'AC. Cependant, une personne dans ce rôle ne peut pas gérer les certificats. Ce rôle est généralement appelé administrateur de l'autorité de certification.
- Demander des certificats. Cette autorisation permet à des utilisateurs, des ordinateurs ou des groupes de demander des certificats à l'AC. Elle ne permet pas l'inscription de certificat, mais permet l'envoi de demandes de certificat à l'autorité de certification. Vous pouvez configurer les autorisations d'inscription dans un modèle de certificat spécifique. Il vous est recommandé que ce soit le groupe des utilisateurs authentifiés qui soit doté de cette autorisation, à moins que vous ne souhaitiez spécifier que seuls certains utilisateurs ou ordinateurs peuvent demander des certificats à une autorité de certification spécifique.

Il est recommandé que les comptes de groupe affectés aux rôles d'administrateur d'autorité de certification ou de gestionnaire de certificats ne soient pas membres du groupe Administrateurs local. En outre, vous devez attribuer des rôles d'autorité de certification seulement à des comptes de groupes, et pas à des comptes d'utilisateurs individuels. Cependant, l'appartenance au groupe Administrateurs local sur l'autorité de certification est requise pour renouveler un certificat d'AC. Les membres de ce groupe peuvent assumer une autorité d'administration sur tous les autres rôles d'autorité de certification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Planification et implémentation de l'archivage et de la récupération de clé

La récupération de clés ou de certificats est l'une des tâches de gestion les plus importantes au cours du cycle de vie des certificats. Vous utiliserez un agent d'archivage et de récupération de clés pour la récupération des données si vous perdez vos clés publiques et privées. Vous pouvez également utiliser des méthodes automatiques ou manuelles d'archivage et de récupération de clés pour pouvoir accéder aux données, dans l'éventualité où vous perdriez vos clés. Dans ce cours, vous découvrirez comment planifier et implémenter l'archivage et la récupération de clés dans AD CS sous Windows Server 2012.

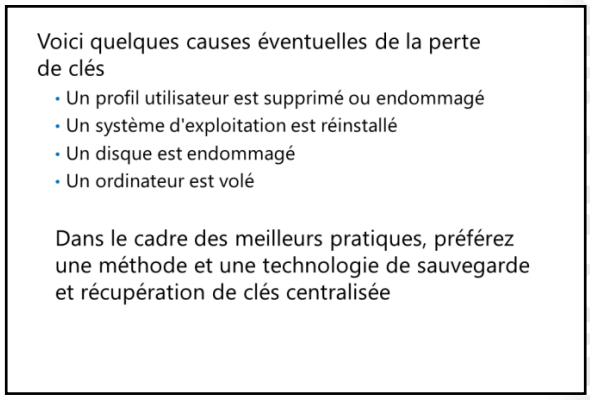
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire des scénarios de récupération de clé privée ;
- décrire les options de configuration de l'archivage des clés ;
- décrire les options de configuration de la récupération des clés ;
- décrire les éléments à prendre en compte pour l'archivage et la récupération des clés.

Scénarios de récupération de clé privée

Quand vous déployez une PKI dans votre environnement, il est capital d'avoir conscience de l'importance de la clé privée dans le certificat. Chaque certificat est associé à une paire de clés, qui se compose d'une clé publique et d'une clé privée. Bien que la clé publique soit accessible sans aucune limitation, la clé privée est accessible uniquement au propriétaire d'un certificat. La clé privée est particulièrement importante si vous utilisez des certificats pour le chiffrement. Lorsque vous chiffrez des données, vous avez besoin de votre clé privée pour les déchiffrer. Si vous perdez vos clé privée, il n'y a aucun autre moyen de déchiffrer les données. Pour cette raison, vous devez planifier et définir des stratégies de protection et de récupération de la clé privée.



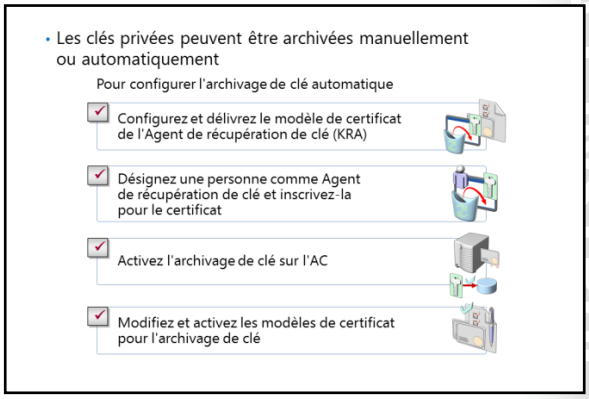
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Beaucoup de situations peuvent provoquer la perte des clés privées de certificat, et le besoin de les récupérer qui en découle. Par exemple, si son profil est endommagé ou supprimé, un utilisateur ne pourra pas accéder à sa clé privée. Si le disque dur tombe en panne et que le système d'exploitation est réinstallé sur un autre lecteur, la clé privée ne sera plus accessible. En outre, un utilisateur peut supprimer le certificat par inadvertance de son magasin personnel, ce qui supprime également la clé privée. De plus, si quelqu'un vole votre ordinateur ou que vous le perdez, vous perdez aussi l'accès à votre clé privée. Dans tous les cas, vous devez récupérer votre clé privée. Dans certains scénarios, vous pouvez exporter la clé privée avec le certificat, par propriétaire de certificat, et la copier dans l'emplacement de sauvegarde. Dans ce scénario, la récupération est très simple. L'utilisateur importe simplement le certificat. Cependant, certaines certificats ne permettent pas l'exportation de la clé privée. D'autres technologies sont donc nécessaires pour la sauvegarde et la restauration de clé.

Dans un environnement AD DS, il est recommandé d'implémenter une méthode centralisée pour l'archivage des clés privées, ainsi qu'une procédure bien définie pour la récupération de clé. Les rubriques suivantes détaillent différentes méthodes d'archivage et de récupération de clé.

Options de configuration de l'archivage des clés

La sauvegarde manuelle est la méthode la plus simple pour archiver les clés. Dans le cas des certificats pour lesquels l'exportation de clé privée est activée, chaque utilisateur peut exporter manuellement le certificat avec la clé privée (au format .pfx) et le copier vers un emplacement sûr, comme un périphérique USB ou un stockage en cloud. Lors de l'exportation d'une clé privée, il est recommandé de la protéger par un mot de passe. Cela empêche un utilisateur d'importer le certificat sans fournir le mot de passe au préalable.



Cependant, la sauvegarde manuelle des certificats est souvent peu fiable. Certains utilisateurs oublieront de sauvegarder leurs certificats, ou perdront tout simplement leur sauvegarde. En outre, certains modèles de certificats ne permettent pas aux utilisateurs d'exporter la clé privée. Cela signifie que vous devrez effectuer la sauvegarde de la clé d'une autre manière.

AD CS dans Windows Server 2012 vous permet de configurer des autorités de certification et des modèles de certificat pour l'archivage de clés privées. Avec cette option, vous pouvez sauvegarder les clés privées dans la base de données de l'autorité de certification, dans le cas des certificats émis selon des modèles de certificats spécifiques. Si la clé privée d'un utilisateur est perdue, vous pourrez la restaurer depuis la base de données de l'autorité de certification en suivant une procédure de récupération d'une clé archivée à partir de la base de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Avant que vous ne puissiez utiliser l'archivage de clé, vous devez effectuer plusieurs étapes de configuration. La fonctionnalité d'archivage de clé n'est pas activée par défaut, et vous devez configurer l'autorité de certification et les modèles de certificats pour l'archivage et la récupération de clé.

Les étapes suivantes détaillent le processus d'archivage de clé automatique :

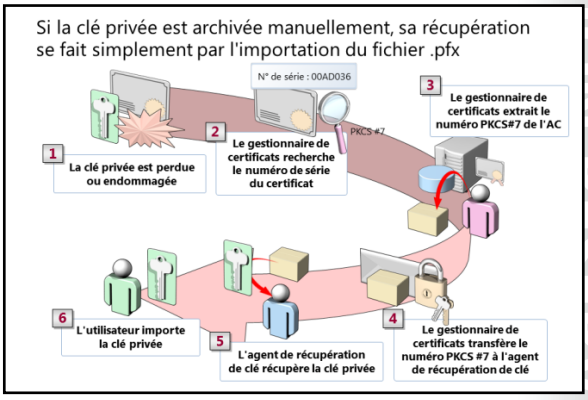
1. Configurer le modèle de certificat de l'Agent de récupération de clé. Seuls les administrateurs de l'entreprise ou les administrateurs du domaine sont autorisés à demander un certificat d'agent de récupération de clé. Si vous souhaitez inscrire un autre utilisateur avec un certificat d'agent de récupération de clé, vous devez le spécifier sur la liste DACL du modèle.
2. Configurer les gestionnaires de certificats. L'autorité de certification définit une personne comme gestionnaire de certificats, le cas échéant. Le gestionnaire de certificats conserve habituellement une clé privée pour les certificats KRA valides. Par défaut, l'administrateur de l'autorité de certification est un gestionnaire de certificats pour tous les utilisateurs, excepté dans les cas où il a une autre définition explicite. Cependant, comme meilleure pratique, vous devez si possible séparer ces deux rôles.
3. Activer l'agent de récupération de clé:
    a. Connectez-vous comme administrateur du serveur ou comme administrateur de l'autorité de certification, si la séparation des rôles est activée.
    b. Dans la console Autorité de certification, cliquez avec le bouton droit sur le nom de l'AC, puis cliquez sur **Propriétés**. Pour permettre l'archivage de clé, sous l'onglet **Agents de récupération**, cliquez sur **Archiver la clé**.
    c. Par défaut, l'autorité de certification utilise un KRA. Cependant, vous devez d'abord sélectionner le certificat KRA pour que l'autorité de certification commence l'archivage. Faites-le en cliquant sur **Ajouter**.
    d. Le système recherche les certificats KRA valides, puis affiche les certificats KRA disponibles. Ceux-ci sont en général publiés dans AD DS par une AC d'entreprise pendant l'inscription. Les certificats KRA sont enregistrés sous le conteneur de KRA de la branche Services de clé publique de la partition de configuration dans AD DS. Puisque une autorité de certification délivre plusieurs certificats KRA, chacun d'eux sera ajouté à l'attribut d'utilisateur à valeurs multiples de l'objet d'autorité de certification.
    e. Sélectionnez un certificat, puis cliquez sur **OK**. Assurez-vous que vous avez sélectionné le certificat souhaité.
    f. Après que vous avez ajouté un ou plusieurs certificats KRA, cliquez sur **OK**. Les certificats KRA sont seulement traités au démarrage du service.
4. Configurer des modèles de certificats :
    a. Dans la console MMC, cliquez avec le bouton droit sur les modèles de certificats pour lesquels vous souhaitez activer l'archivage de clé privée, puis cliquez sur **Propriétés**.
    b. Pour toujours appliquer l'archivage de clé pour l'AC, dans la boîte de dialogue **Propriétés**, sous l'onglet **Traitement de la demande**, activez la case à cocher **Archiver la clé privée de chiffrement du sujet**. Sélectionnez également l'option **Utiliser un algorithme symétrique avancé pour envoyer la clé à l'autorité de certification**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options de configuration de la récupération des clés

Si vous archivez une clé privée au moyen d'une méthode manuelle, la récupération de clé ne requiert aucune procédure spéciale. L'utilisateur doit localiser la sauvegarde de la clé privée, qui fait partie du certificat, puis l'importer vers son profil utilisateur.

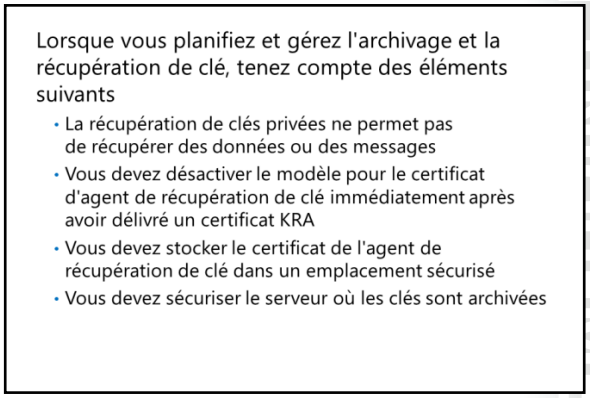


Cependant, si vous exécutez l'archivage de clé au moyen des options sur l'autorité de certification et les modèles de certificats, appliquez la procédure suivante pour récupérer la clé privée :

1. Rechercher les candidats à la récupération.
   Vous aurez besoin de deux informations pour exécuter la récupération de clé. D'abord, le gestionnaire de certificats ou l'administrateur de l'autorité de certification localise l'entrée correcte de certificat dans la base de données de l'autorité de certification. Ensuite, le gestionnaire de certificats ou l'administrateur de l'autorité de certification obtient le numéro de série de l'entrée correcte de certificat et du certificat KRA requis pour la récupération de clé.
2. Récupérer les normes de chiffrement des clés publiques (PKCS) #7 BLOB à partir de la base de données. Cela constitue la première moitié de l'étape de récupération de clé. Un gestionnaire de certificats ou un administrateur d'autorité de certification récupère l'objet BLOB correct dans la base de données de l'AC ; le certificat et la clé privée chiffrée à récupérer sont présents dans le BLOB PKCS #7. La clé privée est chiffrée de même que la clé publique d'un ou de plusieurs KRA.
3. Récupérer le matériel de la clé et l'enregistrer dans le PKCS #12 (.pfx). Ceci constitue la seconde moitié de l'étape de récupération de clé. Le détenteur de l'une des clés privées KRA déchiffre la clé privée qui doit être récupérée. En outre, le détenteur génère un fichier .pfx protégé par mot de passe qui contient le certificat et la clé privée.
4. Importer les clés récupérées. Le fichier .pfx protégé par mot de passe est délivré à l'utilisateur final. Cet utilisateur importe le fichier .pfx dans le magasin de certificats utilisateur local. De plus, le KRA ou un administrateur peut réaliser cette partie de la procédure au nom de l'utilisateur.

Gestion de l'archivage et de la récupération de clé

La récupération de clés ou de certificats est l'une des tâches de gestion les plus importantes que vous pourrez avoir à accomplir au cours du cycle de vie des certificats. Vous utiliserez un agent d'archivage et de récupération de clés pour la récupération des données lorsque vous perdrez vos clés publiques et privées (le cas échéant). Vous pouvez également utiliser des méthodes automatiques ou manuelles d'archivage et de récupération de clés pour que pouvoir accéder aux données si vous perdez vos clés.



Vous utilisez des agents d'archivage et de récupération de clé pour la récupération de données, et vous pouvez vous veiller à ce que les administrateurs d'autorités de certification pourront récupérer des clés privées simplement en les archivant. Les agents de récupération de clé peuvent récupérer le certificat d'origine ainsi que la clé privée et la clé publique ayant servi à crypter les données de la base de données de l'Autorité de certification.

La récupération de clé implique que la partie de clé privée d'une paire de clés publique/privée peut être archivée et récupérée. La récupération de clés privées ne permet pas de récupérer des données ou des messages. Elle permet simplement à un utilisateur de récupérer des clés perdues ou endommagées, et à un administrateur d'évaluer le rôle d'un utilisateur aux fins de l'accès aux données ou de la récupération de données. Dans de nombreuses applications, la récupération de données ne peut pas se produire sans effectuer en premier lieu la récupération de clé.

Une fois que vous avez configuré une autorité de certification pour émettre un certificat d'agent de récupération de clé, tout utilisateur doté des autorisations de Lecture et d'Inscription sur le modèle pour le certificat d'agent de récupération de clé peut s'inscrire et devenir un agent de récupération de clé. Par conséquent, les membres des groupes Administrateurs du domaine et Administrateurs de l'entreprise ont par défaut cette autorisation. Vérifiez que :

- seuls les utilisateurs de confiance peuvent s'inscrire pour ce certificat ;
- la clé de récupération de l'agent de récupération de clé est enregistrée dans un emplacement sécurisé ;
- le serveur où les clés sont archivées est sécurisé ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et implémentation d'une infrastructure AD CS

Scénario

La société A. Datum Corporation s'est développée, de même que ses besoins de sécurité. Le département sécurité est notamment très intéressé par l'activation d'un accès sécurisé aux sites Web critiques et par la fourniture d'une sécurité supplémentaire pour des fonctionnalités comme EFS, les cartes à puce et la fonctionnalité DirectAccess de Windows 7 et Windows 8. Pour faire face à ces exigences de sécurité, A. Datum a décidé d'implémenter une PKI au moyen du rôle AD CS sous Windows Server 2012.

Objectifs

- Planifier le déploiement AD CS.
- Déployer l'infrastructure d'AC.
- Configurer les modèles de certificat.
- Configurer le déploiement et la révocation de certificats.

Configuration de l'atelier pratique

Durée approximative : 100 minutes

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible.
Avant de commencer cet atelier pratique, vous devez effectuer les opérations suivantes :

Ordinateur(s) virtuel(s)	22414B-LON-DC1 22414B-LON-SVR1 22414B-LON-CA1 22414B-LON-CL1
Nom d'utilisateur	**Administrateur**
Mot de passe	**Pa$$w0rd**

1. Sur l'ordinateur hôte, sur **Accueil**, cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22414B-LON-DC1**, puis cliquez sur **Démarrer** dans le volet Actions.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1, 22414B-LON-CA1** et **22414B-LON-CL1**. Ne vous connectez pas avant d'y être invité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Planification du déploiement AD CS

Scénario

Le département sécurité d'A. Datum a spécifié les exigences suivantes pour son déploiement AD CS :

- l'autorité de certification racine d'A. Datum doit demeurer complètement isolée du réseau à tout moment ;
- en raison de l'importance qu'auront les certificats dans le déploiement planifié, il est essentiel que le rôle serveur de l'autorité de certification soit hautement disponible. Les utilisateurs à Londres et à Toronto doivent pouvoir obtenir des certificats et vérifier leur révocation même dans l'éventualité d'une défaillance d'un serveur unique ou d'un réseau WAN unique ;
- A. Datum a plusieurs applications qui nécessitent la validation de l'identité des utilisateurs au moyen de certificats. Seuls les employés internes utilisent les applications développées en interne. En outre, comme les responsables se servent de comptes à privilèges élevés, il est souhaitable de les doter de cartes à puce et de faire en sorte qu'ils n'utilisent que celles-ci lorsqu'ils se connectent ;
- A. Datum a plusieurs serveurs Web qui exécutent des applications pour les clients externes, et la communication entre le serveur et ces clients doit être sécurisée par SSL. Vous devez configurer les certificats du serveur Web de manière à ce qu'ils expirent trois ans après leur déploiement ;
- A. Datum envisage d'implémenter DirectAccess pour tous les utilisateurs équipés d'ordinateurs portables afin qu'ils puissent se connecter au réseau interne sans utiliser un réseau privé virtuel (VPN). Comme A. Datum a des ordinateurs clients Windows 7 et Windows 8, il convient de vérifier que chaque ordinateur Windows 7 qui utilise DirectAccess a un certificat d'ordinateur, mais il faut émettre ces certificats pour les ordinateurs portables. A. Datum souhaite que le certificat de chaque ordinateur soit valable six mois seulement ;
- l'état de révocation de tous les certificats doit être disponible à tous les ordinateurs connectés au réseau interne. L'état de révocation doit être accessible à Londres, à Toronto et à Sydney, tout en réduisant au minimum le trafic réseau nécessaire pour récupérer les informations de révocation des certificats ;
- dans le cadre du déploiement DirectAccess, les informations de révocation des certificats pour les certificats émis aux serveurs DirectAccess doivent être à la disposition des clients sur Internet. Tous les clients DirectAccess se connecteront au centre de données de Londres. L'emplacement accessible publiquement est le serveur Web à Londres avec l'URL publique www.adatum.com.

Les tâches principales de cet exercice sont les suivantes :

1. Lire la documentation fournie avec le produit.
2. Mettre à jour le document de proposition en fonction du plan d'action planifié.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lire le scénario de l'exercice d'atelier pratique

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

Sur la base du scénario de l'atelier pratique, proposez une solution pour la conception d'une d'infrastructure à clé publique (PKI). Appuyez-vous sur les questions suivantes pour élaborer votre conception PKI :

1. Comment allez-vous satisfaire l'exigence stipulant que l'autorité de certification racine d'A. Datum doit demeurer complètement isolée du réseau à tout moment ?
2. Comment allez-vous rendre le rôle d'autorité de certification hautement disponible ?
3. Comment allez-vous réaliser l'authentification des responsables et des applications basée sur les certificats ?
4. Comment allez-vous configurer un certificat de serveur Web pour répondre aux exigences spécifiées ?
5. Comment allez-vous satisfaire l'exigence stipulant que seuls les ordinateurs portables doivent recevoir des certificats pour le déploiement de DirectAccess ?
6. Comment allez-vous satisfaire l'exigence de contrôle de révocation entre les sites ?
7. Comment allez-vous satisfaire l'exigence de contrôle de révocation basé sur Internet ?

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez votre solution avec celle exposée dans le corrigé de l'atelier pratique. Présentez des solutions alternatives et discutez-en avec la classe.

Résultats : À la fin de cet exercice, les stagiaires auront planifié un déploiement d'AD CS.

Exercice 2 : Déploiement de l'infrastructure d'autorité de certification

Scénario

La première étape du déploiement AD CS chez A. Datum consiste à déployer l'infrastructure d'AC. Pour vous conformer à l'impératif de sécurité indiquant que l'autorité de certification racine ne pas être accessible à partir du réseau, vous devez d'abord déployer une AC racine autonome. Vous déploierez ensuite une autorité de certification racine d'entreprise secondaire, qui sera utilisée pour délivrer les certificats.

Les tâches principales de cet exercice sont les suivantes :

1. Installer le rôle AD CS sur un serveur autonome.
2. Configurer la révocation de certificats pour l'AC secondaire.
3. Publier le certificat de l'autorité de certification racine dans le domaine.
4. Configurer le rôle AD CS sur l'AC d'entreprise secondaire.
5. Configurer les certificats pour activer l'approbation secondaire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Installer le rôle AD CS sur un serveur autonome

1. Connectez-vous à LON-CA1 en tant qu'**Administrateur** à l'aide du mot de passe **Pa$$w0rd**.
2. Utilisez l'Assistant Ajout de rôles et de fonctionnalités pour installer le rôle **Services de certificats Active Directory**.
3. Une fois l'installation réussie, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.
4. Configurez le rôle AD CS comme une AC racine autonome. Appelez-la **AdatumRootCA**.
5. Définissez la longueur de clé sur **4096**, puis acceptez toutes autres valeurs en tant que valeurs par défaut.

▶ Tâche 2 : Configurer la révocation de certificats pour l'AC secondaire

1. Dans LON-CA1, ouvrez la console Autorité de certification.
2. Ouvrez la fenêtre Propriétés pour **AdatumRootCA**.
3. Configurez les nouveaux emplacements pour CDP : **http://lon-svr1.adatum.com/CertData/<NomAutoritéCertification><SuffixeNomListeRévocationCertificats><ListeRévocationCertificatsDeltaAutorisée>.crl**.
4. Activez les options **Inclure dans l'extension CDP des certificats émis** et **Inclure dans les listes de révocation des certificats afin de pouvoir rechercher les listes de révocation des certificats delta**.
5. Configurez les nouveaux emplacements AIA comme **http://lon-svr1.adatum.com/CertData/<Nom du serveur DNS>_<NomAutoritéCertification><NomCertificat>.crt**.
6. Activez la case à cocher **Inclure dans l'extension AIA des certificats émis**.
7. Publiez la liste de révocation de certificats sur LON-CA1.
8. Exportez le certificat d'AC racine puis copiez le fichier .cer dans **\\lon-svr1\C$**.
9. Copiez le contenu du dossier **C:\Windows\System32\CertSrv\CertEnroll** dans le dossier **\\lon-svr1\C$**.

▶ Tâche 3 : Publier le certificat de l'autorité de certification racine dans le domaine

1. Sur LON-DC1, dans le Gestionnaire de serveur, ouvrez la console Gestion de stratégie de groupe.
2. Modifiez la stratégie **Default Domain Policy**.
3. Publiez le fichier **RootCA.cer** depuis **\\lon-svr1\C$** dans le magasin d'autorités de certification racines de confiance qui se trouve dans Configuration ordinateur**Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique**.

▶ Tâche 4 : Configurer le rôle AD CS sur l'AC d'entreprise secondaire

1. Connectez-vous à LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd.**
2. Installez le rôle **Services de certificats Active Directory** sur LON-SVR1. Incluez les services de rôle **Autorité de certification** et **Inscription de l'autorité de certification via le Web**.
3. Après l'installation, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.
4. Sélectionnez les services de rôle **Autorité de certification** et **Inscription de l'autorité de certification via le Web**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Configurez LON-SVR1 comme une **Autorité de certification d'entreprise**.
6. Configurez le type d'autorité de certification comme une **Autorité de certification secondaire**.
7. Pour le nom de l'autorité de certification, tapez **Adatum-IssuingCA**.
8. Enregistrez le fichier de demande sur le disque local.

▶ Tâche 5 : Configurer les certificats pour activer l'approbation secondaire

1. Sur LON-SVR1, installez le certificat RootCA.cer dans le magasin Autorité de certification racine de confiance.
2. Accédez au disque local (C:) et copiez les fichiers **AdatumRootCA.crl** et **LON-CA1 _AdatumRootCA.crt** sur **C:\inetpub\wwwroot\CertData**.
3. Copiez le fichier de demande **LON-SVR1.Adatum.com_Adatum- IssuingCA.req** sur **\\LON-CA1\C$**.
4. Basculez vers LON-CA1.
5. Depuis la console Autorité de certification sur LON-CA1, envoyez une nouvelle demande de certificat à l'aide du fichier .req que vous avez copié à l'étape 3.
6. Émettez le certificat et exportez-le au format p7b avec la chaîne complète. Enregistrez le fichier sous **\\lon-svr1\C$\SubCA.p7b.**
7. Basculez vers LON-SVR1.
8. Installez le certificat SubCA sur LON-SVR1 à l'aide de la console Autorité de certification.
9. Démarrez le service.

Résultats : À la fin de cet exercice, les stagiaires auront déployé une infrastructure d'AC.

Exercice 3 : Implémentation de modèles de certificats

Scénario

L'étape suivant du déploiement de l'infrastructure AD CS, après le déploiement des autorités de certification, consiste à configurer les modèles de certificats requis pour satisfaire aux exigences de sécurité.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer des unités d'organisation et des groupes pour les ordinateurs portables.
2. Configurer le modèle de certificat du serveur Web.
3. Configurer le modèle de certificat DirectAccess.
4. Configurer le certificat pour les cartes à puces.
5. Émettre les modèles de certificats.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Configurer des unités d'organisation et des groupes pour les ordinateurs portables

1. Sur LON-DC1, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Dans la console Utilisateurs et ordinateurs Active Directory, créez une nouvelle unité d'organisation nommée **Portables**.
3. Dans l'unité d'organisation **Portables**, créez un groupe de sécurité nommé **Portables**.
4. Déplacez l'ordinateur **LON-CL1** vers l'unité d'organisation **Portables**.
5. Ajoutez **LON-CL1** au groupe de sécurité **Portables**.

▶ Tâche 2 : Configurer le modèle de certificat du serveur Web

1. Sur LON-SVR1, depuis la console certsrv - [Autorité de certification (Local)], ouvrez la Console des modèles de certificat.
2. Dupliquez le modèle **Serveur Web**.
3. Créez un nouveau modèle et nommez-le **Serveur Web d'Adatum**.
4. Configurez la validité à **3 années**.
5. Configurez la clé privée comme exportable.
6. Fermez la Console des modèles de certificat.

▶ Tâche 3 : Configurer le modèle de certificat DirectAccess

1. Sur LON-SVR1, depuis la console certsrv - [Autorité de certification (Local)], ouvrez la Console des modèles de certificat.
2. Dupliquez le modèle **Ordinateur**.
3. Créez un nouveau modèle et nommez-le **Clients DirectAccess**.
4. Configurez la validité à **6 mois**.
5. Configurez les options de sécurité du modèle de sorte que seuls les membres du groupe Portables puissent lire, s'inscrire et s'inscrire automatiquement à ce certificat.

▶ Tâche 4 : Configurer le certificat pour les cartes à puces

1. Dans la Console des modèles de certificat, dupliquez le modèle de certificat **Utilisateur**.
2. Nommez le nouveau modèle **Utilisateur de carte à puce Adatum**.
3. Sous l'onglet **Nom du sujet**, désactivez les cases à cocher **Inclure le nom de compte de messagerie dans le nom du sujet** et **Nom de messagerie électronique**.
4. Ajoutez **Ouverture de session par carte à puce** aux stratégies d'application du nouveau modèle de certificat.
5. Configurez ce nouveau modèle pour remplacer le modèle **Utilisateur**.
6. Permettez aux utilisateurs authentifiés la **Lecture**, de s'**inscrire** et l'**Inscription automatique** pour ce certificat.
7. Fermez la Console des modèles de certificat.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Émettre les modèles de certificats

- Configurez LON-SVR1 pour qu'il délivre des certificats basés sur les modèles **Utilisateur de carte à puce Adatum**, **Clients DirectAccess** et **Serveur Web d'Adatum**.

Résultats : À la fin de cet exercice, les stagiaires auront configuré des modèles de certificats répondant aux exigences de sécurité.

Exercice 4 : Implémentation de la révocation et de la distribution de certificats

Scénario

Une fois les modèles de certificats déployés, vous devez implémenter le plan de publication et de révocation de certificats. Puisque les exigences de sécurité comprennent plusieurs options différentes pour le déploiement des certificats, vous devez configurer l'inscription et l'inscription automatique des certificats via le Web.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer le contrôle de la révocation de certificats.
2. Configurer la vérification de la révocation des certificats pour les clients DirectAccess.
3. Configurer l'inscription automatique pour les certificats DirectAccess.
4. Valider les méthodes d'inscription des certificats.

▶ Tâche 1 : Configurer le contrôle de la révocation de certificats

1. Sur LON-SVR1, utilisez le Gestionnaire de serveur pour ajouter un rôle de répondeur en ligne au rôle AD CS existant.
2. Lorsque le message affiche que l'installation a réussi, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**. Configurez le répondeur en ligne.
3. Sur **LON-SVR1**, ouvrez la console certsrv - [Autorité de certification (Local)].
4. Configurez le nouvel emplacement de la distribution AIA sur Adatum-IssuingCA : **http://lon-svr1/ocsp**.
5. Dans **Adatum-IssuingCA**, publiez le modèle de certificat de signature de réponse OCSP, et autorisez les Utilisateurs authentifiés à s'inscrire.
6. Ouvrez la console ocsp - [Répondeur en ligne : LON-SVR1.Adatum.com] sur LON-SVR1.
7. Ajoutez la configuration de révocation pour **Adatum-IssuingCA**.
8. Inscrivez un certificat de signature de réponse OCSP.
9. Assurez-vous que la configuration de la révocation indique qu'elle est En cours de calcul.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer la vérification de la révocation des certificats pour les clients DirectAccess

1. Sur LON-SVR1, ouvrez la console certsrv - [Autorité de certification (Local)].
2. Ouvrez la fenêtre Propriétés pour **Adatum-IssuingCA**.
3. Configurez de nouveaux emplacements pour CDP : **http://www.adatum.com/CertData/<NomAutoritéCertification><SuffixeNomListeRévocationCertificats><ListeRévocationCertificatsDeltaAutorisée>.crl**.
4. Activez les options **Inclure dans l'extension CDP des certificats émis** et **Inclure dans les listes de révocation des certificats afin de pouvoir rechercher les listes de révocation des certificats delta**.
5. Configurez les nouveaux emplacements AIA comme **http://www.adatum.com/CertData/<Nom du serveur DNS>_<NomAutoritéCertification><NomCertificat>.crt**.
6. Activez la case à cocher **Inclure dans l'extension AIA des certificats émis**.
7. Redémarrez les services AD CS lorsque vous y êtes invité.

▶ Tâche 3 : Configurer l'inscription automatique pour les certificats DirectAccess

1. Sur LON-DC1, ouvrez Gestion des stratégies de groupe.
2. Créez un nouvel objet de stratégie de groupe nommé **DirectAccessCert**, et liez-le à l'unité d'organisation Portables.
3. Ouvrez l'objet de stratégie de groupe **DirectAccessCert** dans l'**Éditeur de gestion des stratégies de groupe**.
4. Accédez au nœud **Configuration ordinateur**, développez successivement **Stratégies**, **Paramètres Windows** et **Paramètres de sécurité**, cliquez sur **Stratégies de clé publique**, puis double-cliquez sur **Client des services de certificats – Inscription automatique**
5. Activez les options de configuration suivantes :
   - Renouveler les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués
   - Mettre à jour les certificats qui utilisent les modèles de certificats
6. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 4 : Valider les méthodes d'inscription des certificats

1. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd.**
2. Sur LON-CL1, actualisez la stratégie de groupe en ouvrant une invite de commandes et en tapant **gpupdate /force**.
3. Créez une nouvelle console MMC et ajoutez-y le composant logiciel enfichable **Certificats**. Gérez les certificats pour le compte d'ordinateur.
4. Vérifiez que le certificat de DirectAccess est publié sur LON-CL1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-CA1** et **22414B-LON-CL1**.

Résultats : Après avoir terminé cet exercice, les stagiaires auront configuré la révocation et la révocation des certificats.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

- Lorsque vous déployez une infrastructure d'autorité de certification, déployez une autorité de certification racine autonome (non jointe à un domaine) et une autorité de certification d'entreprise secondaire (l'autorité de certification émettrice). Une fois que l'autorité de certification secondaire d'entreprise a reçu un certificat de l'autorité de certification racine RootCA, mettez-la hors connexion.
- Délivrez un certificat pour l'autorité de certification racine RootCA valide pour une longue période, comme 15 ou 20 ans.
- Utilisez l'inscription automatique pour les certificats qui sont très utilisés.

Utilisez un agent d'inscription restreint chaque fois que cela est possible.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
L'autorité de certification n'est pas configurée pour inclure des emplacements de points de distribution de liste de révocation de certificats dans les extensions des certificats émis. Les clients peuvent ne pas pouvoir localiser une liste de révocation pour contrôler l'état de révocation d'un certificat, et la validation du certificat peut alors échouer.	
L'autorité de certification a été installée comme AC d'entreprise, mais les paramètres de stratégie de groupe pour l'inscription automatique d'utilisateur n'ont pas été activés. Une AC d'entreprise peut utiliser l'inscription automatique pour simplifier l'émission et le renouvellement de certificats. Si l'inscription automatique n'est pas activée, l'émission et le renouvellement de certificats peuvent ne pas se produire comme prévu.	

Questions de contrôle des acquis

Question : Pouvez-vous récapituler les conditions d'utilisation de l'inscription automatique des certificats ?

Outils

- Console Autorité de certification
- Console Modèles de certificat
- Console Certificats
- Certutil.exe

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 12

Planification et implémentation d'une infrastructure de fédération d'identités

Table des matières :

Vue d'ensemble du module **12-1**

Leçon 1 : Planification et implémentation d'une infrastructure de serveur AD FS **12-2**

Leçon 2 : Planification et implémentation des fournisseurs de revendications et parties de confiance AD FS **12-17**

Leçon 3 : Planification et implémentation des revendications et des règles de revendication AD FS **12-24**

Atelier pratique : Planification et implémentation d'une infrastructure AD FS **12-32**

Contrôle des acquis et éléments à retenir **12-42**

Vue d'ensemble du module

La principale solution de Microsoft pour la fédération d'identités sont les services AD FS (Active Directory® Federation Services), qui fournissent des services d'authentification et d'autorisation basés sur le Web pour les utilisateurs internes et externes. Windows Server® 2003 R2 a introduit les services AD FS, qui était inclus en tant que rôle serveur dans Windows Server® 2008 et Windows Server 2008 R2. Windows Server 2012 inclut également les services AD FS en tant que rôle serveur, avec d'autres améliorations et modifications.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- planifier et implémenter une infrastructure de fédération d'identités, y compris l'accès à l'application prenant en charge les revendications ;
- planifier et implémenter une infrastructure de serveur AD FS ;
- planifier et configurer les fournisseurs de revendications et parties de confiance AD FS ;
- concevoir et déployer les revendications et les règles de revendication AD FS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1

Planification et implémentation d'une infrastructure de serveur AD FS

Avant de planifier et d'implémenter votre infrastructure de serveur AD FS, vous devez comprendre les concepts et les composants d'AD FS, notamment l'intégration d'AD FS avec les services en ligne.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les services AD FS ;
- définir les divers composants AD FS ;
- définir les scénarios de déploiement AD FS de base ;
- décrire les options d'implémentation du rôle serveur AD FS ;
- décrire les éléments des certificats de l'infrastructure à clé publique (PKI) à prendre en compte pour les services AD FS ;
- décrire les éléments à prendre en compte pour choisir un scénario de déploiement AD FS ;
- définir les options de haute disponibilité pour les services AD FS ;
- décrire l'intégration des services AD FS avec les services en ligne.

Que sont les services AD FS ?

Les services AD FS sont une solution d'accès aux identités qui fournit une expérience d'authentification unique basée sur un navigateur à une ou plusieurs applications Web, et fonctionne à la fois pour les utilisateurs internes et externes. Une entreprise peut utiliser les services AD FS pour fournir aux utilisateurs internes l'authentification unique aux applications Web, mais vous les déployez généralement pour permettre aux utilisateurs d'une autre organisation d'accéder aux applications Web de votre réseau en utilisant les informations d'identification et les attributs définis dans l'organisation de l'utilisateur en tant que *domaine d'accueil* de l'utilisateur dans la terminologie de fédération d'identités. Le domaine d'accueil de l'utilisateur peut être une forêt AD DS (Active Directory Domain Services) ou d'autres fournisseurs de connexion qui utilisent des normes telles que Liberty Alliance, les fournisseurs SAML (Security Assertion Markup Language) 2.0 et WS-*, ou qui utilisent le service de compte de Microsoft, Windows Live® ID.

Les services AD FS peuvent être résumés comme suit
- Sont une solution d'accès aux identités
- Fournissent l'authentification unique basée sur un navigateur
  - Peuvent également interagir avec d'autres fournisseurs SAML 2.0, WS-*
- Les améliorations AD FS dans Windows Server 2012 sont
  - Intégration du service de contrôle d'accès (DAC)
  - Expérience d'installation améliorée
  - Applets de commande Windows PowerShell améliorées

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Cela permet à chaque organisation de gérer ses propres identités, y compris les informations d'identification et les attributs. Les services AD FS présentent ensuite ces identités en tant que revendications à vos applications Web pour qu'elles puissent prendre une décision d'accès. Ainsi, il n'est pas nécessaire de conserver des comptes dans votre organisation pour les utilisateurs externes. Lorsque vous implémentez la fédération, chaque organisation peut projeter ses identités à d'autres organisations, tout en continuant à gérer ces identités et à accepter les identités présentées par d'autres organisations.

La version 1.0 d'AD FS a été introduite avec Windows Server 2003 R2, tandis que Windows Server 2008 et Windows Server 2008 R2 ont inclus AD FS 1.1 en tant que rôle serveur. AD FS 2.0 a été commercialisé séparément sur le Web en mai 2010 en tant que package pouvant être installé séparément. Windows Server 2012 inclut désormais la dernière version (AD FS 2.1) en tant que rôle serveur, avec des fonctionnalités ajoutées depuis la version 2.0, notamment :

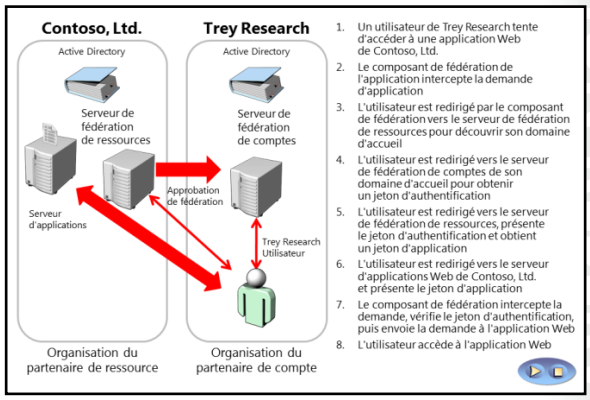
- Intégration avec le contrôle d'accès dynamique (DAC). Les services AD FS peuvent utiliser les revendications d'utilisateur et de périphérique AD DS présentées dans les tickets du protocole d'authentification Kerberos (version 5), quand un utilisateur ou un périphérique est authentifié dans le domaine. Cela permet d'utiliser ces revendications dans les scénarios DAC. Ces revendications AD DS sont intégrées à l'authentification intégrée de Windows®, et les services AD FS peuvent y accéder. Auparavant, les services AD FS ne pouvaient pas accéder aux revendications de périphérique, qui sont des attributs de compte d'ordinateur.
- Installation améliorée à l'aide du Gestionnaire de serveur. L'installation du rôle serveur AD FS est améliorée dans Windows Server 2012. L'Assistant de configuration AD FS du Gestionnaire de serveur effectue des contrôles de validation avant d'installer le rôle serveur AD FS, notamment l'énumération et l'installation des rôles serveur dépendants, tels que le serveur Web ou les services Internet (IIS), et des composants de serveur Web, tels qu'ASP.NET.
- Applets de commande Windows PowerShell® supplémentaires. Les services AD FS dans Windows Server 2012 comprennent de nouvelles applets de commande qui n'étaient pas disponibles dans la version 2.0. Celles-ci fournissent une fonctionnalité d'installation pour le rôle serveur AD FS, et permettent la configuration des serveurs de fédération et des serveurs proxy de fédération.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des services AD FS

Vue d'ensemble des composants AD FS

Le tableau suivant résume les divers composants et la terminologie AD FS dans Windows Server 2012 :



Composant AD FS	Définition
Organisation du partenaire de compte	Il s'agit de l'organisation dont les comptes auront accès aux applications Web fédérées.
Serveur de fédération de comptes	Il s'agit du serveur de fédération dans l'organisation du partenaire de compte, qui est membre de la forêt AD DS de l'organisation. Le serveur de fédération de comptes authentifie les utilisateurs et délivre un jeton de sécurité qui contient les revendications représentant les attributs de l'utilisateur que les services AD FS fournissent ensuite au serveur de fédération de la ressource. Les attributs peuvent comprendre les appartenances au groupe, l'adresse de messagerie et le nom de famille de l'utilisateur.
Base de données de configuration AD FS	Base de données Microsoft® SQL Server® ou fonctionnalité Base de données interne Windows dans Windows Server 2012. Cette base de données représente un service de fédération unique, et il peut y avoir plusieurs serveurs de fédération dans une implémentation du serveur de fédération. Toutefois, il ne peut y avoir qu'une base de données de configuration pour une implémentation du service de fédération. **Remarque :** Si vous utilisez SQL Server, vous pouvez créer la base de données de configuration AD FS à l'aide de l'outil de ligne de commande Fsconfig.exe. Pour une implémentation qui utilise la base de données interne Windows, vous pouvez utiliser l'Assistant Configuration du serveur de fédération AD FS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Composant AD FS	Définition
Agents Web AD FS	Dans Windows Server 2012, les agents Web AD FS 1.1 sont un service de rôle AD FS que vous pouvez installer. En général, vous ne les installez pas dans une nouvelle implémentation d'AD FS. Ils doivent plutôt être utilisés sur des serveurs d'applications qui interagiront avec une implémentation AD FS 1.x existante.
Magasin d'attributs	Dans AD FS, un magasin d'attributs est un répertoire ou une base de données que vous pouvez utiliser pour stocker les comptes d'utilisateurs et leurs attributs associés. Le service de fédération crée des revendications en fonction de ces attributs en les récupérant du magasin d'attributs. En outre, une application ou un service hébergé dans une partie de confiance prend des décisions d'autorisation sur ces revendications.
Revendication	Une revendication est une déclaration d'un fournisseur de revendications concernant un client (généralement un utilisateur). Un exemple de revendication est le privilège, les appartenances au groupe, le nom, l'adresse de messagerie, le nom d'utilisateur principal (UPN) ou le nom de compte du Gestionnaire de comptes de sécurité de l'utilisateur. Lorsqu'un client est authentifié, le fournisseur de revendications lui délivre un jeton contenant les revendications définies pour ce fournisseur de revendications. Le client envoie ce jeton à la partie de confiance. En cas d'acceptation, le client délivre un jeton pour l'application fédérée et le présente à l'application.
Fournisseur de revendications	Il s'agit de l'organisation du partenaire de fédération contenant les utilisateurs qui ont accès aux applications configurées pour la fédération.
Approbation de fournisseur de revendications	Une approbation de fournisseur de revendications est une relation, généralement créée dans une organisation du partenaire de ressource, qui représente l'organisation dont les comptes auront accès aux applications Web hébergées par l'organisation du partenaire de ressource.
Règles de revendication	Une règle de revendication est une instruction de logique métier qui génère une revendication sortante en appliquant des conditions (si *X*, alors *y*) à une revendication entrante. Un exemple de règle de revendication consiste à prendre une revendication UPN entrante et à la transformer en une revendication d'adresse de messagerie sortante.
Métadonnées de fédération	Il s'agit du format de données standardisé pour communiquer entre une partie de confiance et un fournisseur de revendications. Elles permettent la configuration appropriée des approbations de fédération (approbations de partie de confiance et approbations de fournisseur de revendications). SAML 2.0 définit le format, avec une extension supplémentaire dans WS-Federation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Composant AD FS	Définition
Serveur de fédération	Si vous installez le service de rôle Service de fédération, l'ordinateur Windows Server 2012 fera office de serveur de fédération en délivrant des jetons et en servant dans le cadre d'un service de fédération. Les serveurs de fédération fournissent plusieurs fonctions. Ils peuvent notamment : • Héberger un service d'émission de jetons de sécurité (STS) et délivrer des jetons en fonction des informations d'identification fournies par l'utilisateur ou l'application. • Accepter et relayer les demandes d'authentification des clients de navigateur ou des applications Web. • Implémenter les mappages de revendication, qui fournissent des liens entre le répertoire et les attributs que les revendications présentées définissent.
Serveur proxy de fédération	Si vous installez le service de rôle Proxy du service de fédération, l'ordinateur Windows Server 2012 fera office de serveur proxy de fédération. Vous déployez généralement le serveur proxy de fédération dans un réseau de périmètre (également appelé zone démilitarisée ou sous-réseau filtré), qui sert d'intermédiaire entre un navigateur ou un autre client Internet et le service de fédération.
Serveur de fédération principal	Si vous déployez la base de données de configuration AD FS à l'aide de la base de données interne Windows, le premier serveur de fédération du service de fédération héberge la seule copie en lecture/écriture de la base de données de configuration AD FS. Par conséquent, il est désigné sous le nom de serveur de fédération principal, et tous les serveurs de fédération suivants ajoutés au service de fédération contiennent des copies en lecture seule de la base de données de configuration. Si le serveur de fédération principal n'est pas disponible, aucune modification ne peut être apportée au service de fédération.  **Remarque :** Si vous utilisez SQL Server pour la base de données de configuration AD FS, le concept de serveur de fédération principal ne s'applique pas. Tous les serveurs de fédération peuvent avoir un accès en lecture et en écriture à une base de données de configuration AD FS hébergée par SQL Server.
Partie de confiance	Il s'agit de l'organisation du partenaire de ressource qui reçoit et traite les revendications et délivre des jetons pour accéder aux applications Web selon ces revendications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Composant AD FS	Définition
Approbation de partie de confiance	Elle est créée pour établir une relation avec un autre service de fédération ou une autre application qui utilise les revendications provenant du service de fédération dans lequel l'approbation de partie de confiance est créée.
Serveur de fédération de ressources	Il génère des jetons contenant des applications Web auxquelles peuvent accéder les utilisateurs de l'organisation du partenaire de compte.
Organisation du partenaire de ressource	Il s'agit de l'organisation du partenaire de ressource qui héberge le serveur de fédération de ressources. Elle héberge généralement les applications Web fédérées. Dans le service de fédération, cette organisation est un partenaire dans une approbation de partie de confiance.

Flux opérationnel AD FS

Cet exemple montre comment tous les composants AD FS fonctionnent ensemble, en supposant que Trey Research ait déployé les services AD FS et que Contoso, Ltd. héberge les services AD FS et une application fédérée auxquels les utilisateurs de Trey Research peuvent accéder. Par exemple, les employés de Trey Research peuvent accéder à une application hébergée par Contoso, Ltd. pour consulter et gérer leurs prestations de santé. Par conséquent, une relation d'approbation de fédération est établie entre les deux organisations. Le flux opérationnel des services AD FS lorsque un utilisateur de Trey Research accède à l'application Web de Contoso, Ltd. se présenterait comme suit :

1. Un utilisateur de Trey Research tente d'accéder à une application Web de Contoso, Ltd.
2. Le composant de fédération de l'application intercepte la demande d'application.
3. Les services AD FS redirigent l'utilisateur vers le serveur de fédération de ressources de Contoso, Ltd. pour découvrir le domaine d'accueil de l'utilisateur.
4. Le composant de fédération redirige l'utilisateur vers le serveur de fédération de comptes (Trey Research) de son domaine d'accueil pour obtenir un jeton d'authentification.
5. Les services AD FS redirigent l'utilisateur vers le serveur de fédération de comptes de Contoso, Ltd., présentent le jeton d'authentification et obtiennent un jeton d'application.
6. Le composant de fédération redirige l'utilisateur vers le serveur d'applications Web de Contoso, Ltd. et présente le jeton d'application.
7. Le composant de fédération intercepte la demande, vérifie le jeton d'authentification, puis envoie la demande à l'application Web.
8. L'utilisateur accède à l'application Web.

Remarque : Les serveurs de fédération des organisations du partenaire de compte et de ressource ne communiquent pas directement. La seule communication est basée sur le Web, entre l'ordinateur client, les serveurs de fédération du partenaire de compte, les organisations du partenaire de ressource, et entre l'ordinateur client et l'application Web. En outre, elle peut être établie entre l'ordinateur client et le serveur proxy de fédération, si vous déployez cette fonctionnalité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des scénarios de déploiement AD FS

Conceptions AD FS

La majorité des implémentations AD FS présentera l'une des deux conceptions suivantes :

Les deux principales conceptions AD FS sont
- Authentification unique (SSO) Web
  - Héberge tous les utilisateurs au sein de l'organisation, notamment les services AD DS ou le protocole LDAP
  - Ne dispose pas d'approbations de fédération
- Authentification unique Web fédérée
  - Prend en charge les scénarios B2B
  - Configure les approbations de fédération
  - Modélise les approbations sur les contrats ou les partenariats d'entreprise

- Authentification unique (SSO) Web. Cette conception AD FS a pour principal objectif de fournir aux utilisateurs l'authentification unique Web à plusieurs applications ou services prenant en charge les revendications. Tous les utilisateurs sont externes dans cette conception, et tous les comptes d'utilisateurs sont hébergés par votre organisation, par exemple, dans les services AD DS ou le protocole LDAP (Lightweight Directory Access Protocol). Aucune approbation de fédération n'est disponible. Par conséquent, votre organisation agit en tant que partenaire de compte et partenaire de ressource. Il s'agit d'un scénario classique permettant de fournir des applications ou services prenant en charge les revendications et sécurisés par AD FS à différents clients ou consommateurs sur Internet. En général, une organisation héberge les applications ou les services dans un réseau de périmètre, ainsi qu'un magasin de comptes distinct pour les informations d'identification de l'utilisateur.
- Authentification unique Web fédérée. Le scénario Authentification unique Web fédérée est le scénario le plus classique pour la collaboration interentreprises (B2B). Il est utile si deux organisations créent une relation d'approbation de fédération pour permettre aux utilisateurs de l'organisation du partenaire de compte d'accéder aux applications Web, que les services AD FS aident à sécuriser dans l'organisation du partenaire de ressource. Après avoir configuré les approbations de fédération appropriées, l'une ou l'autre des organisations peut être un partenaire de ressource, un partenaire de compte, ou les deux simultanément. Une relation d'approbation de fédération est modélisée sur un contrat au niveau de l'entreprise ou un partenariat entre deux organisations qui requiert une fédération de bout en bout.

Le scénario présenté dans la rubrique précédente, Flux opérationnel AD FS, est un exemple d'authentification unique Web fédérée. Dans l'exemple illustré dans cette diapositive, un serveur de fédération de comptes de Contoso, Ltd. et un serveur de fédération de ressources de Trey Research achemine les demandes d'authentification des utilisateurs de Contoso, Ltd. vers les applications Web de Trey Research.

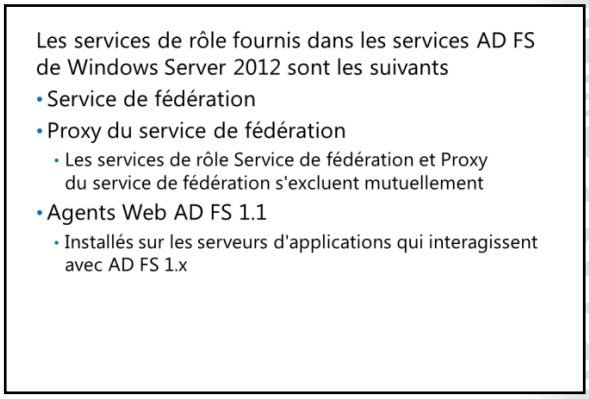
Par souci de simplicité, l'exemple omet le rôle Proxy du service de fédération, mais ce scénario peut inclure un serveur proxy de fédération dans un réseau de périmètre du partenaire de compte, du partenaire de ressource, ou des deux. Vous pouvez utiliser ces serveurs de proxy pour éviter de vous connecter directement depuis Internet aux serveurs de fédération, qui sont membres du domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options d'implémentation du rôle serveur AD FS

Quand vous ajoutez le rôle serveur AD FS dans Windows Server 2012, vous pouvez choisir parmi les services de rôle suivants :

- Service de fédération
- Proxy du service de fédération
- Agents Web AD FS 1.1



Remarque : Un ordinateur Windows Server 2012 où le rôle serveur AD FS est installé est communément appelé un serveur de fédération ou un serveur proxy de fédération, selon le service de rôle installé. Vous pouvez installer un serveur de fédération à l'aide des services de rôle Service de fédération ou Proxy du service de fédération, mais pas les deux. Ces deux services de rôle s'excluent mutuellement.

Implémentation d'un serveur de fédération

Installez le service de fédération sur un serveur connecté aux services AD DS. Vous devez ensuite utiliser le même niveau de sécurité sur ce serveur que sur vos contrôleurs de domaine AD DS, par exemple dans un centre de données ou un autre emplacement physique sécurisé. Cela signifie que vous devez installer le service de rôle Service de fédération sur le réseau d'entreprise et derrière le pare-feu, afin d'éviter toute exposition sur Internet.

Un serveur sur lequel vous appliquez le service de rôle Service de fédération peut être un serveur de fédération de comptes, un serveur de fédération de ressources, ou les deux. Que le serveur fonctionne en tant que compte ou que le serveur de fédération de ressources dépende de la configuration d'AD FS sur ce serveur, vous pouvez modifier la configuration à tout moment.

Implémentation d'un serveur proxy de fédération

Vous installez généralement le service de rôle Proxy du service de fédération dans un réseau de périmètre, sur un serveur installé dans un groupe de travail ou connecté à une forêt sur le réseau de périmètre. Vous ne pouvez pas installer le proxy du service de fédération sur le même ordinateur que le service de fédération.

Le proxy du service de fédération doit accepter les connexions des clients Internet pour le compte du service de fédération, extraire ces connexions et fournir une couche de protection supplémentaire.

Remarque : Le proxy du service de fédération est facultatif, mais nous vous recommandons fortement de l'utiliser si les ordinateurs clients se connectent à partir d'Internet. Vous pouvez également utiliser une solution de publication d'applications, telle que Microsoft Forefront® Unified Access Gateway.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Agents Web AD FS 1.1

Dans Windows Server 2012, les agents Web AD FS 1.1 sont fournis pour être utilisés sur les serveurs d'applications qui interagiront avec une implémentation AD FS 1.x existante. Par conséquent, vous ne les installez pas généralement dans une nouvelle implémentation d'AD FS. En outre, les services AD FS ne prennent pas en charge les applications basées sur des jetons Windows dans Windows Server 2012. Les applications et services peuvent tirer parti de Windows Identity Foundation (WIF) et convertir les jetons SAML en jetons Windows à utiliser dans l'application à l'aide du service d'émission de jetons Revendications vers Windows dans WIF.

Configuration des certificats

Certificats du serveur de fédération

Les certificats utilisés dans les services AD FS sont
- Certificat SSL
- Certificat de communication de service
- Certificat de signature de jetons
- Certificat de déchiffrement de jetons
- Certificat du serveur proxy de fédération
- Certificat d'authentification de serveur

Les serveurs de fédération nécessitent six certificats, mais vous pouvez utiliser le même certificat pour plusieurs fonctions. Les six certificats sont les suivants :

- Certificat SSL (Secure Sockets Layer). Les services AD FS utilisent un certificat SSL standard lié au site Web par défaut dans IIS pour sécuriser la communication entre l'ordinateur client et les divers composants AD FS, notamment le serveur de fédération de comptes, le serveur de fédération de ressources et le serveur Web qui héberge l'application fédérée. Dans une implémentation du service de fédération qui comprend plusieurs serveurs de fédération dans une batterie de fédération, vous utilisez le même certificat SSL pour tous les serveurs de fédération.



Remarque : Tous les clients AD FS doivent approuver le certificat SSL, nous vous recommandons donc d'utiliser un certificat émis par une autorité de certification tierce (publique) de confiance.

- Certificat de communication de service. Ce certificat sécurise les messages WCF (Windows Communication Foundation) entre les serveurs de fédération. Dans une configuration par défaut, le certificat SSL est utilisé en tant que certificat de communication de service, mais vous pouvez modifier ce paramètre à l'aide de la console de gestion AD FS.
- Certificat de signature de jetons. Les services AD FS utilisent les certificats de signature de jetons pour signer et vérifier les jetons d'authentification et d'application utilisés par les services AD FS. Un certificat auto-signé est créé et utilisé par défaut, mais vous pouvez le remplacer par un certificat émis par une autorité de certification dans la console de gestion AD FS.
- Certificat de déchiffrement de jetons. Ce certificat SSL standard déchiffre les jetons entrants reçus d'un serveur de fédération partenaire. Pour permettre au serveur de fédération partenaire de chiffrer ces jetons, les métadonnées de fédération publient la clé publique du certificat de déchiffrement de jetons.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

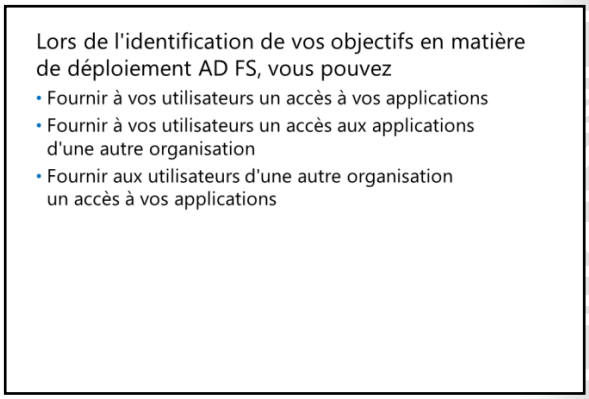
- Certificats du serveur proxy de fédération. Un serveur proxy de fédération ne requiert qu'un seul certificat.
- Certificat d'authentification de serveur. Vous pouvez utiliser ce certificat SSL standard sur le serveur proxy de fédération pour sécuriser les communications entre les clients Internet et le serveur proxy de fédération. Tous les clients doivent l'approuver, il est donc généralement émis par une autorité de certification publique (tierce). Pour réduire le nombre de certificats à gérer, vous pouvez utiliser le même certificat que celui que vous utilisez pour le serveur de fédération.

Pour un serveur proxy de fédération, le certificat d'authentification de serveur doit être lié au site Web par défaut dans IIS pour que l'Assistant Configuration du serveur proxy de fédération puisse s'exécuter avec succès.

Remarque : Si un certificat que vous utilisez a des listes de révocation de certificats (CRL, Certificate Revocation Lists), le serveur doté du certificat configuré doit pouvoir contacter le serveur qui distribue les listes de révocation de certificats.

Sélection d'un scénario de déploiement AD FS

Identification de vos objectifs en matière de déploiement AD FS



La réussite de votre projet AD FS dépend de l'identification correcte de vos objectifs de déploiement. Une fois que vous avez déterminé les objectifs pertinents pour votre projet, vous pouvez ensuite les mapper sur une conception AD FS spécifique. Vous pouvez classer par catégorie la plupart des déploiements AD FS selon un ou plusieurs des trois objectifs de déploiement suivants :

- Fournir aux utilisateurs AD DS un accès à vos applications et services prenant en charge les revendications. Cet objectif décrit le scénario dans lequel vous fournissez un accès par authentification unique pour vos propres employés à vos ressources hébergées. Dans ce scénario, votre organisation agit en tant qu'organisation du partenaire de compte et effectue les opérations suivantes.
- Elle utilise les services AD FS pour sécuriser les applications ou services hébergés par un réseau de périmètre, permettant ainsi aux employés connectés aux services AD DS sur le réseau d'entreprise d'utiliser l'authentification unique pour accéder à ces applications ou services.
- Elle utilise les services AD FS pour permettre aux employés à distance authentifiés par les services AD DS de bénéficier d'un accès fédéré aux applications ou services internes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Cet objectif de déploiement est mappé sur une conception Authentification unique Web.

- Fournir aux utilisateurs AD DS un accès aux applications et services d'autres organisations. Cet objectif décrit le scénario dans lequel vos propres employés bénéficient d'un accès fédéré aux ressources (applications ou services) hébergées par une autre organisation. Par exemple :
- Les employés authentifiés dans AD DS sur le réseau d'entreprise peuvent utiliser l'authentification unique pour accéder aux services ou applications sécurisés par AD FS qui résident dans une autre organisation.
- Les employés à distance dotés d'informations d'identification AD DS peuvent accéder aux services ou applications sécurisés par AD FS qui résident dans une autre organisation en obtenant un jeton AD FS de votre service de fédération.

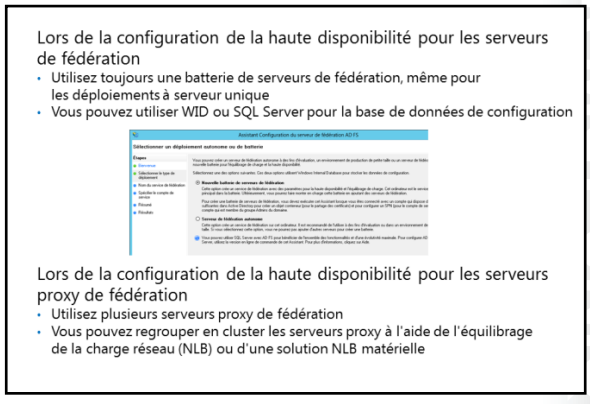
Cet objectif de déploiement est mappé sur une conception Authentification unique Web fédérée dans le partenaire de ressource et, éventuellement, dans le partenaire de compte.

- Fournir aux utilisateurs d'une autre organisation un accès à vos applications et services sécurisés par AD FS. Cet objectif décrit le scénario dans lequel vous hébergez des applications ou services prenant en charge les revendications dans votre organisation, et vous devez fournir un accès fédéré aux utilisateurs d'une autre organisation. Cet objectif a deux variantes légèrement différentes.
- Cet objectif vous permet de fournir un accès fédéré à vos propres utilisateurs et aux utilisateurs des organisations avec lesquelles vous avez établi une approbation de fédération. Cet objectif de déploiement est mappé sur la conception Authentification unique Web fédérée.
- Cet objectif vous permet de fournir un accès fédéré aux utilisateurs qui ne disposent d'aucune association avec votre organisation ou une organisation de confiance, telle que des clients individuels. Un magasin d'attributs sur votre réseau de périmètre héberge ces comptes clients, et le client utilise ces informations d'identification pour accéder à plusieurs applications ou services prenant en charge les revendications, que le réseau de périmètre héberge également.
- Cet objectif de déploiement peut être mappé sur une conception Authentification unique Web fédérée ou une conception Authentification unique Web.

Configuration de la haute disponibilité pour les services AD FS

La haute disponibilité des services AD FS est fournie pour les serveurs de fédération et les serveurs proxy de fédération via l'utilisation de batteries de serveurs de fédération et de batteries de serveurs proxy de fédération, respectivement.

Lorsque vous exécutez pour la première fois l'Assistant Configuration du serveur de fédération AD FS et sélectionnez l'option **Créer un nouveau service de fédération**, vous pouvez choisir de **Créer une nouvelle batterie de serveurs de fédération** ou un **Serveur de fédération autonome**.



Nous recommandons l'option Serveur de fédération autonome uniquement à des fins d'évaluation. Sinon, la nouvelle option Batterie de serveurs de fédération créera une batterie composée d'un serveur, à laquelle vous pouvez ajouter ultérieurement d'autres serveurs de fédération pour la haute disponibilité, l'équilibrage de charge et l'évolutivité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Haute disponibilité pour les serveurs de fédération

La batterie de serveurs de fédération est la principale unité de haute disponibilité pour les serveurs de fédération. Une batterie de serveurs de fédération contient plusieurs serveurs, vous pouvez donc distribuer les connexions des clients AD FS sur tous les serveurs de fédération de la batterie à l'aide de l'équilibrage de la charge réseau (NLB, Network Load Balancing) ou d'une solution NLB matérielle.

Création d'une batterie de serveurs de fédération à l'aide de la base de données interne Windows

Lorsque vous utilisez l'Assistant Configuration du serveur de fédération AD FS pour créer une batterie de serveurs de fédération, il utilise la base de données interne Windows (WID) comme base de données de configuration AD FS. Le premier serveur de la batterie est le *serveur de fédération principal* qui conserve la seule copie accessible en écriture de la base de données de configuration. Cependant, quand vous ajoutez d'autres serveurs à la batterie de serveurs de fédération, la base de données de configuration est répliquée à partir du serveur de fédération principal. Tous les réplicas sont mis à jour lorsque des modifications sont apportées à la batterie de serveurs de fédération.

Remarque : La base de données WID fournit la haute disponibilité pour le service de fédération, mais a un point de défaillance unique pour apporter des modifications de configuration au service de fédération. De plus :

- Une batterie de serveurs de fédération WID est limitée à cinq serveurs de fédération.
- Une batterie de serveurs de fédération WID ne prend pas en charge la résolution d'artefact ou la détection de relecture de jeton. Le protocole SAML définit ces deux fonctionnalités.

Création d'une batterie de serveurs de fédération à l'aide de SQL Server

Lorsque vous utilisez SQL Server comme base de données de configuration AD FS pour créer la batterie de serveurs de fédération, les données de configuration ne sont pas répliquées sur chaque serveur de fédération de la batterie. À la place, tous les serveurs de fédération lisent et écrivent des données dans la même base de données SQL, ce qui permet à tous les serveurs de fédération de la batterie d'apporter des modifications de configuration. Les fonctionnalités de SQL Server fournissent la haute disponibilité pour la base de données de configuration, notamment la mise en miroir de la base de données, le clustering avec basculement et la réplication.

Lorsque vous utilisez SQL Server pour stocker la base de données de configuration AD FS, tous les serveurs de fédération de la batterie peuvent lire et écrire dans la base de données de configuration. C'est la raison pour laquelle le terme « serveur de fédération principal » ne s'applique pas lorsque vous utilisez SQL Server.

Remarque : Lorsque vous utilisez SQL Server pour la batterie de serveurs de fédération, la limitation de cinq serveurs de fédération par batterie ne s'applique pas. En outre, il prend en charge la résolution d'artefact et la détection de relecture de jeton.

Si vous utilisez SQL Server et sa base de données de configuration, vous ne pouvez pas utiliser l'Assistant Configuration du serveur de fédération AD FS. À la place, vous devez utiliser l'outil en ligne de commande **fsconfig**. Si l'administrateur AD FS ne dispose pas des privilèges nécessaires pour créer des bases de données SQL, vous pouvez utiliser l'outil **fsconfig** pour générer les scripts SQL appropriés pour créer la base de données

Haute disponibilité pour les serveurs proxy de fédération

Comme pour les serveurs de fédération, l'unité de haute disponibilité pour les serveurs proxy de fédération est la batterie de serveurs proxy de fédération. Lorsque l'Assistant Configuration du serveur proxy de fédération AD FS est exécuté sur un serveur sur lequel vous avez installé le service de rôle Serveur proxy de fédération, vous configurez le serveur pour protéger le service de fédération spécifié. La configuration de plusieurs serveurs proxy de fédération pour protéger le même service de fédération crée une batterie de serveurs proxy de fédération.

Pour que les serveurs proxy de fédération puissent fournir des services en tant que batterie, vous devez les mettre en cluster en utilisant une adresse IP unique et le nom de domaine complet (FQDN) du système DNS (Domain Name System) qui utilise la base de données NLB ou une solution NLB matérielle. En outre, tous les serveurs proxy de fédération de la batterie doivent utiliser le même certificat d'authentification de serveur.

Intégration des services AD FS avec les services en ligne

En plus de fournir l'authentification unique pour vos utilisateurs internes et de permettre l'accès aux applications ou services prenant en charge les revendications pour les utilisateurs d'autres organisations, vous pouvez également utiliser les services AD FS pour fournir la fonctionnalité d'authentification unique pour vos utilisateurs internes aux services en ligne tels que Microsoft Office 365™ et Windows Azure™.

Les services AD FS peuvent être utilisés avec les services en ligne, notamment

- Office 365
  - Les services AD FS fournissent l'authentification unique à Office 365 pour les utilisateurs AD DS
- Windows Azure
  - Les services AD FS fournissent l'authentification unique à Windows Azure pour les utilisateurs AD DS
  - Le service de contrôle d'accès (ACS) de Windows Azure est le point d'intégration à Windows Azure pour les services AD FS

Services AD FS et Office 365

Le déploiement et la configuration des services AD FS pour une utilisation avec Office 365 sont identiques au scénario Authentification unique Web fédérée décrit précédemment, à une différence près : le partenaire de ressource est Office 365 et vous configurez l'approbation de partie de confiance avec Office 365 au lieu d'une autre organisation. Une autre différence est que lors de la fédération avec Office 365, nous vous recommandons fortement de déployer les proxys du service de fédération et de déployer à la fois la batterie de serveurs de fédération et la batterie de serveurs proxy de fédération avec au moins deux membres pour chaque batterie pour fournir la haute disponibilité pour l'authentification à Office 365.

Avant de configurer les services AD FS pour une utilisation avec Office 365, vous devez installer l'Assistant de connexion Microsoft Online Services et le Module Microsoft Online Services pour PowerShell sur chaque serveur de fédération de la batterie de serveurs de fédération. Une fois que vous avez installé le Module Microsoft Online Services, vous pouvez créer l'approbation de partie de confiance avec Office 365 à l'aide de l'applet de commande Windows PowerShell Convert-MsolDomainToFederated. Si vous disposez d'un domaine principal, tel que treyresearch.com, mais que votre déploiement AD DS utilise des sous-domaines, tels que corp.treyresearch.com, le domaine principal est enregistré dans Office 365 en premier. Vous ajoutez ensuite les sous-domaines, si nécessaire, à l'aide de l'applet de commande New-MsolFederatedDomain.

Remarque : Lorsque vous convertissez votre domaine principal en domaine à authentification unique, tous les utilisateurs sont fédérés. Il n'est pas actuellement possible d'effectuer un déploiement intermédiaire de l'authentification unique vers Office 365.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des services AD FS et d'Office 365 pour l'authentification unique

En supposant que votre infrastructure AD FS est installée et fonctionne correctement, vous pouvez configurer l'authentification unique pour Office 365 comme suit :

1. Sur le premier serveur de fédération, installez la version 64 bits de l'**Assistant de connexion Microsoft Online Services**.
2. À l'aide de l'Assistant Ajout de rôles et de fonctionnalités du Gestionnaire de serveur de Windows Server 2012, installez les **Fonctionnalités .NET Framework 3.5**.
3. Installez la version 64 bits du **Module Microsoft Online Services pour PowerShell**.
4. Répétez les étapes 1 à 3 sur tous les autres serveurs de fédération de la batterie.
5. Sur le premier serveur de fédération, exécutez l'applet de commande Windows PowerShell Connect-MsolService pour vous connecter à votre client Office 365. Entrez vos informations d'identification d'administration dans la boîte de dialogue **Entrer les informations d'identification**.
6. Convertissez votre domaine principal pour utiliser la fédération à l'aide de l'applet de commande Convert-MSOLDomainToFederated –DomainName <*nom_domaine*>.
7. Ajoutez les sous-domaines requis utilisés pour le nom d'utilisateur principal à l'aide de l'applet de commande New-MSOLFederatedDomain –DomainName <*nom_sous-domaine*>.

Outre la configuration de votre approbation de partie de confiance avec Office 365, chaque fois que votre certificat de signature de jetons est renouvelé ou qu'un nouveau certificat est généré, vous devez en informer Office 365 en mettant à jour les métadonnées de fédération d'Office 365. Vous pouvez utiliser l'Outil d'installation de l'automatisation des mises à jour de métadonnées de fédération de Microsoft Office 365 à cet effet.

1. Connectez-vous au serveur de fédération principal à l'aide d'un compte doté de privilèges d'administration AD FS (en général, un compte de service).
2. Téléchargez l'**Outil d'installation de l'automatisation des mises à jour de métadonnées de fédération Microsoft Office 365** sur le serveur de fédération principal.
3. Démarrez Windows PowerShell en tant qu'administrateur, puis basculez vers le répertoire contenant l'**Outil d'installation de l'automatisation des mises à jour de métadonnées de fédération Microsoft Office 365**.
4. À l'invite Windows PowerShell, tapez .\O365-Fed-MetaData-Update-Task-Installation.ps1, puis appuyez sur Entrée.
5. Entrez le domaine fédéré à l'invite Windows PowerShell.
6. Entrez vos nom d'utilisateur et mot de passe d'administration Office 365 lorsque vous y êtes invité.
7. Entrez le mot de passe du compte d'administration AD FS lorsque vous y êtes invité.

À ce stade, le script O365-Fed-MetaData-Update-Task-Installation.ps1 créera une tâche planifiée qui s'exécutera une fois par jour pour mettre à jour les métadonnées de fédération d'Office 365. Cette tâche s'exécutera dans le contexte de sécurité du compte utilisé pour créer la tâche, comme indiqué dans les étapes précédentes.

 **Remarque :** Le script O365-Fed-MetaData-Update-Task-Installation.ps1 doit être exécuté pour chaque domaine fédéré de votre organisation.

Services AD FS et Windows Azure

Dans Windows Azure, vous pouvez configurer les services AD FS en tant que fournisseur d'identité à l'aide du service de contrôle d'accès (ACS) de Windows Azure. Cela permet à vos utilisateurs de s'authentifier auprès des applications ASP.NET hébergées dans Windows Azure à l'aide de leurs informations d'identification AD DS.

Service de contrôle d'accès (ACS) de Windows Azure

Le service de contrôle d'accès permet d'intégrer à Windows Azure des fournisseurs d'identité basés sur des normes tels que les services AD FS, les comptes Microsoft (autrefois Windows Live ID) et Facebook. Cela facilite l'accès des utilisateurs authentifiés et autorisés aux applications et services hébergés par Windows Azure. Vous pouvez configurer les services AD FS en tant que fournisseur d'identité dans le service ACS en procédant comme suit :

1. Ajoutez les services AD FS en tant que fournisseur d'identité dans le portail de gestion ACS.
2. Ajoutez éventuellement un certificat de déchiffrement de jetons au service ACS. Cela déchiffre les jetons reçus des services AD FS dans le portail de gestion ACS.
3. Ajoutez une partie de confiance pour votre espace de noms ACS dans les services AD FS.
4. Ajoutez des règles de revendication pour l'espace de noms ACS dans les services AD FS.

 **Documentation supplémentaire :** Pour plus d'informations sur l'intégration des services AD FS avec le service de contrôle d'accès (ACS) de Windows Azure, rendez-vous sur http://go.microsoft.com/fwlink/?LinkID=285332.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2

Planification et implémentation des fournisseurs de revendications et parties de confiance AD FS

Une fois que vous avez déployé votre infrastructure AD FS, vous pouvez la configurer pour qu'elle fonctionne avec différents magasins d'identités en implémentant des fournisseurs de revendications, et avec des applications ou services en implémentant des parties de confiance.

Objectifs de la leçon

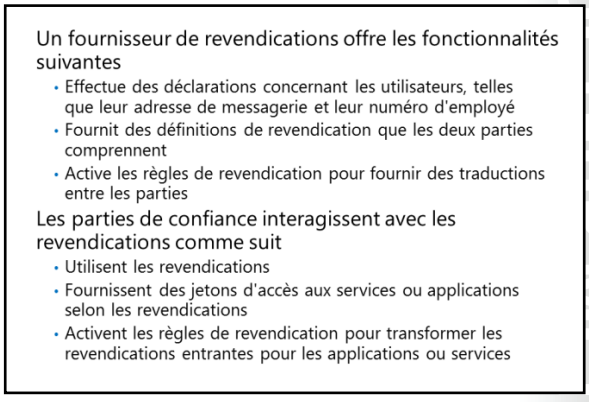
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- fournir une vue d'ensemble des rôles de fournisseur de revendications et de partie de confiance ;
- fournir une vue d'ensemble des applications compatibles AD FS ;
- décrire les options d'implémentation des magasins d'attributs ;
- fournir une vue d'ensemble des composants d'approbation de fournisseur de revendications ;
- fournir une vue d'ensemble des composants d'approbation de partie de confiance ;
- décrire les éléments à prendre en compte pour configurer les approbations de fournisseur de revendications ;
- décrire les éléments à prendre en compte pour configurer les approbations de partie de confiance.

Vue d'ensemble des rôles de fournisseur de revendications et de partie de confiance

Fournisseurs de revendications

Un fournisseur de revendications est l'organisation du partenaire de compte qui fournit des revendications à ses utilisateurs. Les revendications sont des déclarations concernant les utilisateurs que les deux parties d'une fédération comprennent. Ces déclarations correspondent aux valeurs enregistrées par la revendication. Par exemple, une revendication peut être un nom commun, une adresse de messagerie ou un numéro d'employé. Pour établir une relation avec un fournisseur de revendications, vous configurez une approbation de fournisseur de revendications dans l'organisation du partenaire de ressource.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez définir la façon dont les revendications sont échangées entre les partenaires fédérés dans le service de fédération, puis les enregistrer dans la base de données de configuration AD FS. Les revendications proviennent des magasins d'attributs, ou trouvent leur source en appliquant des règles de revendication pour transformer une revendication entrante en une autre valeur. Par exemple, vous pouvez transformer la revendication Administrateurs de domaine en la valeur Administrateurs, puis envoyer cette nouvelle valeur comme revendication sortante. Les services AD FS prennent en charge tout type de revendication, mais sont configurés par défaut avec les types de revendication suivants :

Type de revendication	Description
Adresse de messagerie	Adresse de messagerie de l'utilisateur
Prénom	Prénom de l'utilisateur
Nom	Nom unique de l'utilisateur
Nom d'utilisateur principal	Nom d'utilisateur principal de l'utilisateur
Nom commun	Nom commun de l'utilisateur
Adresse de messagerie AD FS 1.x	Adresse de messagerie de l'utilisateur lors de l'interaction avec AD FS 1.1 ou AD FS 1.0
Groupe	Groupe dont l'utilisateur est membre
Nom d'utilisateur principal AD FS 1.x	Nom d'utilisateur principal de l'utilisateur lors de l'interaction avec AD FS 1.1 ou AD FS 1.0
Rôle	Rôle de l'utilisateur
Nom de famille	Nom de famille de l'utilisateur
PPID	Identificateur personnel privé (PPID) de l'utilisateur
Identificateur de nom	Identificateur de nom SAML de l'utilisateur
Méthode d'authentification	Méthode utilisée pour authentifier l'utilisateur
SID de groupe en refus seul	Identificateur de sécurité (SID) de groupe en refus seul de l'utilisateur
SID principal en refus seul	SID principal en refus seul de l'utilisateur
SID de groupe principal en refus seul	SID de groupe principal en refus seul de l'utilisateur
SID de groupe	SID de groupe de l'utilisateur
SID de groupe principal	SID de groupe principal de l'utilisateur
SID principal	SID principal de l'utilisateur
Nom du compte Windows	Nom du compte de domaine de l'utilisateur sous la forme <domaine>\<utilisateur>

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Partie de confiance

Un service de fédération ou une application qui utilise des revendications dans une transaction particulière est une partie de confiance. La partie de confiance utilise les revendications présentées dans un fournisseur de revendications et agit en tant que service Web pour demander des revendications à partir d'un fournisseur de revendications approuvé. Vous pouvez établir une relation avec une partie de confiance en configurant une approbation de partie de confiance dans l'organisation du partenaire de compte.

En général, une partie de confiance délivre également des jetons aux services ou applications prenant en charge les revendications dans sa propre organisation, selon les revendications contenues dans les jetons de sécurité que le client AD FS lui présente, en supposant qu'un fournisseur de revendications approuvé produit les jetons.

Vous pouvez également configurer des règles de revendication pour transformer les revendications entrantes du fournisseur de revendications en d'autres valeurs, de sorte que vous puissiez présenter des revendications compatibles à l'application ou au service.

Vue d'ensemble des applications compatibles AD FS

Windows Identity Foundation

WIF fournit une interface API (Application Programming Interface) pour tirer profit de la fédération et des revendications dans les applications basées sur un navigateur. Les applications et services utilisent WIF pour traiter les jetons délivrés par AD FS, et prennent des décisions basées sur les identités en fonction des jetons présentés. Vous pouvez également utiliser WIF pour traduire les revendications de fédération en jetons Windows NT en vue d'interagir avec les applications qui ne prennent pas en charge les revendications.

WIF fournit les fonctionnalités suivantes

- Interface API pour les applications basées sur un navigateur prenant en charge les revendications
- Peut également traduire les jetons NT pour les applications qui ne prennent pas en charge les revendications

Les applications et services tiers peuvent être basés sur les protocoles suivants

- SAML
- WS-Federation
- Protocoles WS-Trust

Documentation supplémentaire : Pour plus d'informations sur WIF, rendez-vous sur MSDN à l'adresse http://go.microsoft.com/fwlink/?LinkID=285330.

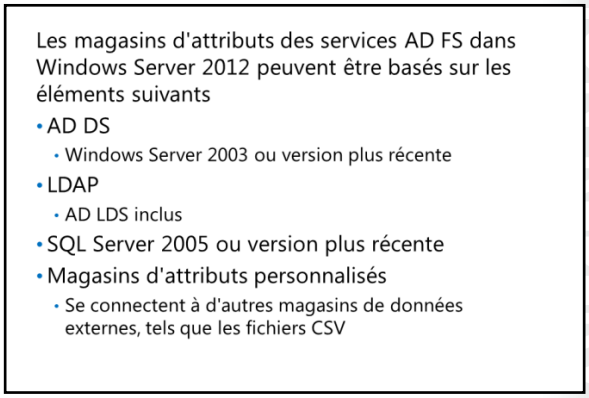
Applications et services tiers

Les services AD FS sont basés sur des normes, ils peuvent donc interagir avec les applications et services basés sur les protocoles SAML, WS-Federation et WS-Trust. RSA SecurID, IBM Tivoli Federated Identity Manager, Shibboleth 2.0 et Ping Identity PingFederate en sont quelques exemples.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options d'implémentation des magasins d'attributs

Un magasin d'attributs est un répertoire ou une base de données dans AD FS qui stocke les comptes d'utilisateurs et leurs attributs associés. Les revendications sont créées en fonction de ces attributs par le service de fédération qui les récupère du magasin d'attributs. Une application ou un service hébergé dans une partie de confiance prend ensuite des décisions d'autorisation en fonction de ces revendications. Les services AD FS dans Windows Server 2012 prennent en charge le magasin d'attributs selon les répertoires ou les bases de données suivants :



- Active Directory (Windows Server 2003 et les versions plus récentes)
- LDAP
- Microsoft SQL Server 2005 et les versions plus récentes
- Magasins d'attributs personnalisés

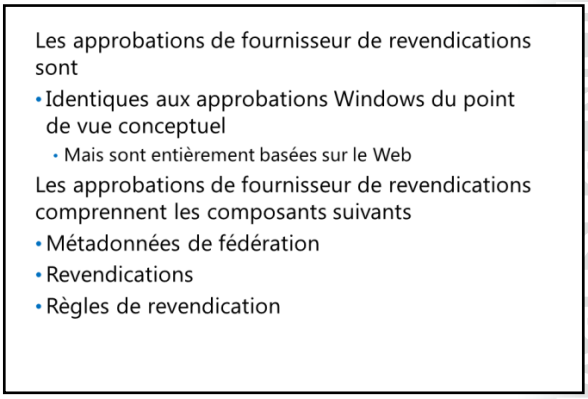
Un exemple de magasin d'attributs LDAP serait un déploiement par authentification unique Web pour fournir des applications ou services à des clients individuels. Dans ce scénario, vous déployez les serveurs de fédération et d'applications dans un réseau de périmètre et enregistrez les comptes clients dans une base de données AD LDS. Dans ce cas, un magasin d'attributs LDAP est créé dans AD FS pour utiliser l'instance AD LDS comme sa source.

Vous pouvez utiliser une définition d'attribut personnalisée pour vous connecter à d'autres magasins de données externes, tels qu'un fichier de valeurs séparées par des virgules (CSV), pour rechercher des informations sur les revendications. La définition et l'utilisation des magasins d'attributs personnalisés sont une tâche de développement personnalisée, qui n'entre pas dans le cadre de ce cours.

Documentation supplémentaire : Pour plus d'informations sur les magasins d'attributs personnalisés, rendez-vous sur MSDN à l'adresse http://go.microsoft.com/fwlink/?LinkID=285331.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des composants d'approbation de fournisseur de revendications



Une approbation de fournisseur de revendications s'apparente du point de vue conceptuel à une approbation Windows, mais elle est entièrement basée sur le Web. Une fois qu'une approbation de fournisseur de revendications est établie, un partenaire de ressource considère comme valides les revendications et les attributs (authentifications) fournis par le partenaire de compte. Ce scénario s'apparente à une approbation Windows dans laquelle le domaine de confiance considère comme valide les authentifications provenant du domaine approuvé. Cependant, il n'existe aucune connectivité entre les serveurs de fédération de compte et de ressource, et l'intégralité du trafic réseau dans un scénario AD FS est basé sur le Web. Un administrateur peut configurer les informations permettant d'établir l'approbation sur les serveurs de fédération de compte et de ressource de trois façons :

- En saisissant manuellement les informations.
- En important un fichier de stratégie fourni par le partenaire d'approbation.
- En important les données relatives au fournisseur de revendications à partir des métadonnées de fédération publiées en ligne via une URL fournie par l'organisation du fournisseur de revendications.

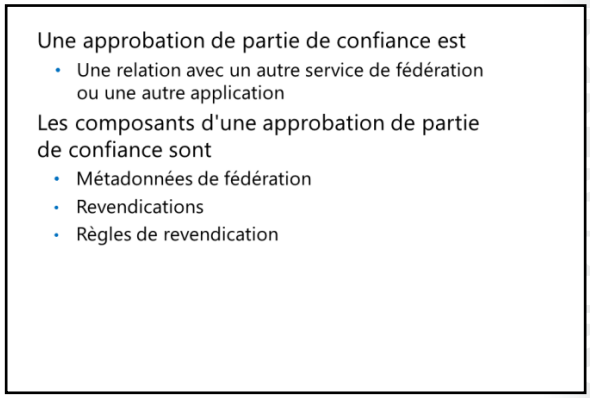
Une approbation de fournisseur de revendications comprend les éléments suivants :

- *Métadonnées de fédération*. Il s'agit des données relatives au fournisseur de revendications. Vous les obtenez à partir d'une URL pour le fournisseur de revendications, les importez à partir d'un fichier fourni par le fournisseur de revendications ou les configurez manuellement.
- *Revendications*. Le fournisseur de revendications définit les revendications disponibles.
- *Règles de revendication*. Les règles de revendication sont définies sur une approbation de fournisseur de revendications et spécifient la façon dont AD FS et ses parties de confiance utilisent les revendications reçues du fournisseur de revendications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des composants d'approbation de partie de confiance

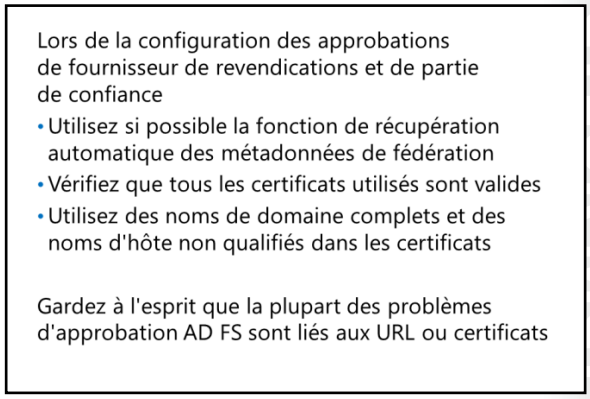
Une approbation de partie de confiance définit une relation avec un autre service de fédération ou une autre application pour permettre à cette entité d'utiliser les revendications provenant du service de fédération dans lequel l'approbation de partie de confiance est créée. Elle s'apparente à une approbation de fournisseur de revendications et comprend les éléments suivants :



- Métadonnées de fédération. Il s'agit des données relatives à la partie de confiance, que vous obtenez à partir d'une URL pour la partie de confiance, importez à partir d'un fichier fourni par la partie de confiance ou configurez manuellement.
- Revendications. Le fournisseur de revendications définit les revendications disponibles.
- Règles de revendication. Les règles de revendication sont définies sur une approbation de partie de confiance pour définir la façon dont les revendications qui transmettent l'approbation sont présentées à la partie de confiance.

Configuration des approbations de fournisseur de revendications et de partie de confiance

Approbations de fournisseur de revendications



- Utilisez la fonction de récupération automatique pour les métadonnées de fédération. Si possible, vous devez configurer une approbation de fournisseur de revendications à l'aide des métadonnées de fédération publiées sur une URL ou dans un fichier fourni par le fournisseur de revendications. Cette méthode de récupération automatique simplifie considérablement le processus de configuration de l'approbation, et elle évite d'avoir à résoudre les problèmes liés à une configuration saisie manuellement.
- Vérifiez que les certificats sont valides. Le certificat de signature de jetons configuré pour l'approbation doit être un certificat valide (actuel et approuvé) et doit être unique pour cette approbation de fournisseur de revendications. Vous l'utilisez pour vérifier que les jetons reçus ont bien été délivrés par le fournisseur de revendications configuré.
- Utilisez des noms de domaine complets. Bien que cela ne relève pas de votre contrôle, les certificats configurés dans les approbations de fournisseur de revendications doivent utiliser des noms de domaine complets (par exemple, myserver.contoso.com), et non un nom d'hôte non qualifié, tel que myserver. Cela permet d'éviter les éventuels problèmes d'emprunt d'identité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Approbations de partie de confiance

Lorsque vous configurez les approbations de partie de confiance, vous devez prendre en compte plusieurs aspects comme vous l'avez fait lorsque vous avez créé les approbations de fournisseur de revendications. Toutefois, lorsque vous configurez une approbation de partie de confiance, il est important de garder à l'esprit que si l'approbation est configurée en utilisant la récupération automatique des métadonnées de fédération à partir d'une URL, vous devez tenir compte du fait qu'AD FS met à jour les métadonnées de fédération toutes les 24 heures. Cela vous évite d'avoir à modifier manuellement l'approbation de fédération lorsque des modifications sont apportées à la partie de confiance, par exemple le renouvellement, l'ajout ou la suppression de certificats.

Remarque : Une règle de base lors de la résolution de la plupart des problèmes de configuration des approbations AD FS est que si le problème ne provient pas des certificats, il est généralement dû à des URL incorrectes. S'il n'est pas dû à des URL incorrectes, il provient généralement des certificats.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Planification et implémentation des revendications et des règles de revendication AD FS

Une fois que vos approbations de fournisseur de revendications et de partie de confiance sont établies, vous pouvez configurer les revendications et les règles de revendication pour définir quelles revendications sont fournies aux clients AD FS et comment transformer les revendications entrantes pour les utiliser avec vos applications ou services.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options de configuration des règles de revendication sur une approbation de fournisseur de revendications ;
- décrire les options de configuration des règles de revendication sur une approbation de partie de confiance ;
- configurer la transformation des revendications ;
- créer des revendications personnalisées à l'aide du langage des règles de revendications ;
- décrire les éléments à prendre en compte pour la conception des revendications AD DS ;
- décrire les options d'intégration avec les versions AD FS précédentes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options de configuration des règles de revendication sur une approbation de fédération

Modèle de règle de revendication

Lorsque vous configurez une règle de revendication à l'aide de l'Assistant Ajouter une règle de revendication de transformation, votre première préoccupation doit être de déterminer le modèle de règle de revendication à utiliser. Les règles de revendication sont spécifiques à une approbation de fédération, et vous ne pouvez pas les utiliser sur d'autres approbations que vous définissez dans le service de fédération. Par conséquent, les services AD FS incluent des modèles de règle de revendication qui simplifient la création des règles de revendications. Ces modèles fournissent des représentations des structures de langage de règles de revendication préconfigurées sous la forme d'une interface utilisateur. Ils sont basés sur les types les plus courants de règles de revendication créées, et incluent les éléments suivants :

Lors de la configuration des règles de revendication, gardez à l'esprit les éléments suivants

- Les modèles de règle de revendication fournissent une structure de langage de règles de revendication préconfigurée
- Les noms de règle de revendication doivent être descriptifs
  - Facilitent la gestion ultérieure du service de fédération
- Les revendications entrantes sont spécifiées avec l'un des modèles suivants
  - Passer ou filtrer une revendication entrante
  - Transformer une revendication entrante
- Les revendications sortantes sont spécifiées avec tous les autres modèles

Modèle de règle de revendication	Description
Passer ou filtrer une revendication entrante	Permet d'accepter ou d'émettre des revendications non modifiées.
Transformer une revendication entrante	Mapper une revendication entrante sur un autre type de revendication ou mapper une valeur de revendication sur une nouvelle valeur. Par exemple, vous pouvez utiliser ce modèle sur une revendication entrante pour remplacer un suffixe de messagerie par une nouvelle valeur, ou transformer une revendication UPN entrante en une revendication d'adresse de messagerie.
Envoyer les attributs LDAP en tant que revendications	Mapper les attributs LDAP sur les revendications afin que vous puissiez extraire les revendications d'un magasin LDAP et des services AD DS. Une règle unique peut émettre plusieurs revendications, mais les performances peuvent être ralenties du fait des recherches LDAP. En outre, vous ne pouvez pas utiliser les filtres LDAP personnalisés pour vos requêtes.
Envoyer l'appartenance à un groupe en tant que revendication	Utiliser avec les magasins d'attributs AD DS. Les règles qui utilisent ce modèle peuvent créer une revendication unique basée sur le groupe spécifié. En outre, étant donné que la règle utilise des SID de groupe pour émettre la revendication, les performances sont très rapides. Cela est dû au fait qu'aucune recherche de compte n'est requise, et une seule revendication basée sur un groupe peut être émise.
Envoyer les revendications en utilisant une règle personnalisée	Permet de créer des règles personnalisées en utilisant le langage des règles de revendication AD FS. Vous pouvez utiliser ce modèle pour d'autres scénarios qui ne sont pas pris en charge par les modèles prédéfinis, par exemple les règles utilisées avec un magasin d'attributs personnalisé, l'envoi de revendications basées sur plusieurs revendications entrantes ou l'utilisation d'un filtre LDAP personnalisé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Nom de la règle de revendication

Indépendamment du modèle utilisé, vous devez définir un nom de règle de revendication. La spécification d'un nom descriptif facilitera la gestion ultérieure du service de fédération. Personne ne saura ce que devait accomplir une règle nommée Règle de revendication 1.

Revendications entrantes

Vous devez spécifier un type de revendication entrante lorsque vous utilisez l'un des deux modèles de revendication suivants :

- **Passer ou filtrer une revendication entrante**
- **Transformer une revendication entrante**

Vous pouvez également spécifier si la règle agira sur toutes les valeurs de revendication, uniquement sur des valeurs de revendication spécifiques, uniquement sur les valeurs de revendication correspondant à un suffixe de messagerie spécifique ou sur les valeurs de revendication qui commencent par une valeur spécifique.

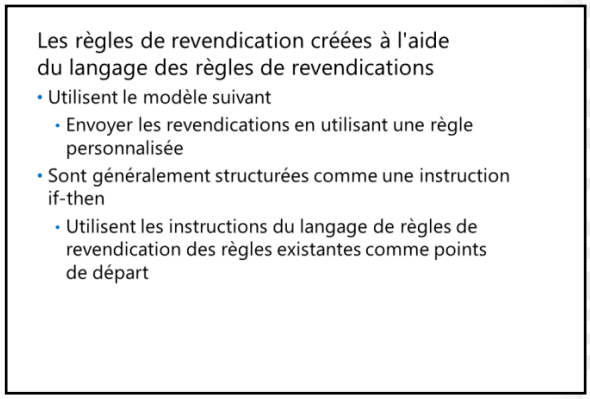
Revendications sortantes

Vous définissez un type de revendication sortante lors de la création de votre règle, sauf pour les règles qui utilisent le modèle Passer ou filtrer une revendication entrante. Selon le type de revendication sortante sélectionné, vous devrez peut-être spécifier la valeur de revendication sortante. Par exemple, vous pouvez utiliser le type de revendication sortante Groupe avec la valeur Administrateur si l'utilisation est membre du groupe Administrateurs du domaine AD DS.

Création de règles de revendication à l'aide du langage des règles de revendications

Langage des règles de revendications

Vous pouvez créer la majorité des règles de revendication à l'aide des modèles de règle de revendication prédéfinis. Cependant, d'autres scénarios peuvent nécessiter l'utilisation d'une règle personnalisée. Le modèle Envoyer les revendications en utilisant une règle personnalisée vous permet de définir une règle à l'aide du langage des règles de revendications AD FS.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Syntaxe du langage des règles de revendications

Dans une structure semblable à de nombreux langages de programmation, le langage des règles de revendications est généralement structuré comme une instruction if-then, comme suit :

- If (la condition a la valeur true), Then (émettez une revendication avec cette valeur)

  Dans le langage des règles de revendications, un opérateur spécial (=>) sépare la condition de l'instruction d'émission, et un point-virgule termine l'instruction. Voici un exemple de règle de revendications :

  ```
  c:[Type == http://contoso.com/department] => issue(Type =
  "http://adatum.com/department", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer,
  Value = c.Value, ValueType = c.ValueType);
  ```

  Dans cet exemple, c:[Type == http://contoso.com/department] est la condition et issue(Type = "http://adatum.com/department", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType) est l'instruction d'émission.

- Vous pouvez combiner plusieurs conditions à l'aide de l'opérateur de conjonction logique &&. Par exemple, la règle suivante émet une revendication uniquement si l'utilisateur a le rôle d'éditeur et une revendication de messagerie :

  ```
  c1:[Type == "http://contoso.com/role", Value=="Editors"] &&
  c2:[Type == "http://contoso.com/email"]
   => issue(claim = c1);
  ```

  En outre, vous pouvez combiner plusieurs revendications entrantes en une seule revendication sortante. Par exemple, la règle suivante prend les revendications entrantes d'emplacement et de rôle et les regroupe en une seule revendication sortante ciblée :

  ```
  c1:[Type == "http://contoso.com/location"] &&
  c2:[Type == "http://contoso.com/role"]
   => issue(Type="http://contoso.com/targeted", Value=c1.value+" "+c2.value);
  ```

  Dans cet exemple, les revendications entrantes de l'emplacement *Seattle* et du rôle *Éditeur* génèreraient la revendication sortante ciblée Éditeur de Seattle.



Documentation supplémentaire : Pour plus d'informations sur le langage des règles de revendications, accédez à la page TechNet relative au langage des règles de revendications AD FS 2.0, à l'adresse http://go.microsoft.com/fwlink/?LinkID=285329.

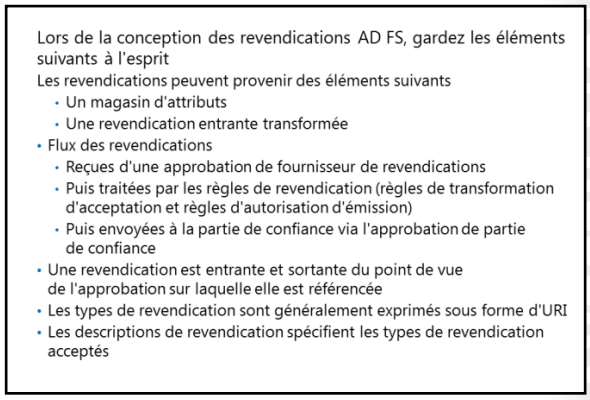
Création de règles à l'aide du langage des règles de revendications

Si vous n'êtes pas familier avec le langage des règles de revendications AD FS, un moyen facile de créer des règles personnalisées et d'apprendre la syntaxe consiste à créer un plus grand nombre de règles de base à l'aide des modèles de règle de revendication disponibles, puis à utiliser les instructions du langage de règles de revendications de ces règles comme points de départ de votre règle personnalisée.

Vous pouvez obtenir le langage des règles de revendication pour une règle existante en ouvrant la boîte de dialogue **Modifier la règle**. Cliquez sur le bouton **Afficher le langage des règles**, puis copiez le langage des règles dans un éditeur de texte.

Conception des revendications AD FS

Lorsque vous déterminez les revendications que votre déploiement AD FS doit utiliser, vous devez prendre en compte plusieurs éléments, qui sont détaillés dans les sections suivantes :



Source des revendications

Le service de fédération définit les revendications échangées entre les partenaires de fédération, qui trouvent leur source de l'une des deux façons suivantes :

- En utilisant les valeurs que vous obtenez à partir d'un magasin d'attributs, par exemple la revendication Directeur commercial est récupérée de l'attribut de titre d'un compte d'utilisateur AD DS.
- À l'aide d'une règle de revendication qui transforme une valeur de revendication entrante en une autre valeur de revendication sortante, par exemple la transformation d'une revendication UPN entrante en une revendication de messagerie sortante.

Flux des revendications

Le service de fédération traite et transmet les revendications d'un fournisseur de revendications à une partie de confiance, via le *pipeline des revendications*. Le pipeline des revendications est une construction logique, dont le flux se présente comme suit :

1. Les revendications sont reçues du fournisseur de revendications et traitées par les règles de revendication (règles de transformation d'acceptation) qui sont définies dans l'approbation de fournisseur de revendications, qui spécifie quelles revendications émises par le fournisseur de revendications doivent être acceptées.
2. Les revendications traitées par les règles de transformation d'acceptation sont ensuite envoyées aux règles d'autorisation d'émission, qui déterminent si l'utilisateur est autorisé à accéder à la partie de confiance. Celles-ci sont définies dans le cadre de l'approbation de partie de confiance.
3. Le résultat des règles de transformation d'acceptation est ensuite utilisé comme entrée pour les règles de transformation d'émission, qui sont également définies sur l'approbation de partie de confiance. Ces règles déterminent les revendications qui seront envoyées à la partie de confiance définie par l'approbation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Revendications entrantes et sortantes

Lorsque vous définissez les règles de revendication, vous devez prendre en compte la source des revendications entrantes et la destination des revendications sortantes, comme indiqué dans le tableau suivant.

Type d'approbation de fédération	Revendications entrantes	Revendications sortantes
Approbation de fournisseur de revendications	Revendications reçues du fournisseur de revendications	Revendications envoyées au service de fédération
Approbation de partie de confiance	Revendications reçues de l'approbation de fournisseur de revendications correspondante via le service de fédération	Revendications envoyées à la partie de confiance (une application ou un autre service de fédération)

Types de revendications

Le type de revendication fournit le contexte d'une valeur de revendication, et le type de revendication est généralement exprimé sous la forme d'un URI (Uniform Resource Identifier). Par défaut, les services AD FS sont configurés avec les types de revendication répertoriés dans le tableau suivant.

Nom	Description	URI
Adresse de messagerie	Adresse de messagerie de l'utilisateur	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Prénom	Prénom de l'utilisateur	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Nom	Nom unique de l'utilisateur	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Nom d'utilisateur principal	Nom d'utilisateur principal de l'utilisateur	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
Nom commun	Nom commun de l'utilisateur	http://schemas.xmlsoap.org/claims/CommonName
Adresse de messagerie AD FS 1.x	Adresse de messagerie de l'utilisateur lors de l'interaction avec AD FS 1.1 ou AD FS 1.0	http://schemas.xmlsoap.org/claims/EmailAddress
Groupe	Groupe dont l'utilisateur est membre	http://schemas.xmlsoap.org/claims/Group
Nom d'utilisateur principal AD FS 1.x	Nom d'utilisateur principal de l'utilisateur lors de l'interaction avec AD FS 1.1 ou AD FS 1.0	http://schemas.xmlsoap.org/claims/UPN

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Nom	Description	URI
Rôle	Rôle de l'utilisateur	http://schemas.microsoft.com/ws/2008/06/identity/claims/role
Nom de famille	Nom de famille de l'utilisateur	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
PPID	Identificateur privé de l'utilisateur	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier
Identificateur de nom	Identificateur de nom SAML de l'utilisateur	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
Méthode d'authen-tification	Méthode utilisée pour authentifier l'utilisateur	http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod
SID de groupe en refus seul	SID de groupe en refus seul de l'utilisateur	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid
SID principal en refus seul	SID principal en refus seul de l'utilisateur	http://schemas.microsoft.com/ws/2008/06/identity/claims/denyonlyprimarysid
SID de groupe principal en refus seul	SID de groupe principal en refus seul de l'utilisateur	http://schemas.microsoft.com/ws/2008/06/identity/claims/denyonlyprimarygroupsid
SID de groupe	SID de groupe de l'utilisateur	http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid
SID de groupe principal	SID de groupe principal de l'utilisateur	http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid
SID principal	SID principal de l'utilisateur	http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid

Descriptions de revendication

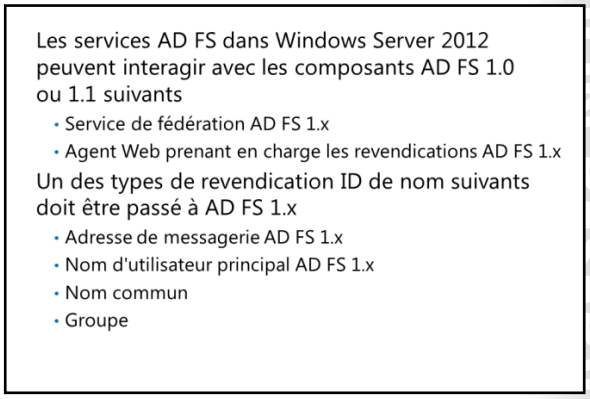
Les descriptions de revendication définissent les types de revendication pris en charge par le service de fédération, et spécifient également les types de revendication acceptés par les services de fédération et les types qu'ils peuvent envoyer. Cette liste des types de revendication est stockée dans la base de données de configuration AD FS et publiée sur les métadonnées de fédération. Chaque description de revendication contient un nom, l'URI du type de revendication, une description et l'état de publication (Accepté et/ou Envoyé).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options d'interaction avec les versions précédentes d'AD FS

Interaction d'AD FS 1.x

Les services AD FS dans Windows Server 2012 peuvent interagir avec AD FS 1.0 (Windows Server 2003 R2) et AD FS 1.1 (Windows Server 2008 ou Windows Server 2008 R2). Windows Server 2012 prend en charge l'interaction de trois façons :



1. Envoi des revendications d'un service de fédération AD FS 1.x vers un service de fédération Windows Server 2012.
2. Envoi des revendications compatibles AD FS 1.x d'un service de fédération Windows Server 2012 vers un service de fédération AD FS 1.x.
3. Envoi des revendications compatibles AD FS 1.x d'un service de fédération Windows Server 2012 vers des serveurs Web exécutant l'agent Web prenant en charge les revendications AD FS 1.x.

Remarque : Windows Server 2012 ne prend pas en charge l'agent Web basé sur les jetons Windows NT AD FS 1.*x* dans les services AD FS.

Type de revendication ID de nom

AD FS 1.x utilise le concept de type de revendication d'identité. Le type de revendication ID de nom de Windows Server 2012 est l'équivalent de ce type de revendication d'identité, et vous devez utiliser une revendication d'identité à chaque interaction avec AD FS 1.x. Une revendication d'identité indique que la revendication appartient à un utilisateur ou un principal de sécurité spécifique. Les services AD FS dans Windows Server 2012 fournissent les formats suivants de type de revendication ID de nom qui sont mappés sur les revendications d'identité AD FS 1.x équivalentes :

- Adresse de messagerie AD FS 1.x
- Nom d'utilisateur principal AD FS 1.x
- Nom commun
- Groupe

Une revendication d'identité envoyée à AD FS 1.x ne peut contenir qu'une revendication ID de nom, et vous devez la configurer au format approprié, comme indiqué dans le paragraphe précédent.

Remarque : En outre, le service de fédération dans AD FS 1.x ne peut accepter que les revendications entrantes dont l'URI commence par http://schemas.xmlsoap.org/claims/.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et implémentation d'une infrastructure AD FS

Scénario

La société A. Datum a établi des relations commerciales avec d'autres sociétés et clients. Certaines de ces sociétés partenaires et de ces clients doivent accéder aux applications métier qui s'exécutent sur le réseau A. Datum. Les groupes de l'entreprise A. Datum souhaitent fournir un niveau maximal de fonctionnalités et d'accès à ces sociétés. Les départements Sécurité et Opérations souhaitent vérifier que les partenaires et les clients peuvent accéder uniquement aux ressources auxquelles ils ont besoin d'accéder et que l'implémentation de la solution n'augmente pas considérablement la charge de travail de l'équipe chargée des opérations.

Pour répondre aux exigences métier, A. Datum a décidé d'implémenter les services AD FS. Dans le cadre du déploiement initial, la société envisage d'utiliser les services AD FS pour implémenter l'authentification unique (SSO) pour les utilisateurs internes qui accèdent à une application sur un serveur Web. A. Datum a également conclu un partenariat avec une autre société, Trey Research, dont les utilisateurs doivent pouvoir accéder à la même application.

Objectifs

- Concevoir le déploiement AD FS.
- Configurer les composants prérequis pour AD FS.
- Déployer les services AD FS pour les utilisateurs internes.
- Déployer les services AD FS pour une organisation partenaire.

Configuration de l'atelier pratique

Durée approximative : 100 minutes

Ordinateurs virtuels	22414B-LON-DC1 22414B-LON-SVR3 22414B-LON-CL1 22414B-PRS-DC1
Noms des utilisateurs	ADATUM\Administrateur TreyResearch\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible.
Avant de commencer cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, sur **Accueil**, cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22414B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22414B-LON-SVR3**, **22414B-LON-CL1** et **22414B-PRS-DC1**.
   - Connectez-vous à **22414-LON-SVR3** en tant qu'**ADATUM\Administrateur**.
   - Ne vous connectez pas à **22414B-LON-CL1** tant qu'il ne vous a pas été demandé de le faire.
   - Sur **22414B-PRS-DC1**, connectez-vous en tant que **TreyResearch\Administrateur** avec le mot de passe **Pa$$w0rd**.

Exercice 1 : Conception du déploiement AD FS

Scénario

Le groupe de sécurité d'A. Datum a identifié les exigences suivantes pour le déploiement AD FS :

- Seuls les utilisateurs des services Recherche et Responsables d'A. Datum doivent pouvoir accéder aux applications protégées par AD FS.
- Les membres du service Recherche doivent être identifiés à l'aide du rôle HighSecurity dans l'application AD FS.
- Les membres du service Responsables doivent être identifiés en tant que responsables dans l'application AD FS.
- Les utilisateurs du groupe Cadres de Trey Research doivent être autorisés à accéder à l'application protégée par AD FS. Seuls ces utilisateurs doivent être identifiés comme rôle ExternalSecure dans l'application AD FS.

Les tâches principales de cet exercice sont les suivantes :

1. Choisir le scénario de déploiement AD FS approprié.
2. Identifier le nombre de serveurs Active Directory® Federation Services (AD FS) requis pour le déploiement, ainsi que le rôle et l'emplacement de chacun des serveurs de fédération que vous déploierez.

▶ Tâche 1 : Choisir le scénario de déploiement AD FS approprié

Selon les exigences identifiées, déterminez si un déploiement par authentification unique Web ou par authentification unique Web fédérée est requis pour qu'A. Datum conclut un partenariat avec Trey Research.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Identifier le nombre de serveurs Active Directory® Federation Services (AD FS) requis pour le déploiement, ainsi que le rôle et l'emplacement de chacun des serveurs de fédération que vous déploierez

1. Pour le déploiement des services AD FS dans A. Datum et Trey Research, identifiez le nombre de serveurs AD FS requis pour le déploiement dans les deux sociétés.
2. Pour les serveurs AD FS identifiés dans l'étape 1, déterminez le rôle et l'emplacement de chacun des serveurs de fédération que vous déploierez.

Résultats : Dans cet exercice, vous devez avoir identifié le scénario de déploiement AD FS approprié à utiliser pour répondre aux exigences définies. Vous devez également avoir identifié le nombre de serveurs AD FS requis pour le déploiement, leur emplacement et le rôle de chacun d'eux dans le déploiement.

Exercice 2 : Configuration des composants prérequis pour AD FS

Scénario

A. Datum a déployé une application WIF en tant qu'application de mise à l'épreuve pour le déploiement AD FS. Vous devez préparer les composants prérequis pour le déploiement AD FS à A. Datum. Ces composants incluent la configuration de la résolution de noms DNS et la configuration des certificats et des approbations de certificat.

Les principales tâches de cet exercice sont les suivantes :

1. Configurer les redirecteurs DNS (Domain Name System).
2. Échanger les certificats racines pour activer des approbations de certificat.
3. Demander et installer un certificat pour le serveur Web.
4. Lier le certificat à l'application prenant en charge les revendications sur le serveur Web et vérifier l'accès à l'application.

▶ Tâche 1 : Configurer les redirecteurs DNS (Domain Name System)

1. Sur **LON-DC1**, créez un redirecteur conditionnel pour le domaine **TreyResearch.net** à l'aide de l'adresse IP **172.16.10.10** du serveur DNS.
2. Sur **PRS-DC1**, créez un redirecteur conditionnel pour le domaine **Adatum.com** à l'aide de l'adresse IP **172.16.0.10** du serveur DNS.

▶ Tâche 2 : Échanger les certificats racines pour activer des approbations de certificat

1. Sur LON-DC1, copiez **PRS-DC1.TreyResearch.net_TreyResearch-PRS-DC1-CA.crt** de **\\PRS-DC1.treyresearch.net\certenroll** vers le dossier **Documents**.
2. Créez une console MMC (Microsoft® Management Console) et ajoutez l'**Éditeur de gestion des stratégies de groupe**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Modifiez l'objet de stratégie de groupe **Default Domain Policy** et importez le certificat racine copié dans le dossier **Autorités de certification racines de confiance**.
4. Sur PRS-DC1, copiez **PRS-DC1.TreyResearch.net_TreyResearch-PRS-DC1-CA.crt** de **\\LON-DC1.Adatum.com\certenroll** vers le dossier **Documents**.
5. Créez une console MMC et ajoutez le composant logiciel enfichable **Certificats** destiné à l'ordinateur local.
6. Importez le certificat racine copié dans le dossier **Autorités de certification racines de confiance**.

▶ Tâche 3 : Demander et installer un certificat pour le serveur Web

1. Sur LON-SVR3, ouvrez la console Gestionnaire des services Internet (IIS).
2. Demandez un nouveau certificat de domaine pour le serveur à l'aide des paramètres suivants :
   - Nom commun : **LON-SVR3.adatum.com**
   - Organisation : **A. Datum**
   - Unité d'organisation : **IT**
   - Ville : **London**
   - Département/région : **England**
   - Pays/région : **GB**
   - Nom convivial : **LON-SVR3.adatum.com**
3. Demandez le certificat à partir de **AdatumCA**.

▶ Tâche 4 : Lier le certificat à l'application prenant en charge les revendications sur le serveur Web et vérifier l'accès à l'application

1. Sur LON-SVR3, dans IIS, créez une liaison de site HTTPS, puis sélectionnez le certificat qui vient d'être créé.
2. Sur LON-DC1, ouvrez Windows Internet Explorer®, puis connectez-vous à **https://lon-svr3.adatum.com/adatumtestapp**.
3. Vérifiez que vous pouvez vous connecter au site, mais que vous recevez une erreur d'accès refusé 401. Cela est normal, car vous n'avez pas encore configuré AD FS pour l'authentification.
4. Fermez Internet Explorer.

Résultats : Dans cet exercice, vous devez avoir configuré le transfert DNS pour activer la résolution de noms entre A. Datum et Trey Research. En outre, vous devez avoir échangé des certificats racines entre les deux organisations, et installé et configuré un certificat Web sur le serveur d'applications.

Exercice 3 : Déploiement des services AD FS pour les utilisateurs internes

Scénario

Le premier scénario de déploiement pour AD FS est destiné aux utilisateurs internes uniquement. Pour implémenter les services AD FS, vous devez installer et configurer le rôle serveur AD FS, puis configurer l'approbation de fournisseur de revendications. Vous configurerez ensuite l'application WIF pour approuver le déploiement AD FS, puis configurerez une approbation de partie de confiance. Enfin, vous configurerez les règles de revendication, puis vérifierez que seuls les utilisateurs internes approuvés peuvent accéder à l'application.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Installer et configurer le rôle de serveur AD FS.
2. Configurer l'approbation de fournisseur de revendications.
3. Configurer l'application WIF pour approuver le déploiement AD FS.
4. Configurer une approbation de partie de confiance et les règles de revendications.
5. Vérifier l'accès à l'application pour les utilisateurs internes.

▶ Tâche 1 : Installer et configurer le rôle de serveur AD FS

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, ajoutez le rôle serveur **Services AD FS (Active Directory Federation Services)**.
2. Sur **LON-DC1**, exécutez l'Assistant Configuration du serveur de fédération AD FS à l'aide des paramètres suivants :
   - Créer un nouveau service de fédération.
   - Créer un déploiement autonome.
   - Utiliser le certificat **LON-DC1.Adatum.com**.
   - Choisir le nom de service **LON-DC1.Adatum.com**.
3. Sur LON-DC1, ouvrez Windows PowerShell, puis utilisez la commande set-ADFSProperties –AutoCertificateRollover $False pour activer la modification des certificats attribués.
4. Dans la console de gestion AD FS, ajoutez le certificat **LON-DC1.Adatum.com** comme nouveau certificat de signature de jetons. Vérifiez que le certificat a l'objet **CN=LON-DC1.Adatum.com** et que ses rôles incluent **Garantit votre identité auprès d'un ordinateur distant** et **Garantit l'identité d'un ordinateur distant**.
5. Faites du nouveau certificat le certificat principal et supprimez l'ancien certificat.

▶ Tâche 2 : Configurer l'approbation de fournisseur de revendications

1. Sur **LON-DC1**, dans la console Gestion AD FS, accédez à **Approbation de fournisseur de revendications**, mettez en surbrillance le magasin **Active Directory**, puis accédez à **Modifier les règles de revendication**.
2. Dans la boîte de dialogue **Modifier les règles de revendication pour Active Directory**, sur l'onglet **Règles de transformation d'acceptation**, démarrez l'Assistant Ajout de règle de revendication de transformation, et exécutez l'Assistant selon les paramètres suivants :
   - Sélectionnez **Envoyer les attributs LDAP en tant que revendications** sous **Modèle de règle de revendication**.
   - Nommez la règle de revendication **Règle d'attributs LDAP sortants**.
   - Choisissez **Active Directory** en tant que **Magasin d'attributs**.
3. Dans **Mappage des attributs LDAP aux types de revendications sortantes**, sélectionnez les valeurs suivantes :
   - E-mail-Addresses : **Adresse de messagerie**
   - User-Principal-Name : **UPN**
   - Display-Name : **Nom (Sélectionnez la première occurrence de la liste)**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer l'application WIF pour approuver le déploiement AD FS

1. Sur **LON-SVR3**, à partir de l'écran d'accueil, démarrez Windows Identity Foundation Federation Utility.
2. Exécutez l'Assistant avec les paramètres suivants :
   - Pointez sur le fichier web.config de l'exemple d'application WIF en accédant à **C:\Inetpub\wwwroot\ AdatumTestApp \web.config**.
   - Spécifiez une zone Application URI (URI d'application) en tapant https://lon-svr3.adatum.com/AdatumTestApp/.
   - Sélectionnez Application URI (URI d'application), puis saisissez le chemin d'accès https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml.
   - Sélectionnez **No encryption** (Aucun chiffrement).

▶ Tâche 4 : Configurer une approbation de partie de confiance et les règles de revendications

1. Sur **LON-DC1**, dans la console Gestion AD FS, dans le volet central, cliquez sur **Requis : ajouter une partie de confiance approuvée**.
2. Exécutez l'Assistant Ajout d'approbation de partie de confiance avec les paramètres suivants :
   - Sélectionnez **Importer les données, publiées en ligne ou sur un réseau local, contenant la partie de confiance**, puis tapez **https://lon-svr3.adatum.com/adatumtestapp**.
   - Spécifiez le **Nom complet Adatum Test App**.
   - Choisissez **Autoriser l'accès de tous les utilisateurs à cette partie de confiance**.
   - À la fin de l'exécution de l'Assistant, acceptez l'option pour ouvrir **Modifier les règles de revendication pour Adatum Test App**.
3. Dans la boîte de dialogue de propriétés **Modifier les règles de revendication pour Adatum Test Application**, choisissez d'ajouter une règle sur l'onglet **Règles de transformation d'émission**.
4. Exécutez l'Assistant Ajout de règle de revendication de transformation avec les paramètres suivants :
   - Dans la liste déroulante **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**.
   - Nommez la règle de revendication **Passer la règle du nom de compte Windows**.
   - Dans la liste déroulante **Type de revendication entrante**, cliquez sur **Nom du compte Windows**.
5. Créez trois règles supplémentaires pour passer par **Adresse de messagerie**, **Nom d'utilisateur principal** et **Nom**.

▶ Tâche 5 : Vérifier l'accès à l'application pour les utilisateurs internes

1. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Brad** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-CL1, cliquez sur le Bureau, ouvrez Internet Explorer, puis connectez-vous à **https://lon-svr3.adatum.com/AdatumTestApp/**.
3. Vérifiez que vous avez accès à l'application.

4. Si vous êtes invité à indiquer vos informations d'identification, tapez **ADATUM\Brad** et le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée. La page s'affiche et vous voyez les revendications qui ont été traitées pour permettre l'accès au site Web.
5. Fermez Internet Explorer.

Résultats : Dans cet exercice, vous devez avoir installé et configuré le rôle serveur AD FS sur LON-DC1. Vous devez également avoir configuré les approbations de fournisseur de revendications et de partie de confiance, puis avoir configuré les règles de revendication nécessaires. Enfin, vous devez avoir configuré l'application WIF pour approuver le déploiement AD FS, puis avoir vérifié que les utilisateurs internes approuvés peuvent accéder à l'application.

Exercice 4 : Déploiement des services AD FS pour une organisation partenaire

Scénario

Le deuxième scénario de déploiement consiste à permettre aux utilisateurs de Trey Research d'accéder à l'application Web. Pour répondre à l'exigence de sécurité consistant à ne pas autoriser l'accès direct à votre serveur AD FS à partir d'Internet, vous devez déployer et configurer un serveur proxy de fédération. Vous devez configurer l'intégration des services AD FS au sein de Trey Research avec AD FS au sein d'A. Datum, puis vérifier que les utilisateurs de Trey Research peuvent accéder à l'application. Vous souhaitez également confirmer que vous pouvez configurer l'accès basé sur les groupes d'utilisateurs.

Les tâches principales de cet exercice sont les suivantes :

1. Ajouter une approbation de fournisseur de revendications pour le serveur AD FS de TreyResearch.net.
2. Configurer une approbation de partie de confiance sur PRS-DC1 pour l'application prenant en charge les revendications A. Datum.
3. Vérifier l'accès à l'application de test A. Datum pour les utilisateurs de Trey Research.
4. Configurer les règles de revendication pour que l'approbation de fournisseur de revendications et l'approbation de partie de confiance autorisent l'accès à un seul groupe.
5. Vérifier les restrictions et l'accessibilité à l'application prenant en charge les revendications.
6. Pour préparer le module suivant.

▶ Tâche 1 : Ajouter une approbation de fournisseur de revendications pour le serveur AD FS de TreyResearch.net

1. Sur **LON-DC1**, dans la console de Gestion AD FS, accédez à **Relations d'approbation**, accédez à **Approbations de fournisseur de revendications**, puis choisissez **Ajouter une approbation de fournisseur de revendications**.
2. Exécutez l'Assistant Ajouter une approbation de fournisseur de revendications avec les paramètres suivants :
   - Choisissez **Importer les données publiées en ligne ou sur un réseau local concernant le fournisseur de revendications**, puis entrez dans **https://prs-dc1.treyresearch.net** en tant que source des données.
   - Dans **Nom complet**, tapez **PRS-DC1.treyresearch.net**.
   - Terminez l'Assistant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la boîte de dialogue **Modifier les règles de revendication pour prs-dc1.treyresearch.net**, utilisez les valeurs suivantes :
   - **Ajoutez une règle** aux règles de transformation d'acceptation.
   - Choisissez **Passer ou filtrer une revendication entrante** dans la liste **Modèle de règle de revendication**.
   - Utilisez **Passer la règle du nom de compte Windows** en tant que nom de la règle de revendication.
   - Choisissez **Nom du compte Windows** en tant que type de revendication entrante, puis choisissez de **Passer toutes les valeurs de revendication**.
   - Terminez la règle.
4. Sur **LON-DC1**, exécutez la commande suivante dans Windows PowerShell :

```
Set-ADFSClaimsProviderTrust –TargetName “PRS-DC1.treyresearch.net” –
SigningCertificateRevocationCheck None
```

5. Fermez la fenêtre Windows PowerShell.

 **Remarque :** Vous devez désactiver la vérification de la révocation des certificats uniquement dans les environnements de test. Dans un environnement de production, vous devez activer la vérification de la révocation des certificats.

▶ Tâche 2 : Configurer une approbation de partie de confiance sur PRS-DC1 pour l'application prenant en charge les revendications A. Datum

1. Sur **PRS-DC1**, dans la console de gestion AD FS, ouvrez l'Assistant Ajouter une approbation de partie de confiance, puis exécutez-le avec les paramètres suivants :
   - Choisissez **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confiance** et tapez **https:// lon-dc1.adatum.com**.
   - Spécifiez le **Nom complet Adatum TestApp**.
   - Choisissez **Autoriser l’accès de tous les utilisateurs à cette partie de confiance**.
   - Acceptez l'option pour ouvrir Modifier les règles de revendication pour lon-dc1.adatum.com à la fin de l'exécution de l'Assistant.
2. Dans la boîte de dialogue de propriétés **Modifier les règles de revendication pour lon-dc1.adatum.com**, sur l'onglet **Règles de transformation d'émission**, cliquez pour ajouter une règle avec les paramètres suivants :
   - Dans la liste des modèles de règle de revendication, sélectionnez **Passer ou filtrer une revendication entrante**.
   - Dans la boîte **Nom de la règle de revendication**, tapez **Passer la règle du nom de compte Windows**.
   - Choisissez **Nom du compte Windows** dans **Type de revendication entrante**.
   - Choisissez de **Passer toutes les valeurs de revendication**.
   - Terminez l'Assistant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Vérifier l'accès à l'application de test A. Datum pour les utilisateurs de Trey Research

1. Sur **PRS-DC1**, ouvrez Internet Explorer, puis connectez-vous à **https://lon-svr3.adatum.com/adatumtestapp/**.
2. Sélectionnez **prs-dc1.treyresearch.com** en tant que domaine d'accueil, et connectez-vous en tant que **TreyResearch\April**, avec le mot de passe **Pa$$w0rd**.
3. Vérifiez que vous avez accès à l'application.
4. Fermez Internet Explorer, puis connectez-vous au même site Web. Vérifiez que cette fois vous n'êtes pas invité à sélectionner un domaine d'accueil.

 **Remarque :** À nouveau, vous n'êtes pas invité à sélectionner un domaine d'accueil. Une fois que les utilisateurs ont sélectionné un domaine d'accueil et ont été authentifiés par une autorité du domaine, le serveur de fédération de la partie de confiance leur délivre un cookie _LSRealm. La durée de vie par défaut pour le cookie est de 30 jours. Par conséquent, pour vous connecter à plusieurs reprises, vous devez supprimer ce cookie après chaque tentative de connexion pour revenir à un état propre.

▶ Tâche 4 : Configurer les règles de revendication pour que l'approbation de fournisseur de revendications et l'approbation de partie de confiance autorisent l'accès à un seul groupe

1. Sur **PRS-DC1**, ouvrez la console de Gestion AD FS et accédez à l'approbation de partie de confiance d'Adatum TestApp.
2. Ajoutez une nouvelle règle de transformation d'émission qui envoie l'appartenance à un groupe en tant que revendication. Nommez la règle **Autoriser la règle du groupe Production**, configurez le groupe d'utilisateurs comme **Production**, configurez le type de revendication sortante comme **Groupe** et la valeur de revendication sortante comme **Production**.
3. Sur LON-DC1, dans la console de Gestion AD FS, modifiez la règle de fournisseur de revendications prs-dc1.treyresearch.net pour créer une nouvelle règle qui passe ou filtre une revendication entrante avec le nom de la règle **Envoyer la règle du groupe Production**. Configurez la règle avec le type de revendication entrante **Groupe**.
4. Modifiez l'approbation de partie de confiance d'Adatum Test App en créant une règle de transformation d'émission qui passe ou filtre une revendication entrante. Nommez la règle **Envoyer la règle du nom de groupe TreyResearch**, puis configurez la règle pour utiliser le type de revendication entrante **Groupe**.
5. Supprimez la règle d'autorisation d'émission qui accorde l'accès à tous les utilisateurs.
6. Créez une règle d'autorisation d'émission qui autorise ou refuse l'accès aux utilisateurs selon la revendication entrante. Configurez la règle avec le nom **Autoriser la règle du groupe Production TreyResearch**, le **Type de revendication entrante Groupe**, la **Valeur de revendication entrante Production**, puis sélectionnez l'option **Autoriser l'accès aux utilisateurs avec cette revendication entrante**.
7. Créez une règle d'autorisation d'émission qui autorise ou refuse l'accès aux utilisateurs selon la revendication entrante. Configurez la règle avec le nom **Temp**, le **Type de revendication entrante UPN**, la **Valeur de revendication entrante @adatum.com**, sélectionnez l'option **Autoriser l'accès aux utilisateurs avec cette revendication entrante**, puis cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Modifiez la règle Temp, puis copiez le langage des règles de revendication dans le presse-papiers.
9. Supprimez la règle Temp.
10. Créez une règle qui envoie les revendications à l'aide d'une règle personnalisée nommée **Règle d'accès utilisateur ADatum**.
11. Cliquez dans la zone **Règle personnalisée**, puis appuyez sur les touches Ctrl + V pour coller le contenu du presse-papiers dans la zone. Modifiez la première URL afin qu'elle corresponde au texte suivant, puis cliquez sur **Terminer** :

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn", Value =~
"^(?i).+@adatum\.com$"]=> issue(Type =
“http://schemas.microsoft.com/authorization/claims/permit”, Value =
“PermitUsersWithClaim”);
```

▶ Tâche 5 : Vérifier les restrictions et l'accessibilité à l'application prenant en charge les revendications

1. Sur PRS-DC1, ouvrez Internet Explorer, puis connectez-vous à **https://lon-svr3.adatum.com/adatumtestapp/**.
2. Vérifiez que **TreyResearch\April** n'a plus accès à l'application de test A. Datum.
3. Effacez l'historique de navigation dans Internet Explorer.
4. Connectez-vous à **https://lon-svr3.adatum.com/adatumtestapp/**.
5. Vérifiez que **TreyResearch\Morgan** a accès à l'application de test A. Datum. Morgan est membre du groupe Production.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR3**, **22414B-PRS-DC1** et **22414B-LON-CL1**.

Résultats : Dans cet exercice, vous devez avoir configuré une approbation de fournisseur de revendications pour TreyResearch sur Adatum.com ainsi qu'une approbation de partie de confiance pour Adatum sur TreyResearch. Vous devez également avoir vérifié l'accès à l'application prenant en charge les revendications d'A. Datum, puis avoir configuré l'application pour limiter l'accès à partir de TreyResearch aux groupes spécifiques. Enfin, vous devez avoir vérifié l'accès approprié.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MICROSOFT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quelle est la différence entre une approbation de fournisseur de revendications et une approbation de partie de confiance ?

Outils

- Console de gestion AD FS
- Autorité de certification d'infrastructure à clé publique (PKI)
- Windows PowerShell
- Gestionnaire de serveur

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 13

Planification et implémentation d'une infrastructure de gestion des droits relatifs à l'information (IRM)

Table des matières :

Vue d'ensemble du module **13-1**

Leçon 1 : Planification et implémentation d'un cluster AD RMS **13-3**

Leçon 2 : Planification et implémentation de modèles et stratégies AD RMS **13-22**

Leçon 3 : Planification et implémentation de l'accès externe aux services AD RMS **13-33**

Leçon 4 : Planification et implémentation de l'intégration d'AD RMS au contrôle d'accès dynamique **13-46**

Atelier pratique : Planification et implémentation d'une infrastructure AD RMS **13-54**

Contrôle des acquis et éléments à retenir **13-67**

Évaluation du cours **13-68**

Vue d'ensemble du module

La protection des informations et des données sensibles contre une utilisation négligente ou malveillante est l'un des principaux défis auxquels sont confrontées aujourd'hui les entreprises. Le nombre croissant de vols d'informations et l'augmentation de nouvelles exigences réglementaires mettent en évidence la nécessité de mieux protéger les contenus numériques. Le recours croissant aux ordinateurs dans la création et l'utilisation d'informations confidentielles, l'introduction d'une connectivité étendue via les réseaux privés et publics (Internet inclus) et l'apparition d'ordinateurs de plus en plus puissants ont fait de la protection des données des organisations un aspect essentiel de la sécurité.

Lorsque nous parlons de contenu numérique, il peut s'agir de rapports dynamiques de bases de données d'un portail d'information, de messages électroniques confidentiels, de documents de planification stratégiques, de rapports militaires ou d'autres fichiers sensibles. Pour aider les organisations à protéger cette propriété intellectuelle précieuse, Microsoft® a développé AD RMS (Active Directory® Rights Management Service) comme rôle de serveur principal, conçu pour aider à garantir la protection de ce type de données. Ce module décrit comment vous pouvez planifier et implémenter un déploiement AD RMS pour protéger le contenu.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- planifier et implémenter un déploiement AD RMS ;
- planifier et gérer l'accès et les modèles AD RMS ;
- planifier et implémenter l'accès externe aux services AD RMS ;
- planifier et implémenter l'intégration d'AD RMS au contrôle d'accès dynamique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification et implémentation d'un cluster AD RMS

À l'aide d'AD RMS et du client AD RMS, vous pouvez accroître la stratégie de sécurité d'une organisation en protégeant les informations au travers de stratégies d'utilisation permanentes, qui demeurent avec les informations, indépendamment de l'endroit où vous les déplacez. En outre, vous pouvez utiliser AD RMS pour empêcher que les informations confidentielles, telles que les rapports financiers, les spécifications de produit, les données client et les messages électroniques confidentiels, ne tombent intentionnellement ou accidentellement entre de mauvaises mains. Cette leçon décrit les concepts et les composants AD RMS, les scénarios d'utilisation, et l'implémentation et l'administration des services AD RMS.

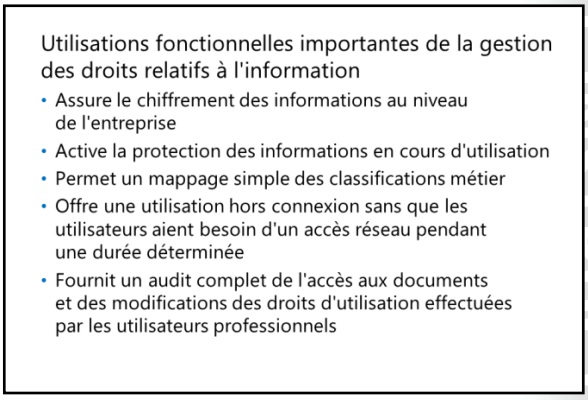
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- planifier, implémenter et gérer un cluster AD RMS.

Qu'est-ce que la gestion des droits relatifs à l'information (IRM) ?

La gestion des droits relatifs à l'information (IRM) est une technologie Microsoft qui fournit des autorisations de niveau fichier permanentes afin d'empêcher les utilisateurs non autorisés d'imprimer, de transférer ou de copier les informations confidentielles. Une fois que vous avez limité les autorisations pour un document ou un message à l'aide de cette technologie, les restrictions d'utilisation font partie du contenu du fichier et accompagnent le document ou le message électronique. La technologie IRM permet d'identifier explicitement ce qu'il est possible de faire ou pas avec les informations (qui se présentent généralement sous forme de documents ou de messages électroniques). En outre, elle vous permet de fournir les contrôles destinés à créer, afficher, modifier et distribuer ces informations séparément. En général, une entreprise utilise un système IRM pour protéger les informations d'un scénario B2B, comme celles relatives aux données financières, à la propriété intellectuelle ou aux communications de la direction.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La gestion des droits relatifs à l'information aide les entreprises et les utilisateurs à satisfaire deux besoins essentiels :

1. Autorisation restreinte pour les informations confidentielles. IRM empêche les utilisateurs non autorisés d'accéder aux informations confidentielles et de les réutiliser. Les organisations protègent leur propriété intellectuelle sensible en s'en remettant aux pare-feu, aux mesures de sécurité relatives à la connexion aux réseaux d'entreprise, et autres technologies réseau. L'un des défauts élémentaires de ces technologies est que les utilisateurs légitimes ayant accès aux informations peuvent les partager avec des personnes non autorisées. Il peut alors en résulter une faille de sécurité.
2. Confidentialité, contrôle et intégrité des informations. Les professionnels de l'information travaillent souvent avec des informations confidentielles ou sensibles. Avec IRM, les employés ne sont pas soumis à la discrétion de leurs collègues pour s'assurer que les éléments sensibles demeurent à l'intérieur de la société. IRM supprime la possibilité pour les utilisateurs de transférer, copier ou imprimer les informations confidentielles en permettant de désactiver ces fonctions dans les documents et les messages ayant des autorisations restreintes.

Pour les responsables informatiques, IRM simplifie la mise en application des stratégies d'entreprise existantes en matière de confidentialité des documents, de flux de travail et de rétention des courriers électroniques. Pour le PDG et le responsable de la sécurité, IRM réduit le risque que les utilisateurs non autorisés accèdent aux informations clés de l'organisation, que ce soit par hasard ou avec l'intention de nuire.

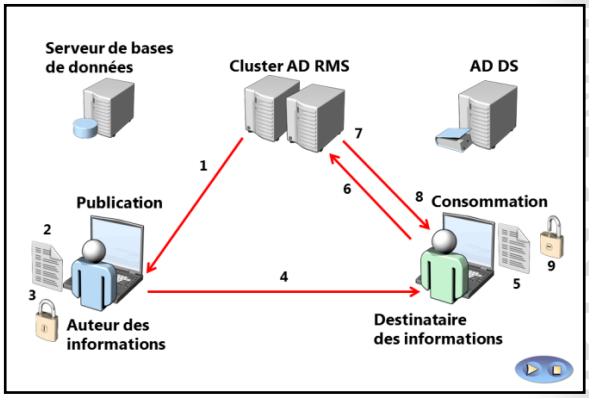
Les principales utilisations fonctionnelles d'IRM sont les suivantes :

- Chiffrement des informations au niveau de l'entreprise.
- Protection des informations en cours d'utilisation, comme la limitation des opérations copier et coller, le blocage de la copie d'écran et l'interdiction de l'impression.
- Stratégie des droits d'utilisation, qui permet un mappage simple des secteurs d'activité et des informations.
- Utilisation hors connexion sans avoir besoin d'accéder au réseau pendant une durée déterminée.
- Audit complet de l'accès aux documents et des modifications des droits d'utilisation effectuées par les utilisateurs professionnels.

La gestion des droits relatifs à l'information (IRM) peut être désignée sous différentes appellations : Gestion des droits de l'entreprise, Gestion des droits numériques de l'entreprise, Gestion des droits des documents et Gestion des droits de propriété intellectuelle.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fonctionnement d'AD RMS



AD RMS est une technologie IRM de Windows Server® 2012 qui fonctionne avec les applications AD RMS pour protéger les informations numériques contre l'utilisation non autorisée, aussi bien en ligne que hors connexion, à l'intérieur comme à l'extérieur du pare-feu. Les organisations peuvent utiliser AD RMS pour protéger les informations sensibles ou propriétaires, telles que les rapports financiers, les spécifications de produit, les données client et les messages électroniques confidentiels.

AD RMS applique les stratégies d'utilisation, lesquelles incluent les droits et les conditions d'utilisation qui demeurent associées aux informations indépendamment de leur emplacement. Les stratégies d'utilisation protègent les informations et améliorent la stratégie de sécurité d'une organisation. Comme AD RMS protège en permanence tout format binaire de données, les droits d'utilisation restent avec les informations, et pas sur le réseau de l'organisation. Quand un destinataire autorisé accède aux informations, que ce soit en ligne, hors connexion, à l'intérieur ou à l'extérieur de l'organisation, il applique les droits d'utilisation.

Les composants d'un système AD RMS comprennent un serveur Windows Server 2012 exécutant le rôle serveur AD RMS qui gère les certificats et les licences, ainsi qu'un serveur de base de données et un client AD RMS. Les systèmes d'exploitation Windows® 8 et Windows 7 incluent la version la plus récente du client AD RMS.

Le déploiement AD RMS fournit plusieurs avantages à une organisation :

- Protection des informations confidentielles. Vous pouvez assurer la protection des informations confidentielles à l'aide d'AD RMS afin de protéger les applications RMS, telles que traitements de texte, clients de messagerie et autres applications métier. Vous pouvez, ensuite, définir les personnes autorisées notamment à ouvrir, modifier, imprimer et transférer ces informations, et vous pouvez créer les modèles personnalisés de stratégie d'utilisation qui marquent les données comme confidentielles et en lecture seule. Vous pouvez alors appliquer directement ces modèles aux informations.
- Protection permanente. AD RMS assure une meilleure protection des informations en ajoutant les solutions de sécurité du périmètre existant, comme les pare-feu et les listes de contrôle d'accès (ACL). Il verrouille les droits d'utilisation du document et contrôle la façon dont le destinataire utilise les informations après son ouverture.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Technologie flexible et personnalisable. Pour utiliser AD RMS et protéger les informations confidentielles, les éditeurs indépendants de logiciels et les développeurs peuvent activer AD RMS pour n'importe quel serveur ou application, comme les serveurs de systèmes de gestion de contenu ou les serveurs de portail qui s'exécutent sur Windows ou autre système d'exploitation. En outre, cela permet aux éditeurs d'intégrer la protection des informations dans les solutions serveur, telles que la gestion des enregistrements et des documents, les passerelles de messagerie, les systèmes d'archivage, les flux de travail automatisés et l'inspection de contenu.
- Outils de développement et prise en charge des technologies du secteur. Les organisations peuvent créer des solutions fiables de protection des informations grâce à AD RMS. Il fournit les outils de développement et les technologies de sécurité du secteur, notamment le chiffrement, les certificats et l'authentification. Vous pouvez utiliser le kit de développement logiciel (SDK) AD RMS pour créer des solutions AD RMS personnalisées.

Fonctionnalités AD RMS

Utilisez le Gestionnaire de serveur de Windows 8 ou Windows PowerShell® pour configurer les fonctionnalités AD RMS suivantes :

- AD RMS. Le service de rôle AD RMS est obligatoire : il installe les composants AD RMS que vous pouvez utiliser pour publier et consommer le contenu protégé par des droits.
- Prise en charge de la fédération des identités. Le service de rôle de prise en charge de la fédération des identités est facultatif. Il permet aux identités fédérées d'utiliser le contenu protégé par des droits à l'aide des services AD FS (Active Directory Federation Services).

Lors de la publication du contenu, les clients AD RMS demandent et acquièrent de nouvelles licences pour protéger le contenu selon les droits et les conditions d'utilisation que vous choisissez, en tant qu'éditeur, d'autoriser pour le contenu à protéger.

Lorsque vous créez un document, puis choisissez de le protéger sous forme de droits, le client AD RMS acquiert un certificat de licence client, qui lui permet de protéger le contenu. Il utilise ensuite ce certificat de licence client pour chiffrer le document, ainsi que pour créer et signer une licence de publication, et associe ensuite une copie de la licence de publication au contenu chiffré. Le contenu est ainsi mieux protégé contre les utilisations incorrectes, même si vous le partagez avec d'autres employés à l'intérieur ou à l'extérieur de votre organisation.

Lorsque les autres utilisateurs reçoivent le contenu protégé, ils ne peuvent pas y accéder et l'utiliser sans recourir au préalable à une application à base de droits, telle que Microsoft Office, pour demander et obtenir une licence d'utilisateur final pour le contenu. Pour obtenir la licence d'utilisateur final, le client AD RMS doit d'abord déterminer si le destinataire se conforme aux stratégies définies dans la licence de publication que vous avez utilisée pour protéger le contenu. Si le client AD RMS détermine que l'utilisateur est habilité à accéder au contenu, le client AD RMS vérifie que l'utilisateur satisfait aux conditions indiquées dans la licence d'utilisation finale, qui peut restreindre certaines actions. Cette vérification garantit le niveau de protection des documents souhaité par leurs auteurs et leurs éditeurs, et atteste que les destinataires consomment les documents conformément aux stratégies de droits attribuées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous devez implémenter les serveurs AD RMS comme un ensemble de composants de service Web qui s'exécutent sur Microsoft Internet Information Services (IIS) et fonctionnent en liaison avec Microsoft SQL Server® et AD DS (Active Directory® Domain Services).

Quand un utilisateur protège un document et souhaite lui associer un niveau d'accès particulier pour les autres utilisateurs ou groupes, plusieurs étapes se présentent. Même si l'utilisateur final ne se rend pas compte de la plupart de ces processus, il est important que vous compreniez ce qui se passe quand un utilisateur recourt à AD RMS pour protéger un document.

La séquence suivante présente le flux de travail AD RMS :

1. Quand l'auteur protège initialement le contenu, le cluster AD RMS émet un certificat de compte de droits et un certificat de licence client, qui établit les informations d'identification AD RMS de l'auteur. L'auteur peut alors publier les informations qu'AD RMS permet de sécuriser.
2. L'auteur crée un fichier et spécifie les droits et les conditions d'utilisation, à l'aide d'une application AD RMS. AD RMS génère une licence de publication qui contient les stratégies d'utilisation, puis lie la licence de publication au fichier protégé.
3. L'application chiffre le fichier avec une clé symétrique, que la clé publique du cluster AD RMS chiffre. AD RMS insère la clé dans la licence de publication, puis la lie au fichier.
4. L'auteur distribue le fichier. Le courrier électronique, les bibliothèques de documents Microsoft SharePoint® et les serveurs de fichiers constituent des exemples de méthodes de distribution.
5. Le destinataire reçoit le fichier et l'ouvre à l'aide d'une application AD RMS. Si le destinataire ne possède pas un certificat de compte de droits sur l'ordinateur actuel, le cluster AD RMS émet le certificat.
6. L'application demande une licence d'utilisation via le cluster AD RMS qui a émis la licence de publication concernant les informations sécurisées.
7. Le cluster AD RMS confirme le niveau d'autorisation du destinataire, vérifie que le destinataire est un utilisateur nommé et crée une licence d'utilisation. Le serveur déchiffre la clé symétrique à l'aide de la clé privée du serveur, puis chiffre à nouveau la clé symétrique avec la clé publique du destinataire. Le serveur ajoute ensuite la clé symétrique chiffrée à la licence d'utilisation, qui comprend aussi, le cas échéant, la date d'expiration du contenu.
8. Une fois que le cluster AD RMS a confirmé le niveau d'autorisation du destinataire, le serveur de licences renvoie la licence d'utilisation à l'ordinateur client du destinataire.
9. Après avoir reçu la licence d'utilisation, l'application vérifie la licence et le certificat de compte du destinataire afin de déterminer si un certificat, dans l'une ou l'autre des chaînes d'approbation, exige une liste de révocation. Si tel est le cas, l'application recherche une copie locale de la liste de révocation en cours de validité. Le cas échéant, elle récupère une copie à jour de la liste de révocation. L'application applique ensuite les conditions de révocation appropriées dans le contexte en cours. Si les conditions de révocation autorisent l'accès au fichier, l'application affiche les données. Les utilisateurs peuvent alors appliquer les droits qui leur sont accordés.

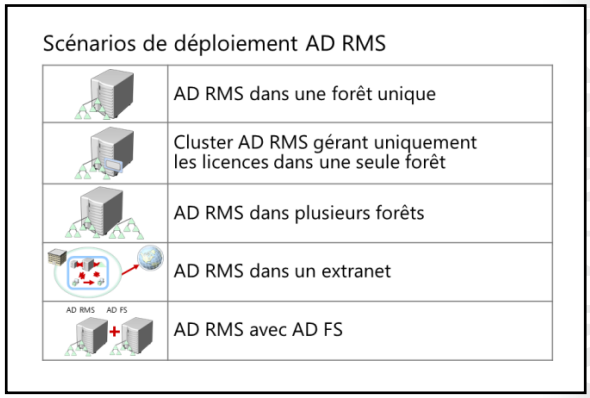
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Scénarios de déploiement AD RMS

Déploiement d'AD RMS dans une forêt unique

AD RMS requiert AD DS pour gérer les utilisateurs et les groupes et attribuer des privilèges spécifiques aux documents. Une gestion saine d'AD DS est essentielle pour un déploiement des services AD RMS.

En concevant votre environnement AD RMS, vous devez tenir compte des aspects suivants de votre implémentation AD DS :



- L'étendue d'une installation AD RMS est la forêt AD DS. Si des utilisateurs ont été déployés dans plusieurs forêts, chacune d'elles requiert son propre serveur AD RMS.
- Il est conseillé d'utiliser un nom virtuel pour le cluster de certification AD RMS. En général, ce nom est un nom de cluster à équilibrage de charge.

Déploiement d'un cluster d'administration de licences AD RMS

Le cas échéant, vous pouvez déployer des serveurs pour répondre à des exigences spécifiques en matière de licence, telles que :

- Prendre en charge les exigences spécifiques de gestion des droits d'un service. Par exemple, un groupe de votre organisation peut avoir un ensemble différent de modèles de stratégies de droits qui ne doivent pas être partagés avec toute l'organisation. Comme une forêt ne peut avoir qu'un seul cluster racine, la configuration d'un cluster racine distinct n'est possible que si vous créez une nouvelle forêt. Dans ce cas, vous pouvez installer un cluster d'administration de licences que vous dédiez aux besoins du groupe, puis définir séparément les modèles de stratégies de droits pour ce cluster d'administration de licences.
- Prendre en charge la gestion des droits pour les partenaires commerciaux externes, dans le cadre d'un extranet qui requiert une séparation marquée et un suivi des ressources des partenaires commerciaux spécifiques.

Déploiement d'AD RMS dans un environnement à plusieurs forêts

Si vous disposez d'approbations de forêt AD DS avec d'autres partenaires, vous devez créer un déploiement AD RMS à plusieurs forêts. Cela nécessite une installation AD RMS par forêt. Après l'attribution d'un certificat SSL (Secure Sockets Layer) sur chaque site Web qui héberge un cluster AD RMS, vous devez étendre le schéma de forêt AD DS pour inclure les objets AD RMS. Si vous utilisez Microsoft Exchange dans les forêts, vous disposez déjà de ces extensions. Enfin, toutes les forêts concernées devront approuver le compte de service AD RMS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Déploiement des services AD RMS dans un extranet

Un extranet est une extension du réseau de votre organisation vers une source externe, et vous pouvez étendre le cluster AD RMS à Internet afin que les utilisateurs puissent consommer le contenu protégé par des droits même lorsqu'ils ne sont pas connectés au réseau interne.

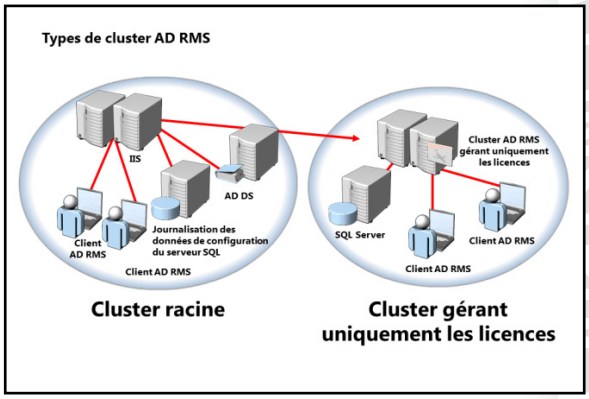
Déploiement d'AD RMS avec AD FS

Vous pouvez établir une approbation fédérée entre deux forêts à l'aide d'AD FS. Cette solution est également utile si les services AD RMS ne sont pas installés dans une forêt, mais que ses utilisateurs doivent consommer le contenu protégé par des droits d'une autre forêt. Nous recommandons cette méthode de connexion entre deux partenaires qui exécutent Windows Server® 2008 ou une version plus récente.

> **Question :** Les services AD RMS sont-ils implémentés dans votre environnement ? Si oui, quel scénario de déploiement utilisez-vous ? Si vous n'en utilisez pas actuellement, mais prévoyez de le faire à l'avenir, à quels scénarios de déploiement recourriez-vous ?

Composants AD RMS

Dans un cluster AD RMS, tous les serveurs AD RMS sont de l'un des deux types suivants : serveur de certification racine ou serveur de licences. Le premier serveur AD RMS d'une forêt AD DS assume le rôle de certificat racine Active Directory. Il ne peut y avoir qu'un seul serveur de certification racine dans chaque forêt Active Directory. Le serveur de licences est le rôle assumé par tout serveur AD RMS supplémentaire ou secondaire que vous ajoutez pour fournir des options de stratégie indépendantes à certains groupes au sein d'une forêt Active Directory.



Chaque composant joue un rôle dans le flux de travail AD RMS, comme le détaille le tableau suivant.

Composant serveur	Il exécute les tâches suivantes :
Cluster de serveurs de certification AD RMS	Vous l'utilisez pour administrer et configurer AD RMS. Il assure toutes les fonctions AD RMS majeures, y compris la gestion des licences, la publication, la certification de compte et la récupération. Chaque forêt AD DS comporte une limite d'un seul cluster de serveurs de certification AD RMS, ou *cluster racine*.
Cluster AD RMS gérant uniquement les licences	Les serveurs d'un cluster gérant uniquement les licences ne fournissent que les services de publication et de gestion des licences.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Composant serveur	Il exécute les tâches suivantes :
Service Web d'administration	Le serveur AD RMS héberge le service Web, que vous pouvez utiliser pour gérer AD RMS via la console d'administration AD RMS ou les commandes Windows PowerShell pour AD RMS.
Certification de compte	Les serveurs AD RMS génèrent des certificats de compte de droits qui associent les utilisateurs à des ordinateurs spécifiques.
Gestion des licences	Les serveurs AD RMS émettent les licences d'utilisateur final, qui permettent aux applications clientes AD RMS d'accéder au contenu protégé au sein des restrictions utilisateur que l'éditeur de contenu définit.
Publication	Les serveurs AD RMS créent aussi les certificats de licence client qui permettent aux éditeurs de contenu de définir les stratégies que vous pouvez énumérer dans une licence d'utilisateur final.
Précertification	Elle permet à un serveur de demander un certificat de compte de droits au nom d'un utilisateur afin qu'Exchange puisse attribuer une pré-licence de contenu aux utilisateurs de Microsoft Office Outlook®.
Localisateur de service	Fournit à AD DS l'URL (Uniform Resource Locator) de la certification de compte, de la gestion des licences et des services de publication de telle sorte que les clients AD RMS puissent les découvrir.
Composant client	**Il exécute les tâches suivantes :**
Client AD RMS	Windows Vista®, Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012 incluent le client. Il existe également un client complémentaire pour les versions antérieures du système d'exploitation Windows et du navigateur Internet Explorer®. Le client AD RMS fait office de composant client et interagit avec le cluster de serveurs de certificats AD RMS pour chiffrer et déchiffrer les données.
Application AD RMS	Certaines applications sont activées pour les services AD RMS et peuvent interagir avec eux. Un auteur peut utiliser ces applications pour créer un contenu et le protéger. En outre, les destinataires peuvent utiliser ces applications pour lire le contenu protégé.
Auteur	Utilisateur ou service qui génère le document protégé par des droits.
Certificat de licence client	Attribue une autorisation d'auteur pour publier un contenu protégé par des droits sans se connecter au réseau de l'entreprise.
Particulier	Utilisateur ou service qui accède au document protégé par des droits.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Composant serveur	Il exécute les tâches suivantes :
Licence d'utilisateur final	Cette licence déchiffre le contenu et applique les droits énumérés dans la licence d'un utilisateur spécifique.
Licence d'émission	Cette licence répertorie les utilisateurs qui peuvent déchiffrer le contenu protégé et les droits auxquels ils peuvent accéder.
Composants supplémentaires autres que les composants AD RMS	**Il exécute les tâches suivantes :**
AD DS	AD DS est un prérequis AD RMS, lequel utilise AD DS pour stocker les comptes d'utilisateurs et les groupes. Les clients interrogent AD DS pour que le point de connexion de service découvre les services AD RMS inscrits.
Base de données SQL Server	La base de données AD RMS stocke la configuration et les données du journal. Vous pouvez utiliser la base de données interne Windows à la place de SQL Server, mais elle ne sera pas prise en charge dans un environnement de production.

Démonstration : Installation d'un cluster AD RMS

L'objectif d'un déploiement AD RMS est de protéger les informations, indépendamment du trajet qu'elles empruntent ou du point où elles aboutissent. Une fois que vous ajoutez la protection AD RMS à un fichier numérique, la protection demeure avec le fichier. Par défaut, seul le propriétaire du contenu peut supprimer la protection du fichier. Le propriétaire accorde aux autres utilisateurs le droit d'exécuter certaines actions sur le contenu, comme afficher, copier ou imprimer le fichier.

Procédure de démonstration

Préparer l'infrastructure AD RMS

1. Ouvrez Utilisateurs et ordinateurs Active Directory, puis créez le compte **ADRMSSRVC**. Ajoutez le compte au groupe Admins du domaine.
2. Ajoutez les adresses de messagerie du compte d'utilisateur Hani Loza et du groupe Research, tous deux situés dans l'unité d'organisation Research. Les adresses sont, respectivement, hani@adatum.com et Research@adatum.com**.**
3. Créez et partagez un dossier nommé **ConfidentialResearch**, puis sélectionnez **Lecture/écriture** pour le groupe **Research**. Ensuite, créez et partagez un dossier nommé **Public**, puis sélectionnez **Lecture** pour le groupe **Tout le monde**.

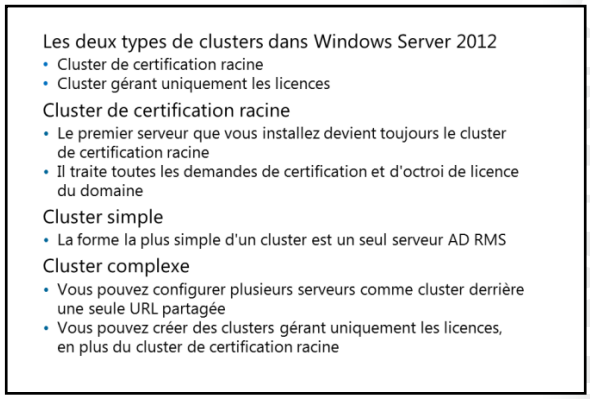
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Installer et configurer AD RMS

1. Démarrez l'Assistant Ajout de rôles et de fonctionnalités, puis installez le rôle AD RMS.
2. Une fois que l'Assistant s'est terminé avec succès, exécutez la configuration requise pour la tâche **Services AD RMS (Active Directory Rights Management Services)** dans **Gestionnaire de serveur**.
3. Une fois que la tâche de configuration s'est terminée avec succès, ouvrez la console AD RMS.

Options de configuration des clusters AD RMS

Un cluster AD RMS est un serveur unique exécutant AD RMS ou un groupe de serveurs qui partagent les demandes de publication et de gestion de licences AD RMS provenant des clients AD RMS. La forme la plus simple d'un cluster est un seul serveur AD RMS. Dans les déploiements plus complexes, vous pouvez configurer plusieurs serveurs comme cluster derrière une seule URL partagée.



Lorsque vous configurez le premier serveur AD RMS d'une forêt Active Directory, ce serveur devient toujours le cluster racine. Vous pouvez configurer plusieurs serveurs, puis les ajouter au cluster AD RMS à tout moment.

Vous pouvez configurer deux types de clusters dans les services AD RMS Windows Server 2012 :

- les clusters de certification racine, qui gèrent toutes les demandes de certification et de gestion des licences pour le domaine AD DS dans lequel vous installez le cluster ;
- les clusters gérant uniquement les licences, dans lesquels les serveurs ne fournissent que les services de publication et de gestion des licences.

La plupart des entreprises déploient des clusters gérant uniquement les licences pour répondre aux exigences spécifiques en matière de licence spécifiques, comme :

- Prise en charge des exigences uniques de gestion des droits d'un service. Par exemple, un groupe de votre organisation peut avoir un ensemble différent de modèles de stratégies de droits qu'ils ne peuvent pas partager avec le reste de l'organisation. Comme une forêt ne peut avoir qu'un seul cluster de certification racine, la configuration d'un cluster racine distinct n'est possible que si vous créez une nouvelle forêt. Dans ce cas, vous pouvez configurer un cluster gérant uniquement les licences qui soit dédié aux besoins du département, puis définir des modèles distincts de stratégies de droits pour ce cluster gérant uniquement les licences.
- Prise en charge de la gestion des droits pour les partenaires commerciaux externes, dans le cadre d'un extranet qui requiert une séparation marquée et un suivi des ressources des partenaires commerciaux spécifiques.
- Suppression des tâches de gestion des licences du cluster de certification racine.

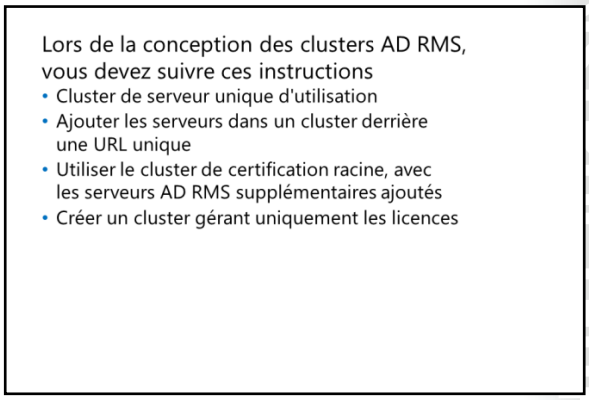
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous ne pouvez pas équilibrer la charge entre les clusters de certification racine et les clusters de gestion des licences. Pour cette raison, nous vous recommandons d'utiliser uniquement un cluster de certification racine, pas un cluster gérant uniquement les licences, et d'associer les serveurs AD RMS supplémentaires au cluster de certification racine. Le cluster (ou serveur) de certification racine est le premier composant d'un déploiement AD RMS, et tous les autres composants en dépendent, mais chaque forêt Active Directory ne peut en avoir qu'un. Le cluster de certification racine exécute tous les services AD RMS, y compris le service de certification de compte qui fournit les certificats de compte de droits aux clients AD RMS. Vous pouvez ajouter des serveurs à l'installation d'AD RMS pour créer un cluster de certification racine, que vous pouvez ensuite utiliser pour la redondance et l'équilibrage de charge.

Un cluster gérant uniquement les licences est facultatif, et ne fait pas partie du cluster de certification racine. Il est sous-inscrit sous le cluster de certification racine. Un cluster gérant uniquement les licences dépend du cluster de certification racine pour la certification et autres services. Pour établir la redondance et l'équilibrage de charge, vous pouvez ajouter des serveurs à l'installation afin de créer un cluster gérant uniquement les licences. Les clusters gérant uniquement les licences sont le plus souvent déployés pour répondre aux exigences spécifiques en matière de licence, telles que la prise en charge des exigences de gestion des droits d'un service. Par exemple, un groupe de votre organisation peut avoir besoin de modèles de stratégies de droits spécifiques auxquels aucun autre service ne peut accéder.

Instructions pour la conception de clusters AD RMS

Lors de la conception des clusters AD RMS, vous devez suivre ces instructions :



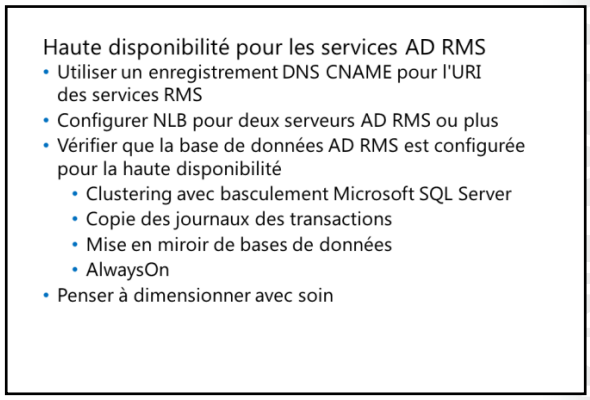
- Dans un environnement de petite taille aux ressources limitées, utilisez un cluster de serveur unique. Un cluster de serveur unique est suffisant pour un environnement où vous ne prévoyez pas une charge élevée sur les serveurs AD RMS.
- Ajoutez les serveurs d'un cluster derrière une URL unique pour fournir une haute disponibilité. Si AD RMS est une ressource critique, vous devez le rendre hautement disponible. Sachez qu'un cluster AD RMS n'est pas identique à un cluster de basculement dans Windows Server 2012. Dans le cas d'AD RMS, un seul serveur AD RMS unique peut être un cluster en tant que tel. Vous pouvez obtenir la haute disponibilité en ajoutant des serveurs au cluster AD RMS derrière une seule URL, mais pas en configurant un cluster de basculement dans Windows Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Utilisez uniquement un cluster de certification racine, chaque fois que possible, puis associez-lui des serveurs AD RMS supplémentaires. Vous ne pouvez pas équilibrer la charge entre les clusters de certification racine et les clusters de gestion des licences.
- Créez un cluster gérant uniquement les licences pour un environnement complexe ou pour un environnement ayant des exigences spécifiques en matière de licence. Pour fournir l'équilibrage de charge et éviter d'avoir un seul point de défaillance, nous vous recommandons de séparer la fonctionnalité de gestion des licences en déployant un cluster gérant uniquement les licences.
- Assurez la redondance et l'équilibrage de charge pour la gestion des licences en ajoutant des serveurs à l'installation, puis en créant un cluster gérant uniquement les licences.

Configuration de la haute disponibilité pour les services AD RMS

Vous devez vérifier que votre infrastructure AD RMS est hautement disponible, dans la plupart des cas. Pendant les opérations quotidiennes, les applications telles que Microsoft Office n'ont pas besoin d'entrer en contact avec AD RMS pour consommer une licence active. Cependant, la perte d'AD RMS signifierait qu'un auteur ne peut pas créer de certificats de licence client pour un nouveau contenu ou que le système peut émettre de nouvelles licences d'utilisateur final. Par conséquent, la fourniture de la haute disponibilité est souhaitable.



Équilibrage de la charge réseau

La forme la plus simple d'un cluster est un seul serveur AD RMS. Dans les déploiements plus complexes, vous pouvez configurer plusieurs serveurs comme cluster derrière une seule URL partagée. Pour assurer une haute disponibilité du service, vous devez utiliser l'équilibrage de la charge réseau pour ces serveurs. Les clients AD RMS ne peuvent pas trouver correctement le cluster AD RMS configuré comme équilibrage de la charge réseau à moins que vous ne créiez un alias de service DNS (Domain Name System) ou un enregistrement de nom canonique (CNAME) pour l'URL du cluster AD RMS. Comme certaines tâches AD RMS, telles que l'extension de groupe, exigent la connectivité d'AD RMS avec un contrôleur de domaine de catalogue-groupe, vérifiez si l'accès redondant est disponible.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Serveurs de base de données

Les serveurs de cluster AD RMS s'intègrent étroitement au serveur de base de données. Le serveur de base de données AD RMS stocke la configuration, la journalisation et les informations AD DS utilisées par AD RMS. AD RMS utilise les bases de données suivantes :

- Base de données de configuration. La base de données de configuration est un composant essentiel d'une installation AD RMS. Elle stocke, partage et récupère toutes les données de configuration et autres informations nécessaires pour gérer la certification de compte d'un cluster, la gestion des licences et les services de publication. La façon dont vous gérez votre base de données de configuration affecte directement la sécurité et la disponibilité d'un contenu protégé par des droits. Chaque cluster AD RMS possède une base de données de configuration. La base de données de configuration du cluster racine contient la liste des identités d'utilisateurs Windows et chaque certificat de compte de droits. Si AD RMS gère la clé de cluster de manière centralisée, la paire de clés de certificat est chiffrée avec la clé de cluster AD RMS avant d'être stockée dans la base de données. Les bases de données de configuration des clusters gérant uniquement les licences ne contiennent pas ces informations.
- Base de données de journalisation. Pour chaque racine ou cluster gérant uniquement les licences, par défaut, AD RMS installe une base de données de journalisation dans la même instance de serveur de base de données que celle qui héberge la base de données de configuration. Cette base de données peut finir par occuper beaucoup de place. Par conséquent, vous devez disposer d'un plan pour maintenir les services et les performances à un niveau adéquat.

Bien que la fourniture de la haute disponibilité à la base de données AD RMS soit un service extrêmement important, un service immédiat et ininterrompu n'est pas toujours nécessaire. Votre scénario ne peut pas imposer que vous appliquiez un cluster de basculement SQL Server pour AD RMS, mais vous pouvez en utiliser un si le serveur est mis en cluster pour d'autres raisons. Le clustering avec basculement nécessite généralement au moins deux serveurs SQL Server et un sous-système de disque SAN (Storage Area Network). L'envoi de journaux est une alternative meilleur marché que le cluster de basculement, mais requiert de fait une certaine intervention manuelle en cas de défaillance SQL Server. Tant que le service de base de données peut récupérer en quelques minutes, la plupart des fonctionnalités AD RMS ne seront pas altérées. La mise en miroir de bases de données implique la répétition, aussi rapide que possible, sur la base de données miroir de chaque opération d'insertion, de mise à jour et de suppression intervenue sur la base de données principale. Vous pouvez exécuter cette répétition en envoyant un flux des enregistrements du journal des transactions actif au serveur miroir, qui applique les enregistrements du journal à la base de données miroir, dans l'ordre, et aussi rapidement que possible. La mise en miroir de bases de données fonctionne au niveau de l'enregistrement du journal physique. L'envoi de journaux et la mise en miroir de bases de données requièrent deux serveurs SQL. SQL Server 2012 possède une nouvelle fonctionnalité, Groupes de disponibilité AlwaysOn, qui remplacera la mise en miroir de bases de données dans les prochaines versions. Les groupes AlwaysOn autorisent jusqu'à quatre serveurs SQL pour héberger une base de données en miroir. Cependant, vous devez configurer ces quatre serveurs SQL dans un cluster de basculement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Windows Server 2012 présente une nouvelle conception du processus de configuration AD RMS pour permettre une meilleur prise en charge du déploiement distant d'AD RMS et des serveurs SQL. Dans les versions antérieures de Windows Server, l'installation d'AD RMS nécessitait que le compte utilisé pour installer le rôle serveur AD RMS bénéficiât des privilèges d'administrateur local sur tous les ordinateurs qui hébergeaient une installation de SQL Server pour la prise en charge d'AD RMS. La raison en était qu'AD RMS devait lire les paramètres de base de données SQL à partir du Registre Windows pendant le processus de configuration.

Pour Windows Server 2012, AD RMS présente désormais les conditions requises suivantes pour l'accès SQL Server :

- Le compte du programme d'installation d'AD RMS doit avoir les autorisations d'administrateur système dans l'instance SQL Server.
- Pour obtenir de l'aide lors de l'accès et de la recherche des instances SQL Server disponibles, le service SQL Server Browser doit également s'exécuter sur le serveur où vous envisagez d'installer AD RMS.
- AD RMS prend en charge les instances nommées SQL Server sur Windows Server 2008 R2 et Windows Server 2012. Pour utiliser les instances nommées SQL Server, le service SQL Server Browser doit s'exécuter sur le serveur de bases de données.
- L'ordinateur SQL Server qui prend en charge AD RMS doit avoir les exceptions de pare-feu activées pour les ports SQL Server identifiés. Par exemple, le service SQL Server Browser utilise le port 1434 du protocole UDP (User Datagram Protocol), et le port TCP SQL Server par défaut est 1433. Ces ports par défaut, s'ils sont utilisés pour votre installation SQL Server, doivent avoir les exceptions de port dans le Pare-feu Windows.
- Les ports TCP autres que par défaut doivent être activés pour les exceptions configurées avec votre installation SQL Server, s'ils souhaitent accéder aux instances SQL Server. Pour les instances SQL par défaut, le port TCP 1433 est généralement attribué. Si vous avez configuré les instances SQL Server destinées à être utilisées avec AD RMS de telle sorte qu'elles utilisent un port TCP non défini par défaut, ces ports doivent être activés pour les exceptions du Pare-feu Windows afin que le programme d'installation d'AD RMS puisse se connecter à votre installation SQL Server ciblée.

En outre, si vous souhaitez récupérer la base de données d'AD RMS dans un autre système, vous devez configurer votre base de données AD RMS pour utiliser un enregistrement DNS CNAME qui fait référence au serveur de bases de données. N'appelez pas le serveur de base de données par son nom propre. Utilisez un alias pendant l'installation pour pointer AD RMS vers le serveur de base de données approprié.

Dimensionnement d'AD RMS

L'évolutivité des serveurs de gestion des licences AD RMS doit être le premier aspect à prendre en compte. Les serveurs de licences sont impliqués dans l'émission de chaque publication de contenu ou licence d'accès, ainsi que dans la création des certificats de compte de droits de l'utilisateur. La charge qu'ils doivent gérer est proportionnelle à la taille du déploiement, au nombre de documents à protéger et à la fréquence de consommation.

AD RMS exige d'importantes ressources processeur, car il utilise le chiffrement pour générer et valider les certificats. En général, les capacités des stratégies d'accès centralisé du serveur AD RMS sont liées au processeur ; celui-ci offre une augmentation des performances presque linéaire jusqu'à 4 cœurs et une bonne évolutivité jusqu'à 16 cœurs. Huit cœurs fournissent un très bon rapport coûts/performances.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tests en laboratoire de Microsoft et les déploiements de production montrent que chaque cœur d'une UC serveur traditionnelle peut traiter 100 000 demandes de licence par heure en situation de charge maximale, ce qui peut se produire dans une grande entreprise. Cependant, en général, ciblez 50 % de la charge maximale, afin de permettre les éventuelles fluctuations. Dans ce cas, 50 000 demandes par heure doivent être la charge maximale pour chaque cœur du processeur.

Vous pouvez utiliser la mémoire vive (RAM) dans les serveurs AD RMS pour mettre en cache les certificats, stocker les demandes pendant leur traitement et gérer la file d'attente des demandes sortantes adressées à SQL Server. L'augmentation de la mémoire dans chaque serveur AD RMS entraîne une certaine réduction de la charge de l'UC et augmente la capacité de faire face aux demandes de pointe. Cependant, une RAM de 2 Go peut fournir une capacité de mise en cache conséquente et suffit dans la plupart des cas. Une RAM de 4 Go ou plus est nécessaire uniquement pour les serveurs ayant un nombre élevé de processeurs.

En général, une entreprise n'utilisera pas un disque local des serveurs AD RMS de manière intensive, à moins qu'elle n'utilise également une installation locale de SQL Server ou SQL Server Express (configuration non recommandée dans les environnements à charge élevée). Cependant, votre disque doit être à tolérance de panne pour fournir la disponibilité que la plupart des environnements requièrent. Par conséquent, un contrôleur RAID (Redundant Array of Independent Disk) deux disques est la recommandation minimale pour un serveur de production et représente une configuration qui devrait couvrir la plupart des scénarios.

La bande passante réseau peut constituer une limite pour les grands serveurs, car chaque demande de gestion des licences utilise entre 24 Ko et 30 Ko. Par conséquent, un serveur qui reçoit 200 000 demandes de licence par heure, peut utiliser plus de 10 Mo par seconde (Mbits/s) sur le réseau. Ce scénario est possible et peut se produire quand un message électronique protégé est envoyé à une grande entreprise et que de nombreux utilisateurs tentent de le lire simultanément. Un serveur haut de gamme peut aisément affaiblir une liaison 100 Mbits/s s'il fonctionne à des charges maximales. En outre, quand AD RMS émet les licences complexes, avec un grand nombre de droits individuels exprimés, chaque licence peut atteindre jusqu'à 1 Mo. Dans ce cas, un grand nombre de licences peut surcharger la capacité d'un réseau 1 Go par seconde (Gbits/s). Cela signifie que même si AD RMS peut évoluer vers un grand nombre de cœurs de processeur par ordinateur, l'interface réseau peut devenir un goulot d'étranglement pour les systèmes très importants. Nous vous recommandons de rester proche de la configuration recommandée, à savoir entre quatre et huit cœurs par serveur, puis d'ajouter un nouveau serveur chaque fois que nécessaire.

Planification de la gestion AD RMS

Windows Server 2012 spécifie trois rôles administratifs que vous pouvez utiliser pour déléguer le contrôle de votre environnement AD RMS. Vous pouvez ajouter ces rôles en tant que groupes de sécurité locaux quand vous installez le rôle AD RMS. Chacun des rôles possède un niveau d'accès différent à AD RMS.

Rôles administratifs AD RMS
- Administrateurs d'entreprise AD RMS
- Administrateurs de modèles AD RMS
- Auditeur AD RMS

Vous pouvez utiliser les rôles administratifs pour déléguer les tâches AD RMS sans leur donner le contrôle administratif complet de la totalité du cluster AD RMS. Nous vous recommandons de créer un groupe de sécurité Active Directory pour chaque rôle administratif, puis d'ajouter le rôle au groupe de sécurité local correspondant. De cette façon, vous pouvez mettre votre déploiement AD RMS à l'échelle sur plusieurs serveurs, sans ajouter des comptes d'utilisateurs spécifiques à chaque serveur AD RMS.

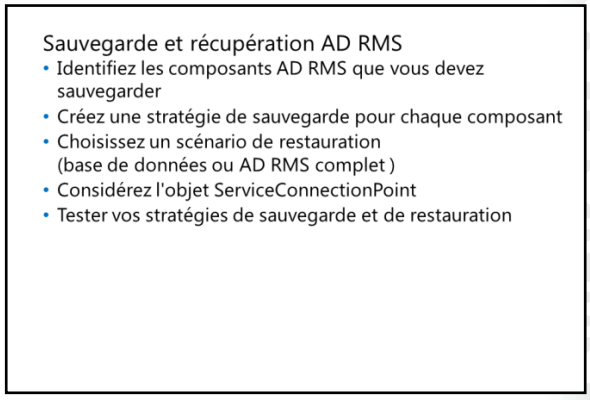
Nouveaux rôles administratifs :

- *Administrateurs d'entreprise AD RMS*. Les membres peuvent gérer l'ensemble des stratégies et paramètres AD RMS. Pendant la mise en service, AD RMS ajoute le compte d'utilisateur qui installe le rôle serveur AD RMS au rôle Administrateurs d'entreprise AD RMS. Il est recommandé d'attribuer ce rôle uniquement aux comptes d'utilisateurs ayant besoin du contrôle administratif AD RMS total.
- *Administrateurs de modèles AD RMS*. Les membres peuvent gérer les modèles de stratégies de droits. Plus particulièrement, ils peuvent lire les informations sur le cluster, ainsi que répertorier, créer, modifier et exporter les modèles de stratégies de droits.
- *Auditeurs AD RMS*. Les membres peuvent gérer les journaux et les rapports. Le rôle est en lecture seule ; les membres peuvent uniquement lire les informations sur le cluster et les paramètres de journalisation, et exécuter les rapports disponibles sur le cluster AD RMS.

Il est recommandé d'utiliser ces rôles et de ne pas attribuer le rôle Administrateurs d'entreprise AD RMS à plusieurs personnes. Vous ne devez pas utiliser le rôle fréquemment, excepté si vous installez AD RMS. Vous devez attribuer le rôle Administrateurs de modèles AD RMS aux utilisateurs qui gèrent les droits et les modèles de stratégies de droits, et vous devez attribuer le rôle Auditeurs AD RMS aux utilisateurs qui surveillent AD RMS.

Implémentation d'une stratégie de sauvegarde et de récupération AD RMS

Quand vous installez AD RMS, considérez ce qui se produirait si vous perdiez le service AD RMS. Vous pouvez perdre le service de façon inattendue si l'un des composants AD RMS tombe en panne : la connexion intranet utilisée par le serveur AD RMS, le cluster de certification racine AD RMS, le cluster AD RMS gérant uniquement les licences ou même les serveurs de base de données qui hébergent les bases de données de configuration AD RMS.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous devez développer une stratégie de sauvegarde pour chacun des composants suivants, afin qu'AD RMS soit aussi disponible et fiable que possible :

- Connectivité intranet et Internet
- Pipelines de certification et d'octroi de licence
- Serveurs de base de données
- Services d'annuaire

Si vous devez restaurer AD RMS, vous pouvez :

- restaurer une base de données ;
- restaurer une précédente installation d'AD RMS.

 **Documentation supplémentaire :** Pour restaurer une base de données, suivez les procédures régulières de restauration de base de données sur SQL Server.

Consultez la page http://go.microsoft.com/fwlink/?LinkID=285335 pour la présentation des procédures.

Pour restaurer une précédente installation AD RMS, vous devez d'abord déterminer si le serveur défectueux était membre d'un cluster et s'il s'agissait du serveur de configuration racine. Si le serveur était membre d'un cluster, vous pouvez supprimer le nœud et le réparer, réinstaller le logiciel (si nécessaire) et joindre de nouveau le nœud au cluster comme s'il s'agissait d'un nouveau nœud. Si le serveur défectueux n'était pas membre d'un cluster, vous pouvez récupérer le serveur en corrigeant le problème sous-jacent (en acquérant un nouveau matériel, par exemple), en réinstallant le système d'exploitation et le logiciel AD RMS (si nécessaire) et en remettant en service le serveur.

Si le serveur était le serveur de configuration racine AD RMS et qu'AD DS possède un objet **ServiceConnectionPoint** pour AD RMS, le serveur tente de se mettre en service lui-même comme serveur sous-inscrit gérant uniquement les licences, ce qui ne fonctionne pas. Pour résoudre le problème, vous pouvez :

- supprimer manuellement l'objet **ServiceConnectionPoint** dans AD DS et redémarrer le processus de mise en service ;
- remettre le serveur en service.

Lorsque la page **ProvisionLicensing.aspx** s'affiche, remplacez le nom de page dans l'URL par **ProvisionCertification.aspx**, puis appuyez sur Entrée.

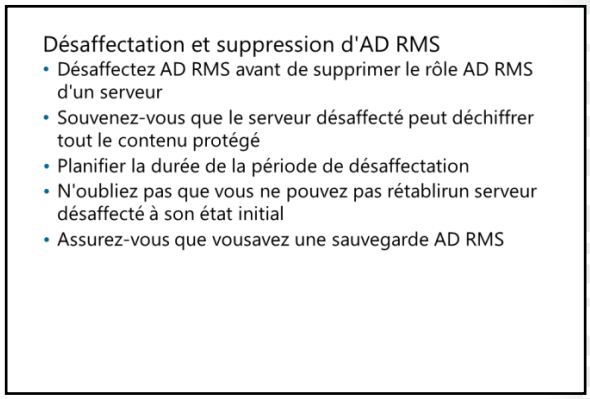
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lors de la conception d'une stratégie de sauvegarde et de restauration pour AD RMS, vous devez :

- sauvegarder et gérer la clé privée AD RMS dans le cadre du plan de sécurité, car AD RMS utilise les clés privées pour chiffrer le contenu ;
- conserver en permanence une sauvegarde de la base de données AD RMS ;
- fournir un lien Internet redondant pour AD RMS si vous desservez des clients externes ;
- sauvegarder tous les certificats qui sont sur AD RMS ;
- sauvegarder les modèles personnalisés qui sont sur AD RMS ;
- tester votre sauvegarde.

Désaffectation et suppression d'AD RMS

Si vous décidez de supprimer le rôle AD RMS d'un serveur, vous devez d'abord désaffecter AD RMS. Lorsque vous désaffectez AD RMS, le cluster AD RMS fournit une clé qui déchiffre le contenu protégé par des droits qu'il a publié précédemment. Vous pouvez utiliser cette clé pour sauvegarder le contenu sans protection AD RMS. Cette option est utile si vous cessez d'utiliser AD RMS dans votre organisation, mais que vous continuez d'avoir besoin des informations protégées.



Vous devez autoriser la désaffectation sur chaque serveur du cluster assez longtemps pour que les utilisateurs puissent enregistrer le contenu sans protection AD RMS, et que les administrateurs réseau et système puissent empêcher tous les clients AD RMS d'utiliser le service.

Après que vous avez activé la désaffectation, la console AD RMS affiche seulement la page **Informations relatives à la désaffectation du serveur** dans le volet de résultats. Vous ne pouvez rien faire d'autre pour administrer AD RMS.

Remarque : Vous ne pouvez pas inverser le processus. Après avoir désaffecté AD RMS, vous devez le supprimer complètement. Procédez ainsi via le Gestionnaire de serveur, puis réinstallez AD RMS.

Dans certains cas, vous devez retirer un serveur AD RMS ou supprimer complètement un cluster AD RMS. Au préalable, vous devez sauvegarder toutes les bases de données AD RMS que le serveur ou le cluster utilise, notamment la base de données de configuration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Après avoir sauvegardé les bases de données, vous pouvez supprimer le serveur. La façon de procéder varie selon le rôle du serveur et la topologie de l'installation AD RMS. Sélectionnez l'une des méthodes suivantes :

- Supprimer un serveur d'un cluster. Si vous souhaitez retirer un serveur AD RMS d'un cluster comportant d'autres serveurs qui sont encore actifs et requis, annulez la mise en service et désinstallez AD RMS du serveur que vous voulez retirer, puis supprimez le serveur de la rotation de l'équilibrage de charge. Pour plus d'informations sur la suppression d'un serveur, consultez la documentation sur l'équilibrage de charge.
- Retirer un serveur autonome. Si vous souhaitez retirer un serveur qui est le seul serveur d'un cluster, commencez par la désaffectation, l'annulation de la mise en service et la désinstallation du serveur. Puis, supprimez-le du réseau, et installez et mettez aussitôt en service AD RMS sur un serveur de remplacement. Configurez le nouveau serveur AD RMS, ce qui crée un nouveau cluster à serveur unique. Utilisez les mêmes URL et base de données de configuration que le serveur retiré. Jusqu'à ce que vous ayez installé et mis en service le serveur de remplacement, les utilisateurs ne peuvent pas lire le contenu protégé par des droits que le cluster original à serveur unique a publié.
- Remplacer un cluster AD RMS par un cluster AD RMS existant. Parfois, vous devrez peut-être retirer un cluster AD RMS et le remplacer par un autre cluster AD RMS existant, comme lorsque deux sociétés fusionnent et que les deux exécutent AD RMS. Dans ce cas, exportez le domaine d'utilisateur approuvé et le domaine de publication approuvé à partir du cluster AD RMS que vous retirez. Puis, importez le domaine d'utilisateur approuvé et le domaine de publication approuvé dans le cluster AD RMS toujours actif. Vous pouvez ainsi vérifier que les utilisateurs du cluster actif lisent le contenu que le cluster AD RMS retiré protégeait.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Planification et implémentation de modèles et stratégies AD RMS

AD RMS améliore la stratégie de sécurité d'une organisation en protégeant les informations au travers de stratégies d'utilisation permanentes, ou *droits d'utilisation* et *conditions*, qui demeurent avec les informations, indépendamment de l'endroit où celles-ci se trouvent. AD RMS protège constamment les données, de telle sorte que leurs droits d'utilisation restent avec les informations, et non comme droits résidant simplement sur le réseau d'une organisation. Les droits d'utilisation peuvent ainsi être appliqués après qu'un destinataire autorisé a accédé aux informations, que ce soit en ligne ou hors connexion, et à l'intérieur ou à l'extérieur de l'organisation. Un modèle de stratégie de droits est un document qui contient une stratégie d'utilisation prédéfinie. Vous pouvez ensuite appliquer le modèle pour protéger le contenu, et éviter ainsi d'avoir à définir et mettre en œuvre la stratégie manuellement. Votre application peut appliquer un modèle pour générer une licence d'émission plus facilement qu'en recréant une stratégie complète. Un administrateur du serveur AD RMS crée généralement les modèles, puis les enregistre dans la base de données de configuration, les copie sur un dossier partagé et les distribue à l'aide de la stratégie de groupe, de Systems Management Server ou d'un autre mécanisme. Cette leçon explique comment planifier et implémenter ces modèles et stratégies.

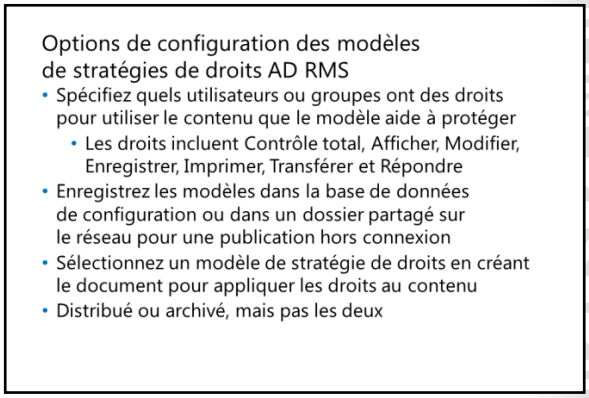
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- planifier, implémenter et gérer les stratégies d'utilisation et les modèles de stratégies de droits AD RMS ;
- planifier la façon dont les applications clientes peuvent implémenter ces stratégies efficacement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options de configuration des modèles de stratégies de droits AD RMS



Les droits AD RMS fournissent le moyen de contrôler comment un utilisateur peut accéder au contenu protégé par des droits, l'utiliser et le redistribuer. Les applications AD RMS ou les navigateurs appliquent certains droits exclusivement, tandis que le client AD RMS applique principalement d'autres droits, même si les applications peuvent appliquer leur propre interprétation des droits. Les droits appliqués par le client AD RMS contrôlent la façon dont vous pouvez utiliser les informations de licence, comme, par exemple, la possibilité ou non d'utiliser la licence pour chiffrer à nouveau le contenu précédemment déchiffré. Les applications AD RMS, telles que celles de Microsoft Office, interprètent et appliquent les droits qui contrôlent la façon dont les utilisateurs utilisent le contenu. Par exemple, les applications Microsoft Office appliquent le droit Afficher en permettant à un utilisateur de déchiffrer et d'afficher le contenu d'un document protégé si l'utilisateur a le droit Afficher. Les droits qu'AD RMS active par défaut, quand un utilisateur souhaite protéger le contenu, comprennent Contrôle total, Afficher, Modifier, Enregistrer, Imprimer, Suivant et Répondre. Les droits supplémentaire disponibles comprennent Exporter (Enregistrer sous), Répondre à tous, Extraire, Autoriser les macros, Afficher les droits et Modifier les droits. En outre, vous pouvez aussi créer des droits personnalisés.

Les modèles de stratégies de droits contrôlent l'accès en imposant les droits et conditions d'utilisation. Vous pouvez distribuer les modèles de différentes manières, selon les systèmes d'exploitation utilisés par une organisation. Les modèles de stratégies de droits contrôlent les droits des utilisateurs et des groupes pour une partie spécifique du contenu protégé par des droits. Les modèles peuvent inclure différentes conditions, telles que destinataires ou groupes AD DS spécifiques, durée de validité d'une licence d'utilisation du contenu et période pendant laquelle un utilisateur peut lire le contenu après la publication. Les droits AD RMS font partie du modèle de stratégie de droits.

Les modèles peuvent contenir les informations suivantes :

- un nom et une description ;
- les utilisateurs et groupes auxquels peuvent être accordées les licences de contenu ;
- les droits et les conditions associées accordés aux utilisateurs ;
- la stratégie d'expiration de contenu ;
- un ensemble de stratégies étendues ;
- la stratégie de révocation des modèles ;
- une liste de révocation ;
- un intervalle d'actualisation de la liste de révocation ;
- un fichier de clé publique pour la liste de révocation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Voici quelques exemples de modèles de stratégies de droits :

- Confidentiel. Vous pouvez utiliser ce modèle pour permettre aux employés d'afficher le contenu, mais leur interdire de le transférer, le copier ou l'enregistrer.
- Expire dans 30 jours. Vous pouvez utiliser ce modèle pour garantir que le contenu n'est plus valide après 30 jours. Les utilisateurs peuvent lire un appel d'offre ou le brouillon d'un document pendant une durée limitée.
- Doit être connecté pour consommer. Ce modèle garantit que les destinataires sont connectés à un serveur de licences et qu'ils n'utilisent pas les copies mises en cache d'une licence d'utilisation pour consommer le contenu. Vous pouvez l'utiliser si un modèle est l'objet de modifications et que vous souhaitez que le lecteur ne puisse accéder qu'en lecture seule à la dernière version. En outre, si un ordinateur est perdu ou volé, le contenu protégé par des droits est inaccessible à la personne qui a trouvé ou volé l'ordinateur.

Pour faciliter l'administration des modèles de stratégies de droits, AD RMS dans Windows Server 2012 propose un Assistant Créer un modèle de stratégie de droits distribué.

Question : Une organisation peut-elle utiliser AD RMS sans recourir aux modèles de stratégies de droits ? Si oui, quelles sont les limites ?

Planification d'une distribution des modèles AD RMS

Méthode	Procédure d'installation	Avantages	Inconvénients
Propagation automatique	• Aucune installation nécessaire • Exécutée comme tâche planifiée	• Intervention utilisateur minimale	• Prise en charge uniquement sur Windows Vista avec SP1 ou version ultérieure
Ordinateur local	• Utiliser un script pour la copie • Utiliser un pack d'installation Office 2003 personnalisé pour la configuration • Utiliser la stratégie de groupe, le Gestionnaire de configuration 2007 ou 2012, ou Systems Management Server 2003, ainsi qu'une tâche de distribution de modèles dans Windows Management Instrumentation (WMI)	• Permet aux utilisateurs de protéger les documents en utilisant les modèles de stratégies de droits sur l'ordinateur avec lequel ils sont connectés	• Requiert que vous mettiez à jour et mainteniez le modèle pour chaque utilisateur sur chaque ordinateur
Dossier partagé	• Définir le chemin d'accès interne pour localiser les modèles	• Fournit un seul point d'accès aux modèles de stratégies de droits	• L'absence de connexion des clients AD RMS peut *désactiver* les modèles et les supprimer ainsi du menu de l'utilisateur
Dossier partagé utilisant les dossiers hors connexion	• Définir le chemin d'accès interne pour localiser les modèles	• Offre un point unique à partir duquel accéder aux modèles de stratégies de droits et configurer l'utilisation du dossier hors connexion	• Requiert des paramètres de configuration supplémentaires • Requiert une formation de l'utilisateur final

Lors de la publication du contenu protégé, l'auteur choisit le modèle de stratégie de droits parmi les modèles disponibles sur l'ordinateur local. Pour que les modèles de stratégies de droits soient accessibles à la publication hors connexion, vous devez les déployer sur les ordinateurs clients à partir d'un dossier partagé. Dans Windows Vista avec Service Pack 1 (SP1), Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2 et Windows Server 2012, le client AD RMS gère automatiquement les modèles de stratégies de droits. AD RMS interroge un pipeline de distribution de modèles pour les mises à jour. Si vous ajoutez, modifiez ou supprimez un modèle de stratégie de droits, le client AD RMS détecte la modification, puis met à jour les modèles de stratégies de droits locaux lors de l'actualisation suivante.

Les ordinateurs qui exécutent Windows Vista avec SP1 ou version ultérieure enregistrent les modèles de stratégies de droits dans le dossier %localappdata%\Microsoft\DRM\templates. Les ordinateurs qui exécutent Windows XP, Windows 2000 ou Windows Server 2003 stockent les modèles dans le dossier %appdata%\Microsoft\DRM\templates.

Vous pouvez également enregistrer les modèles de stratégies de droits dans la base de données de configuration ou dans un dossier partagé. Les utilisateurs doivent avoir accès aux modèles afin de pouvoir accéder au contenu protégé par des droits. La plupart des administrateurs préfèrent placer les modèles de stratégies de droits sur chaque ordinateur client, ce qui permet aux utilisateurs de recourir aux modèles pour publier le contenu protégé par des droits aussi bien hors connexion qu'en ligne.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si vous modifiez un modèle de stratégie de droits sur le serveur AD RMS et que vous configurez le cluster AD RMS pour spécifier un emplacement de fichier pour stocker les copies des modèles de stratégies de droits, le serveur met à jour le modèle dans la base de données de configuration et dans le dossier partagé. Si vous utilisez un client AD RMS autre que Windows Vista avec SP1 ou version ultérieure, et que vous modifiez un modèle de stratégie de droits, vous devez redéployer le modèle sur les ordinateurs clients afin que les utilisateurs aient la version la plus récente disponible.

Si l'ordinateur exécute une version du client AD RMS antérieure à Windows Server 2008 et Windows Vista avec SP1, vous pouvez utiliser la stratégie de groupe, Microsoft System Center Configuration Manager 2007 ou 2012, ou Microsoft Systems Management Server (SMS) 2003 pour distribuer les modèles de stratégies de droits.

Depuis Windows Server 2008, vous pouvez distribuer les modèles de stratégies de droits aux ordinateurs clients et archiver tous les modèles de stratégies de droits que vous ne voulez pas distribuer. Par défaut, tous les modèles de stratégies de droits sont distribués. Vous ne devez pas supprimer un modèle de stratégie de droits, car, si vous le faites, le contenu protégé par le modèle de stratégie de droits n'est pas accessible.

Le tableau suivant répertorie les trois méthodes de distribution des modèles de stratégies de droits, ainsi que les avantages et les inconvénients de chacune d'elles.

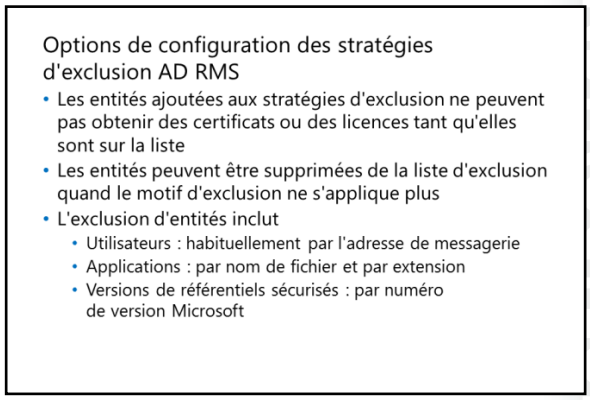
Méthode	Procédure d'installation	Avantages	Inconvénients
Propagation automatique	• Aucune installation nécessaire. • Exécutée comme tâche planifiée.	• Intervention utilisateur minimale.	• Prise en charge uniquement sur Windows Vista avec SP1 ou version ultérieure.
Ordinateur local	• Utiliser un script pour la copie. • Utiliser un pack d'installation Office 2003 personnalisé pour la configuration. • Utiliser la stratégie de groupe, le Gestionnaire de configuration 2007 ou 2012, ou Systems Management Server 2003, ainsi qu'une tâche de distribution de modèles dans Windows Management Instrumentation (WMI).	• Permet aux utilisateurs de protéger les documents en utilisant les modèles de stratégies de droits sur l'ordinateur avec lequel ils sont connectés.	• Requiert que vous mettiez à jour et mainteniez le modèle pour chaque utilisateur sur chaque ordinateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Méthode	Procédure d'installation	Avantages	Inconvénients
Dossier partagé	• Définir le chemin d'accès interne pour localiser les modèles.	• Fournit un seul point d'accès aux modèles de stratégies de droits.	• L'absence de connexion des clients AD RMS peut *désactiver* les modèles et les supprimer ainsi du menu de l'utilisateur.
Dossier partagé utilisant les dossiers hors connexion	• Définir le chemin d'accès interne pour localiser les modèles.	• Offre un point unique à partir duquel accéder aux modèles de stratégies de droits et configurer l'utilisation du dossier hors connexion.	• Requiert des paramètres de configuration supplémentaires. • Requiert une formation de l'utilisateur final.

Options de configuration des stratégies d'exclusion AD RMS



Vous pouvez implémenter les stratégies d'exclusion afin d'interdire à certaines entités la possibilité d'obtenir des certificats et de demander des licences. Windows Server 2012 AD RMS a trois façons de définir les stratégies d'exclusion : par utilisateur, par application et par version de référentiel sécurisé.

Une fois que vous implémentez une stratégie d'exclusion, toute licence d'utilisation de cette entité spécifique sera restreinte par sa présence dans la liste des exclusions. Si vous décidez de supprimer la restriction de l'entité, telle qu'une approbation en cours d'établissement ou en raison d'une nouvelle instruction de la direction, vous pouvez supprimer l'entité de la liste des exclusions. Lorsque vous ajoutez de nouveaux certificats ou recevez des demandes de nouvelles licences, l'exclusion ne s'applique plus à cette entité.

Assurez-vous que tous les certificats émis avant l'établissement de la liste des stratégies d'exclusion pour cette entité ont expiré lors de la suppression d'une entité d'une liste d'exclusion. Dans le cas contraire, les certificats anciens et nouveaux permettront que le contenu soit déchiffré, ce qui n'était peut-être pas l'intention de la direction de votre organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exclure des utilisateurs

Des conditions s'appliquent aux utilisateurs ajoutés à une liste d'exclusion. Vous pouvez notamment :

- Empêcher un compte d'utilisateur d'obtenir des licences d'utilisation d'un cluster AD RMS en spécifiant l'adresse de messagerie de l'utilisateur ou la chaîne de clé publique du certificat de compte de droits associé au certificat de compte de droits de l'utilisateur.
- Exclure les utilisateurs par leurs adresses de messagerie s'ils ne sont pas autorisés à consommer le contenu protégé par des droits, mais qu'ils ont des comptes de messagerie dans votre forêt AD DS.
- Exclure un utilisateur approuvé, mais dont les informations d'identification AD RMS deviennent compromises, en excluant uniquement la clé publique du certificat de compte de droits compromis. Lorsque vous procédez ainsi, AD RMS refuse les nouvelles demandes de licences d'utilisation qui impliquent ce certificat de compte de droits. Après que vous avez exclu un certificat de compte de droits, la prochaine fois où l'utilisateur tente d'acquérir une licence d'utilisation pour le nouveau contenu, la demande est refusée. Pour acquérir une licence d'utilisation, l'utilisateur doit récupérer un nouveau certificat de compte de droits avec une nouvelle paire de clés.
- Exclure les utilisateurs externes qui ne font pas partie de votre forêt AD DS, tels que les utilisateurs Windows Live ®, les utilisateurs fédérés et les utilisateurs identifiés par un domaine d'utilisateur approuvé. Vous pouvez aussi spécifier un certificat de compte de droits pour exclure leurs clés publiques.
- Exclure un utilisateur sur tous les clusters gérant uniquement les licences, si vous ajoutez un utilisateur à la liste d'exclusion du cluster racine AD RMS. Chaque cluster AD RMS possède des listes d'exclusion indépendantes.

Exclure des applications

Les conditions suivantes s'appliquent aux applications ajoutées à une liste d'exclusion :

- Vous pouvez spécifier la version d'une application AD RMS par rapport à laquelle AD RM vérifie toutes les demandes de licences. Les horodatages d'exclusion d'applications utilisent une licence avec la condition que la licence puisse uniquement être liée au contenu protégé par des droits pour lequel elle est émise, si l'application qui demande la licence ne figure pas sur la liste exclue.
- Les administrateurs système peuvent utiliser leur mécanisme habituel pour que les ordinateurs clients installent la mise à jour, lors du déploiement d'une mise à jour pour une application AD RMS. Les administrateurs peuvent alors déterminer les stratégies d'exclusion d'applications qu'ils définissent à l'aide des informations de version de l'application. Cette stratégie d'exclusion empêche AD RMS d'émettre des licences aux clients qui exécutent les versions précédentes du logiciel.
- Vous devez configurer l'exclusion d'applications sur chaque cluster pour lequel vous souhaitez qu'elle s'applique.
- Vous pouvez appliquer cette stratégie d'exclusion sur votre cluster, mais n'oubliez pas que les clients ne peuvent pas utiliser l'application exclue pour demander de nouvelles licences d'utilisation et les lier au contenu protégé. Cependant, les clients peuvent continuer à utiliser l'application exclue pour consommer les fichiers précédemment sous licence.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exclure les versions de référentiel sécurisé

Les conditions suivantes s'appliquent aux versions de référentiel sécurisé ajoutées à une liste d'exclusion :

- Les référentiels sécurisés stockent la clé privée d'un utilisateur. Si une faille est détectée dans une certaine version d'un référentiel sécurisé, Microsoft diffuse un nouveau référentiel sécurisé. Vous pouvez vérifier que les clients utilisent une version minimale du logiciel client AD RMS à l'aide de la version de référentiel sécurisé associée au client pour exclure les versions clientes AD RMS précédentes. Lorsque vous activez cette fonctionnalité, vous spécifiez la dernière version minimale du référentiel sécurisé que le service d'activation Microsoft a signée. Vous activez alors l'exclusion du référentiel sécurisé sur chaque cluster AD RMS où vous souhaitez qu'elle s'applique. AD RMS contrôle toutes les demandes de certification et d'octroi de licence pour s'assurer que le référentiel sécurisé satisfait aux critères de version minimale.
- Si vous activez une exclusion basée sur la version de référentiel sécurisé, les clients qui utilisent une version du logiciel de référentiel sécurisé plus ancienne que la version spécifiée ne peuvent pas acquérir de certificats de compte de droit ou de licences d'utilisation, car AD RMS refusera leurs demandes. Ces clients doivent installer une nouvelle version du logiciel client AD RMS pour acquérir un nouveau référentiel sécurisé qui utilise la version logicielle actuelle.
- Si un utilisateur ayant un référentiel sécurisé exclu s'est vu émettre précédemment des licences pour le contenu, il peut consommer ce contenu sans acquérir un nouveau référentiel sécurisé.

Démonstration : Ajout d'entités utilisateur à une stratégie d'exclusion

Vous pouvez aussi exécuter la tâche décrite par cette procédure avec Windows PowerShell :

1. Pour activer l'exclusion des certificats de compte de droits, à l'invite de commandes Windows PowerShell, tapez l'instruction suivante et appuyez sur Entrée :

```
Set-ItemProperty -Path <lecteur>:\ExclusionPolicy\User -Name IsEnabled -Value $true
```

2. Pour exclure le certificat de compte de droits d'un utilisateur en spécifiant l'adresse de messagerie de l'utilisateur, entrez l'instruction suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
New-Item -Path <lecteur>:\ExclusionPolicy\User -Name <nom_utilisateur>@<domaine>
```

   Où <lecteur> désigne le nom du lecteur Windows PowerShell, <nom_utilisateur> le nom d'utilisateur de l'utilisateur dont vous excluez le certificat de compte de droits et <domaine> la partie domaine de l'adresse de messagerie de l'utilisateur dont vous excluez le certificat de compte de droits.

3. Pour exclure le certificat de compte de droits d'un utilisateur en spécifiant la clé publique du certificat de compte de droits de l'utilisateur, entrez l'instruction suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
New-Item -Path <lecteur>:\ExclusionPolicy\User -PublicKey “<clé>”
```

   Où <drive> est le nom du lecteur Windows PowerShell et <clé> la clé publique du certificat de compte de droits de l'utilisateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Pour interrompre l'exclusion du certificat de compte de droits d'un utilisateur, à l'invite de commandes Windows PowerShell, entrez l'instruction suivante et appuyez sur Entrée :

```
Get-ChildItem -Path <lecteur>:\ExclusionPolicy\User
```

   Où <lecteur> est le nom du lecteur Windows PowerShell. Notez l'ID de l'utilisateur dont vous souhaitez arrêter l'exclusion du certificat de compte de droits.

5. À l'invite de commandes Windows PowerShell, entrez l'instruction suivante, puis appuyez sur Entrée :

```
Remove-Item -Path <lecteur>:\ExclusionPolicy\User\<ID_utilisateur>
```

   Où <lecteur> est le nom du lecteur Windows PowerShell et <ID_utilisateur> l'identificateur de l'utilisateur trouvé lors de l'étape précédente.

Procédure de démonstration

Exclure les certificats de compte de droit Créer un certificat de compte de droit

- Connectez-vous et protégez un document Microsoft Word. Enregistrez le document sur **\\LON-DC1\ConfidentialResearch**.

Créer une exclusion de certificat de compte de droits

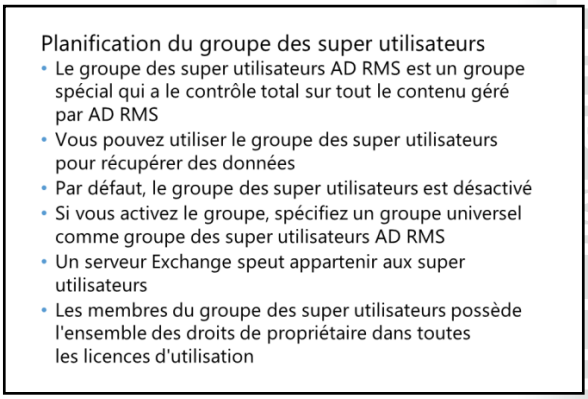
1. Ouvrez la console Administrateur AD RMS.
2. Dans le nœud **Stratégies d'exclusion**, **Utilisateurs**, cliquez sur **Activer l'exclusion d'utilisateurs**, puis excluez hani@adatum.com.

Arrêter l'exclusion de certificat de compte de droits pour des utilisateurs spécifiques

- Dans le nœud **Stratégies d'exclusion**, **Utilisateurs**, supprimez **hani@adatum.com**.

Planification du groupe des super utilisateurs AD RMS

Le groupe des super utilisateurs AD RMS est un groupe spécial qui a le contrôle total sur tout le contenu protégé par des droits et géré par le cluster. Les membres du groupe ont les droits de propriétaire complets dans toutes les licences d'utilisation émises par le cluster AD RMS sur lequel le groupe des super utilisateurs est configuré. Cela signifie que les membres du groupe peuvent déchiffrer n'importe quel fichier de contenu protégé par des droits et en enlever la protection.



Vous pouvez utiliser le groupe des super utilisateurs pour récupérer des données. Par exemple, vous pouvez l'utiliser si l'auteur d'un document quitte l'organisation ou si la totalité de l'accès à un document expire. Nous vous recommandons, si vous activez le groupe des super utilisateurs, d'activer également l'audit de succès et d'échec pour Auditer la gestion des comptes et Auditer l'accès au service d'annuaire. Cela vous permet de suivre les modifications d'appartenance. Nous vous recommandons également de n'activer le groupe des super utilisateurs que si vous devez récupérer des données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Par défaut, le groupe des super utilisateurs n'est pas activé et ne comprend pas de membres. Si vous l'activez, en définissant le paramètre **Super utilisateurs** dans la console AD RMS, vous pouvez spécifier un groupe universel AD DS à utiliser en tant que groupe des super utilisateurs AD RMS. Le groupe doit être dans la même forêt que l'installation d'AD RMS. Tous les comptes d'utilisateurs qui appartiennent au groupe spécifié comme groupe des super utilisateurs AD RMS obtiennent automatiquement les autorisations du groupe des super utilisateurs.

Si vous intégrez AD RMS à Microsoft Exchange Server 2010 ou Exchange Server 2013, vous devez exécuter des étapes supplémentaires. Pour permettre à Exchange Server de déchiffrer les messages et les pièces jointes que le cluster AD RMS protège, vous devez ajouter un compte d'utilisateur représentant Exchange Server au groupe des super utilisateurs AD RMS. Cependant, vous devez d'abord créer un groupe universel à extension messagerie (liste de distribution) qui contient le compte d'utilisateur Boîte aux lettres de remise fédérée (intitulé FederatedEmail.4c1f4d8b-8179-4148-93bf- 00a95fa1e042), ou vous devez ajouter ce compte à un groupe universel à extension messagerie que vous utilisez en tant que groupe des super utilisateurs dans AD RMS. Comme le compte d'utilisateur Boîte aux lettres de remise fédérée est une boîte aux lettres système, il n'est pas visible dans la console de gestion Exchange ou la console d'administration Exchange. Cependant, vous pouvez accéder à la boîte aux lettres de remise fédérée à l'aide de l'environnement de ligne de commande Exchange Management Shell.

Commandes Windows PowerShell équivalentes

Pour installer un groupe de super utilisateurs :

1. À l'invite de commandes Windows PowerShell, tapez les instructions suivantes et appuyez sur Entrée :

```
Set-ItemProperty -Path <lecteur>:\SecurityPolicy\SuperUser -Name IsEnabled -Value
$true
Set-ItemProperty -Path<lecteur>:\SecurityPolicy\SuperUser -Name SuperUserGroup -Value
<adresse_groupe>
```

   Où <lecteur> désigne le nom du lecteur Windows PowerShell et <adresse_groupe> l'adresse de messagerie du groupe universel que vous souhaitez indiquer comme groupe des super utilisateurs AD RMS. Par exemple, pour un lecteur Windows PowerShell nommé Z, pour indiquer un groupe nommé SecurityAdmins à l'adresse fabrikam.com comme groupe des super utilisateurs AD RMS, vous entrez les instructions suivantes à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Set-ItemProperty -Path Z:\SecurityPolicy\SuperUser -Name IsEnabled -Value $true
Set-ItemProperty -Path Z:\SecurityPolicy\SuperUser -Name SuperUserGroup -Value
securityadmins@fabrikam.com
```

2. Vous devez vérifier que vous activez le groupe des super utilisateurs uniquement lorsque vous en avez besoin. Désactivez-le quand vous n'en avez plus besoin.

Pour désactiver le groupe des super utilisateurs :

1. À l'invite de commandes Windows PowerShell, tapez l'instruction suivante et appuyez sur Entrée :

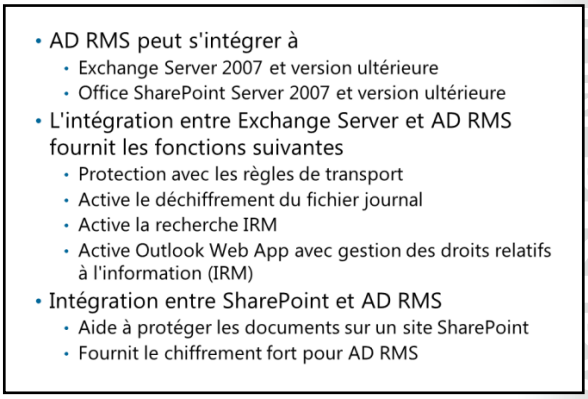
```
Set-ItemProperty -Path <lecteur>:\SecurityPolicy\SuperUser -Name IsEnabled -Value
$false
```

   Où <lecteur> est le nom du lecteur Windows PowerShell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification des applications clientes AD RMS

Vous pouvez également intégrer AD RMS à d'autres produits Microsoft pour fournir une protection automatique ou semi-automatique de différents types de documents. Le plus souvent, les entreprises intègrent AD RMS à Exchange Server et SharePoint.



Intégration d'AD RMS à Exchange Server

Exchange Server 2010 et Exchange Server 2013 peuvent être intégrés à la technologie de gestion des droits relatifs à l'information (IRM), qui peut aider les organisations à éviter de divulguer les informations confidentielles par courrier électronique. Associés à AD RMS dans Windows Server 2012, Exchange Server 2010 et Exchange Server 2013 peuvent aider à sécuriser automatiquement les messages contenant des informations confidentielles, tout en permettant d'analyser et d'archiver ces mêmes messages non chiffrés.

AD RMS active les fonctionnalités suivantes d'Exchange Server 2010 et Exchange Server 2013 :

- Règles de protection du transport, qui aident à protéger automatiquement les messages électroniques avec IRM.
- Déchiffrement du transport, qui donne aux agents approuvés l'accès sous la forme de texte en clair aux messages qu'IRM aide à protéger. Vous pouvez utiliser cette fonctionnalité pour archiver les messages et les pièces jointes, et les analyser pour détecter les programmes malveillants éventuels.
- Déchiffrement du rapport de journal, que vous pouvez utiliser pour la journalisation des messages protégés par IRM.
- Déchiffrement IRM pour la recherche, qu'Exchange Search peut utiliser pour indexer le contenu des messages qu'IRM aide à protéger.
- Microsoft Outlook Web Application avec la gestion des droits relatifs à l'information (IRM) activée, qui vous permet d'envoyer et d'ouvrir les messages qu'IRM aide à protéger, en utilisant Outlook Web Application dans un navigateur pris en charge, sans avoir à installer le logiciel client.
- IRM pour messagerie unifiée, que les utilisateurs peuvent utiliser pour écouter les messages vocaux protégés dans Outlook Web App, dans Outlook et au téléphone, et qui fournit une stratégie Ne pas transférer pour les messages vocaux privés.
- Le fait d'attribuer une pré-licence associe une pré-licence aux messages protégés. De cette façon, le client n'a pas besoin de s'adresser de façon répétée au serveur AD RMS pour récupérer une licence d'utilisation. Cette fonctionnalité permet également aux utilisateurs d'afficher hors connexion les messages et les pièces jointes qu'IRM aide à protéger, puis de consulter les messages dans Outlook Web App.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Intégration d'AD RMS à SharePoint

Si vous souhaitez intégrer SharePoint 2010 ou SharePoint 2013 à AD RMS, vous devez installer AD RMS et SharePoint sur des serveurs distincts. Vous ne pouvez pas installer AD RMS et SharePoint sur le même serveur, parce qu'ils doivent contrôler les mêmes ressources de serveur web.

Avec SharePoint, les utilisateurs peuvent collaborer facilement aux documents en les publiant sur un site SharePoint, à partir duquel ils peuvent accéder aux documents sur le réseau d'entreprise. L'objectif de l'intégration de SharePoint à AD RMS est de protéger les documents que les utilisateurs téléchargent depuis le serveur SharePoint.

Cependant, il est important de noter que l'intégration de SharePoint à AD RMS ne protège pas les documents tant qu'ils sont sur le serveur. Quand un utilisateur télécharge un document sur un site SharePoint, le serveur supprime toute protection jusqu'à ce qu'il reçoive une demande de téléchargement. À ce stade, le serveur applique les restrictions appropriées au document avant que l'ordinateur client ne le télécharge.

Utilisation du chiffrement fort pour AD RMS

AD RMS permet d'augmenter la puissance de chiffrement en invoquant le chiffrement fort via un mode avancé appelé mode de chiffrement 2.

AD RMS en mode de chiffrement fort fournit une implémentation mise à jour et améliorée pour prendre en charge un chiffrement et des clés de chiffrement beaucoup plus forts. Par exemple, en mode 2, le chiffrement RSA (Rivest-Shamir-Adleman) passe du chiffrement 1024 bits au chiffrement 2048 bits. Les clés de chiffrement sont également plus longues. L'ancien mode utilisait les clés 160 bits, alors que le mode de chiffrement fort utilise les clés 256 bits. En outre, il existe une option pour utiliser les normes de l'algorithme de hachage SHA-2 (Secure Hash Algorithm 2) (clés SHA-2/SHA-256).

Le chiffrement fort dans AD RMS permet à votre organisation de satisfaire la conformité réglementaire avec les normes de sécurité définies par le NIST (National Institute of Standards and Technology). NIST a publié un document « Special Publication 800-57 », qui recommande l'utilisation des clés RSA 2048 bits. Les agences fédérales américaines doivent se conformer aux recommandations du NIST, en accord avec les règlements gouvernementaux américains. En outre, beaucoup d'organisations privées et d'autres pays implémentent cette recommandation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Planification et implémentation de l'accès externe aux services AD RMS

De façon croissante, les organisations concluent des partenariats et autres relations commerciales avec les fournisseurs, les clients et les vendeurs. Ces relations requièrent souvent de partager des informations confidentielles par courrier électronique ou autre mécanisme de remise numérique. Ces informations confidentielles peuvent inclure les plans de projet et la propriété intellectuelle sensible. Les organisations impliquées dans ces relations ont rarement une infrastructure d'identité et de sécurité commune. Il en résulte une certaine difficulté à garantir que, lorsqu'une personne partage des informations confidentielles avec une personne de l'organisation partenaire, la communication est sécurisée. AD RMS fournit plusieurs solutions alternatives pour aider les organisations partenaires à partager les informations confidentielles tout en maintenant les infrastructures indépendantes.

Dans cette leçon, vous allez découvrir les options pour planifier et implémenter l'accès AD RMS pour les utilisateurs externes, et comment intégrer les applications à AD RMS.

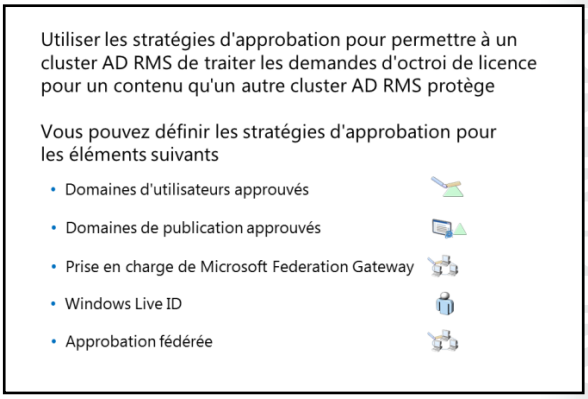
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les options pour permettre aux utilisateurs externes d'accéder à AD RMS ;
- décrire les options d'activation des applications pour les clients AD RMS ;
- planifier les domaines d'utilisateurs approuvés ;
- planifier les domaines de publication approuvés ;
- intégrer AD RMS avec la prise en charge Microsoft Federation Gateway ;
- partager les documents protégés par AD RMS à l'aide de Windows Live ID ;
- intégrer AD RMS à AD FS ;
- décrire les autres points à prendre en compte pour permettre aux utilisateurs externes d'accéder à AD RMS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options pour permettre aux utilisateurs externes d'accéder à AD RMS



Les utilisateurs externes sont les employés qui ne se connectent pas à votre réseau d'entreprise ou les utilisateurs d'autres organisations. Vous devez vérifier que les deux types d'utilisateurs peuvent accéder à AD RMS. Les utilisateurs peuvent partager le contenu protégé par des droits à travers les forêts AD DS internes ou externes. Cependant, quand une organisation avec plusieurs forêts AD DS déploie AD RMS, et qu'elle déploie des serveurs de certification dans chaque forêt qui héberge les comptes d'utilisateurs, elle nécessite la configuration de stratégies d'approbation. Vous pouvez prendre en charge plusieurs forêts et offrir l'accès aux utilisateurs externes à l'aide de l'une des méthodes suivantes :

- Domaines d'utilisateurs approuvés. Ce type de stratégie d'approbation permet à un serveur AD RMS d'approuver les certificats de compte de droits qu'un autre serveur de certification racine AD RMS génère. Il fournit également les licences d'utilisation aux utilisateurs dont les certificats de compte de droits proviennent du serveur AD RMS d'une autre organisation.
- Domaines de publication approuvés. Un domaine de publication approuvé permet qu'un cluster AD RMS émette des licences d'utilisation en fonction des licences de publication émises par un autre cluster AD RMS. Pour ajouter un domaine de publication approuvé, importez le certificat de licence serveur et la clé privée du serveur à approuver.
- Prise en charge de Microsoft Federation Gateway. La prise en charge de Microsoft Federation Gateway permet à un cluster AD RMS de se fédérer à Microsoft Federation Gateway. Microsoft Federation Gateway agit comme courtier d'approbation entre les organisations. En établissant cette relation de fédération, les organisations peuvent permettre aux applications telles que Microsoft Exchange Server 2010 SP1 et Exchange Server 2013 de créer des messages sécurisés AD RMS auxquels les utilisateurs appartenant à une organisation externe peuvent accéder.
- Informations d'identification Windows Live ID. Les utilisateurs qui reçoivent un contenu protégé par des droits, mais qui n'ont pas leur propre infrastructure AD RMS peuvent utiliser les informations d'identification Windows Live ID pour obtenir une licence d'utilisation. Le créateur de contenu peut envoyer un message électronique au destinataire, qui spécifie les droits attribués aux informations d'identification Windows Live ID du destinataire.
- Approbation fédérée. Vous pouvez utiliser une approbation fédérée pour authentifier les utilisateurs externes via AD FS. Une fois qu'AD FS a authentifié les utilisateurs, AD RMS applique les stratégies et fournit automatiquement aux utilisateurs externes les licences de contenu appropriées pour le contenu protégé.

Question : Dans quels scénarios devez-vous fournir l'accès externe à AD RMS ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

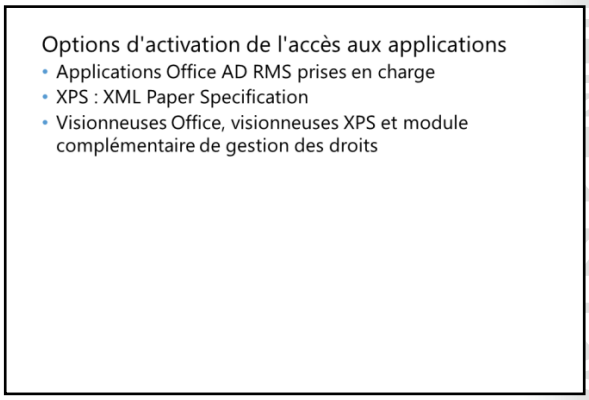
UTILISATION RÉSERVÉE À L'INSTRUCTEUR UNIQUEMENT

Options d'activation de l'accès aux applications pour les clients AD RMS

Applications Office AD RMS prises en charge

Microsoft Office a plusieurs applications, mais certaines applications des différentes suites Microsoft Office ne prennent pas en charge la gestion des droits.

Le tableau suivant décrit les applications AD RMS que les versions et éditions Microsoft Office spécifiques prennent en charge.



Applications AD RMS	Microsoft Office 2003	Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013	Microsoft Office Mobile
Microsoft Word	√	√	√
Microsoft Excel®	√	√	√
Microsoft PowerPoint®	√	√	√
Microsoft Outlook	√	√	√
Microsoft InfoPath®	Non fourni	√	Non fourni

Toutes les éditions Office ne peuvent pas créer des documents protégés par la gestion des droits, mais toutes les éditions des versions Office (Office 2003, Office 2007, Office 2010 et Office 2013) avec la gestion des droits activée peuvent consommer les documents protégés par la gestion des droits.

Le tableau ci-dessous illustre les fonctions de gestion des droits des différentes éditions Office et visionneuses associées avec la gestion des droits activée.

Version Office	Édition	Créer des documents Word, Excel, et PowerPoint protégés par IRM	Lire et modifier les documents Word et Excel protégés par IRM	Lire et modifier les documents PowerPoint protégés par IRM	Envoyer des messages électroniques protégés par des droits	Recevoir des messages électroniques protégés par des droits et y répondre	Créer ou utiliser des formulaires InfoPath protégés
Office 2007	Famille et Étudiant		√	√			
	Standard		√	√		√	
	PME		√	√		√	

(suite)

Version Office	Édition	Créer des documents Word, Excel, et PowerPoint protégés par IRM	Lire et modifier les documents Word et Excel protégés par IRM	Lire et modifier les documents PowerPoint protégés par IRM	Envoyer des messages électroniques protégés par des droits	Recevoir des messages électroniques protégés par des droits et y répondre	Créer ou utiliser des formulaires InfoPath protégés
	Professionnel		√	√		√	
	Professionnel Plus	√	√	√	√	√	√
	Entreprise	√	√	√	√	√	√
	Édition Intégrale	√	√	√	√	√	√
	Lecteurs Office téléchargeables		√ (lecture seule)				
Office 2010, Office 2013	Professionnel Plus	√	√	√	√	√	√
	Professionnel	√	√	√	√	√	√
	Familiale et professionnelle		√			√	
	Famille et Étudiant		√				
	Professionnel Éducation (Office 2010) Université (Office 2013)		√			√	
	Visionneuses Word et Excel		√ (lecture seule)				

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

XPS – XML Paper Specification

XPS (XML Paper Specification) est une spécification Microsoft qui décrit la conception du format de document XPS, représentation du papier électronique basée sur XML. Le format de document XPS est un format ouvert et multiplateforme qui permet aux utilisateurs de créer, partager, imprimer et archiver sans peine les documents paginés.

Les applications qui s'exécutent sur Windows XP et versions ultérieures peuvent créer un document XPS, et les utilisateurs peuvent afficher ces documents s'ils disposent de Windows XP ou d'un système d'exploitation plus récent, avec .NET Framework 3.0 SP1 ou l'une des visionneuses XPS autonomes disponibles en téléchargement. Windows Vista et les systèmes d'exploitation plus récents ont une visionneuse XPS installée par défaut.

L'extension de nom de fichier des documents XPS est .xps. Toute application qui peut imprimer des documents sur l'imprimante virtuelle Microsoft XPS Document Writer peut créer des documents XPS, ou vous pouvez les créer en utilisant l'option Enregistrer sous dans Office 2007 ou version plus récente, puis en choisissant Document XPS. Vous pouvez ainsi étendre la gestion des droits aux autres applications d'Office 2007 ou version plus récente. Par exemple, vous pouvez enregistrer une création Microsoft Visio® 2010 comme document XPS, ce qui garantit que le document fait l'objet d'une gestion des droits. Il en est de même pour Office 2007 ou les versions plus récentes de Microsoft Office Access®, Microsoft Office Publisher et Microsoft Office OneNote®. Si vous n'avez pas Microsoft Office 2007 ou version plus récente, ou que vous utilisez une version antérieure, vous pouvez également créer des documents XPS avec gestion des droits à l'aide de la visionneuse gratuite Microsoft XPS.

Visionneuses Office, visionneuses XPS et module complémentaire de gestion des droits

L'application des droits se produit au niveau de l'application, et une application AD RMS, comme Office 2003, Office 2007 ou Office 2010, est requise pour créer et consommer des informations protégées par des droits. Pour les utilisateurs qui n'exécutent pas une version Office compatible, Microsoft a créé la visionneuse Microsoft Office, la visionneuse XPS et un module complémentaire gratuit de gestion des droits pour Windows Internet Explorer qui permet aux utilisateurs d'afficher les informations protégées tout en continuant d'appliquer les droits.



Documentation supplémentaire : Ces outils peuvent être téléchargés gratuitement depuis le site Web de Microsoft, à l'adresse http://go.microsoft.com/fwlink/?LinkID=285336.

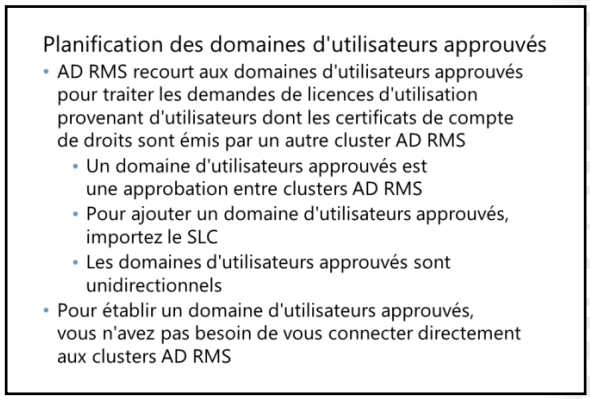
Module complémentaire de gestion des droits pour Internet Explorer

Le module complémentaire Windows Rights Management pour Internet Explorer offre un moyen aux utilisateurs des systèmes d'exploitation Windows pris en charge d'afficher, sans pouvoir les modifier, les fichiers avec une autorisation restreinte. Ces restrictions, comme pour tout contenu protégé par RMS, permettent aux auteurs d'empêcher que les documents sensibles, les informations basées sur le Web et les messages électroniques ne soient transférés, modifiés ou copiés par des entités non autorisées. Ces restrictions fournissent une protection, non seulement pendant que les informations sont en transit, mais même après leur réception par le destinataire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification des domaines d'utilisateurs approuvés

Par défaut, AD RMS ne traite pas les demandes de service d'un utilisateur si un autre cluster AD RMS a émis le certificat de compte de droits de l'utilisateur. Cependant, parfois vous devez autoriser AD RMS à traiter ces types de demandes, de telle sorte que les utilisateurs puissent partager les documents protégés par AD RMS entre organisations ayant leurs propres clusters AD RMS. Pour ce faire, vous pouvez ajouter des domaines AD RMS à la liste des domaines d'utilisateurs approuvés d'un cluster AD RMS.



Un domaine d'utilisateur approuvé désigne une approbation entre clusters AD RMS qui demande à un serveur de licences d'accepter les certificats de compte de droits d'un serveur AD RMS d'une autre forêt Active Directory. Une approbation AD RMS n'est pas identique à l'approbation Active Directory, mais elle est similaire, car elle permet à un environnement d'accepter les identités d'un autre environnement comme valides.

Pour ajouter un domaine d'utilisateur approuvé, importez le certificat de licence serveur à partir d'un cluster AD RMS que vous voulez approuver vers le cluster AD RMS qui délivre l'approbation. Pour ce faire :

1. Vérifiez que chaque forêt AD DS possède son propre cluster AD RMS.
2. Demandez à l'administrateur du domaine que vous souhaitez approuver d'exporter le certificat de licence du service du domaine à partir de leur cluster AD RMS. Puis, demandez-leur de vous envoyer le fichier de certificat, en tant qu'administrateur du cluster AD RMS d'approbation.
3. Importez le certificat en spécifiant l'emplacement du fichier. Vous ne transférez pas les informations de clé privée lorsque vous installez un domaine d'utilisateur approuvé.
4. Spécifiez les domaines de messagerie que vous souhaitez approuver pour chaque domaine d'utilisateur approuvé. Il s'agit d'une étape importante de sécurité parce que, si vous ne le faites pas, un utilisateur d'un domaine approuvé peut emprunter l'identité d'un utilisateur interne.

Comme les domaines d'utilisateur approuvés sont unidirectionnels, si les utilisateurs de chaque forêt doivent accéder aux documents de l'autre forêt, vous devez exécuter le processus deux fois (une fois par forêt).

Vous établissez une approbation hors connexion et, ainsi, vous n'avez pas besoin de vous connecter directement aux clusters AD RMS ou à leurs forêts Active Directory. Cependant, si vous souhaitez accéder au contenu de l'autre forêt, un utilisateur doit accéder au cluster de gestion des licences ayant émis la licence de publication. Par conséquent, le cluster AD RMS qui approuve et publie le contenu doit être accessible depuis Internet ou via un réseau privé.

Vous pouvez établir un domaine de confiance d'utilisateur approuvé entre les forêts qui n'ont pas d'approbation de forêt Active Directory entre elles. Cependant, si les deux forêts font partie de la même organisation, vous pouvez aussi vouloir établir une approbation de forêt Active Directory. Vous pouvez ainsi authentifier les utilisateurs distants avec leurs propres informations d'identification, plutôt qu'en activant l'accès anonyme à l'URL du pipeline correspondant dans le cluster AD RMS d'approbation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Une approbation de forêt rend possible l'extension de groupe, ce qui en retour facilite l'application de droits aux documents touchant un grand nombre de personnes. Si vous souhaitez activer l'extension de groupe, et que vous n'avez pas d'approbation de forêt, vous devez effectuer un travail supplémentaire conséquent pour synchroniser l'appartenance de groupe entre les forêts.

Dans une organisation ayant plusieurs forêts, vous pouvez synchroniser les listes d'adresses globales entre les forêts pour faciliter l'identification des destinataires par les créateurs de contenu.

Planification des domaines de publication approuvés

Un domaine de publication approuvé permet qu'un cluster AD RMS émette des licences d'utilisation correspondant aux licences de publication émises par un autre cluster AD RMS.

Lors de l'utilisation des domaines de publication approuvés, vous

- Pouvez utiliser un domaine de publication approuvé pour permettre à un cluster AD RMS d'émettre les licences d'utilisation correspondant aux licences de publication émises par un autre cluster AD RMS
  - La plupart des entreprises utilisent un domaine de publication approuvé uniquement si elles acquièrent une autre société qui a déjà AD RMS
- Doit partager la clé privée pour le serveur
- Doit configurer le Registre du client
- Doit synchroniser les -modèles de stratégies de droits

Par défaut, un cluster AD RMS peut émettre les licences d'utilisation qui correspondent uniquement aux licences de publication du même cluster. Cependant, si vous configurez un domaine de publication approuvé, le cluster AD RMS peut accorder les licences d'utilisation pour le contenu qu'un autre cluster AD RMS protège, dans la même organisation ou dans une organisation distincte. Vous pouvez configurer plusieurs domaines de publication approuvés pour un cluster AD RMS.

Un domaine de publication approuvé est utile si une société acquiert une autre société ayant déjà une implémentation AD RMS dont elle doit supprimer les privilèges d'accès ou si une société supprime un cluster d'une implémentation AD RMS. Avec un domaine de publication approuvé, AD RMS peut émettre les licences d'utilisateur final et les certificats de licence client à partir d'un seul et même emplacement. De même, les utilisateurs peuvent continuer à lire les documents que les deux clusters AD RMS protègent, même si vous annulez un cluster.

Remarque : Configurez un domaine de publication approuvé avec soin. Le partage de la clé privée requiert que vous approuviez fortement le destinataire.

Pour ajouter un domaine de publication approuvé :

1. Exportez le certificat de licence du service, la clé privée et tous les modèles de stratégies de droits du cluster AD RMS original vers un fichier protégé par mot de passe.
2. Importez ces éléments sur le cluster AD RMS du domaine que vous souhaitez approuver en spécifiant l'emplacement du fichier et le mot de passe.

Remarque : Si la clé privée se trouve dans un module de sécurité matériel (HSM), vous devez utiliser une procédure spéciale pour exporter la clé privée. Cependant, il se peut que cela ne soit pas possible sur certains modules de sécurité matériels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si un client doit obtenir une licence d'utilisation du cluster AD RMS local, vous devez configurer le Registre du client pour mapper le chemin d'accès d'origine du serveur de licences avec le nouveau chemin d'accès. De cette façon, les utilisateurs peuvent obtenir les licences d'utilisation sans accéder au serveur de licences original, lequel peut résider dans un réseau distinct ou ne plus exister.

Pour configurer le Registre et mapper correctement :

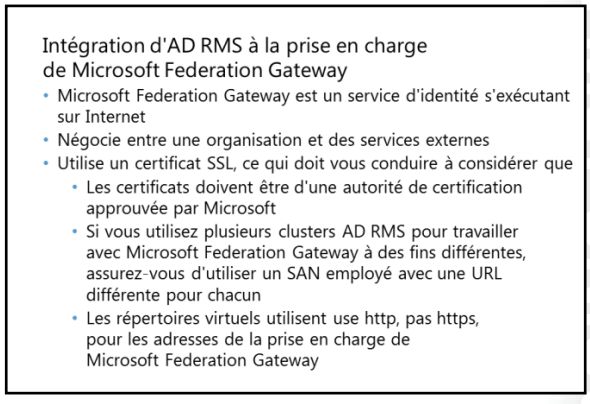
1. Ouvrez **regedit.exe**, et ajoutez la clé **DRM** et la sous-clé **AdminTemplatePath** avec la valeur définie sur le dossier local des modèles de l'utilisateur, **%LocalAppData%\Microsoft\DRM\Templates**.
2. Utilisez la clé de Registre : **HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\DRM**
3. Fermez **regedit.exe**.

Comme le serveur qui héberge les objets des licences d'utilisation effectue une extension de groupe, si vous utilisez un domaine de publication approuvé, vous n'avez pas besoin d'une approbation de forêt. Par conséquent, le domaine de publication approuvé nécessite un traitement administratif et du trafic moindre que les domaines d'utilisateur approuvés. Cependant, vous souhaiterez peut-être établir une approbation de forêt, afin de pouvoir synchroniser les listes d'adresses globales, ce qui facilite pour un créateur de contenu l'identification des destinataires.

Si vous avez un domaine de publication approuvé, vous devez synchroniser les modèles de stratégies de droits régulièrement pour qu'ils soient à jour dans le système de destination. Vous n'avez pas besoin de synchroniser les modèles si vous utilisez un domaine de publication approuvé pour remplacer un cluster que vous supprimez du service.

Si vous implémentez un domaine de publication approuvé, vous devez partager la clé privée d'un cluster. Cependant, ce partage présente un risque important, car un utilisateur malveillant peut utiliser la clé pour usurper l'identité d'un cluster AD RMS, puis déchiffrer les licences et le contenu que le cluster gère. Pour cette raison, vous implémentez généralement un domaine de publication approuvé au sein d'une seule et même organisation. La plupart des organisations implémentent un domaine de publication approuvé pour émettre les licences des documents qu'un cluster annulé protège.

Intégration d'AD RMS à la prise en charge de Microsoft Federation Gateway



La prise en charge de Microsoft Federation Gateway est une fonctionnalité AD RMS apparue dans le pack SP1 de Windows Server 2008 R2. La prise en charge de Microsoft Federation Gateway permet à un cluster AD RMS de s'unir à la passerelle Microsoft Federation Gateway, qui fait office de courtier d'approbation entre les organisations. En établissant ces relations de fédération, les organisations peuvent configurer les applications telles que Microsoft Exchange Server 2010 SP1 et Exchange Server 2013 afin qu'elles puissent créer des messages sécurisés AD RMS accessibles par les utilisateurs d'une organisation externe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Microsoft Federation Gateway est un service d'identité qui s'exécute sur Internet et qui sert de médiateur entre une organisation ou une entreprise et les services externes que l'organisation souhaite utiliser. La passerelle connecte les utilisateurs et autres identités aux services avec lesquels elle collabore, afin que les administrateurs n'aient à gérer qu'une seule relation de fédération d'identités pour permettre aux identités d'accéder à tous les services Microsoft qu'ils autorisent.

Microsoft Federation Gateway utilise les certificats SSL pour prouver la propriété des domaines et fournit aux applications une méthode simple et normalisée de création d'approbation entre organisations distinctes, car les organisations se fédèrent avec la passerelle, et non entre elles. Il est beaucoup plus facile pour une organisation d'établir des relations d'approbation avec plusieurs partenaires que d'utiliser la fédération classique de type un-à-un ou autres relations d'approbation. Vous pouvez contrôler l'étendue AD RMS en créant les listes vertes ou les listes d'exclusion des utilisateurs et domaines pour l'octroi des licences, ainsi qu'en spécifiant les domaines à même de recevoir les licences de publication. De cette façon, seules les organisations que vous approuvez reçoivent l'accès aux informations sécurisées.

Prenez en compte les points suivants avant d'installer AD RMS avec Microsoft Federation Gateway :

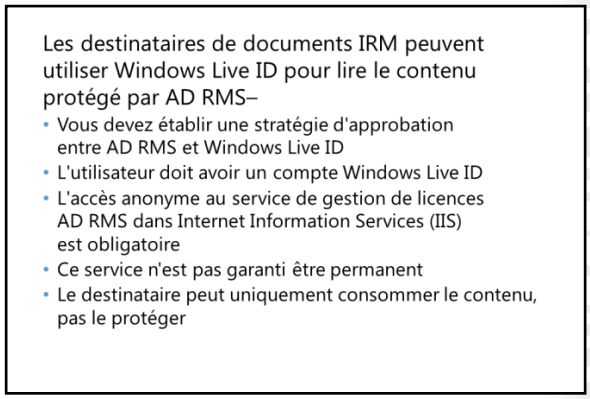
- Configurez le cluster AD RMS pour qu'il utilise une connexion chiffrée SSL recourant à un certificat approuvé par Microsoft Federation Gateway. Pour prouver la propriété du domaine que vous souhaitez fédérer, vous devez posséder le certificat SSL X.509 pour ce domaine. Ce certificat doit provenir de l'une des autorités de certification racine approuvées configurées dans Microsoft Federation Gateway.
- Vérifiez que le certificat SSL que vous inscrivez auprès de Microsoft Federation Gateway affiche la propriété de l'URL de l'extranet du cluster AD RMS. Si le cluster AD RMS est configuré avec une URL intranet différente de l'URL extranet, et si l'URL intranet n'est pas un nom de domaine auquel les utilisateurs peuvent accéder depuis Internet, vous devez installer le certificat SSL associé à l'URL extranet sur ce serveur AD RMS. Vous devez alors sélectionner ce certificat durant l'inscription auprès de Microsoft Federation Gateway.
- Assurez-vous que si le certificat SSL contient un autre nom de l'objet, la dernière entrée de celui-ci doit être le nom de domaine complet du domaine que vous souhaitez inscrire.
- Évitez les conflits en n'inscrivant pas votre cluster AD RMS auprès de Microsoft Federation Gateway à l'aide de la même URL que celle utilisée pour fédérer une autre ressource. Parmi les autres relations fédérées avec Microsoft Federation Gateway figurent, sans s'y limiter, les fédérations avec Microsoft Online et Microsoft Exchange Server. Si vous avez choisi l'URL que votre cluster AD RMS utilise comme URL externe à fédérer avec Microsoft Federation Gateway à une autre fin, vous devez inscrire le cluster AD RMS auprès de Microsoft Federation Gateway. À cette fin, créez et utilisez un certificat qui contient l'URL d'AD RMS comme dernière entrée de l'autre nom de l'objet, et ce avec un nom commun qui n'est pas le même que celui de la ressource inscrite. Par exemple, si le nom DNS de votre serveur AD RMS est resource.contoso.com et que ce nom a été utilisé par une autre ressource fédérée à Microsoft Federation Gateway, vous pouvez créer un certificat au format suivant pour éviter les conflits de fédération :

```
Copy Subject: CN=adrmsservice.adatum.com
 SAN:
DNS Name=adrmsservice.adatum.com
DNS Name=resource.adatum.com
```

- Configurez votre pare-feu pour permettre aux données http:// de le franchir, car les répertoires virtuels qui sont créés pour être utilisés par la prise en charge de Microsoft Federation Gateway recourent à http://. Cependant, les transactions http:// pour la prise en charge de Microsoft Federation Gateway utilisent la sécurité de niveau message.

Intégration d'AD RMS à Windows Live ID

AD RMS utilise l'adresse de messagerie de chaque utilisateur pour l'identification. Normalement, seuls les utilisateurs du même domaine de messagerie peuvent accéder au contenu protégé, ce qui signifie en général que seuls les utilisateurs de la même entreprise peuvent consommer un contenu protégé. Les rubriques précédentes expliquent comment configurer AD RMS pour travailler en dehors des limites de votre organisation, si l'autre partie dispose d'une infrastructure AD RMS distincte.



Cependant, si vous souhaitez partager le contenu protégé par AD RMS avec les utilisateurs qui n'ont pas d'infrastructure AD RMS locale, vous ne pouvez pas tirer parti de technologies telles que les domaines d'utilisateurs approuvés ou le domaine de publication approuvé.

Si vous souhaitez partager le contenu avec un utilisateur d'une organisation où AD RMS n'est pas installé, l'utilisateur peut accéder au contenu avec une adresse de messagerie Windows Live ID. Windows Live ID est un service Microsoft d'identité et de messagerie électronique basé sur le Cloud et qui permet à quiconque d'ouvrir un compte, puis de l'utiliser pour le courrier électronique et autres services. Microsoft fournit un service AD RMS pour les comptes Windows Live ID, et vous pouvez intégrer ce service à AD RMS en définissant une approbation.

Remarque : Microsoft fournit le service de certification et d'octroi de licence Windows Live ID comme service provisoire et se réserve le droit d'interrompre le service à tout instant.

Si vous installez une approbation avec Windows Live ID, un utilisateur AD RMS peut envoyer le contenu protégé par des droits à un destinataire ayant un Windows Live ID. Le destinataire peut lire le contenu, et l'expéditeur peut le protéger, puis appliquer des autorisations spécifiques pour les utilisateurs Windows Live ID.

Cette solution fonctionne uniquement si le nombre d'utilisateurs externes est réduit et qu'ils ont uniquement à lire le contenu, sans le protéger. Les destinataires ne peuvent pas protéger le contenu eux-mêmes.

Microsoft fournit un service de certification de compte qui utilise Windows Live ID pour établir le certificat de compte de droits de l'utilisateur. Si vous souhaitez que les utilisateurs de ce service titulaires d'un certificat de compte de droits puissent obtenir les licences d'utilisation auprès de votre cluster AD RMS, installez un domaine d'utilisateur approuvé qui accepte les informations d'identification à partir du service AD RMS en ligne de Microsoft.

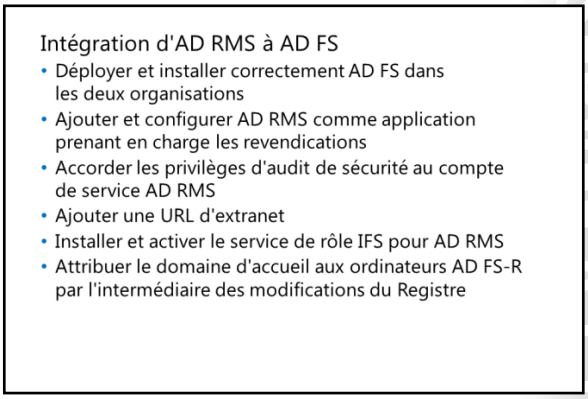
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les utilisateurs avec des certificats de compte de droits basés sur Windows Live ID ne pourront pas acquérir de licences à moins que vous ne configuriez dans IIS l'accès anonyme au service de gestion de licences AD RMS. Ce point est essentiel parce que, par défaut, le service de gestion de licences est configuré pour utiliser l'authentification Windows intégrée.

Après la configuration de l'accès Windows Live ID, vous pouvez exclure les utilisateurs de ce service en fonction de leurs adresses de messagerie, si nécessaire.

Intégration d'AD RMS à AD FS

Vous pouvez affecter AD RMS aux utilisateurs d'AD FS alors qu'ils se connectent via une approbation fédérée. Une organisation peut ainsi partager l'accès au contenu protégé par des droits avec une autre organisation, sans avoir à établir une approbation Active Directory ou une infrastructure AD RMS distincte.



AD FS est un rôle Active Directory, à savoir un service basé sur des normes et qui fournit la fédération d'identités en implémentant l'authentification par revendications entre les forêts. L'authentification par revendications est le processus d'authentification de l'utilisateur fondé sur un ensemble de revendications relatives à l'identité de l'utilisateur que contient un jeton approuvé. Une entité qui peut authentifier l'utilisateur par d'autres moyens, et qui est approuvée par l'entité exécutant l'authentification par revendications, publie le jeton.

Vous pouvez créer une fédération d'identités entre deux organisations en établissant l'approbation entre deux domaines de sécurité. Un serveur AD FS d'un côté, appelé Accounts, authentifie l'utilisateur via les méthodes standard d'AD DS, puis publie un jeton contenant une série de revendications sur l'utilisateur, identité de l'utilisateur incluse. De l'autre côté, appelé Resources, un serveur AD FS valide le jeton, puis délivre un autre jeton qui autorise les serveurs locaux à accepter l'identité revendiquée. Le système peut ainsi fournir un accès contrôlé à ses ressources ou services aux utilisateurs appartenant à un autre domaine de sécurité, sans requérir que les utilisateurs aient à s'authentifier à nouveau sur l'autre système, et sans que les deux systèmes aient à partager une base de données d'identités d'utilisateurs ou de mots de passe.

Pour bénéficier de la fédération d'identités, un service doit accepter les identités fédérées. AD RMS est l'un de ces systèmes, et il est conçu pour accepter les demandes de licences des utilisateurs distants via un agent d'authentification unique (SSO) ou une authentification unique Web. Puis, il les redirige vers le serveur de fédération local, qui est le serveur du côté ressources de la fédération, ou AD FS-R. Ce serveur, à son tour, demande à l'utilisateur de s'authentifier sur son propre côté, à savoir AD FS-A, le serveur Accounts du réseau de l'utilisateur. Ce serveur demande alors l'authentification à Active Directory et émet le jeton de sécurité correspondant. Le sous-système de sécurité de l'utilisateur présente ensuite ce jeton à l'authentification unique (SSO) Web, qui valide le jeton, puis fournit l'identité au serveur AD RMS. AD RMS émet alors les licences que l'utilisateur demande.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'intégration d'AD FS pour AD RMS présente quelques limites par rapport à d'autres solutions alternatives, telles que les domaines d'utilisateurs approuvés et le domaine de publication approuvé. L'une des limites significatives est son implémentation actuelle. AD RMS avec AD FS ne fournit pas les fonctions d'extension de groupe pour les groupes distants, ce qui signifie que les utilisateurs distants qui appartiennent aux groupes auxquels ont été attribués les droits sur un document ne pourront pas exercer ces droits, à moins que les droits n'aient été également attribués aux utilisateurs individuellement.

Une autre limite est que l'intégration AD FS dépend de la capacité du client à accéder aux documents protégés. Les anciens clients Windows Mobile ne peuvent pas s'authentifier via AD FS. Ces clients ne peuvent pas consommer les documents protégés par AD RMS, à moins qu'ils ne soient dans la même forêt que le serveur AD RMS qui a publié la licence de publication ou que les organisations qui utilisent les domaines d'utilisateurs approuvés ou le domaine de publication approuvé pour intégrer les infrastructures AD RMS de chaque forêt. Autre point à prendre en compte, la visionneuse de documents du module complémentaire Gestion des droits, qui, en général, est utilisée lorsque le destinataire n'a pas d'applications IRM, ne prend pas en charge l'authentification AD FS.

L'utilisation d'AD FS pour AD RMS crée certaines exigences d'infrastructure importantes, telles que l'accès aux serveurs AD RMS à partir d'Internet et de configurations clients spécifiques. Les problèmes clients incluent la nécessité de configurer les URL pour les serveurs de fédération distants dans la zone de sites de confiance d'Internet Explorer et d'ajouter les URL pour les serveurs de fédération locaux à la zone intranet.

Documentation supplémentaire : Les clients Windows Phone peuvent utiliser certaines fonctionnalités étendues, que décrit l'article à l'adresse http://go.microsoft.com/fwlink/?LinkID=285333. Tous ces paramètres clients disparates peuvent accroître les coûts du support technique.

Même avec ces limites, AD FS peut offrir des avantages majeurs, notamment dans les environnements où les organisations partenaires ne peuvent pas implémenter leurs propres serveurs AD RMS, car il offre des solutions qui requièrent une approbation minimale entre les organisations.

L'intégration d'AD RMS à AD FS requiert d'abord que vous établissiez une infrastructure AD FS entre un AD FS-A et un AD FS-R. Après la configuration d'AD FS dans les deux forêts pour les fédérer entre eux, vous devez également configurer AD RMS pour qu'il fonctionne avec AD FS. D'abord, ajoutez et configurez AD RMS comme application prenant en charge les revendications à l'aide de la console de gestion AD FS. Puis, autorisez le compte de service AD RMS à générer des événements d'audit de sécurité quand il utilise AD FS. Pour accorder les privilèges d'audit de sécurité au compte de service AD RMS, utilisez l'attribution des droits utilisateur de la stratégie de sécurité locale des serveurs AD RMS. Ensuite, spécifiez les URL extranet du cluster AD RMS dans la console de gestion AD RMS. Après avoir spécifié les URL extranet du cluster, vous pouvez ajouter le service de rôle de support de fédération d'identités au serveur AD RMS.

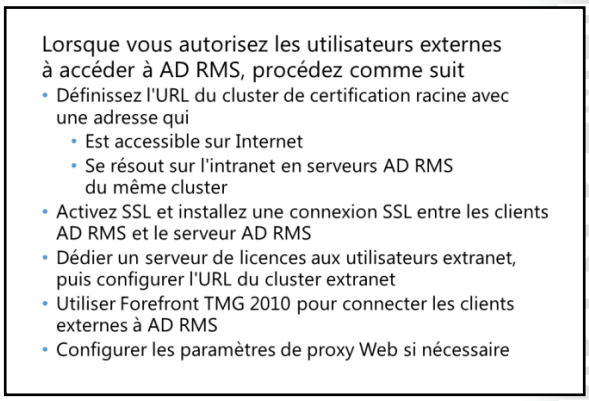
Après avoir ajouté le service de rôle de support de fédération d'identités, activez la prise en charge des identités fédérées pour le cluster AD RMS. Dès lors, la prise en charge des identités fédérées permet aux comptes d'utilisateurs d'utiliser les informations d'identification établies par une relation d'approbation fédérée via AD FS pour obtenir un certificat de compte de droits à partir d'un cluster AD RMS. Enfin, vous devez configurer les ordinateurs clients du domaine Active Directory FS-R pour la prise en charge de la fédération avec AD RMS. L'entrée du Registre HKLM\Software\Microsoft\MSDRM\Federation\FederationHomeRealm attribue le domaine d'accueil AD FS pour AD RMS.

Documentation supplémentaire : Pour plus d'informations, consultez http://go.microsoft.com/fwlink/?LinkID=285334.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour l'activation de l'accès des utilisateurs externes à AD RMS

Lors de la conception de l'accès à AD RMS, suivez les instructions ci-après pour améliorer la fiabilité et la sécurité :



- Activez les clients internes et externes pour qu'ils accèdent à l'URL de la licence de publication en définissant l'URL du cluster de certification racine avec une adresse à laquelle les clients peuvent accéder via Internet. En outre, elle doit se résoudre sur l'intranet en cluster de certification racine.
- Activez SSL et installez une connexion SSL entre les clients AD RMS et le serveur AD RMS.
- Dédiez un serveur de licences aux utilisateurs extranet, puis configurez l'URL du cluster extranet.
- Utilisez la sécurité du client Forefront TMG 2010 pour connecter les clients externes à AD RMS.
- Configurez les paramètres de proxy Web si nécessaire.

Si vous contrôlez l'accès aux ressources en dehors de la forêt locale en utilisant un serveur proxy Web, vous devrez peut-être configurer AD RMS pour qu'il utilise le proxy, si nécessaire. Par exemple, cela peut être nécessaire dans les cas suivants :

- Votre entreprise possède des clients de Windows Rights Management Services (RMS) 1.0 qui ne disposent pas d'une connexion Internet. Windows RMS 1.0 est antérieur à AD RMS. Microsoft doit activer les clients Windows RMS 1.0 sur Internet avant la première utilisation. Le client essaie d'utiliser le proxy de cluster AD RMS pour la demande d'activation, mais si le cluster AD RMS ne répond pas, le client tente d'obtenir les informations d'identification directement via une connexion Internet sur l'ordinateur local. Windows RMS 1.0 avec SP1 ou SP2 ne requiert pas l'activation des clients AD RMS sur Internet.
- Vous approuvez les certificats de compte de droits à partir des utilisateurs Windows Live ID. Le cluster AD RMS doit pouvoir valider l'utilisateur par rapport aux sites et services Windows Live ID.
- Votre entreprise possède plusieurs forêts qu'un serveur proxy Web sépare, et vous établissez des approbations entre elles. Ce scénario est similaire à celui avec Windows Live ID, en ce sens que le Registre des comptes d'utilisateurs sur lesquels le cluster AD RMS doit effectuer la validation se trouve derrière le serveur proxy Web.

Les clients AD RMS externes utilisent les URL du cluster extranet pour se connecter au cluster AD RMS aux fins de licence et de certification. Assurez-vous que vous inscrivez les URL dans le DNS, puis vérifiez que le DNS est disponible à partir d'Internet. Si vous ajoutez les URL pour un extranet cluster à un cluster AD RMS existant, les clients AD RMS doivent obtenir de nouveaux certificats de licence client. Les URL de cluster extranet font partie du champ URL-Extranet-Acquisition-Licence de la licence d'émission. En outre, les clients utilisent ces URL pendant le processus de découverte de service. Pour ce faire, vous devez au moins être membre du groupe local Administrateurs d'entreprise AD RMS ou d'un groupe équivalent.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4

Planification et implémentation de l'intégration d'AD RMS au contrôle d'accès dynamique

Parmi les nouvelles fonctionnalités de Windows Server 2012, le contrôle d'accès dynamique propose une nouvelle méthode aux auteurs de documents pour appliquer la protection IRM au niveau du stockage, au lieu de simplement s'en remettre à la sécurité des paramètres d'un administrateur dans les autorisations de partage et de service de fichiers NTFS. Lorsque vous associez AD RMS et le contrôle d'accès dynamique, cette association améliore la protection IRM pour sécuriser le transport et le stockage des documents sensibles.

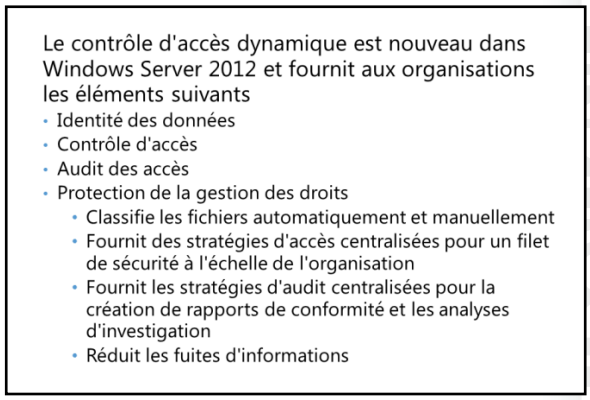
Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- planifier l'intégration d'AD RMS et du contrôle d'accès dynamique.

Qu'est-ce que le contrôle d'accès dynamique ?

Le contrôle d'accès dynamique dans Windows Server 2012 offre aux organisations de nouvelles méthodes pour contrôler l'accès aux données des fichiers et surveiller la conformité réglementaire. Le contrôle d'accès dynamique fournit les contrôles d'autorisation et d'audit de la prochaine génération, ainsi que les fonctions de classification qui vous permettent d'appliquer la gouvernance de l'information aux données non structurées des serveurs de fichiers.



Dans Windows Server 2012, vous appliquez la gouvernance des données aux serveurs de fichiers pour contrôler les personnes autorisées à accéder aux informations et pour auditer celles qui y ont accédé. Le contrôle d'accès dynamique permet les actions suivantes :

- Gérer l'accès aux données de manière centralisée selon les exigences métier et les besoins de conformité.
- Accéder aux informations qui doivent être auditées à des fins de conformité et d'analyse.
- Protéger les informations confidentielles où qu'elles aillent.
- S'assurer que les propriétaires de contenu sont responsables de leurs informations. Les administrateurs informatiques ne doivent pas faire office de bibliothécaires.
- Maintenir la productivité des professionnels de l'information.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

En règle générale, la sécurité des fichiers est gérée au niveau fichier et au niveau dossier. Les professionnels de l'informatique avaient peu de contrôle sur la façon dont les utilisateurs géraient quotidiennement la sécurité. Aujourd'hui, vous pouvez utiliser le contrôle d'accès dynamique pour limiter l'accès aux fichiers sensibles, indépendamment des actions des utilisateurs, en établissant et en appliquant la stratégie de sécurité des fichiers au niveau domaine. Puis, cette stratégie est appliquée à tous les serveurs de fichiers Windows Server 2012. Par exemple, si un ingénieur en électricité publie par erreur des dossiers confidentiels sur un dossier partagé, ces fichiers peuvent demeurer protégés contre l'accès par des utilisateurs non autorisés.

Avec le contrôle d'accès dynamique, l'audit de sécurité est plus puissant que jamais et les outils d'audit permettent de prouver plus facilement la conformité aux critères de réglementation, tels que la condition obligatoire selon laquelle l'accès aux informations sanitaires et biomédicales est correctement protégé et contrôlé régulièrement.

Le contrôle d'accès dynamique Windows Server 2012 fournit de nouvelles méthodes améliorées pour contrôler l'accès à vos fichiers tout en fournissant aux utilisateurs autorisés les ressources dont ils ont besoin :

- Identité des données. Le contrôle d'accès dynamique active la classification automatique et manuelle des fichiers à l'aide d'une infrastructure de classification des fichiers améliorée. Le contrôle d'accès dynamique comprend plusieurs méthodes pour appliquer manuellement ou automatiquement les balises de classification aux fichiers des serveurs d'une organisation.
- Contrôle d'accès. Le contrôle d'accès centralisé subvient aux besoins de votre gouvernance de l'information. Vous pouvez contrôler l'accès aux fichiers classés en appliquant des stratégies d'accès centralisées. Les stratégies d'accès centralisées sont une nouvelle fonctionnalité AD DS qui vous permet de définir et d'appliquer des exigences très spécifiques en matière d'attribution de l'accès aux fichiers classés. Par exemple, vous pouvez définir les utilisateurs qui peuvent avoir accès aux fichiers contenant les informations d'intégrité au sein de l'organisation en utilisant les revendications y compris le statut d'emploi (salarié à plein temps ou sous-traitant, par exemple) ou la méthode d'accès (ordinateur géré ou invité, par exemple). Vous pouvez même exiger une authentification à deux facteurs, telle que celle que fournissent les cartes à puce. La fonctionnalité du contrôle d'accès centralisé inclut la capacité de fournir une mise à jour automatique des accès refusés lorsque les utilisateurs rencontrent des problèmes pour accéder aux fichiers et aux partages.
- Audit des accès. Audit de l'accès aux fichiers pour l'analyse et la conformité légales. Vous pouvez auditer l'accès aux fichiers à l'aide des stratégies d'accès centralisées, pour identifier, par exemple, qui a accédé (ou tenté d'accéder) à des informations hautement confidentielles.
- Protection de la gestion des droits. Le contrôle d'accès dynamique prévoit le chiffrement basé sur la classification. Vous pouvez contrôler la protection à l'aide du chiffrement AD RMS automatique pour les documents sensibles. Par exemple, vous pouvez configurer le contrôle d'accès dynamique pour appliquer automatiquement la protection AD RMS à tous les documents contenant les informations HIPAA (Health Insurance Portability and Accountability Act). Cette fonctionnalité requiert un environnement AD RMS préalablement mis en service.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'ensemble des fonctionnalités du contrôle d'accès dynamique est basé sur les investissements d'infrastructure que les partenaires et les applications LOB peuvent utiliser ; les fonctionnalités peuvent être d'une grande valeur pour les organisations qui utilisent AD DS. Cette infrastructure comprend :

- un nouveau moteur d'autorisation et d'audit Windows, qui peut traiter les expressions conditionnelles et les stratégies centralisées ;
- la prise en charge de l'authentification du protocole Kerberos version 5 pour les revendications d'utilisateur et les revendications de périphérique ;
- améliorations de l'infrastructure de classification des fichiers ;
- prise en charge de l'extensibilité RMS afin que les partenaires puissent fournir des solutions de chiffrement des fichiers autres que les fichiers Microsoft.

Vue d'ensemble du processus de configuration du contrôle d'accès dynamique

Les règlements de conformité et métier guident la nécessité de protéger les informations dans les organisations de niveau d'entreprise et ont eu comme conséquence une tendance à la consolidation où un grand nombre d'informations des bureaux des utilisateurs et des partages de fichiers départementaux sont déplacées vers les serveurs de fichiers gérés de manière centralisée. L'initiative du déploiement et de l'application d'une stratégie d'autorisation peut s'expliquer par différentes raisons et provenir de plusieurs niveaux de l'organisation :

Processus de configuration du contrôle d'accès dynamique

- Mapper une demande métier à une stratégie d'accès centralisée
- Comprendre et traduire l'intention métier
- Exprimer la stratégie d'accès dans les constructions Windows Server 2012
- Déterminer les groupes d'utilisateurs, les propriétés des ressources et les types de revendication
- Créer des partages de fichiers sur les serveurs de fichiers
- Déterminer les serveurs auxquels la stratégie doit s'appliquer

- Stratégie d'autorisation à l'échelle de l'organisation. Généralement déclenchée par le bureau de sécurité des informations, cette stratégie d'autorisation répond à un souci de conformité ou à une exigence de très haut niveau de l'organisation ; elle est pertinente dans l'ensemble de l'organisation. Par exemple : les fichiers à l'impact métier élevé sur l'activité doivent être uniquement accessibles par les employés à plein temps.
- Stratégie d'autorisation départementale. Chaque service d'une organisation possède certaines exigences particulières en matière de gestion des données et qu'il souhaite appliquer. Cette situation est très répandue dans les organisations distribuées. Par exemple, le service financier peut souhaiter limiter l'accès aux serveurs de données financières à ses seuls employés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Stratégie spécifique de gestion des données. Cette stratégie se rapporte habituellement aux exigences de conformité et aux exigences métier, et vise à protéger les accès autorisés aux informations que vous gérez. Par exemple, vous pouvez souhaiter empêcher la modification ou la suppression des fichiers qui sont sous rétention. En outre, vous pouvez souhaiter empêcher la modification ou la suppression de fichiers sous découverte électronique (eDiscovery), processus dans lequel les données électroniques sont recherchées, localisées, sécurisées et retrouvées dans le but d'être utilisées comme preuves dans les procédures légales civiles ou criminelles.
- Nécessité de connaître la stratégie. Il s'agit d'un type de stratégie d'autorisation fourre-tout et, en général, vous l'utilisez conjointement à d'autres types de stratégie. C'est le cas notamment des fournisseurs qui souhaitent uniquement accéder aux fichiers en relation avec un projet sur lequel ils travaillent et les modifier.

  Dans les institutions financières, les cloisons entre les informations sont importantes pour que les analystes n'accèdent pas aux informations de courtage et que les courtiers n'accèdent pas aux informations d'analyse.

Pour mapper une demande métier à une stratégie d'accès centralisée :

1. Déterminez qu'une stratégie d'accès centralisée est nécessaire.
2. Exprimez clairement la stratégie d'accès.
3. Exprimez la stratégie d'accès dans les constructions Windows Server 2012.
4. Déterminez les propriétés de fichier requises par la stratégie.
5. Déterminez les types de revendication et/ou les groupes de sécurité que requiert la stratégie.
6. Déterminez les serveurs auxquels la stratégie doit s'appliquer.

Comprendre et traduire l'intention métier

Décidez du contenu auquel vous souhaitez appliquer les stratégies. Puis, créez une liste de toutes les stratégies que vous souhaitez appliquer à votre contenu. Par exemple, certaines stratégies courantes qui s'appliquent au service financier d'une organisation peuvent être les suivantes :

- Les documents financiers archivés doivent être accessibles uniquement en lecture par les membres du département financier.
- Les membres du service financier doivent pouvoir accéder aux documents uniquement dans leur propre pays.
- Seuls les administrateurs financiers doivent disposer d'un accès en écriture. Une exception est autorisée pour les membres du groupe FinanceException. Ce groupe doit disposer de l'accès en lecture.

Exprimer la stratégie d'accès dans les constructions Windows Server 2012

L'étape suivante du processus de planification consiste à traduire les stratégies requises en expressions. Une stratégie d'accès centralisée vise à permettre de traduire facilement les exigences d'une entreprise en autorisations.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Une stratégie centralisée dans Windows Server 2012 se compose des parties distinctes suivantes :

- Applicabilité. Condition qui définit les données auxquelles s'applique la stratégie, telle que :

  Resource.BusinessImpact=High

- Conditions d'accès. Liste d'une ou plusieurs entrées de contrôle d'accès qui définit les personnes autorisées à accéder aux données, notamment :

  Autoriser | Contrôle total | User.EmployeeType=FTE

- Exception. Liste supplémentaire d'une ou plusieurs entrées de contrôle d'accès qui définissent une exception pour la stratégie, comme :

  MemberOf (HBIExceptionGroup)

Déterminer les groupes d'utilisateurs, les propriétés des ressources et les types de revendication

Dans cette étape, vous décomposez les expressions que vous avez créées, puis déterminez les types de revendication, propriétés de ressources et revendications de périphérique que vous devez créer pour déployer vos stratégies.

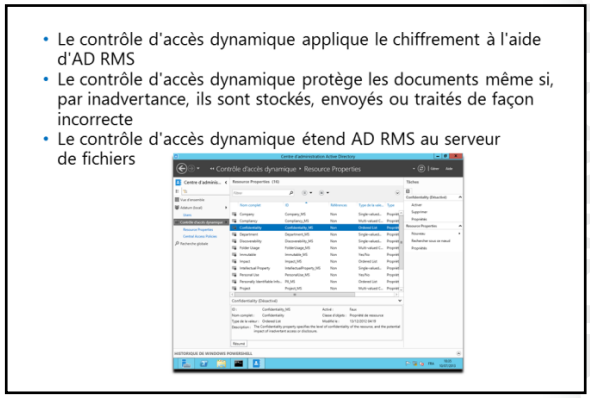
Créer des partages de fichiers sur les serveurs de fichiers

Dans cette étape, vous devez déterminer les partages de fichiers et les serveurs de fichiers.

Déterminer les serveurs auxquels la stratégie doit s'appliquer

L'étape suivante consiste à déterminer sur quels serveurs de fichiers vous souhaitez déployer les stratégies d'accès que vous avez choisies. Par exemple, vous pouvez avoir une stratégie d'accès financière que vous souhaitez déployer uniquement sur les serveurs de fichiers financiers.

Intégration d'AD RMS et du contrôle d'accès dynamique



L'atténuation du risque pour l'organisation constitue, en fin de compte, un objectif fondamental pour tous les services informatiques. Lors du traitement d'informations confidentielles, et de leur partage et diffusion via le courrier électronique et Internet, non seulement la sécurité des données est prééminente, mais il en est de même de la satisfaction des différents règlements de conformité, tels que le HIPAA (Health Insurance Portability Accountability Act) ou le PCI-DSS (Payment Card Industry Data Security Standard). Ces règlements commandent la façon dont les informations doivent être chiffrées. En outre, il existe de nombreuses raisons professionnelles de chiffrer les informations métier sensibles. Cependant, le chiffrement des informations est onéreux et peut affecter la productivité de l'entreprise. Par conséquent, les organisations ont tendance à avoir des approches et des priorités différentes pour chiffrer leurs informations.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez configurer le contrôle d'accès dynamique Windows Server 2012 pour chiffrer automatiquement les fichiers sensibles Microsoft Office, selon leur classification. Cette opération est effectuée en appelant la protection AD RMS pour les documents sensibles quelques secondes après qu'AD RMS a identifié le fichier comme sensible sur le serveur de fichiers et vous pouvez l'activer en exécutant les tâches continues de gestion de fichiers sur le serveur de fichiers.

Le chiffrement AD RMS offre une couche de protection supplémentaire pour les fichiers. Même si une personne avec accès à un fichier sensible envoie par inadvertance ce fichier par courrier électronique, le chiffrement AD RMS se maintient avec le fichier. Les utilisateurs qui souhaitent accéder au fichier doivent d'abord s'authentifier auprès d'un serveur AD RMS pour recevoir la clé de déchiffrement.

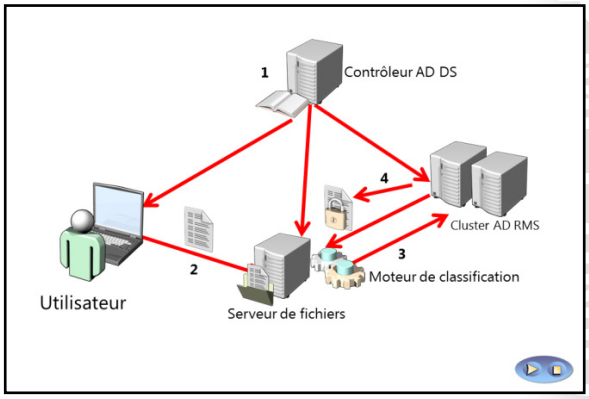
La prise en charge des formats de fichier autres que les formats Microsoft peut être disponible via des éditeurs de logiciels indépendants, qui écrivent le code à partir des attributs Microsoft. Une fois qu'un auteur a protégé un fichier par chiffrement AD RMS, ou que la protection intervient automatiquement via le déploiement du contrôle d'accès dynamique, les fonctionnalités de gestion des données, telles que la fonctionnalité de recherche ou la classification basée sur le contenu, ne sont plus disponibles pour ce fichier.

AD RMS permet aux personnes et aux administrateurs, via les stratégies IRM, de spécifier les autorisations d'accès aux documents, classeurs et présentations. Cela permet d'empêcher que les informations confidentielles ne soient imprimées, transférées ou copiées par des personnes non autorisées. Une fois que vous-même ou le contrôle d'accès dynamique avez restreint l'autorisation d'un fichier avec IRM, AD RMS applique les restrictions d'accès et d'utilisation, quel que soit l'emplacement des informations, car l'autorisation du fichier est enregistrée dans le fichier lui-même.

Le contrôle d'accès dynamique des services de fichiers et de stockage vous permet d'installer et de gérer les serveurs de fichiers qui fournissent des emplacements centralisés sur votre réseau, où vous pouvez stocker les fichiers et les partager avec les utilisateurs. Les administrateurs de serveurs de fichiers peuvent configurer les tâches de gestion de fichiers qui invoquent la protection AD RMS pour les documents sensibles quelques secondes après qu'AD RMS a identifié le fichier comme fichier sensible sur le serveur de fichiers, fournissant ainsi les ~~tâches~~ continues de gestion de fichiers sur le serveur de fichiers.

Comment AD RMS s'intègre au contrôle d'accès dynamique

Le contrôle d'accès dynamique vous permet de protéger automatiquement les informations confidentielles avec AD RMS. Par exemple, vous pouvez appliquer AD RMS si un fichier contient le mot *confidentiel*, comme suit :



1. Une règle est créée pour appliquer automatiquement la protection RMS à tout fichier contenant le mot *confidentiel*.
2. Un utilisateur crée un fichier avec le mot *confidentiel* dans le texte, puis l'enregistre.
3. Le moteur de classification du contrôle d'accès dynamique AD RMS, conformément aux règles définies dans la stratégie d'accès centralisée, découvre le document avec le mot *confidentiel*, puis lance la protection AD RMS en conséquence.
4. AD RMS applique un modèle et un chiffrement au document sur le serveur de fichiers, puis le chiffre et le classe.

Démonstration : Déployer le chiffrement des fichiers Office

Commandes Windows PowerShell équivalentes

Pour activer les propriétés des ressources, effectuez les tâches suivantes :

- Les applets de commande Windows PowerShell suivantes exécutent la même fonction que la procédure suivante. Tapez chaque applet de commande sur une seule ligne, même si elle se présente ici sur plusieurs lignes en raison de contraintes de mise en forme. Pour activer les propriétés des ressources, tapez la commande suivante à l'invite de commandes, puis appuyez sur Entrée :

```
Set-ADResourceProperty –Enabled:$true –Identity:"CN=Impact_MS,CN=Resource
Properties,CN=Claims Configuration,CN=Services,CN=Configuration,DC=adatum,DC=com"
Set-ADResourceProperty –Enabled:$true –Identity:"CN=PII_MS,CN=Resource
Properties,CN=Claims Configuration,CN=Services,CN=Configuration,DC=adatum,DC=com"
```

Pour créer la règle de classification à impact élevé, exécutez ce qui suit :

- Les applets de commande Windows PowerShell suivantes exécutent la même fonction que la procédure suivante. Entrez chaque applet de commande sur une seule ligne, même si elle se présente ici sur plusieurs lignes en raison de contraintes de mise en forme. Tapez l'applet suivante, puis appuyez sur Entrée :

```
Update-FSRMClassificationPropertyDefinition
$date = Get-Date
$AutomaticClassificationScheduledTask = New-FsrmScheduledTask -Time $date -Weekly
@(3, 2, 4, 5,1,6,0) -RunDuration 0;
Set-FsrmClassification -Continuous -schedule $AutomaticClassificationScheduledTask
New-FSRMClassificationRule -Name "Impact métier haut" -Property "Impact_MS" -
Description "Détermine si le document contient un impact métier haut basé sur la
présence de la chaîne 'Confidentiel Adatum'" -PropertyValue "3000" -Namespace
@(“C:\Finance Documents”) -ClassificationMechanism "Classifieur de contenus" -
Parameters @("StringEx=Min=1;Expr=Confidentiel Adatum") -ReevaluateProperty Overwrite
```

Pour protéger les documents avec AD RMS, exécutez ce qui suit :

- Les applets de commande Windows PowerShell suivantes exécutent la même fonction que la procédure suivante. Entrez chaque applet de commande sur une seule ligne, même si elle se présente ici sur plusieurs lignes en raison de contraintes de mise en forme. Tapez l'applet suivante, puis appuyez sur Entrée :

```
$fmjRmsEncryption = New-FSRMFmjAction -Type 'Rms' -RmsTemplate 'Administrateur
financier Adatum uniquement'
$fmjCondition1 = New-FSRMFmjCondition -Property 'PII_MS' -Condition 'Equal' –Value
'5000'
$date = get-date
$schedule = New-FsrmScheduledTask -Time $date -Weekly @('Sunday')
$fmj1=New-FSRMFileManagementJob -Name "Impact haut" -Description "Protection RMS
automatique pour les documents contenant des informations personnelles
d'identification hautes" -Namespace @('C:\Finance Documents') -Action
$fmjRmsEncryption -Schedule $schedule -Continuous -Condition @($fmjCondition1
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

Implémenter l'intégration AD RMS au contrôle d'accès dynamique

Activer les propriétés des ressources

- Ouvrez le **Centre d'administration Active Directory**. Sous **Resource Properties** (Propriétés de ressource) du **Contrôle d'accès dynamique**, attribuez une valeur aux propriétés **Impact** et **Personally Identifiable Information** (Informations d'identification personnelle). Publiez les deux stratégies dans **Global Resource Property List** (Liste des propriétés de ressources globales).

Créer les règles de classification

1. Ajoutez le rôle de service **Gestionnaire de ressources du serveur de fichiers des services de fichiers et de stockage**.
2. Dans Windows PowerShell, mettez à jour les **propriétés des ressources globales** pour permettre l'accès FSRM.
3. Ouvrez **FSRM**, puis accédez au nœud **Gestion de la classification**, **Règles de classification**. Activez la **planification des classifications** pour permettre la classification continue.
4. Créez une nouvelle règle comme suit : attribuez **High** (Haut) à la propriété **Impact** lorsque la mention de texte Confidentiel Adatum est incluse dans un document.

Protéger automatiquement les documents avec AD RMS

1. Dans FSRM, accédez à **Tâches de gestion de fichiers**, puis créez une tâche qui assure la protection AD RMS automatique aux documents à impact élevé.
2. Sélectionnez la planification pour qu'elle s'exécute de façon continue pour tous les fichiers.

Vérifier le déploiement

1. Sur **LON-SVR1**, examinez la feuille de propriétés du document dans le dossier **Finance Documents**. Notez l'absence de valeurs sous l'onglet **Classification**.
2. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Hani**, puis ouvrez le document **Finance Memo**. Ajoutez **Confidentiel Adatum** au texte, puis enregistrez le fichier.
3. Revenez sur l'ordinateur virtuel **LON-SVR1**, puis notez la valeur sous l'onglet **Classification** des propriétés du document.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et implémentation d'une infrastructure AD RMS

Scénario

En raison de la nature hautement confidentielle des travaux de l'équipe de recherche d'A. Datum Corporation, l'équipe chargée de la sécurité souhaite implémenter une sécurité supplémentaire pour certains documents créés par le département de recherche. En particulier, l'équipe chargée de la sécurité souhaite s'assurer que les utilisateurs à l'intérieur et en dehors de l'organisation ne puissent pas partager les documents confidentiels avec des utilisateurs non autorisés.

Vous devez organiser et implémenter une solution AD RMS qui fournira le niveau de protection demandé par l'équipe chargée de la sécurité.

Objectifs

À la fin de cet exercice, vous serez à même d'effectuer les tâches suivantes :

- créer le plan AD RMS ;
- implémenter AD RMS pour les utilisateurs internes ;
- implémenter l'intégration d'AD RMS au contrôle d'accès dynamique ;
- implémenter l'intégration d'AD RMS à une organisation partenaire.

Configuration de l’atelier pratique

Durée approximative : 60 minutes

Ordinateur(s) virtuel(s)	22414B-LON-DC1 22414B-LON-SVR1 22414B-LON-CL1 22414B-PRS-DC1 22414B-PRS-CL1
Nom d'utilisateur	ADATUM\Administrateur TREYRESEARCH\Administrateur
Mot de passe	Pa$$w0rd

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateurs virtuels disponible.
Avant de commencer cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, sur **Accueil**, cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22414B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **Administrateur**
   - Mot de passe : **Pa$$w0rd**
   - Domaine : **ADATUM**
5. Répétez les étapes 2 à 4 pour **22414B-LON-SVR1** et **22414B-PRS-DC1.** Pour PRS-DC1, connectez-vous au domaine TREYRESEARCH.
6. Répétez les étapes 2 à 3 pour **22414B-LON-CL1** et **22414B-PRS-CL1**. Ne vous connectez pas tant qu'il ne vous a pas été demandé de le faire.

Exercice 1 : Planification du déploiement AD RMS

Scénario

Le département de sécurité a identifié les exigences suivantes pour le déploiement AD RMS :

- Vous devez utiliser AD RMS pour définir tous les documents enregistrés dans le dossier ConfidentialResearch comme confidentiels et protégés.
- Seuls les membres des groupes Research et Managers doivent pouvoir accéder aux documents.
- Les employés d'A. Datum doivent pouvoir partager le contenu protégé par AD RMS avec les utilisateurs de Trey Research.
- Aucun contenu protégé par AD RMS ne doit être sécurisé de telle façon que personne ne puisse y accéder.

Les tâches principales de cet exercice sont les suivantes :

1. Lire la documentation fournie avec le produit.
2. Mettre à jour le document de proposition en fonction du plan d'action planifié.
3. Examiner les propositions suggérées dans le corrigé de l'atelier pratique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Lire la documentation fournie avec le produit

Lire la documentation.

Documentation fournie avec le produit

----- Message d'origine -----
De : Charlotte Weiss [Charlotte@contoso.com]
Envoyé : 03 fév. 2013 08:45
À : Ed@contoso.com
Objet : AD RMS

Ed,

En raison de la nature hautement confidentielle de la recherche que l'équipe Research exécute au sein d'A. Datum, l'équipe en charge de la sécurité chez A. Datum Corporation souhaite implémenter une sécurité supplémentaire pour certains documents créés par le département de recherche. En particulier, l'équipe chargée de la sécurité souhaite s'assurer que les utilisateurs à l'intérieur et en dehors de l'organisation ne puissent pas partager les documents confidentiels avec des utilisateurs non autorisés.

Vous devez organiser et implémenter une solution AD RMS qui fournira le niveau de protection exigé par l'équipe chargée de la sécurité.

Veuillez proposer un plan pour installer AD RMS chez A. Datum et chez Trey Research, et pour intégrer le reste des actions à entreprendre.

Merci !

Charlotte

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

Concevez une solution en réponse à la proposition.

Répondez aux questions du document Plan IRM A. Datum : AD RMS, proposé ci-après.

Plan IRM A. Datum : AD RMS	
Numéro de référence du document : GW00612	
Auteur du document	Charlotte Weiss
Date	6 février

Présentation des exigences

- Concevez un déploiement AD RMS pour les sociétés A. Datum et Trey Research.
- L'objectif du déploiement AD RMS est de pouvoir protéger les informations, quelle que soit leur destination. Une fois que vous ajoutez la protection AD RMS à un fichier numérique, la protection demeure avec le fichier. Par défaut, seul le propriétaire du contenu peut supprimer la protection du fichier. Le propriétaire accorde aux autres utilisateurs le droit d'exécuter certaines actions sur le contenu, comme afficher, copier ou imprimer le fichier.
- Tous les documents stockés dans le dossier ConfidentialResearch doivent être automatiquement définis comme confidentiels et protégés avec AD RMS.
- Seuls les membres des groupes Research et Managers doivent pouvoir accéder aux documents.

(suite)

Plan IRM A. Datum : AD RMS
Présentation des exigences (*suite*) • Configurez l'intégration du déploiement AD RMS au contrôle d'accès dynamique. • Les employés d'A. Datum doivent pouvoir partager le contenu protégé par AD RMS avec les utilisateurs de Trey Research. • L'équipe chargée de la sécurité chez A. Datum souhaite vérifier qu'aucun contenu protégé par AD RMS n'est sécurisé de telle façon que personne ne puisse accéder aux informations.
Informations supplémentaires Nous devons réduire le nombre total de serveurs requis. Envisagez d'utiliser la base de données interne plutôt qu'un déploiement SQL Server complet. Le déploiement AD RMS sur les contrôleurs de domaine existants est autorisé.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

Comparer votre solution au corrigé de l'atelier pratique

1. Combien de clusters AD RMS devez-vous déployer pour répondre aux exigences de sécurité des deux sociétés ?
2. Quelle solution de base de données devez-vous déployer ?
3. Quels comptes de service, le cas échéant, devez-vous créer ?
4. Quelles sont vos exigences en termes de certificats SSL ? Comment répondez-vous à ces exigences dans les deux forêts ?

Exercice 2 : Déploiement de l'infrastructure AD RMS pour les utilisateurs internes

Scénario

La première étape du déploiement AD RMS chez A. Datum consiste à déployer AD RMS pour les utilisateurs internes. Vous commencerez en configurant les enregistrements DNS appropriés et le compte de service AD RMS, puis continuerez avec l'installation et la configuration du premier serveur AD RMS. Vous déploierez aussi le second serveur AD RMS dans le bureau de Toronto et activerez le groupe des super utilisateurs AD RMS. Après le déploiement des serveurs AD RMS, l'étape suivante consiste à configurer les modèles de stratégies de droits et les stratégies d'exclusion pour l'organisation.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les conditions préalables AD RMS.
2. Déployer le premier serveur du cluster AD RMS.
3. Déployer le cluster AD RMS dans la forêt Trey Research.
4. Configurer les modèles AD RMS.
5. Configurer les stratégies d'exclusion AD RMS.
6. Valider le déploiement interne.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Configurer les conditions préalables AD RMS

Créer et configurer les comptes

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory**, puis créez le compte d'utilisateur suivant dans le conteneur **Users** (Utilisateurs) :
   - Nom : **ADRMSSRVC**
   - Mot de passe : **Pa$$w0rd**
   - Désactivez la case à cocher L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
   - Appartenance au groupe : **Admins du domaine**
2. Créer des adresses de messagerie pour chaque utilisateur **Hani Loza**, **Limor Henig**, **Stuart Glasson** et **Toni Poe**, dans l'onglet Général des feuilles de propriétés des utilisateurs avec le format **utilisateur@adatum.com**.
3. Dans le conteneur Users, créez les groupes de sécurité universels suivants : **Management**, **Employees**.
4. Créez une adresse de messagerie pour les groupes suivants : **Employees**, **Management** et **Research**. Utilisez le format **groupe@adatum.com**.
5. Affectez les utilisateurs suivants aux groupes :
   - Limor Henig-Management, Employees
   - Toni Poe-Management
   - Stuart Glasson-Employees

Créer les dossiers partagés sur LON-DC1

1. Sur LON-DC1, ouvrez l'Explorateur de fichiers, puis créez et partagez **C:\ConfidentialResearch**.
2. Définissez les autorisations de partage pour que le groupe **Research** ait l'autorisation **Lecture/écriture** et répétez l'opération pour le groupe **Management**.
3. Créez et partagez le dossier **C:\Public**.
4. Définissez l'autorisation de partage sur le groupe **Tout le monde** ayant l'autorisation **Lecture**.

▶ Tâche 2 : Déployer le premier serveur du cluster AD RMS

Déployer le cluster AD RMS dans Adatum.com

1. Dans l'Assistant Ajout de rôles et de fonctionnalités de **LON-DC1**, ajoutez le rôle **Services AD RMS (Active Directory Rights Management Services)**.
2. Acceptez les fonctionnalités requises. Lorsque vous avez terminé, cliquez sur **Fermer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour configurer un nouveau cluster racine AD RMS

1. Dans **Gestionnaire de serveur**, exécutez la **Configuration supplémentaire** comme indiqué sous **Notifications**. Utilisez les valeurs suivantes :
   - Cluster AD RMS : **Créer un nouveau cluster racine AD RMS**
   - **Base de données de configuration** : **Base de données interne Windows**
   - **Compte de service :**
     Nom : ADATUM\ADRMSSRVC
     Mot de passe : Pa$$w0rd
   - **Mode de chiffrement : Mode de chiffrement 2 (clés RSA 2048 bits/hachages SHA-256)**
   - **Stockage de clé de cluster : gestion centralisée**
   - **Mot de passe de clé de cluster : Pa$$w0rd**
   - **Site Web de cluster : Default Web Site** (Site Web par défaut)
   - **Adresse du cluster :**
     http://LON-DC1.Adatum.com
   - **Certificat de licence :** LON-DC1
   - **Inscription du SCP :** Enregistrer le point de connexion de service maintenant
2. Déconnectez-vous de **LON-DC1**, puis reconnectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

Ouvrir la console Services AD RMS (Active Directory Rights Management Services)

1. Sur **LON-DC1**, à partir du Gestionnaire de serveur, ouvrez la console Services AD RMS (Active Directory Rights Management Services).
2. Vérifiez que la console s'ouvre sans aucune erreur.
3. Fermez la console Services AD RMS (Active Directory Rights Management Services).

▶ Tâche 3 : Déployer le cluster AD RMS dans la forêt Trey Research

Ajouter le compte ADRMSSRVC à PRS-DC1

1. Connectez-vous à **PRS-DC1** en tant que **TREYRESEARCH\Administrateur** à l'aide du mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory**, puis créez le compte d'utilisateur suivant dans le conteneur **Users** (Utilisateurs) :
   - Nom : **ADRMSSRVC**
   - Mot de passe : **Pa$$w0rd**
   - Désactivez la case à cocher L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
   - Appartenance au groupe : **Admins du domaine**
3. Fermez la console **Utilisateurs et ordinateurs Active Directory**.

Ajouter le rôle de serveur AD RMS

1. Sur **PRS-DC1**, utilisez l'Assistant Ajout de rôles et de fonctionnalités pour ajouter le rôle **Services AD RMS (Active Directory Rights Management Services)**.
2. Acceptez les fonctionnalités requises. Lorsque vous avez terminé, cliquez sur **Fermer**.
3. Dans **Gestionnaire de serveur**, exécutez la **Configuration supplémentaire** comme indiqué sous **Notifications**. Utilisez les valeurs suivantes :
   - Cluster AD RMS : **Créer un nouveau cluster racine AD RMS**
   - **Base de données de configuration** : **Base de données interne Windows**
   - **Compte de service :**
     Nom : TREYRESEARCH\ADRMSSRVC
     Mot de passe : Pa$$w0rd
   - **Mode de chiffrement : Mode de chiffrement 2 (clés RSA 2048 bits/hachages SHA-256)**
   - **Stockage de clé de cluster : gestion centralisée**
   - **Mot de passe de clé de cluster : Pa$$w0rd**
   - **Site Web de cluster : Default Web Site** (Site Web par défaut)
   - **Adresse du cluster :**
     http://PRS-DC1.TreyResearch.net
   - **Certificat de licence :** PRS-DC1
   - **Inscription du SCP :** Enregistrer le point de connexion de service maintenant
4. Déconnectez-vous de **PRS-DC1** puis reconnectez-vous en tant que **TREYRESEARCH\Administrateur** avec le mot de passe **Pa$$w0rd**.

Ouvrir la console Services AD RMS (Active Directory Rights Management Services)

1. Sur **PRS-DC1**, vérifiez que la console Services AD RMS (Active Directory Rights Management Services) s'ouvre sans erreur.
2. Fermez la console Services AD RMS (Active Directory Rights Management Services).

▶ Tâche 4 : Configurer les modèles AD RMS

Configurer les modèles AD RMS

1. Basculez sur **LON-DC1**, et ouvrez la console Services AD RMS (Active Directory Rights Management Services).
2. Accédez au nœud **Modèles de stratégies de droits**, puis configurez l'emplacement du fichier des modèles comme **\\LON-DC1\Public**.
3. Créez un modèle de stratégie de droits nommé **Adatum.com RC** qui donne au groupe **Management** l'accès **Afficher** et au groupe **Research** l'accès **Contrôle total**.
4. Cliquez sur **Terminer**, et fermez la console Services AD RMS (Active Directory Rights Management Services).
5. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Ouvrez **Tâches planifiées**, puis activez **AD RMS Rights Policy Template Management (Automated)** (Gestion des modèles de stratégies de droits AD RMS (automatisée)) dans le **Planificateur de tâches** local.
7. Ouvrez **regedit.exe**, et ajoutez la clé **DRM** et la sous-clé **AdminTemplatePath** avec la valeur définie sur le dossier local des modèles de l'utilisateur, **%LocalAppData%\Microsoft\DRM\Templates**.
8. Utilisez la clé de Registre : **HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\DRM** Fermez **regedit.exe**.
9. Déconnectez-vous de LON-CL1.

▶ Tâche 5 : Configurer les stratégies d'exclusion AD RMS

Adatum a fait appel à un groupe de conseil en gestion. À cet effet, Toni Poe, conseillère en gestion de ce groupe, a été équipée d'un espace de bureau et du système informatique d'Adatum Corp. pour effectuer son travail. Un compte a été créé dans Active Directory pour elle et elle a été placée dans le groupe universel Management. Cependant, nous devons exclure les autorisations en lecture sur les fichiers Research Confidential restreints auxquels le groupe Management a accès. À cet effet, nous allons créer pour elle une stratégie d'exclusion sur le cluster AD RMS.

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\toni** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez Microsoft Word, puis créez un document.
3. Attribuez la protection du nouveau document pour Toni uniquement et enregistrez-le sous le nom **Text.docx** dans la bibliothèque Documents. À la demande d'authentification, fournissez **ADATUM\Toni** avec le mot de passe **Pa$$w0rd**.
4. Déconnectez-vous de **LON-CL1**.
5. Rebasculez vers **LON-DC1**. Ouvrez la console Services AD RMS (Active Directory Rights Management Services).
6. Accédez au nœud **Stratégies d'exclusion– Utilisateurs**.
7. Ajoutez le **certificat de compte de droits** de **toni@adatum.com** à la **Stratégie d'exclusion**.
8. Fermez la console Services AD RMS (Active Directory Rights Management Services).

▶ Tâche 6 : Valider le déploiement interne

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Hani** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez Internet Explorer et modifiez la zone Intranet local, puis ajoutez **http://LON-DC1.adatum.com**.
3. Déconnectez-vous de LON-CL1.
4. Répétez les étapes 1 à 3 pour **ADATUM\Limor.**
5. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Hani**.
6. Ouvrez Microsoft Word, puis tapez **Les employés de Management peuvent lire ce document, mais ne peuvent pas le modifier, l'imprimer ou le copier. Les membres du groupe Research ont le contrôle total**.
7. Protégez le document à l'aide de la façon suivante : Le groupe **Management** à l'accès **Lire** et le groupe **Research** à l'accès **Modifier**.
8. Enregistrez le document sous **\\LON-DC1\ConfidentialResearch\ADRMS-TST.docx**.
9. Déconnectez-vous de LON-CL1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Limor**.
11. Ouvrez l'Explorateur de fichiers et accédez au partage **\\LON-DC1\ConfidentialResearch**. Ouvrez **ADRMS-TST**, puis testez les autorisations.
12. Déconnectez-vous de LON-CL1.
13. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Toni**. Essayez d'ouvrir **\\LON-DC1\ConfidentialResearch\ADRMS-TST.docx**.
14. Déconnectez-vous de LON-CL1.

Résultats : Vous devez avoir un cluster AD RMS en fonctionnement dans les forêts Adatum.com et TreyResearch.net, ainsi que pouvoir protéger avec IRM les documents Microsoft Office et voir les résultats de cette protection.

Exercice 3 : Implémentation de l'intégration AD RMS au contrôle d'accès dynamique

Scénario

Pour vérifier qu'AD RMS protège automatiquement tous les documents du dossier ConfidentialResearch, vous devez configurer l'intégration d'AD RMS et du contrôle d'accès dynamique, ainsi que les revendications de certificats de compte de droits, les classifications de fichiers et les stratégies d'accès centralisées.

Les tâches principales de cet exercice sont les suivantes :

1. Activer les propriétés des ressources.
2. Créer les règles de classification.
3. Protéger automatiquement les documents avec AD RMS.
4. Vérifier le déploiement.

▶ Tâche 1 : Activer les propriétés des ressources

Pour activer les propriétés des ressources

1. Sur LON-DC1, dans le Gestionnaire de serveur, ouvrez le **Centre d'administration Active Directory**, puis basculez vers **Arborescence**.
2. Accédez à **Resource Properties** (Propriétés de ressource) du **Contrôle d'accès dynamique**. Activez les propriétés **Impact** et **Personally Identifiable Information** (Informations d'identification personnelle), puis publiez les deux propriétés dans **Global Resource Property List** (Liste des propriétés de ressources globales).
3. Si les stratégies sont déjà dans **Global Resource Property List** (Liste des propriétés de ressources globales), cliquez sur **Annuler**.

▶ Tâche 2 : Créer les règles de classification

Cette étape explique comment créer la règle de classification **Impact haut**. Cette règle explore le contenu des documents et si elle trouve la chaîne « Confidentiel Adatum », elle classe le document en comme ayant un impact haut sur l'activité. Cette classification remplace toute classification précédemment attribuée d'impact bas sur l'activité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous créerez également une règle **Informations identification personnelle hautes**. Cette règle explore le contenu des documents et si elle trouve un numéro de sécurité sociale, elle classe le document comme ayant des informations d'identification personnelle élevées.

1. Connectez-vous à **LON-SVR1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, démarrez l'Assistant Ajout de rôles et de fonctionnalités, puis ajoutez le rôle de service **Gestionnaire de ressources du serveur de fichiers des services de fichiers et de stockage (FSRM)**.
3. Ouvrez Windows PowerShell, puis mettez à jour les **propriétés de ressources globales** pour autoriser l'accès au Gestionnaire de ressources du serveur de fichiers (FSRM). À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
Update-FSRMClassificationPropertyDefinition
```

4. Ouvrez le **Gestionnaire de ressources du serveur de fichiers**, et accédez au nœud **Gestion de la classification, Règles de classification**. Activez la **planification de la classification** pour permettre la classification continue des nouveaux fichiers.
5. Créez deux règles, comme suit :
   - **Impact métier haut :** Lorsque le texte **Confidentiel Adatum** est inclus dans un document. Classez la propriété **Impact** comme **High** (Haute). Elle devrait gérer le dossier C:\Research Documents. Remplacez également toutes les valeurs de propriété existantes.
   - **Informations identification personnelle hautes :** Si un numéro de compte de sécurité social est ajouté, classez la propriété **Informations d'identification personnelle** comme **High** (Haute). Elle devrait gérer le dossier C:\Research Documents. Remplacez également toutes les valeurs de propriété existantes. Utilisez l'expression suivante (Remarque : Il n'y a aucun saut de ligne dans l'expression. La chaîne ne forme qu'un seul bloc.) Entrez l'expression suivante :

```
^(?!000)([0-7]\d{2}|7([0-7]\d|7[012]))([ -]?)(?!00)\d\d\3(?!0000)\d{4}$)
```

▶ Tâche 3 : Protéger automatiquement les documents avec AD RMS

Maintenant que vous avez créé des règles de classification automatique des documents en fonction du contenu, l'étape suivante consiste à créer une tâche de gestion des fichiers qui utilise AD RMS pour protéger automatiquement certains documents selon leur classification. Dans cette étape, vous allez créer une tâche de gestion de fichiers qui protège automatiquement tous les documents ayant des informations identification personnelle hautes. Seuls les membres du groupe Research auront accès aux documents qui contiennent des informations identification personnelle hautes.

1. Sur LON-SVR1, ouvrez Internet Explorer, modifiez la zone Intranet local, puis ajoutez **http://LON-DC1.adatum.com**.
2. Dans le **Gestionnaire de ressources du serveur de fichiers**, accédez à **Tâches de gestion de fichiers**, et créez une tâche qui assurera la protection automatique AD RMS du dossier **C:\Research Documents** quand la propriété **Personally Identifiable Information** (Informations d'identification personnelle) a la valeur **High** (Haut).
3. Configurez la planification pour qu'elle s'exécute de façon continue pour tous les fichiers.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Vérifier le déploiement

1. Sur LON-SVR1, ouvrez l'Explorateur de fichiers et accédez à **C:\Research Documents**.
2. Examinez les propriétés des deux documents du dossier Research Documents. Notez qu'ils n'ont pas de valeurs définies sous l'onglet **Classification**.
3. Basculez vers **LON-CL1**, et connectez-vous en tant qu'**ADATUM\Hani** avec le mot de passe **Pa$$w0rd**.
4. À partir du Bureau, tapez **\\LON-SVR1\Research Documents**, et appuyez sur Entrée.
5. Ouvrez le document **Finance Memo**. Tapez **Confidentiel Adatum**. Enregistrez le document, puis fermez Microsoft Word.
6. Ouvrez le document **Request for Approval to Hire**. Tapez **Sécurité sociale # :** Appuyez sur la touche Entrée, puis sur une nouvelle ligne, tapez **777-77-7777**. L'expression doit figurer sur une nouvelle ligne pour être remarquée rapidement par le contrôle d'accès dynamique. Enregistrez le document, puis fermez Microsoft Word.
7. Basculez vers **LON-SVR1**, puis accédez à **C:\Research Documents**. Notez les valeurs de l'onglet **Classification** des propriétés des deux documents.
8. Sur tous les ordinateurs, fermez toutes les fenêtres actives, puis déconnectez-vous.

Résultats : Les règles de classification du contrôle d'accès dynamique doivent être appliquées au contenu protégé par la gestion des droits relatifs à l'information (IRM).

Exercice 4 : Implémentation de l'intégration AD RMS avec des utilisateurs externes

Scénario

Les tâches principales de cet exercice sont les suivantes :

1. Exporter la stratégie des domaines d'utilisateurs approuvés.
2. Exporter la stratégie des domaines de publication approuvés.
3. Importer la stratégie de domaine d'utilisateur approuvé à partir du domaine partenaire.
4. Importer la stratégie des domaines de publication approuvés à partir du domaine partenaire.
5. Configurer l'accès anonyme au serveur de licences AD RMS.
6. Vérifier l'accès utilisateur au document protégé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Exporter la stratégie des domaines d'utilisateurs approuvés

Exporter la stratégie des domaines d'utilisateurs approuvés

1. Sur **LON-DC1**, ouvrez la console **Services AD RMS (Active Directory Rights Management Services)**, accédez à **Stratégies d'approbation – Domaines d'utilisateurs approuvés**, puis exportez la stratégie vers un fichier nommé **C:\ADRMS_LON-DC1_LicensorCert.bin**.
2. Répétez l'étape 1 ci-dessus sur **PRS-DC1** et enregistrez le fichier comme **C:\ADRMS_PRS-DC1_LicensorCert.bin**.

▶ Tâche 2 : Exporter la stratégie des domaines de publication approuvés

Exporter la stratégie des domaines de publication approuvés

1. Dans LON-DC1, ouvrez la console **Services AD RMS (Active Directory Rights Management Services)**, puis accédez à **Stratégies d'approbation – Domaines de publication approuvés**.
2. Sélectionnez le certificat **LON-DC1**, puis exportez-le, en enregistrant le fichier sous **C:\AdatumTrustedPubDomain.xml,** avec le mot de passe **Pa$$w0rd.**
3. Répétez les étapes 1 et 2 ci-dessus sur **PRS-DC1**, en sélectionnant le certificat **PRS-DC1** et en utilisant le nom de fichier **C:\TreyTrustedPublDomain.xml**, avec le mot de passe **Pa$$word**.

▶ Tâche 3 : Importer la stratégie de domaine d'utilisateur approuvé à partir du domaine partenaire

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils** et, dans la zone de liste déroulante, cliquez sur **DNS**. Développez **LON-DC1**, sélectionnez **Redirecteurs conditionnels** et cliquez avec le bouton droit, puis cliquez sur **Nouveau redirecteur conditionnel**.
2. Sous **Domaine DNS**, tapez **TreyResearch.net**. Dans **Adresses IP des serveurs maîtres**, tapez **172.16.10.10**. Appuyez sur Entrée, puis cliquez sur **OK**. Fermez le Gestionnaire DNS.
3. Sur **PRS-DC1**, répétez les étapes 1 à 2. Utilisez le domaine DNS **Adatum.com** et **Adresses IP des serveurs maîtres 172.16.0.10**.
4. Sur **LON-DC1**, ouvrez la console Services AD RMS (Active Directory Rights Management Services), accédez à **Stratégies d'approbation – Domaines d'utilisateurs approuvés**, puis importez le fichier **\\PRS-DC1\C$\ADRMS_PRS-DC1_LicensorCert.bin**. Nommez le fichier **TreyResearch**.
5. Répétez l'étape 4 ci-dessus sur **PRS-DC1**, en utilisant le fichier **\\LON-DC1\C$\ADRMS_LON-DC1_LicensorCert.bin**. Nommez le fichier **Adatum**.

▶ Tâche 4 : Importer la stratégie des domaines de publication approuvés à partir du domaine partenaire

Ajouter un domaine de publication approuvé

1. Sur **LON-DC1**, ouvrez la console Services AD RMS (Active Directory Rights Management Services), accédez à **Stratégies d'approbation – Domaines de publication approuvés**, puis importez **\\PRS-DC1\c$\TreyTrustedPubDomain.xml**. Utilisez **Pa$$w0rd** comme mot de passe et comme **Nom complet Domaine TreyResearch**.
2. Répétez l'étape 1 ci-dessus sur **PRS-DC1** en utilisant le fichier **\\LON-DC1\C$\AdatumTrustedPubDomain.xml**. Utilisez le mot de passe **Pa$$w0rd** et comme **Nom complet Domaine Adatum**.

▶ Tâche 5 : Configurer l'accès anonyme au serveur de licences AD RMS

- Sur LON-DC1, ouvrez le Gestionnaire des services Internet (IIS), puis activez **Authentification anonyme** et désactivez **Authentification Windows** sur les deux fichiers sous LON-DC1\Sites\Default Web Site_wmcs\Licensing :
  - **license.asmx**
  - **ServiceLocator.asmx**

▶ Tâche 6 : Vérifier l'accès utilisateur au document protégé

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Hani**, ouvrez le document **ADRMS-TST.docx** du dossier **\\LON-DC1\ConfidentialResearch**, ajoutez **liberty@treyresearch.net** avec l'autorisation **Lire** définie sur **Accès restreint**, puis enregistrez le document. Fermez toutes les fenêtres ouvertes, puis déconnectez-vous.

   Remarque : À l'invite Microsoft Word, cliquez sur **Changer d'utilisateur**, puis à l'invite **Sélectionner l'utilisateur**, cliquez sur **OK**.

2. Sur **LON-DC1** connectez-vous en tant qu'**ADATUM\Administrateur**, copiez le document **ADRMS-TST.docx** depuis **C:\ConfidentialReseach** vers le partage **\\PRS-DC1\Public**.
3. Connectez-vous à **PRS-CL1** en tant que **TREYRESEARCH\Liberty**,, puis ouvrez le fichier **ADRMS-TST.docx** dans le partage **\\PRS-DC1\Public**. Observez que le document est protégé par des droits et qu'il ne peut pas être enregistré ou imprimé. Déconnectez-vous de tous les ordinateurs virtuels.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-CL1**, **22414B-PRS-DC1** et **22414B-PRS-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Sachez qu'il est possible d'utiliser les certificats auto-signés, mais que les certificats de serveur des serveurs de cluster AD RMS doivent être ajoutés au magasin des Autorités de certification approuvées (impliqué dans la protection IRM) d'un ordinateur.	
Lorsque vous avez installé le cluster AD RMS dans l'atelier pratique, vous avez utilisé la base de données interne de Windows. Cependant, si vous avez l'intention d'utiliser plusieurs serveurs AD RMS dans le cluster, vous devez utiliser une version SQL Server complète pour pouvoir ajouter les éléments de base de données de plusieurs serveurs.	

Outils

- Console d'administration AD RMS (Active Directory Rights Management Service)
- Gestionnaire de ressources des services de fichiers
- Centre d'administration Active Directory
- Regedit.exe
- Windows PowerShell

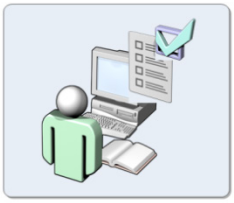
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Évaluation du cours

Votre évaluation de ce cours aidera Microsoft à comprendre la qualité de votre expérience de formation.

Consultez votre formateur pour accéder au formulaire d'évaluation du cours.

Votre évaluation est strictement confidentielle et vos réponses à cette enquête seront utilisées dans le seul but d'améliorer la qualité des prochains cours Microsoft. Vos commentaires ouverts et honnêtes sont très précieux.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 1 : Vue d'ensemble de la gestion dans un centre de données d'entreprise

Atelier pratique : Éléments à prendre en compte pour implémenter un centre de données d'entreprise

Exercice 1 : Planification de l'implémentation sécurisée de services dans un centre de données d'entreprise

▶ Tâche 1 : Examiner les exigences métier et du service informatique

▶ Tâche 2 : Déterminer comment répondre aux exigences métier et du service informatique

1. Comment allez-vous répondre à la nécessité de fournir un outil unique pour gérer les hôtes de virtualisation et les ordinateurs virtuels ?

   Réponse : VMM fournit une interface de gestion unique pour gérer les hôtes de virtualisation et les ordinateurs virtuels.

2. Comment allez-vous répondre à la nécessité pour les administrateurs de division de gérer leurs applications et leurs ordinateurs virtuels ?

   Réponse : Il y a plusieurs manières de fournir cette fonctionnalité. Dans VMM, vous pouvez déléguer l'accès à certaines parties de l'infrastructure. Les autorisations sont répercutées dans App Controller lorsqu'il est utilisé comme site libre-service pour VMM. App Controller, Service Manager et Orchestrator fournissent tous des options de délégation de différents niveaux d'autorisation.

3. Comment allez-vous répondre à la nécessité de fournir des informations détaillées sur les performances de tous les composants du centre de données ?

   Réponse : Operations Manager fournit cette fonctionnalité.

4. Comment allez-vous répondre à la nécessité d'automatiser les processus dans le centre de données ?

   Réponse : Les outils de System Center fournissent un grand nombre d'options d'automatisation. Vous pouvez utiliser Service Manager pour automatiser les réponses aux problèmes. Vous pouvez utiliser des Runbooks Orchestrator pour automatiser une séquence de tâches complexe.

5. Comment allez-vous répondre à la nécessité de garantir la haute disponibilité des applications requises ?

   Réponse : Votre approche variera selon l'application ou le service que vous voulez rendre hautement disponible. Exchange Server fournit une solution de haute disponibilité intégrée. SQL Server, utilisé en tant que serveur principal pour les sites Web frontaux, fournit également des options de haute disponibilité. Vous aurez probablement recours à l'équilibrage de charge pour rendre les sites Web hautement disponibles. Vous pouvez rendre une application qui s'exécute sur un serveur Windows 2000 hautement disponible en virtualisant le serveur. Pour ce faire, utilisez une conversion P2V (physique-à-virtuel), puis utilisez le clustering avec basculement pour rendre l'ordinateur virtuel hautement disponible.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Comment allez-vous répondre aux exigences du service de sécurité ?

   Réponse : Toutes les configurations requises nécessiteront des certificats. Vous devrez donc déployer une infrastructure à clé publique (PKI) interne, telle qu'AD CS.

7. Comment allez-vous répondre à la nécessité d'améliorer les performances du site Web de ventes ?

   Réponse : Vous pouvez utiliser les outils de System Center pour automatiser la gestion des performances du site Web. Vous pouvez utiliser Operations Manager pour surveiller les performances du site Web. Lorsque les performances atteignent un seuil spécifique, vous pouvez utiliser Orchestrator pour déclencher un Runbook qui déploie un serveur Web supplémentaire ou qui attribue davantage de ressources au serveur SQL Server. Lorsque le nombre de demandes diminue, les composants de System Center peuvent automatiquement rétablir l'état précédent de l'environnement.

8. Comment allez-vous répondre à la nécessité de permettre l'intégration à Trey Research ?

   Réponse : En déployant AD RMS, vous pouvez activer la protection des documents une fois qu'ils sont sortis de votre organisation.

9. Comment allez-vous répondre à la nécessité de fournir l'accès requis au site Web partenaire ?

   Réponse : Vous pouvez utiliser AD FS pour fournir différents niveaux d'accès à un site aux comptes d'utilisateurs des domaines distants.

▶ Tâche 3 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

Résultats : À la fin de cet exercice, vous aurez identifié les composants que vous devrez inclure dans la conception du centre de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 2 : Planification et implémentation d'une stratégie de virtualisation de serveur

Atelier pratique : Planification et implémentation d'une stratégie de virtualisation de serveur

Exercice 1 : Planification du déploiement de l'hôte Hyper-V

▶ Tâche 1 : Lire la documentation fournie avec le produit

Lisez la documentation fournie dans le manuel du stagiaire.

▶ Tâche 2 : Mettre à jour le document de proposition

- Répondez aux questions de la section Propositions du document Stratégie de virtualisation de serveur pour A. Datum.

1. Est-il possible de disposer d'un seul serveur VMM pour prendre en charge la configuration requise, ou est-il nécessaire d'en implémenter trois avec App Controller ?

   Oui, il est possible de répartir les composants VMM entre les filiales, puis de configurer les groupes d'hôtes appropriés. Déployez App Controller et un seul serveur Virtual Machine Manager.

2. Combien de serveurs de bibliothèque est-il nécessaire de déployer ?

   Au moins un par site. Cependant, la succursale de Londres envisage un centre de données principal et un secondaire. Par conséquent, il serait bon de déployer quatre serveurs de bibliothèque pour fournir une disponibilité supérieure pour les clusters du siège social.

3. Est-il possible d'empêcher des ordinateurs virtuels de se mettre hors tension au cours de la journée ?

   Oui, il est possible de configurer une planification pour l'optimisation de l'alimentation.

4. Quelle procédure suivre pour n'utiliser qu'un faible nombre de modèles pour le déploiement de serveurs ?

   Établissez des objets équivalents qui vérifient que toutes les bibliothèques disposent des mêmes fichiers ISO (Internation Organization for Standardization) et des mêmes disques durs virtuels (VHD).

5. Quelles mesures seront prises pour éviter l'utilisation de la bande passante ?

   Installez des objets équivalents, puis sur chaque site, déployez des services WSUS (Windows Server Update Services), déployez des services de déploiement Windows, et établissez une bibliothèque.

6. Quels serveurs hôtes peuvent exiger des paramètres de réserve de ressources différents ? Où sont-ils installés ?

   La filiale et les serveurs hôtes de maintenance peuvent exiger des réserves différentes. Elles sont définies au niveau du groupe d'hôtes ou sur chaque hôte.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Quel est l'avantage du coût de maintenance ? Elle apparaît comme un gaspillage de ressources. Peut-elle apporter autre chose ?

   Le déploiement d'un hôte de maintenance constitue une bonne pratique, car il est possible de déployer des ordinateurs virtuels vers celui-ci sans affecter les systèmes de production. En outre, il est également possible d'effectuer des tests des performances et de charge sur les charges de travail. En outre, ces serveurs peuvent également agir en tant que serveurs de bibliothèque de votre filiale.

8. Comment obtenir des rapports sur les économies d'énergie ?

   Les rapports sur les paramètres d'alimentation sont disponibles par l'intermédiaire de l'intégration de VMM avec Operations Manager.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions à celles présentées ci-dessus.

Exercice 2 : Configuration de groupes d'hôtes Hyper-V

▶ Tâche 1 : Ajouter un hôte Hyper-V à VMM

Ajouter un hôte Hyper-V

1. Dans la barre de tâches, sur **LON-VMM1**, cliquez sur **Console Virtual Machine Manager**.
2. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session de Microsoft Windows** est sélectionnée, puis cliquez sur **Connecter**. La console Virtual Machine Manager s'ouvre.
3. Cliquez sur l'espace de travail **Ensemble fibre optique**.
4. Sur le ruban, cliquez sur **Ajouter des ressources**, puis sélectionnez **Clusters et hôtes Hyper-V**. L'Assistant Ajout d'une ressource démarre.
5. Dans la page **Emplacement de la ressource**, cliquez sur **Ordinateurs Windows Server dans un domaine Active Directory approuvé**, puis sur **Suivant**.
6. Dans la page **Informations d'identification**, cliquez sur **Entrer manuellement les informations d'identification**, puis utilisez les informations d'identification suivantes.
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
7. Cliquez sur **Suivant**.
8. Dans la page **Étendue de la découverte**, cliquez sur **Spécifier les ordinateurs Windows Server par noms**, dans le champ **Noms des ordinateurs**, tapez **LON-HOST1**, puis cliquez sur **Suivant**.
9. Dans la page **Ressources cibles**, cliquez sur **lon-host1.adatum.com**, puis sur **Suivant**. Sur l'avertissement concernant le rôle Hyper-V, cliquez sur **OK**
10. Dans la page **Paramètres de l'ordinateur hôte**, cliquez sur **Tous les ordinateurs hôtes**, puis sur **Suivant**.
11. Dans la page **Résumé**, cliquez sur **Terminer**.
12. Examinez l'état, puis fermez la fenêtre Travaux une fois la tâche terminée. Un message d'avertissement peut paraître et indiquer que MPIO (multipath I/O) n'est pas activé. Vous pouvez ignorer ce message pour cette tâche.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer les groupes d'hôtes

Créer les groupes d'hôtes

1. Sur **LON-VMM1**, à partir de la console Virtual Machine Manager, cliquez sur **Ordinateurs virtuels et services**.
2. Dans le volet de navigation, cliquez sur le nœud **Tous les ordinateurs hôtes**.
3. Sur le ruban, cliquez sur **Créer un groupe hôte**, puis remplacez le nom par défaut par **Hôtes de London**.
4. Répétez les étapes 2 et 3 pour créer les hôtes suivants :
   - **Hôtes de Toronto ;**
   - **Hôtes de Sydney.**

▶ Tâche 3 : Configurer les groupes d'hôtes

Configurer les groupes d'hôtes

1. Sur **LON-VMM1**, à partir de la console Virtual Machine Manager, cliquez sur **Ordinateurs virtuels et services**.
2. À partir de l'espace de travail Ordinateurs virtuels et services, cliquez avec le bouton droit de la souris sur **Hôtes de London**, puis cliquez sur **Propriétés**.
3. Cliquez sur **Réserves de ressources de l'ordinateur hôte**, décochez la case en regard de **Utiliser les paramètres des réserves de l'ordinateur hôte groupe hôte parent**, cliquez sur le champ **Mémoire**, puis modifiez la valeur sur **1024 Mo**.
4. Cliquez sur **Optimisation dynamique**, puis décochez la case en regard de **Utiliser les paramètres d'optimisation dynamique du groupe hôte parent**.
5. Cliquez sur la case à cocher **Migrer automatiquement les ordinateurs virtuels vers l'équilibrage de charge à cette fréquence (minutes)**, puis modifiez la valeur sur **60 minutes**.
6. Cliquez sur la case à cocher **Activer l'optimisation de l'alimentation**, cliquez sur **Paramètres**, examinez les paramètres, puis cliquez sur **OK**.
7. Cliquez sur **OK** pour appliquer les modifications.
8. Dans l'espace de travail Ensemble fibre optique, cliquez pour développer **Serveurs**, puis cliquez sur et faites glisser **lon-host1** vers le groupe d'hôtes **Hôtes de London**.
9. À partir de l'espace de travail **Ordinateurs virtuels et services**, cliquez avec le bouton droit de la souris sur **Hôtes de Toronto**, puis cliquez sur **Propriétés**.
10. Cliquez sur **Optimisation dynamique**, puis décochez la case en regard de **Utiliser les paramètres d'optimisation dynamique du groupe hôte parent**.
11. Cliquez sur la case à cocher **Migrer automatiquement les ordinateurs virtuels vers l'équilibrage de charge à cette fréquence (minutes)**, puis modifiez la valeur sur **60 minutes**.
12. Cliquez sur la case à cocher **Activer l'optimisation de l'alimentation**, puis cliquez sur **Paramètres**.
13. Configurez une absence d'optimisation d'alimentation du lundi au vendredi entre 7 am (du matin) et 19 pm. Cliquez sur **OK**.
14. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de Hôtes de Toronto**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Configuration de bibliothèques VMM

▶ Tâche 1 : Configurer un serveur et un partage de bibliothèque

Configurer un serveur et un partage de bibliothèque

1. Sur **TOR-SVR1,** sur le Tableau de bord du Gestionnaire de serveurs, cliquez sur **Services de fichiers et de stockage**, puis sur **Partages**.
2. Dans l'espace de travail Partages, cliquez sur **TÂCHES**, puis sur **Nouveau partage**.
3. Dans la page **Sélectionner le profil de ce partage**, cliquez sur **Partage SMB – Rapide**, sur **Suivant**, et dans la page **Emplacement du partage**, cliquez sur **Suivant**. Sur la page **Nom de partage**, dans le champ **Nom du partage**, tapez **TORVMMLibrary**, puis cliquez sur **Suivant**.
4. Dans la page **Autres paramètres**, cliquez sur **Suivant**, et dans la page **Autorisations**, cliquez sur **Suivant**. Dans la page **Confirmation**, cliquez sur **Créer**, puis sur **Fermer**.
5. Sur **LON-VMM1**, dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Bibliothèque**.
6. Sur le ruban, cliquez sur **Ajouter un serveur de bibliothèque**.
7. Dans la page **Entrer les informations d'identification**, cliquez sur Entrez un nom d'utilisateur et un mot de passe, entrez les informations d'identification suivantes, puis cliquez sur **Suivant** :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
8. Dans la page **Sélectionner des serveurs de bibliothèque**, cliquez sur **Rechercher**.
9. Dans la page **Rechercher un ordinateur**, dans le champ **Nom de l'ordinateur**, tapez **TOR-SVR1**, puis cliquez sur **Rechercher**.
10. Dans la zone Résultats de recherche, cliquez sur **tor-svr1.adatum.com**, sur **Ajouter**, sur **OK**, puis sur **Suivant**.
11. Dans la page **Ajouter des partages de bibliothèque**, cliquez sur la case à cocher en regard de **TORVMMLibrary**, puis sur celle en regard de **Ajouter des ressources par défaut**. Cliquez sur **Suivant**, puis, dans la page **Résumé**, cliquez sur **Ajouter des serveurs de bibliothèque**.
12. Examinez l'état du travail, puis fermez la fenêtre Travaux une fois le travail terminé.

▶ Tâche 2 : Copier les fichiers requis vers le centre de données de la filiale

Copier manuellement des fichiers vers des partages de bibliothèques

1. Sur **LON-VMM1**, dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Bibliothèque**.
2. Développez **Serveurs de bibliothèque**, puis cliquez sur **LON-VMM1.Adatum.com**.
3. Dans le volet d'informations, cliquez avec le bouton droit de la souris sur **Disque vierge – Petit.vhdx**, puis cliquez sur **Ouvrir l'emplacement du fichier**.
4. Dans la fenêtre des disques durs virtuels, cliquez sur **Affichage**, puis sélectionnez la case à cocher en regard de **Extensions de noms de fichiers**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans la fenêtre des disques durs virtuels, cliquez avec le bouton droit de la souris sur **Disque vierge – Petit.vhdx**, et cliquez sur **Copier**. Fermez la fenêtre VHDs, et dans le volet de navigation, développez **Serveurs de bibliothèque**, puis développez **tor-svr1.adatum.com**.
6. Cliquez avec le bouton droit de la souris sur **TORVMMLibrary**, puis cliquez sur **Explorer**. Dans la fenêtre TORVMMLibrary, cliquez avec le bouton droit de la souris sur un espace vide, puis cliquez sur **Coller**.
7. Fermez la fenêtre TORVMMLibrary. Cliquez avec le bouton droit de la souris sur **tor-svr1.adatum.com**, puis cliquez sur **Actualiser**. Vérifiez que le fichier **Disque vierge – Petit.vhdx** apparaît dans la liste d'objets.

▶ Tâche 3 : Attribuer une bibliothèque à un groupe d'hôtes

Attribuer une bibliothèque à un groupe d'hôtes

1. Sur **LON-VMM1**, dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Bibliothèque**.
2. Développez **Serveurs de bibliothèque**, cliquez avec le bouton droit de la souris sur **tor-svr1.adatum.com**, puis cliquez sur **Propriétés**.
3. Cliquez sur la zone de liste déroulante **Groupe hôte :**, puis sélectionnez le groupe d'hôtes **Hôtes de Toronto**. Cliquez sur **OK**.
4. Fermez la console Virtual Machine Manager.

▶ Pour préparer le module suivant

N'éteignez pas les ordinateurs virtuels, car vous en aurez besoin pendant le module suivant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 3 : Planification et implémentation des réseaux et du stockage pour la virtualisation

Atelier pratique : Planification et implémentation des réseaux et du stockage de virtualisation

Exercice 1 : Planification d'une infrastructure de stockage pour la virtualisation

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation fournie dans le manuel du stagiaire.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

- Répondez aux questions de la section Propositions du document de stratégie de stockage d'A. Datum Toronto.

1. Les serveurs fournis ont une seule carte réseau intégrée de 10 Go avec toutes les dernières configurations iSCSI. Pour la redondance vous souhaitez en acquérir davantage. Il existe trois emplacements PCI Express disponibles. Que devez-vous acheter ?

   Réponse :

   Une seule carte Ethernet de 10 Go devrait être suffisante pour le nombre d'ordinateurs virtuels. Juste une carte réseau supplémentaire permettrait de fournir la haute disponibilité pour votre chemin d'accès de stockage.

2. L'équipe réseau avec laquelle vous travaillez vous informe que le coût et les délais seront importants pour implémenter un réseau iSCSI distinct. Le réseau actuel est relativement récent et dispose d'environ 10 Go de capacité bien que limité en nombre de connexions. Vous devez indiquer à l'équipe le nombre de connexions de 10 Go nécessaires.

   Réponse :

   Chaque hôte Hyper-V aurait besoin de deux cartes Ethernet de 10 Go, et chaque serveur cible iSCSI aurait besoin de deux cartes Ethernet de 10 Go.

   Huit ports Ethernet de 10 Go sont requis pour fournir les chemins d'accès de stockage entièrement redondants.

3. Vous envisagez d'avoir un autre serveur hôte en tant qu'hôte de maintenance, mais votre budget ne le permet pas. Quelle solution proposer ?

   Réponse :

   Compte tenu du coût élevé des cartes Ethernet de 10 Go, vous pourriez choisir d'utiliser plusieurs cartes de 1 Go. Cela permettrait éventuellement d'avoir un autre serveur hôte plus petit qui pourrait jouer le rôle de serveur de déploiement et de maintenance. Vous pouvez déterminer les configurations requises en analysant l'utilisation actuelle du disque et du réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Vous avez identifié la protection des données comme un risque et un goulot d'étranglement potentiels. D'après vous, à quoi cela est-il dû, et comment vous pouvez résoudre le problème ?

   Réponse :

   Les sauvegardes ne sont pas mentionnées dans le scénario, mais en fonction des 20 téraoctets de données environ à sauvegarder, vous devez vérifier si la société applique actuellement une stratégie de sauvegarde, et si c'est le cas, poursuivez-la. En outre, vous devez vérifier que les sauvegardes s'achèveront sans affecter les performances de production. Vous pouvez inclure une mise à niveau sur vos serveurs de sauvegarde. Cependant, avant d'acheter des cartes Ethernet de 10 Go, vérifiez que le nombre de disques source de votre réseau SAN et le nombre de disques cibles présents sur vos serveurs de sauvegarde peuvent fournir suffisamment d'E/S pour garantir 10 Go.

5. Quelle fonctionnalité Windows Server pouvez-vous activer pour continuer à exécuter vos ordinateurs virtuels en cas de défaillance d'un composant de stockage réseau, tel qu'une carte réseau ou un commutateur réseau ?

   Réponse :

   MPIO est la fonctionnalité que vous devez activer pour autoriser Windows à communiquer avec le stockage sur plusieurs chemins d'accès.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions à celles présentées ci-dessus.

▶ Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Préparez-vous à discuter de vos propositions avec la classe.

Exercice 2 : Planification d'une infrastructure réseau pour la virtualisation

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation fournie dans le manuel du stagiaire.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

1. Parmi les réseaux répertoriés, lesquels devriez-vous virtualiser pour atteindre l'objectif ?

   Réponse :

   Infrastructure, Application et éventuellement Sauvegarde, s'ils sont virtualisés.

2. Où et comment pouvez-vous configurer des réseaux virtualisés ?

   Réponse :

   Une fois que vous activez le pilote de filtre de virtualisation réseau, vous pouvez utiliser Windows PowerShell pour installer et configurer la virtualisation réseau ou VMM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Quelle est la procédure de configuration des réseaux virtualisés ?

   Réponse :

   Ceci dépend des configurations requises, mais en résumé :

   - Identifier les ordinateurs et les réseaux virtuels.
   - Activer le pilote de filtre de virtualisation réseau sur les cartes réseau des hôtes Hyper-V.
   - Configurer les réseaux et les passerelles d'ordinateurs virtuels.
   - Attribuer les adresses IP des ordinateurs virtuels.

4. Existe-t-il d'autres moyens d'héberger les ordinateurs virtuels qui se chevauchent ?

   Réponse :

   Vous pouvez utiliser les réseaux VLAN. Cependant, vous devez déterminer si vous allez déplacer les ordinateurs virtuels entre les hôtes, ou s'ils doivent communiquer avec d'autres ordinateurs virtuels qui se trouvent sur le réseau isolé de différents hôtes. Si oui, vous devez configurer le routage et les réseaux VLAN sur toute l'infrastructure réseau où transite le trafic.

5. Où pouvez-vous rechercher les commandes Windows PowerShell pour configurer la virtualisation réseau ?

   Réponse :

   Les commandes Windows PowerShell pour la virtualisation réseau sont présentes dans le module NetWNV.

6. Vous avez attribué le pilote du filtre de virtualisation réseau au commutateur Ethernet virtuel, qui est associé à la carte réseau physique. Est-ce correct ?

   Réponse :

   Vous devez attribuer le pilote de filtre de virtualisation réseau à la carte réseau physique ou à la carte d'association réseau.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions à celles présentées ci-dessus.

▶ Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Préparez-vous à discuter de vos propositions avec la classe.

Exercice 3 : Implémentation d'une infrastructure de stockage pour la virtualisation

▶ Tâche 1 : Configurer les cibles iSCSI pour le déploiement d'ordinateurs virtuels

Ajouter le service du rôle de serveur cible iSCSI

1. Sur **LON-SVR1**, dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, dans la page **Avant de commencer**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionner des rôles de serveurs**, développez **Service de fichiers et de stockage (Installé)**, **Services de fichiers et iSCSI (Installé)**, activez la case à cocher **Serveur cible iSCSI**, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
8. Une fois l'installation terminée, cliquez sur **Fermer**.

Créer un pool de stockage

1. Sur **LON-SVR1**, maintenez la touche Windows appuyée, appuyez sur **X**, puis cliquez sur **Gestion du disque**.
2. Dans la page **Gestion des disques**, cliquez sur **Action**, puis sur **Créer un disque dur virtuel**. Dans le champ **Emplacement**, tapez **E:\iSCSI1.vhdx**.
3. Dans le champ **Taille du disque dur virtuel**, tapez **50**, cliquez sur **Mo**, puis sélectionnez **Go**. Cliquez sur **VHDX**, puis sur **OK**.
4. Répétez l'étape 2 à 3 pour créer deux fichiers vhdx supplémentaires nommés **iSCSI2** et **iSCSI3**.
5. Cliquez avec le bouton droit sur **Disque2**, puis cliquez sur **Initialiser le disque**. Notez que les trois disques doivent être sélectionnés. Cliquez sur **OK**.
6. Fermez la fenêtre Gestion des disques.
7. Dans le Gestionnaire de serveur, dans le volet de navigation, cliquez sur **Services de fichiers et de stockage**, puis sur **Pools de stockage**.
8. Confirmez que les disques que vous avez ajoutés sont visibles dans la section Disques physiques. Si ce n'est pas le cas, dans la section Pool de stockage, cliquez sur **TÂCHES**, puis sur **Actualiser**.
9. Dans la section POOLS DE STOCKAGE, cliquez sur **TÂCHES**, puis sur **Nouveau pool de stockage**.
10. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
11. Dans le champ **Nom du pool de stockage**, tapez **VMPool**, puis cliquez sur **Suivant**.
12. Dans la page **Disques physiques**, activez les trois disques, puis cliquez sur **Automatique**. Notez que vous pouvez attribuer un hôte de réserve. Conservez le paramètre **Automatique** sélectionné, puis cliquez sur **Suivant**.
13. Dans la page **Confirmation**, cliquez sur **Créer**.
14. Dans la page **Résultats**, cliquez sur **Créer un disque virtuel lorsque l'Assistant se ferme**, puis cliquez sur **Fermer**. L'Assistant Nouveau disque virtuel se lance.
15. Dans la page **Avant de commencer**, cliquez sur **Suivant** et dans la page **Pool de stockage**, cliquez sur **Suivant**. Dans la page **Nom du disque dur virtuel**, dans le champ **Nom**, tapez **VMStorage**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Dans la page **Disposition du stockage**, cliquez sur **Parity** (Parité), puis sur **Suivant**. Dans la page **Type de mise en service**, cliquez sur **Fin**, puis sur **Suivant**.
17. Dans la zone **Taille**, sous **Taille du disque virtuel**, tapez **100**, puis cliquez sur **Suivant**.
18. Dans la page **Confirmation**, vérifiez les paramètres, puis cliquez sur **Créer**.
19. Dans la page **Afficher les résultats**, cliquez sur **Fermer**.
20. L'Assistant Nouveau volume se lance, dans la page **Avant de commencer**, cliquez sur **Suivant**. Dans la page **Serveur et disque**, dans la zone Disque, cliquez sur le **Disque virtuel VMStorage**, puis cliquez sur **Suivant**. Dans la page **Taille**, conservez la valeur par défaut **(99,9) Go**, puis cliquez sur **Suivant**.
21. Dans la page **Lettre de lecteur ou dossier**, conservez la Lettre du lecteur **F**, puis cliquez sur **Suivant**. Dans la page **Paramètres du système de fichiers**, cliquez sur le champ **Nom de volume**, puis tapez **VMStorage**. Cliquez sur **Suivant**, vérifiez les paramètres, cliquez sur **Créer**, puis dans la page **Résultats**, cliquez sur **Fermer**.
22. Dans le volet Services de fichiers et de stockage, cliquez sur **iSCSI**.
23. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES**, puis dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
24. Dans l'Assistant Nouveau disque virtuel iSCSI, dans la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur **F:**, puis sur **Suivant**.
25. Dans la page **Indiquer le nom du disque dur virtuel iSCSI**, tapez **iSCSIDisk1**, puis cliquez sur **Suivant**.
26. Dans la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone **Taille**, tapez **99**, vérifiez que **Go** est sélectionné dans la zone de liste déroulante, puis cliquez sur **Suivant**.
27. Dans la page **Affecter la cible iSCSI**, cliquez sur **Nouvelle cible iSCSI**, puis sur **Suivant**.
28. Dans la page **Indiquer le nom de la cible**, dans la zone **Nom**, tapez **LON-SVR1**, puis cliquez sur **Suivant**.
29. Dans la page **Indiquer les serveurs d'accès**, cliquez sur **Ajouter**.
30. Dans la boîte de dialogue **Sélectionnez une méthode pour identifier l'initiateur**, cliquez sur **Entrer une valeur pour le type sélectionné**, puis, dans la zone de liste déroulante **Type**, sélectionnez **Adresse IP**. Dans le champ **Valeur**, tapez **172.16.0.31**, puis cliquez sur **OK**.
31. Dans la page **Indiquer les serveurs d'accès**, cliquez sur **Suivant**.
32. Dans la page **Activer l'authentification**, cliquez sur **Suivant**.
33. Dans la page **Confirmer les sélections**, cliquez sur **Créer**.
34. Dans la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.
35. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES**, puis dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
36. Dans l'Assistant Nouveau disque virtuel iSCSI, dans la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur **C:**, puis sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

37. Dans la page **Indiquer le nom du disque dur virtuel iSCSI**, tapez **iSCSIDisk2**, puis cliquez sur **Suivant**.
38. Dans la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone **Taille**, tapez **5**, vérifiez que **Go** est sélectionné dans la zone de liste déroulante, puis cliquez sur **Suivant**.
39. Dans la page **Affecter la cible iSCSI**, cliquez sur **lon-svr1**, puis sur **Suivant**.
40. Dans la page **Confirmer les sélections**, cliquez sur **Créer**.
41. Dans la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.

▶ Tâche 2 : Configurer les initiateurs iSCSI

Configurer les initiateurs iSCSI

1. Sur **LON-HOST1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Initiateur iSCSI**. Lorsque vous êtes invité à démarrer le service Microsoft iSCSI, cliquez sur **Oui**.
2. Dans la page **Cibles**, dans le champ **Cible**, tapez **172.16.0.12**. Cliquez sur **Connexion rapide**, cliquez sur **Terminer**, puis cliquez sur **OK** pour fermer la page.
3. Sur **LON-HOST1**, maintenez appuyée la touche Windows de votre clavier, appuyez sur **X**, puis cliquez sur **Gestion du disque**.
4. Recherchez le nouveau **disque de 99 Go**, cliquez avec le bouton droit sur le disque, cliquez sur **En ligne**. Cliquez de nouveau avec le bouton droit et sélectionnez **Initialiser le disque**, puis dans la page **Initialiser le disque**, cliquez sur **OK**.
5. Cliquez avec le bouton droit sur l'espace non alloué, puis cliquez sur **Nouveau volume simple**
6. Dans la page d'accueil, cliquez sur **Suivant**, puis dans la page **Spécifier la taille du volume**, conservez la valeur par défaut et cliquez sur **Suivant**.
7. Dans la page **Attribuer une lettre de lecteur ou de chemin d'accès**, cliquez sur la zone de liste déroulante, puis sélectionnez la lettre **V**. Cliquez sur **Suivant**
8. Dans la page **Formater une partition**, sous le champ **Nom de volume**, tapez **VMStorage**. Cliquez sur **Suivant**, vérifiez les paramètres, puis cliquez sur **Terminer**.
9. Fermez la fenêtre **Gestion des disques**.

Exercice 4 : Implémentation d'une infrastructure réseau pour la virtualisation

▶ Tâche 1 : Configurer des réseaux logiques que votre création requiert

Créer le réseau logique

1. Sur **LON-VMM1**, sur la barre des tâches, cliquez sur le bouton **Console Virtual Machine Manager**. Dans la boîte de dialogue **Connexion au serveur**, cliquez sur **Connecter**.
2. Cliquez sur l'espace de travail **Ensemble fibre optique**, dans le ruban, cliquez sur **Créer**, puis sur **Réseau logique**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans le champ **Nom**, tapez **Réseau de production de Toronto**, puis dans le champ **Description**, tapez **Adatum Toronto – Réseau logique de production**. Cliquez sur **Autoriser les nouveaux réseaux d'ordinateurs virtuels créés sur ce réseau logique à utiliser la virtualisation de réseau**, puis cliquez sur **Suivant**.
4. Dans la page **Sites réseau**, cliquez sur **Ajouter**, puis dans la section **Groupes hôtes pouvant utiliser ce site réseau**, sélectionnez **Tous les ordinateurs hôtes**.
5. Cliquez sur **Insérer une ligne**, puis cliquez dans le champ **Réseau local viruel**. Tapez **0**, cliquez sur le champ **Sous-réseau IP**, puis tapez **172.16.3.0/24**, cliquez sur **Suivant**, puis sur **Terminer**.
6. Fermez la fenêtre Travaux.

Créer un pool IP

1. Cliquez sur l'espace de travail **Ensemble fibre optique**, dans le ruban, cliquez sur **Créer**, puis sur **Pool d'adresses IP**. Dans la page **Nom**, dans le champ **Nom**, tapez **Applications de Toronto**, puis dans le champ Description, tapez **Pool IP de l'application de production de Toronto**. Cliquez dans la zone de liste déroulante **Réseau logique**, cliquez sur **Réseau de production de Toronto**, puis cliquez sur **Suivant**. Dans la page **Site réseau**, cliquez sur **Utiliser un site réseau existant**, sélectionnez **Réseau de production de Toronto_0**, cliquez dans la zone de liste déroulante **Sous-réseau IP**, sélectionnez **172.16.3.0/24**, puis cliquez sur **Suivant**.
2. Dans la page **Plage d'adresses IP**, dans le champ **Adresses IP réservées pour les adresses IP virtuelles d'équilibrage de charge**, tapez **172.16.3.100-172.16.3.120**, puis cliquez sur **Suivant**.
3. Dans la page **Passerelle**, cliquez sur **Insérer**, cliquez dans le champ **Adresse de la passerelle**, tapez **172.16.3.1**, puis cliquez sur **Suivant**.
4. Dans la page **DNS**, cliquez sur **Suivant**, puis dans la page **WINS**, cliquez sur **Suivant**.
5. Dans la page **Résumé**, cliquez sur **Terminer**.

Créer un profil de port natif

1. Dans le ruban, cliquez sur **Créer**, puis sur **Profil de port natif**.
2. Dans la page **Général**, dans le champ **Nom**, tapez **Carte réseau par défaut de Toronto**, cliquez sur **Profil de port de liaison montante**, conservez les paramètres par défaut d'équilibrage de charge et d'association de cartes réseau tels quels, puis cliquez sur **Suivant**.
3. Dans la page **Configuration réseau**, sous **Sites réseau**, cliquez sur **Réseau de production de Toronto_0**, sur l'option **Activer la virtualisation de réseau Windows**, puis cliquez sur **Suivant**.
4. Dans la page **Résumé**, cliquez sur **Terminer**.
5. Fermez la fenêtre Travaux.

Créer un commutateur logique

1. Dans le ruban, cliquez sur **Créer**, puis sur **Commutateur logique**.
2. Dans la page **Mise en route,** cliquez sur **Suivant**. Dans la page **Général**, dans le champ **Nom**, tapez **Commutateur logique de Toronto**, puis dans le champ **Description**, tapez **Commutateur Hyper-V de production de Toronto**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la page **Extensions**, conservez les extensions par défaut, puis cliquez sur **Suivant**.
4. Dans la page **Liaison montante**, cliquez sur **Ajouter**, **Profil de port**, puis sélectionnez la **Carte réseau par défaut de Toronto**. Cliquez sur **OK**, puis sur **Suivant**.
5. Dans la page **Port virtuel**, cliquez sur **Ajouter**, **Parcourir**, **Gestion de l'ordinateur hôte**, sur **OK**, l'option **Inclure un profil de port de carte réseau virtuelle dans ce port virtuel**, cliquez sur **Profil de port de carte réseau virtuelle natif**, **Gestion de l'ordinateur hôte**, puis cliquez sur **OK**.
6. Répétez l'étape 5 et ajoutez les classifications de port et les profils de port de carte réseau virtuelle natif suivants :

   Classifications de ports :

   - **Charge de travail de migration dynamique**
   - **Charge de travail du cluster hôte**
   - **Bande passante élevée**

   Profils de port de carte réseau virtuelle :

   - **Migration en direct**
   - **Cluster**
   - **Carte à haute bande passante**
7. Dans la page **Port virtuel**, cliquez sur **Suivant**, puis dans la page **Résumé**, cliquez sur **Terminer**.
8. Fermez la fenêtre Travaux**.**

Ajouter la carte de bouclage Microsoft

1. Sur **LON-HOST1**, placez la souris dans l'angle inférieur gauche de l'écran jusqu'à ce que l'icône Accueil s'affiche, cliquez sur l'icône Accueil sur l'écran Accueil, cliquez sur **Panneau de configuration**. Dans le Panneau de configuration, cliquez sur **Matériel**, dans la page Matériel, cliquez sur **Gestionnaire de périphériques**.
2. Dans le Gestionnaire de périphériques, cliquez avec le bouton droit sur **LON-HOST1**, cliquez sur **Ajouter un matériel d'ancienne génération**. L'Assistant Ajout de matériel se lance.
3. Dans l'écran d'accueil, cliquez sur **Suivant**, **Installer le matériel que je sélectionne manuellement dans la liste (utilisateur expérimenté)**, puis **Suivant**, faites défiler l'affichage vers le bas jusqu'à ce que les cartes réseau apparaissent, cliquez sur **Cartes réseau**, puis **Suivant**, sous Fabricant, cliquez sur **Microsoft**. Sous Carte réseau, faites défiler l'affichage vers le bas jusqu'à ce que la carte de bouclage Microsoft KM-TEST apparaisse, cliquez sur **Carte de bouclage Microsoft KM-TEST**, puis **Suivant**. L'Assistant Ajout de matériel devrait à présent indiquer que le matériel est prêt pour l'installation, cliquez sur **Suivant**, puis dans la page Fin de l'Assistant Ajout de matériel, cliquez sur **Terminer**.
4. Fermez le **Gestionnaire de périphériques** et le **Panneau de configuration.**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Actualiser LON-HOST1

1. Sur **LON-VMM1**, ouvrez la console Virtual Machine Manager.
2. Cliquez sur l'espace de travail **Ensemble fibre optique**, développez **Serveurs**, **Tous les ordinateurs hôtes**, développez **Hôtes de London**, cliquez avec le bouton droit sur **lon-host1**, puis sur **Actualiser**.
3. Dans le ruban, cliquez sur le bouton **Travaux**, attendez que le travail d'actualisation de l'hôte se termine, puis fermez la fenêtre Travaux.

Mettre les hôtes Hyper-V à jour pour utiliser les réseaux logiques

1. Depuis l'espace de travail Ensemble fibre optique, cliquez avec le bouton droit sur **lon-host1**, sur **Propriétés**, **Commutateurs virtuels**, **Nouveau commutateur virtuel**, puis sur **Nouveau commutateur logique**.
2. Avec l'option **Commutateur logique de Toronto** sélectionnée, sous **Cartes physiques**, cliquez sur la liste déroulante **Carte**, puis sélectionnez **Carte de bouclage Microsoft KM-TEST**.
3. Dans la page Propriétés, cliquez sur **Matériel**, puis faites défiler l'écran et développez **Cartes réseau**. Cliquez sur la **Carte de bouclage Microsoft KM-TEST** ; vous pouvez voir que la carte est disponible pour le placement.
4. Cliquez sur **Connectivité de réseau logique** qui est répertorié sous la Carte de bouclage Microsoft KM-TEST, puis à droite de la page Matériel sous **Connectivité de réseau logique**, cliquez sur **Réseau de production de Toronto**, sur **OK**, lisez l'avertissement, puis cliquez sur **OK**.

▶ Tâche 2 : Configurer la virtualisation réseau

Activer le pilote du filtre de virtualisation réseau Windows

1. Sur LON-HOST1, dans le Gestionnaire de serveur, cliquez sur **Serveur local**, puis dans la zone **PROPRIÉTÉS**, cliquez sur **172.16.0.31, Compatible IPv6**. La page **Connexions réseau** s'affiche.
2. Dans la page **Connexions réseau**, cliquez avec le bouton droit sur la carte physique, puis cliquez sur **Propriétés**.
3. Activez la case à cocher en regard du **Pilote du filtre de virtualisation réseau Windows**, puis cliquez sur **OK**.

Actualiser LON-HOST1

1. Sur **LON-VMM1**, ouvrez la console Virtual Machine Manager.
2. Cliquez sur l'espace de travail **Ensemble fibre optique**, développez **Hôtes de London**, cliquez avec le bouton droit sur **lon-host1**, puis sur **Actualiser**.
3. Dans le ruban, cliquez sur le bouton **Travaux**, attendez que le travail d'actualisation de l'hôte se termine, puis fermez la fenêtre Travaux.

Configurer un réseau d'ordinateurs virtuels pour les serveurs d'applications à l'aide de la virtualisation réseau

1. Dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Ordinateurs virtuels et services**. Dans le ruban, cliquez sur **Créer un réseau d'ordinateurs virtuels**.
2. Dans la page **Nom**, dans le champ **Nom**, tapez **Réseau d'ordinateurs virtuels Applications de Toronto**, cliquez sur le champ **Description**, puis tapez **Serveurs d'application de Toronto**. Cliquez dans la zone de liste déroulante **Réseau logique**, sélectionnez **Réseau de production de Toronto**, puis cliquez sur **Suivant**.

3. Dans la page **Isolation**, cliquez sur **Isoler l'aide de la virtualisation réseau Hyper-V**, puis sur **Suivant**.
4. Dans la page **Sous-réseaux d'ordinateurs virtuels**, cliquez sur **Ajouter**, et dans le champ **Nom**, tapez **Serveurs d'application de Toronto**. Dans le champ **Sous-réseau**, tapez **172.16.3.0/24**, puis cliquez sur **Suivant**.
5. Dans la page **Passerelle**, laissez l'option **Aucune connectivité** sélectionnée, puis cliquez sur **Suivant**. Examinez le résumé, puis cliquez sur **Terminer**.
6. Fermez la fenêtre Travaux.
7. Répétez les étapes 1 à 6 pour créer un nom de réseau d'ordinateurs virtuels **Réseau d'ordinateurs virtuels Applications Partenaire de Toronto**, puis utilisez le même sous-réseau.

Créer des pools IP de réseau d'ordinateurs virtuels

1. Dans l'espace de travail Ordinateurs virtuels et services, cliquez sur **Réseaux d'ordinateurs virtuels**, cliquez sur **Réseau d'ordinateurs virtuels Applications de Toronto**, puis cliquez avec le bouton droit et sélectionnez **Créer un pool d'adresses IP**.
2. Dans la page **Nom**, cliquez sur le champ **Nom**, puis tapez **Pool IP du réseau d'ordinateurs virtuels Applications de Toronto**. Vérifiez que le réseau d'ordinateurs virtuels est défini sur **Réseau d'ordinateurs virtuels Applications de Toronto** et que le sous-réseau d'ordinateurs virtuels est défini sur **Serveurs d'application de Toronto (172.16.3.0/24)**, puis cliquez sur **Suivant**.
3. Dans la page **Plage d'adresses IP**, conservez les paramètres par défaut, puis cliquez sur **Suivant**.
4. Dans la page **Passerelle**, cliquez sur **Suivant**, puis dans la page **DNS**, cliquez sur **Suivant**. Dans la page **WINS**, cliquez sur **Suivant**, puis dans la page **Résumé**, cliquez sur **Terminer**. Fermez la fenêtre Travaux.

▶ Tâche 3 : Attribuer des ordinateurs virtuels aux réseaux d'ordinateurs virtuels

Attribuez des ordinateurs virtuels aux réseaux d'ordinateurs virtuels

1. Dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Ordinateurs virtuels et services**. Dans le ruban, dans l'onglet Accueil, cliquez sur la moitié supérieure du bouton **Créer un ordinateur virtuel**.
2. Dans la page **Sélectionner une source**, cliquez sur **Créer l'ordinateur virtuel avec un disque dur virtuel vide**, puis sur **Suivant**.
3. Dans la page **Spécifier l'identité de l'ordinateur virtuel**, dans le champ **Nom de l'ordinateur virtuel**, tapez **TOR-CRM1**, puis cliquez sur **Suivant**.
4. Dans la page **Configurer le matériel**, cliquez sur **Carte réseau 1**, puis sous **Connectivité**, cliquez sur **Connecté à un réseau d'ordinateurs virtuels**. Cliquez sur **Parcourir**, puis sélectionnez **Réseau d'ordinateurs virtuels Applications de Toronto**, puis cliquez sur **OK**. Sous la section **Profil de port**, cliquez dans la zone de liste déroulante **Classification**. Il s'agit de l'emplacement où vous pouvez attribuer les profils de carte virtuelle de port natif. Sélectionnez **Bande passante élevée** et cliquez sur **Suivant**.
5. Dans la page **Sélectionner la destination**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans la page **Sélectionner l'ordinateur hôte**, dans la section Détails, cliquez sur **Explication de l'évaluation**, vous devriez voir le message indiquant que : **Cette destination répond à toutes les conditions requises de cet ordinateur virtuel**, puis cliquez sur **Suivant**.
7. Dans la page **Configurer les paramètres**, conservez les paramètres par défaut, puis cliquez sur **Suivant** à deux reprises. Dans la page **Ajouter des propriétés**, cliquez sur **Suivant**, puis dans la page **Résumé**, cliquez sur **Créer**.
8. Fermez la fenêtre Travaux.

Vérification de l'ordinateur virtuel

1. Dans l'espace de travail Ordinateurs virtuels et services, dans le ruban, cliquez sur **Ordinateurs virtuels**, cliquez avec le bouton droit sur **TOR-CRM1**, puis cliquez sur **Propriétés**.
2. Cliquez sur **Configuration matérielle**, puis sur **Carte réseau 1**. Le réseau d'ordinateurs virtuels et le commutateur logique s'affichent. Cliquez sur **Détails de la** pour visualiser les détails des adresses IP attribuées à partir du pool. Cliquez sur **Fermer**, puis sur **Annuler**.

▶ Pour préparer le module suivant

- N'éteignez pas les ordinateurs virtuels, car vous en aurez besoin pour le module suivant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4 : Planification et déploiement d'ordinateurs virtuels

Atelier pratique : Planification et implémentation d'une stratégie de déploiement et de gestion d'ordinateurs virtuels

Exercice 1 : Planification des conversions de serveurs P2V (physical-to-virtual)

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation fournie dans le manuel du stagiaire.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

Répondez aux questions de la section Propositions du document Stratégie de virtualisation.

1. Tous les serveurs peuvent-ils être convertis en utilisant le service de conversion P2V intégré à Microsoft® System Center 2012 – Virtual Machine Manager (VMM) ?

   Réponse :

   Non, Windows® 2000 Server n'est pas indiqué comme étant pris en charge. Le cluster SQL Server® n'est pas pris en charge en tant que cluster mais peut être converti et recréé en tant que cluster invité.

2. Comment accélérer le processus de conversion ? Par exemple, existe-t-il des serveurs que vous pouvez convertir en exécutant des scripts ? Si oui, lesquels ?

   Réponse :

   Vous pouvez gagner du temps en exécutant des scripts pour la migration des serveurs de batterie de serveurs Web.

3. Comment pouvez-vous distribuer les serveurs ?

   Réponse :

   Pratiquement chaque service est distribué avec sa propre disponibilité de formulaire. Vous pouvez donc configurer uniquement le serveur d'autorité de certification (AC) et les systèmes de développement pour la sélection élective automatique. Vous devez configurer des règles de sélection élective par affinité afin de garantir que le nouvel ordinateur virtuel accomplisse la redondance des hôtes physiques.

4. Si vous ne disposez pas d'hôte de maintenance, quel plan pouvez-vous utiliser pour importer les serveurs physiques ?

   Réponse :

   Vous pouvez configurer un nœud dans le cluster de telle sorte qu'il ne comporte pas de systèmes réels, puis le désigner pour qu'il reçoive les migrations entrantes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions avec celles du corrigé de l'atelier pratique.

▶ Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Préparez-vous à discuter de vos propositions avec la classe.

Résultats : À la fin de cet exercice, vous devriez avoir examiné et planifié la virtualisation et la consolidation.

Exercice 2 : Planification des modèles d'ordinateurs virtuels et de services

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation fournie dans le manuel du stagiaire.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

- Répondez aux questions de la section Propositions du document de référence des modèles de services de développement.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

Comparez vos propositions avec celles du corrigé de l'atelier pratique.

1. De combien de profils matériels, de profils de système d'exploitation invité et de profils SQL Server avez-vous besoin ?

   Réponse :

   Cinq systèmes différents avec une configuration matérielle différente signifierait que vous avez besoin de cinq profils matériels.

2. Devez-vous utiliser des modèles de services ou des modèles d'ordinateurs virtuels ?

   Réponse :

   Vous devez disposer d'un modèle d'ordinateur virtuel avant de créer un modèle de service. Vous pouvez créer un modèle de service pour l'application en utilisant trois serveurs, et vous pouvez choisir d'inclure les clients ou de les déployer séparément.

▶ Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Préparez-vous à discuter de vos propositions avec la classe.

Résultats : À la fin de cet exercice, vous devriez avoir planifié un modèle de service de base basé sur l'infrastructure existante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Configuration des profils et des modèles VMM

▶ Tâche 1 : Configurer un profil de système d'exploitation invité

Configurer un profil de système d'exploitation invité

(Remarque : si nécessaire, effectuez les étapes 1 et 2 pour démarrer la console VMM)

1. Sur LON-VMM1, dans la barre de tâches, cliquez sur **Console Virtual Machine Manager**.
2. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session Microsoft Windows** est activée, puis cliquez sur **Connecter**.
3. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Profils**, puis cliquez sur **Profils de système d'exploitation invité**.
4. Dans le ruban, cliquez sur **Créer**, puis sur **Profil de système d'exploitation invité**.
5. Dans la boîte de dialogue **Nouveau profil de système d'exploitation invité**, dans la page **Général**, dans la zone de texte **Nom**, tapez **Profil de système d'exploitation TOR-WEB**, puis dans la zone de texte **Description**, tapez **Profil de système d'exploitation invité du nouveau serveur Web de développement**.
6. Cliquez sur **Profil de système d'exploitation invité**.
7. Dans la page **Profil de système d'exploitation invité**, sous **Paramètres généraux**, cliquez sur **Informations d'identité**.
8. Dans la zone de texte **Nom de l'ordinateur**, tapez **TOR-WEB#**.
9. Cliquez sur **Mot de passe de l'administrateur**, puis sur **Spécifier le mot de passe du compte d'administrateur local**. Dans les zones de texte **Mot de passe** et **Confirmer**, tapez **Pa$$w0rd**.
10. Cliquez sur **Clé du produit**, puis dans la zone **Clé du produit**, tapez **XC9B7-NBPP2-83J2H-RHMBY-92BT4**.
11. Cliquez sur **Système d'exploitation**, puis vérifiez que **64-bit edition of Windows Server 2012 Standard** (Édition 64 bits de Windows Server 2012 Standard) est sélectionné.
12. Sous **Mise en réseau**, cliquez sur **Domaine / groupe de travail**.
13. Cliquez sur **Domaine**, puis dans la zone de texte **Domaine**, tapez **adatum.com**.
14. Sous **Informations d'identification du domaine**, cliquez sur **Spécifiez les informations d'identification à utiliser pour**.
15. Dans la zone de texte **Utilisateur du domaine**, tapez **ADATUM\Administrateur**. Dans les zones de texte **Mot de passe** et **Confirmer**, tapez **Pa$$w0rd**.
16. Cliquez sur **OK** pour fermer la boîte de dialogue **Nouveau profil de système d'exploitation invité**.

▶ Tâche 2 : Configurer un profil matériel

Configurer un profil matériel

1. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Profils**, puis cliquez sur **Profils matériels**.
2. Dans le ruban, cliquez sur **Créer**, puis sur **Profil matériel**.

3. Dans la boîte de dialogue **Nouveau profil matériel**, dans la page **Général**, dans la zone de texte **Nom**, tapez **WsStd2012**, puis dans la zone de texte Description, tapez **Profil matériel pour les nouveaux serveurs Windows Server 2012**.
4. Cliquez sur **Profil matériel**.
5. Dans la page **Profil matériel**, sous **Compatibilité**, cliquez sur **Profils de capacité du cloud**.
6. Activez la case à cocher **Hyper-V**.
7. Dans la section **Général**, cliquez sur **Processeur**, puis activez la case à cocher **Autoriser la migration vers un ordinateur hôte d'ordinateur virtuel avec une version de processeur différente**.
8. Cliquez sur **Mémoire**, vérifiez que **Statique** est sélectionné, puis modifiez l'option **Mémoire de l'ordinateur virtuel** sur **1024 Mo**.
9. Dans la section Cartes réseau, cliquez sur **Carte réseau 1**. Sous **Connectivité**, cliquez sur **Connecté à un réseau d'ordinateurs virtuels**, cliquez sur **Parcourir**, sur **Réseau externe**, puis sur **OK**.
10. Cliquez sur **OK** pour fermer la boîte de dialogue **Nouveau profil matériel**. Le nouveau profil s'affiche dans le volet de résultats.

▶ Tâche 3 : Configurer un profil SQL Server

Configurer un profil SQL Server

1. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Profils**, puis cliquez sur **Profils SQL Server**.
2. Dans le ruban, cliquez sur **Créer**, puis sur **Profil SQL Server**.
3. Dans la boîte de dialogue **Nouveau profil SQL Server**, dans la page **Général**, dans la zone de texte **Nom**, tapez **SQLDev1**, puis dans la zone de texte **Description**, tapez **Modèle pour les nouveaux serveurs SQL**.
4. Cliquez sur **Configuration de SQL Server**.
5. Dans la page **Configuration de SQL Server,** en regard de **Ajouter**, cliquez sur **Déploiement de SQL Server**. Configurez les paramètres suivants :
   - Dans le champ **Nom**, tapez **SQLDev1**.
   - Dans le champ **Nom de l'instance**, tapez **MSSQLSERVER**.
   - Dans le champ **ID de l'instance**, tapez **DefaultInstance**.
6. Sous **Compte d'identification de l'installation**, cliquez sur **Parcourir**. Dans la boîte de dialogue **Parcourir les comptes d'identification**, cliquez sur **Administrateur**, puis sur **OK**.
7. Cliquez sur **Configuration**.
8. Dans la zone de texte **Source du média**, tapez **C:\SQLInstall**.
9. Dans la zone Administrateurs de SQL Server, tapez ADATUM\Administrateur, puis cliquez sur Ajouter.
10. En regard de **Mode de sécurité**, vérifiez qu'**Authentification Windows** est sélectionné.
11. Activez la case à cocher **Utiliser TCP\IP pour activer les connexions distantes**, puis cliquez sur **Comptes de service**.
12. Sous **Compte d'identification du service SQL Server**, cliquez sur **Parcourir**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

13. Dans la boîte de dialogue **Parcourir les comptes d'identification**, cliquez sur **Administrateur**, puis sur **OK**.
14. Sous **Compte d'identification du service SQL Server**, cliquez sur **Parcourir**.
15. Dans la boîte de dialogue **Parcourir les comptes d'identification**, cliquez sur **Administrateur**, puis sur **OK**.
16. Sous **Compte d'identification des services de création de rapports**, cliquez sur **Parcourir**.
17. Dans la boîte de dialogue **Parcourir les comptes d'identification**, cliquez sur **Administrateur**, puis sur **OK**.
18. Cliquez sur **OK** pour fermer la boîte de dialogue **Nouveau profil SQL Server**.

▶ Tâche 4 : Configurer un modèle d'ordinateur virtuel

Configurer un modèle d'ordinateur virtuel

1. Sur LON-VMM1, ouvrez l'Explorateur de fichiers.
2. Dans la barre d'adresses, tapez **\\LON-HOST1\e$\Program Files\Microsoft Learning\Base**, puis appuyez sur Entrée.
3. Cliquez avec le bouton droit sur le fichier **Base12A-WS12-TMP_FR.vhd**, puis cliquez sur **Copier**.
4. Dans la barre d'adresses, tapez **\\lon-vmm1\MSSCVMMLibrary\vhds**, puis appuyez sur Entrée. Dans la fenêtre de l'Explorateur de fichiers, cliquez avec le bouton droit sur un espace vide, puis cliquez sur **Coller**. Le processus de copie du fichier prend quelques minutes.
5. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Serveurs de bibliothèque**, **LON-VMM1.Adatum.com**, **MSSCVMMLibrary**, puis cliquez sur **VHDs**.
6. Vérifiez que la copie du fichier est terminée, cliquez avec le bouton droit sur **VHDs**, puis cliquez sur **Actualiser**. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Modèles**, puis cliquez sur **Modèles d'ordinateur virtuel**.
7. Dans le ruban, cliquez sur **Créer un modèle d'ordinateur virtuel**.
8. Dans l'Assistant Créer un modèle d'ordinateur virtuel, dans la page **Sélectionner une source**, cliquez sur **Utiliser un modèle d'ordinateur virtuel existant ou un disque dur virtuel stocké dans la bibliothèque**, puis sur **Parcourir**.
9. Dans la boîte de dialogue **Sélectionner la source du modèle d'ordinateur virtuel**, cliquez sur Base12A-WS12-TMP_FR.vhd, puis sur **OK**.
10. Dans la page **Sélectionner une source**, cliquez sur **Suivant**.
11. Dans la page **Identité du modèle d'ordinateur virtuel**, dans la zone de texte Nom du modèle d'ordinateur virtuel, tapez **Serveur d'applications Web ADATUM**, puis dans la zone de texte Description, tapez **Serveur Web hébergeant l'application Web** ADATUM, puis cliquez sur **Suivant**.
12. Dans la page **Configurer le matériel**, dans la zone de liste déroulante **Profil matériel**, cliquez sur **WsStd2012**. Notez que les paramètres du profil matériel sont importés dans le modèle. Cliquez sur **Suivant**.
13. Dans la page Configurer le système d'exploitation, dans la zone de liste déroulante Profil de système d'exploitation invité, cliquez sur Profil de système d'exploitation TOR-WEB.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

14. Sous **Rôles et fonctions**, cliquez sur **Rôles**.
15. Activez la case à cocher **Serveur Web (IIS)**, puis cliquez sur **Suivant**.
16. Dans la page **Configurer les applications**, dans la zone de liste déroulante **Profil d'application**, cliquez sur **Aucune – n'installer aucune application**, puis sur **Suivant**.
17. Dans la page **Configurer SQL Server**, dans la zone de liste déroulante **Profil SQL Server**, cliquez sur **Aucun - aucun paramètre de configuration SQL Server**, puis sur **Suivant**.
18. Dans la page **Résumé**, cliquez sur **Créer**.

▶ Tâche 5 : Configurer un modèle de service

Configurer un modèle de service

1. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Modèles**, puis cliquez sur **Modèles de service**.
2. Dans le ruban, cliquez sur **Créer un modèle de service**.
3. Dans le Concepteur de modèles de services Virtual Machine Manager, dans la boîte de dialogue **Nouveau modèle de service**, dans la zone de texte **Nom**, tapez **Service Web ADATUM**.
4. Sous **Modèles**, cliquez sur **Ordinateur simple (v1.0)**, puis sur **OK**. Patientez pendant que le service Web ADATUM se charge dans le concepteur de modèles.
5. Sous **Modèles d'ordinateur virtuel**, cliquez sur le **Serveur d'applications Web ADATUM** et faites-le glisser vers la section **Ajouter des applications** de la couche.
6. Dans le ruban, cliquez sur **Enregistrer et valider**.
7. Fermez le Concepteur de modèles de services Virtual Machine Manager - Service Web ADATUM nouveau.

Résultats : À la fin de cet exercice, vous devriez avoir configuré les profils et les modèles VMM.

Exercice 4 : Déploiement d'ordinateurs virtuels à l'aide de modèles VMM

▶ Tâche 1 : Déployer des ordinateurs virtuels à l'aide du modèle de service

Déployer des ordinateurs virtuels à l'aide du modèle de service

1. Dans la console VMM, cliquez sur l'espace de travail **Bibliothèque**, développez **Modèles**, puis cliquez sur **Modèles de service**.
2. Cliquez avec le bouton droit sur **Service Web ADATUM**, puis cliquez sur **Configurer le déploiement**.
3. Dans la boîte de dialogue **Sélectionner le nom et la destination**, dans la zone de texte **Nom**, tapez **Service Web ADATUM**, puis cliquez sur **OK**.
4. Dans la fenêtre Déployer le service – Service Web ADATUM, vérifiez que la couche a été placée sur un hôte. Vous devrez peut-être cliquer sur **Actualiser l'aperçu** pour mettre à jour les résultats.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans la fenêtre Déployer le service – Service Web ADATUM, dans le ruban, cliquez sur **Déployer le service**.
6. Dans la boîte de dialogue **Déployer le service**, cliquez sur **Déployer**. Patientez quelques minutes pour que la fenêtre Travaux s'ouvre.
7. Analysez le déploiement du service à l'aide de la fenêtre Travaux. Le déploiement du service durera approximativement 10 minutes.
8. Une fois le service déployé, cliquez sur l'espace de travail **Ordinateurs virtuels et services**.
9. Dans le ruban, cliquez sur **Services**.
10. Dans le volet de résultats, cliquez avec le bouton droit sur **Service Web ADATUM**, puis cliquez sur **Arrêt**.

▶ Pour préparer le module suivant

- N'éteignez pas les ordinateurs virtuels, car vous en aurez besoin pour le module suivant.

Résultats : À la fin de cet exercice, vous devriez avoir déployé un service de couche en utilisant un modèle d'ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 5 : Planification et implémentation d'une solution d'administration de la virtualisation

Atelier pratique : Planification et implémentation d'une solution d'administration pour la virtualisation

Exercice 1 : Configuration de l'automatisation des processus dans System Center

▶ Tâche 1 : Installer et configurer les packs d'intégration System Center

Installer le pack d'intégration System Center pour VMM

1. Sur LON-DC1, dans la barre des tâches, cliquez sur **Explorateur de fichiers**.
2. Dans l'Explorateur de fichiers, accédez à **E:\Labfiles\Module5**.
3. Double-cliquez sur **System_Center_2012_Orchestrator_Integration_Packs.EXE**. Cliquez sur **Ok**, puis une nouvelle fois sur **OK** pour fermer le message **Extraction Complete** (Extraction terminée).
4. Fermez l'Explorateur de fichiers.
5. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'icône **Accueil** apparaisse, cliquez sur l'icône **Accueil**, puis lorsque la page de démarrage apparaît, cliquez sur **Deployment Manager**.
6. Dans la console Deployment Manager, cliquez avec le bouton droit sur **Packs d'intégration**, puis cliquez sur **Inscrire le pack d'intégration auprès d'Orchestrator Management Server**.
7. Dans la page **Bienvenue**, cliquez sur **Suivant**, puis dans la page **Sélectionner les packs d'intégration ou les correctifs logiciels**, cliquez sur **Ajouter**.
8. Dans la page **Ouvrir**, dans le champ **Nom du fichier**, tapez **\\lon-dc1\Labfiles\Module5\SC2012_Virtual_Machine_Manager_Integration_Pack.oip**. Cliquez sur **Ouvrir**, sur **Suivant**, puis dans la page Dernière étape, cliquez sur **Terminer**. Dans la page **Contrat de Licence Utilisateur Final**, cliquez sur **Accepter**.
9. Attendez que l'inscription soit terminée, cliquez pour développer **Orchestrator Management Server**, puis cliquez sur **Packs d'intégration**.
10. Cliquez avec le bouton droit sur **System Center Integration Pack for System Center 2012 Virtual Machine Manager**, puis cliquez sur **Déployer le pack d'intégration sur le serveur Runbook Server ou sur Runbook Designer**.
11. Dans la page **Bienvenue**, cliquez sur **Suivant**, et dans la page **Déployer les packs d'intégration ou les correctifs logiciels**, activez la case à cocher à côté de **System Center Integration Pack for System Center 2012 Virtual Machine Manager**, puis cliquez sur **Suivant**.
12. Dans la page **Sélection de l'ordinateur**, dans le champ **Ordinateur**, tapez **LON-OR1**, cliquez sur **Ajouter**, puis sur **Suivant**.
13. Dans la page **Options d'installation**, cliquez sur **Suivant**, puis dans la page Dernière étape, cliquez sur **Terminer**.
14. Passez en revue les Entrées de journal, puis fermez Orchestrator Deployment Manager.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Définissez la stratégie d'exécution de Windows PowerShell sur RemoteSigned

1. Sur **LON-OR1**, dans la barre des tâches, cliquez avec le bouton droit sur **Windows PowerShell**, puis sous Tâches, cliquez sur **Exécuter en tant qu'administrateur**.
2. À l'invite Windows PowerShell, tapez **set-executionpolicy remotesigned**, appuyez sur Entrée, tapez **O**, puis appuyez sur Entrée.
3. Fermez la fenêtre Windows PowerShell.
4. Sur **LON-VMM1**, dans la barre des tâches, cliquez avec le bouton droit sur **Windows PowerShell**, puis sous **Tâches**, cliquez sur **Exécuter en tant qu'administrateur**.
5. À l'invite Windows PowerShell, tapez **set-executionpolicy remotesigned**, appuyez sur Entrée, tapez **O**, puis appuyez sur Entrée.
6. Fermez la fenêtre Windows PowerShell.

Activer les hôtes approuvés par la Gestion à distance

1. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche de l'écran. L'icône **Accueil** s'affiche. Cliquez avec le bouton droit sur l'icône **Accueil**, puis cliquez avec le bouton droit sur **Exécuter**. Dans la page **Exécuter**, dans le champ **Ouvrir**, tapez **gpedit.msc**, puis cliquez sur **OK**.
2. À gauche, sous **Stratégie Ordinateur local\Configuration ordinateur**, cliquez pour développer **Modèles d'administration**, puis développez **Composants Windows** et **Gestion à distance de Windows (WinRM)**.
3. Cliquez sur **Client WinRM**, puis à droite, sous Client WinRM, double-cliquez sur **Hôtes approuvés**.
4. Dans la page **Hôtes approuvés**, cliquez sur **Activé** et dans le champ **TrustedHostsList**, tapez **LON-VMM1**, puis cliquez sur **OK**.
5. Fermez l'Éditeur de stratégie de groupe local.

Configurer le pack d'intégration System Center pour VMM

1. Sur **LON-OR1**, cliquez sur l'écran Accueil, puis sur **Runbook Designer**.
2. Dans le menu, cliquez sur **Options**, puis sur **SC 2012 Virtual Machine Manager**.
3. Dans la page **Prerequisite Configuration**, cliquez sur **Add** (Ajouter) et dans la page **Add Configuration** (Ajouter une configuration), dans le champ **Name** (Nom), tapez **LON-VMM1**, puis cliquez sur le bouton Parcourir.
4. Dans la page **Item Selection** (Sélection d'éléments), cliquez sur **System Center Virtual Machine Manager**, puis sur **OK**.
5. Dans la page **Add Configuration** (Ajouter une configuration), sous **Properties** (Propriétés), dans le champ **VMM Administrator Console** (Console Administrateur VMM), tapez **LON-VMM1**. Dans le champ **VMM Server** (Serveur VMM), tapez **LON-VMM1** et dans le champ **User** (Utilisateur), tapez **ADATUM\Administrateur**, supprimez le texte du champ **Domain** (Domaine), puis dans le champ **Password** (Mot de passe), tapez **Pa$$w0rd**.
6. Cliquez dans le champ **Authentication Type (remote only)** (Type d'authentification (à distance uniquement), cliquez sur le bouton **Parcourir**, sur **Negociate** (Négocier), puis sur **OK**. Cliquez une nouvelle fois sur **OK**, puis dans la page **Prerequisite Configuration**, cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer l'automatisation dans Orchestrator

Créer un runbook de base

1. Sur **LON-OR1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'icône **Accueil** apparaisse, cliquez sur l'icône **Accueil**, puis lorsque l'interface utilisateur Windows apparaît, cliquez sur **Runbook Designer**.
2. Dans le volet Connexions, cliquez avec le bouton droit sur **Runbook**, cliquez sur **Nouveau**, sur **Dossier**, puis appuyez sur la touche Suppr, tapez **22414 Runbooks**, puis appuyez sur Entrée.
3. Cliquez avec le bouton droit sur le dossier **22414 Runbooks**, cliquez sur **Nouveau**, sur **Runbook** et en haut du volet central, cliquez avec le bouton droit sur **Nouveau Runbook**, cliquez sur **Renommer**, sur **Oui** pour confirmer la modification de ce runbook, tapez **Analyse de la bibliothèque VMM**, puis appuyez sur Entrée.
4. Dans le volet de droite, sous Activités, développez **Gestion de fichiers**, puis cliquez sur l'activité **Analyser le dossier** et faites-la glisser au milieu du volet central.
5. Cliquez avec le bouton droit sur l'activité **Analyser le dossier**, cliquez sur **Renommer**, puis tapez **Analyse de la bibliothèque VMM**. Appuyez sur Entrée.
6. Cliquez sur **Analyse de la bibliothèque VMM**, cliquez sur **Propriétés**, puis sur **Général**. Dans la page **Informations générales**, dans le champ **Description**, tapez **Ce runbook analyse la bibliothèque VMM pour les nouveaux disques durs virtuels**.
7. Cliquez sur **Détails**, sous Dossier à analyser, dans le champ **Chemin d'accès**, tapez **\\LON-VMM1\MSSCVMMLibrary**, puis cliquez sur **Inclure les sous-dossiers**.
8. Dans la section **Filtres de fichiers**, cliquez sur **Ajouter** et dans la page **Paramètres de filtre**, cliquez sur la zone de liste déroulante **Nom**, cliquez sur **Nom du fichier** et dans le champ **Valeur**, tapez ***.vhd**, puis cliquez sur **OK**.
9. À gauche, cliquez sur **Déclencheurs** et, dans la section **Déclencher si**, activez la case à cocher **Nombre de fichiers :**, cliquez sur la zone de liste déroulante **Nombre de fichiers :**, sélectionnez **greater than**, puis dans le champ **greater than**, tapez **0**.
10. Cliquez sur **Authentification** et dans le champ **Nom d'utilisateur**, tapez **ADATUM\Administrateur** et dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Terminer**.
11. Sous Activités, cliquez sur **Notification**, puis cliquez sur l'activité **Envoyer un message du journal des événements** et faites-la glisser au milieu du volet central et à droite de l'activité **Analyse de la bibliothèque VMM**.
12. Placez le pointeur de la souris sur l'activité **Analyse de la bibliothèque VMM** et une petite flèche doit apparaître sur la droite. Placez le pointeur de la souris sur la flèche et celui-ci doit prendre la forme d'une croix. Cliquez sur la flèche, puis faites-la glisser dans **Envoyer un message du journal des événements**. Un lien avec une flèche doit maintenant apparaître entre les deux activités.
13. Cliquez avec le bouton droit sur la flèche entre les deux activités, cliquez sur **Propriétés**, puis lorsque la page **Lier Propriétés** s'affiche, vérifiez le filtre, puis cliquez sur **Terminer**.
14. Cliquez avec le bouton droit sur **Envoyer un message du journal des événements**, cliquez sur **Propriétés**, puis dans la page **Détails**, dans la section Propriétés, dans le champ **Ordinateur**, tapez **LON-OR1**. Dans le champ **Message**, tapez **Un fichier de disque dur virtuel a été créé ou mis à jour dans la bibliothèque LON-VMM1** et dans la section Gravité, cliquez sur **Avertissement**, puis sur **Terminer**.
15. Dans le ruban, cliquez sur **Enregistrer**, puis sur **Exécuter**.

16. Dans la barre des tâches de Windows, cliquez sur l'icône de l'**Explorateur de fichiers**. Dans le champ de la barre d'adresses, tapez **\\lon-vmm1\MSSCVMMLibrary\VHDs**.
17. Dans le ruban de la fenêtre des disques durs virtuels, cliquez sur **Affichage**, puis sélectionnez la case à cocher à côté de **Extensions de noms de fichiers**.
18. Cliquez avec le bouton droit sur l'un des fichiers **Disque vierge – Grand.vhd**, cliquez sur **Copier**, puis cliquez avec le bouton droit sur un espace vide dans la fenêtre de l'Explorateur de fichiers, cliquez sur **Coller** et un nouveau fichier nommé Disque vierge – Grand – Copie.vhd est créé.
19. Basculez vers la page Accueil, tapez **Événement**, puis cliquez sur **Observateur d'événements**. Au centre, dans le volet Résumé des événements d'administration, développez **Avertissement** et vous verrez qu'il existe un ID de l'événement avec l'identificateur 1 et une source d'Orchestrator Runbook. Double-cliquez sur **Événement Orchestrator**, puis examinez l'événement.
20. Fermez l'**Observateur d'événements**, puis la fenêtre de l'Explorateur de fichiers.
21. Dans Runbook Designer, dans le ruban, cliquez sur **Arrêter**, puis sur **Orchestration Console**. Examinez la console Orchestration et dans le Résumé, sous Statistiques des instances (historique), vous devez voir une opération Réussite.
22. Fermez **Orchestration Console**.

Créer un runbook de base à l'aide des activités VMM

1. Dans Orchestrator Runbook Designer, dans le volet Connexions, développez **Runbook**, cliquez avec le bouton droit sur le dossier **22414 Runbooks**, cliquez sur **Nouveau**, sur **Runbook** et en haut du volet central, cliquez avec le bouton droit sur **Nouveau Runbook**, cliquez sur **Renommer**, sur **Oui** pour confirmer la modification de ce runbook, tapez **Point de contrôle VM**, puis appuyez sur Entrée.
2. Sous la section Activités, cliquez sur **SC 2012 Virtual Machine Manager**, cliquez sur l'activité **Shut Down VM** (Arrêter l'ordinateur virtuel) et faites-la glisser dans l'espace de travail central, puis cliquez sur l'activité **Create CheckPoint** (Créer un point de contrôle) et faites-la glisser dans l'espace de travail central, en la plaçant à droite de l'activité **Shut Down VM** (Arrêter l'ordinateur virtuel).
3. Cliquez sur l'activité **Start VM** (Démarrer l'ordinateur virtuel) et faites-la glisser dans l'espace de travail central, en la plaçant à droite de l'activité Create CheckPoint (Créer un point de contrôle).
4. Placez le pointeur de la souris sur l'activité **Shut Down VM** (Arrêter l'ordinateur virtuel), puis lorsqu'une petite flèche apparaît à droite, placez le pointeur de la souris sur la flèche. Le pointeur de la souris doit prendre la forme d'une croix. Cliquez sur la flèche, puis faites-la glisser dans **Create CheckPoint** (Créer un point de contrôle). Un lien avec une flèche doit apparaître entre les deux activités.
5. Répétez l'étape précédente, cette fois pour créer un lien entre l'activité **Create CheckPoint** (Créer un point de contrôle) et l'activité **Start VM** (Démarrer l'ordinateur virtuel).
6. Cliquez avec le bouton droit sur l'activité **Shut Down VM** (Arrêter l'ordinateur virtuel), cliquez sur **Propriétés** et dans la page **Properties** (Propriétés), dans la section Configuration, cliquez sur **...** à côté du champ **Name** (Nom). Lorsque la page **Item Selection** (Sélection d'éléments) s'ouvre, cliquez sur **LON-VMM1**, puis cliquez sur **OK**.
7. Dans la section Properties (Propriétés), dans le champ **VM ID** (ID de l'ordinateur virtuel), cliquez sur **...** pour parcourir, puis dans les options de la page **VM ID** (ID de l'ordinateur virtuel), cliquez sur l'ID qui commence par **(TOR-WEB1.Adatum.com)**. Cliquez sur **OK**, puis sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Cliquez avec le bouton droit sur l'activité **Create CheckPoint** (Créer un point de contrôle), cliquez sur **Propriétés** et dans la page **Properties** (Propriétés), dans la section Configuration, cliquez sur **...** à côté du champ **Name** (Nom). La page **Item Selection** (Sélection d'éléments) s'ouvre et dans la page **Item Selection** (Sélection d'éléments), cliquez sur **LON-VMM1**, puis sur **OK**.
9. Dans la section Properties (Propriétés), cliquez sur **...** à côté du champ **VM ID** (ID de l'ordinateur virtuel) à parcourir, puis dans les options de la page **VM ID** (ID de l'ordinateur virtuel), cliquez sur l'ID qui commence par **(TOR-WEB1.Adatum.com)**. Cliquez sur **OK**.
10. Cliquez sur **Optional Properties** (Propriétés optionnelles) et dans la page **Add/Remove Property** (Ajouter/Supprimer une propriété), cliquez sur **Description**, sur **>>**, sur **Name** (Nom), sur **>>**, puis sur **OK**. Dans la section Propriétés, dans le champ **Description**, tapez **Point de contrôle VM initial du service Web**. Dans le champ **Name** (Nom), tapez **Image de départ**, puis cliquez sur **Terminer**.
11. Cliquez avec le bouton droit sur l'activité **Start VM** (Démarrer l'ordinateur virtuel), cliquez sur **Propriétés**, puis dans la page **Properties** (Propriétés), dans la section Configuration, cliquez sur **...** à côté du champ **Name** (Nom). Lorsque la page **Item Selection** (Sélection d'éléments) s'ouvre, cliquez sur **LON-VMM1**, puis cliquez sur **OK**.
12. Dans la section Properties (Propriétés), cliquez dans le champ **VM ID** (ID de l'ordinateur virtuel), cliquez pour parcourir les options de la page VM ID (ID de l'ordinateur virtuel), cliquez sur l'ID qui commence par **(TOR-WEB1.Adatum.com)**, cliquez sur **OK**, puis sur **Terminer**.
13. Sur LON-OR1, dans la console Runbook Designer, dans le ruban, cliquez sur **Enregistrer**.
14. Sur **LON-VMM1**, dans la barre de tâches, cliquez sur **Console Virtual Machine Manager**.
15. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session Microsoft Windows** est activée, puis cliquez sur **Connecter**. La console VMM s'ouvre.
16. Cliquez sur l'espace de travail **Ordinateurs virtuels et services**.
17. Confirmez que l'ordinateur virtuel TOR-WEB1 est en cours d'exécution. Si ce n'est pas le cas, cliquez avec le bouton droit sur **TOR-WEB1**, cliquez sur **Marche**, puis attendez que l'ordinateur virtuel démarre.
18. Sur LON-OR1, dans la console Orchestrator Runbook Designer, dans le ruban, cliquez sur **Exécuter**.
19. Dans la console Virtual Machine Manager, le serveur TOR-WEB1 doit s'arrêter. Créez le point de contrôle, puis redémarrez-le. Au démarrage, sous Ordinateurs virtuels, cliquez sur **TOR-WEB1**, puis dans le ruban, cliquez sur **Gérer les points de contrôle**. Vous devez voir le point de contrôle de l'image de départ. Cliquez sur **OK**, puis fermez la console Virtual Machine Manager.
20. Sur **LON-OR1**, fermez Orchestrator Runbook Designer.

Résultats : À la fin de cet atelier pratique, vous aurez installé les packs d'intégration Virtual Machine Manager, créé un runbook de base dans Orchestrator Runbook Designer et examiné la console Web Orchestrator.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Planification de la délégation administrative et du libre-service dans System Center 2012

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lisez la documentation fournie dans le manuel du stagiaire.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

Répondez aux questions de la section Propositions du document Stratégie d'administration de la virtualisation.

1. Quel est le rôle d'administration le plus adapté pour fournir l'objectif de contrôle principal de l'équipe d'administration du développement ?

   Réponse :

   L'administrateur délégué de l'ensemble fibre optique doit permettre aux administrateurs du développement de gérer un groupe étendu de ressources. Celui-ci doit se composer de clouds privés et de groupes d'hôtes. Diverses ressources peuvent être ajoutées, si nécessaire.

2. La plupart des développeurs auront besoin de la fonction de création des comptes en libre-service, quel sera donc le rôle d'administration le mieux adapté pour eux ?

   Réponse :

   Les développeurs auront besoin de moins d'autorisations que les administrateurs du développement, les rôles de client ou de libre-service seront donc adaptés.

3. Que pouvez-vous faire pour aider à réduire les charges administratives des administrateurs du développement ?

   Réponse :

   Veillez à configurer le libre-service pour ces utilisateurs qui réclament le plus souvent de nouveaux systèmes. En outre, implémentez Orchestrator et peut-être même Service Manager.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

- Comparez vos propositions à celles présentées ci-dessus.

▶ Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur

- Préparez-vous à discuter de vos propositions avec la classe.

Exercice 3 : Configuration de l'administration déléguée et du libre-service dans VMM

▶ Tâche 1 : Configurer un rôle d'administrateur délégué dans VMM

Créer un cloud privé

1. Sur **LON-VMM1**, dans la barre de tâches, cliquez sur **Console Virtual Machine Manager**.
2. Dans la boîte de dialogue **Connexion au serveur**, vérifiez que la case à cocher **Utiliser l'identité actuelle de session Microsoft Windows** est activée, puis cliquez sur **Connecter**. La console Virtual Machine Manager s'ouvre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Cliquez sur l'espace de travail **Ordinateurs virtuels et service**, puis dans le ruban, cliquez sur **Créer un cloud**.
4. Dans la page **Général**, dans le champ **Nom**, tapez **Développement de London** et dans le champ **Description**, tapez **Cloud Développement de London**, puis cliquez sur **Suivant**.
5. Dans la page **Ressources**, sélectionnez **Hôtes de London**, puis cliquez sur **Suivant**.
6. Dans la page **Réseaux logiques**, sélectionnez **Réseau externe**, puis cliquez sur **Suivant**.
7. Dans la page **Équilibrages de charge**, sélectionnez **Microsoft Network Load Balancing (NLB)** (Équilibrage de charge réseau Microsoft (NLB)), puis cliquez sur **Suivant**.
8. Dans la page **Modèles d'adresse IP virtuelle**, cliquez sur **Suivant**.
9. Dans la page **Classifications de port**, sélectionnez **Équilibrage de la charge réseau**, **Bande passante moyenne** et **Bande passante élevée**, puis cliquez sur **Suivant**.
10. Dans la page **Stockage**, cliquez sur **Suivant**.
11. Dans la page **Bibliothèque**, dans la section Partages de bibliothèque en lecture seule, cliquez sur **Ajouter**. Sélectionnez **MSSCVMMLibrary**, cliquez sur **OK**, puis sur **Suivant**.
12. Dans la page **Capacité**, passez en revue les options de capacité. Supprimez la coche à côté de chaque ressource sélectionnée, puis attribuez ce qui suit :
    - 8 processeurs virtuels
    - 12 Go de mémoire
    - 250 Go de stockage
    - Quota personnalisé (points) : 15
    - 4 ordinateurs virtuels
13. Cliquez sur **Suivant**.
14. Dans la page **Profils de capacité**, sélectionnez **Hyper-V**, puis cliquez sur **Suivant**.
15. Vérifiez la page **Résumé**, puis cliquez sur **Terminer**.
16. Fermez la fenêtre Travaux.

Configurer l'administration déléguée dans VMM

1. Dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Paramètres**, puis dans le ruban, cliquez sur **Créer un rôle d'utilisateur**.
2. Dans la page **Nom et description**, dans le champ **Nom**, tapez **DevAdmin** et dans le champ **Description**, tapez **Administrateurs de l'équipe de développement**, puis cliquez sur **Suivant**.
3. Dans la page **Profil**, cliquez sur **Administrateur de l'ensemble fibre optique (administrateur délégué)**, puis cliquez sur **Suivant**.
4. Dans la page **Membres**, cliquez sur **Ajouter** et dans la boîte de dialogue **Sélectionnez des utilisateurs**, **des ordinateurs ou des groupes**, dans le champ **Entrez les noms des objets à sélectionner**, tapez **Rob Cason**, cliquez sur **OK**, puis sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans la page **Étendue**, sélectionnez le cloud **Développement de London** et le groupe d'hôtes **Hôtes de London**, puis cliquez sur **Suivant**.
6. Dans la page **Serveurs de bibliothèque**, cliquez sur **Ajouter**, sélectionnez **LON-VMM1.Adatum.com**, cliquez sur **OK**, puis sur **Suivant**.
7. Dans la page **Comptes d'identification**, cliquez sur **Ajouter**, sélectionnez le compte **Administrateur**, cliquez sur **OK**, puis sur **Suivant**.
8. Examinez le Résumé, puis cliquez sur **Terminer**.
9. Fermez la fenêtre Travaux.

▶ Tâche 2 : Configurer l'administration du libre-service dans VMM

Configurer le libre-service dans VMM

1. Dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Paramètres**, puis dans le ruban, cliquez sur **Créer un rôle d'utilisateur**.
2. Dans la page **Nom et description**, dans le champ **Nom**, tapez **DevFournisseurs** et dans le champ **Description**, tapez **Fournisseurs de l'équipe de développement**, puis cliquez sur **Suivant**.
3. Dans la page **Profil**, cliquez sur **Administrateur d'application (utilisateur libre-service)**, puis sur **Suivant**.
4. Dans la page **Membres**, cliquez sur **Ajouter**, tapez **Adam**, cliquez sur **OK**, puis sur **Suivant**.
5. Dans la page **Étendue**, cliquez sur **Développement de London**, puis cliquez sur **Suivant**.
6. Dans la page **Quotas pour le cloud Développement de London**, laissez les quotas par défaut, puis cliquez sur **Suivant**.
7. Dans la page **Mise en réseau**, cliquez sur **Ajouter**, sur **Réseau externe**, sur **OK**, puis sur **Suivant**.
8. Dans la page **Ressources**, cliquez sur **Ajouter** et dans la page **Ajouter des ressources**, maintenez enfoncée la touche Ctrl de votre clavier, puis cliquez sur chaque élément de la liste. Lorsque tout est sélectionné, cliquez sur **OK**, puis cliquez sur **Suivant**.
9. Dans la page **Actions**, attribuez les actions autorisées suivantes :
   - **Connexion à distance**
   - **Arrêt**
   - **Démarrer**
   - **Arrêter**
10. Lorsque vous avez sélectionné les actions autorisées, cliquez sur **Suivant**.
11. Dans la page **Résumé**, vérifiez les paramètres, puis cliquez sur **Terminer**.
12. Si vous recevez le message d'erreur **« Impossible d'effectuer le travail, car un ou plusieurs des objets sélectionnés sont verrouillés par un autre travail. »**, cliquez sur **OK** pour fermer le message.
13. Fermez la fenêtre Travaux, si elle s'affiche.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Valider la configuration

Vérifier la délégation de l'administration

1. Dans le menu supérieur de la console Virtual Machine Manager, au-dessus du ruban, cliquez sur la flèche, puis cliquez sur **Ouvrir une nouvelle connexion**. La page **Connexion au serveur** s'ouvre.
2. Dans la page **Connexion au serveur**, cliquez sur l'option **Spécifier les informations d'identification**, et entrez les données suivantes :
   - Nom d'utilisateur : **ADATUM\Rob**
   - Mot de passe : **Pa$$w0rd**
3. Cliquez sur l'espace de travail **Ordinateurs virtuels et services**.
4. Développez **Clouds**, cliquez avec le bouton droit sur **Développement de London**, puis cliquez sur **Créer un ordinateur virtuel**.
5. Dans la page **Sélectionner une source**, cliquez sur **Créer l'ordinateur virtuel avec un disque dur virtuel vide**, puis sur **Suivant**.
6. Dans la page **Spécifier l'identité de l'ordinateur virtuel**, cliquez sur le champ **Nom de l'ordinateur virtuel**, tapez **RobVM**, puis cliquez sur **Suivant**.
7. Dans la page **Configurer le matériel**, sous Compatibilité, cliquez sur **Profils de capacité du cloud**, sélectionnez le profil de capacité **Hyper-V**, puis cliquez sur **Suivant**.
8. Dans la page **Sélectionner la destination**, sélectionnez **Déployer l'ordinateur virtuel sur un cloud privé**, puis cliquez sur **Suivant**.
9. Dans la page **Sélectionner le cloud**, cliquez sur **lon-host1.adatum.com**, puis sur **Suivant**.
10. Dans la page **Ajouter des propriétés**, cliquez sur **Suivant**.
11. Dans la page **Résumé**, cliquez sur **Créer**. Fermez la fenêtre Travaux, puis fermez l'instance DevAdmin de la console Virtual Machine Manager.
12. Dans l'instance Administrateur de la console Virtual Machine Manager, cliquez sur l'espace de travail **Ordinateurs virtuels et services**, puis cliquez sur la flèche à côté de Clouds, et vous devez voir le cloud Développement de London.
13. Cliquez sur le cloud **Développement de London**, puis dans le ruban, cliquez sur **Vue d'ensemble**. Notez que vous pouvez voir les rôles d'utilisateurs et les propriétaires d'ordinateur virtuel. Confirmez que vous pouvez voir les rôles **DevAdmin** et **DevFournisseurs**. Cliquez pour développer ces rôles et afficher les utilisateurs qui leur sont attribués. Examinez les détails dans cette page.

Vérifier le libre-service dans VMM

1. Dans le menu supérieur de la console Virtual Machine Manager, au-dessus du ruban, cliquez sur la flèche, puis cliquez sur **Ouvrir une nouvelle connexion**. La page **Connexion au serveur** s'ouvre.
2. Connectez-vous à la console Virtual Machine Manager en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Adam**
   - Mot de passe : **Pa$$w0rd**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Cliquez sur l'espace de travail **Ordinateurs virtuels et services**. Cliquez sur la flèche à côté de Clouds.
4. Cliquez avec le bouton droit sur le cloud **Développement de London**, puis cliquez sur **Créer un ordinateur virtuel**.
5. Dans la page **Sélectionner une source**, cliquez sur **Créer l'ordinateur virtuel avec un disque dur virtuel vide**, puis sur **Suivant**.
6. Dans la page **Spécifier l'identité de l'ordinateur virtuel**, dans le champ **Nom de l'ordinateur virtuel**, tapez **AdamVM**, puis cliquez sur **Suivant**.
7. Dans la page **Configurer le matériel**, cliquez sur **Suivant**.
8. Une page d'avertissement doit s'afficher indiquant que vous ne disposez pas de l'autorisation requise pour effectuer cette opération. Cliquez sur **OK** pour fermer l'avertissement. Cliquez sur **Annuler**, puis sur **Oui**.
9. Fermez l'instance **DevFournisseurs** de la console Virtual Machine Manager.

Connecter App Controller à VMM

1. Sur **LON-VMM1**, déplacez la souris sur le coin inférieur gauche jusqu'à ce que l'icône **Accueil** apparaisse, cliquez sur l'icône **Accueil**, puis lorsque l'interface utilisateur Windows apparaît, cliquez sur **App Controller**.
2. Dans la page **Entrez vos informations d'identification pour vous connecter**, dans le champ **Nom d'utilisateur**, tapez **ADATUM\Administrateur** et dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Connexion**.
3. Dans la page **Vue d'ensemble**, sous État, cliquez sur **Connecter un serveur Virtual Machine Manager et des clouds**. Dans la page **Ajouter une nouvelle connexion VMM**, cliquez sur le champ **Nom de la connexion**, puis tapez **LON-VMM1.adatum.com**. Dans le champ Description, tapez **Accès au serveur VMM de London**. Dans le champ **Nom du serveur**, tapez **LON-VMM1.adatum.com**, puis cliquez sur **OK**.
4. Dans la page **Vue d'ensemble**, dans le coin supérieur droit du navigateur, cliquez sur **Déconnexion**.

Vérifier le libre-service dans App Controller

1. Dans la page **Entrez vos informations d'identification pour vous connecter**, dans le champ **Nom d'utilisateur**, tapez **ADATUM\Adam** et dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Connexion**.
2. Dans la page **Vue d'ensemble**, sous Étapes suivantes, cliquez sur **Déployer un nouveau service ou un nouvel ordinateur virtuel**. La fenêtre Nouveau déploiement s'ouvre. Au centre de l'écran, cliquez sur **Configurer**.
3. Dans la page **Sélectionner un cloud pour ce déploiement**, cliquez sur **OK** et dans la section MODÈLE, cliquez sur **Sélectionner un modèle** et dans la page **Choisir un modèle**, cliquez sur **Service Web Adatum**, puis sur **OK**.
4. Dans la section SERVICE, cliquez sur **Configurer**, dans la page **Propriétés de Service Web ADATUM service**, dans le champ **Nom du service**, tapez **Service Fournisseur** et dans le champ **Centre de coûts**, tapez **Développement de London**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans la section INSTANCE, cliquez sur **Configurer** et dans le champ **Nom de l'ordinateur**, tapez **LON-WEB1**, cliquez sur **OK**, puis sur **Déployer**.
6. À gauche de la console App Controller, cliquez sur l'espace de travail **Travaux**. Vous devez voir le travail Créer un déploiement du service avec l'état En cours. Le déploiement prendra un certain temps, vous pouvez donc revenir à la console Virtual Machine Manager pour vérifier l'état de déploiement dans le détail.
7. Pour examiner l'état de déploiement détaillé, dans la console Virtual Machine Manager, cliquez sur l'espace de travail **Travaux**, puis dans la section Travail en cours de exécution, cliquez sur **Créer une instance de service**. La partie inférieure de l'écran affiche les étapes individuelles et le fichier de déploiement, en bits par seconde (bits/s) via HTTPS, vous donnera une indication de la progression.
8. Lorsque le déploiement est terminé, fermez toutes les consoles.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez les ordinateurs virtuels à leur état initial en procédant comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-VMM1**, **22414B-LON-OR1** et **22414B-TOR-SVR1**.
5. Sur **LON-HOST1**, cliquez sur l'écran Accueil, puis sur **Panneau de configuration**. Cliquez sur **Désinstaller un programme**, puis désinstallez **Microsoft System Center Virtual Machine Manager Agent (x64)** et **Microsoft System Center Virtual Machine Manager DHCP Server (x64)**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 6 : Planification et implémentation d'une stratégie d'analyse des serveurs

Atelier pratique : Implémentation d'une stratégie d'analyse des serveurs

Exercice 1 : Configuration de l'analyse des serveurs à l'aide de Windows Server 2012

▶ Tâche 1 : Configurer le Gestionnaire de serveur pour surveiller plusieurs serveurs

1. Sur TOR-SVR1, dans le Gestionnaire de serveur, sur le Tableau de bord, cliquez sur **Ajouter d'autres serveurs à gérer**.
2. Dans la boîte de dialogue **Ajouter des serveurs**, dans la zone **Nom (CN)**, tapez **TOR-SS1**, puis cliquez sur **Rechercher maintenant**.
3. Dans les résultats de recherche, cliquez sur **TOR-SS1**, cliquez sur la flèche pointant vers la droite pour ajouter le serveur à la zone **Sélectionné**, puis cliquez sur **OK**.
4. Dans le **Tableau de bord**, cliquez sur **Créer un groupe de serveurs**.
5. Dans la boîte de dialogue **Créer un groupe de serveurs**, dans la zone **Nom du groupe de serveurs**, tapez **Serveurs de Toronto**.
6. Dans la liste des serveurs, cliquez sur **TOR-SVR1.Adatum.com**, puis appuyez sur la touche Ctrl et cliquez sur **TOR-SS1.Adatum.com**.
7. Cliquez sur la flèche pointant vers la droite pour ajouter les serveurs à la zone **Sélectionné**, puis cliquez sur **OK**.
8. Dans le Gestionnaire de serveur, cliquez sur **Serveurs de Toronto**.
9. Dans la zone **SERVEURS**, cliquez sur **TOR-SS1**.
10. Dans le Gestionnaire de serveur, faites défiler l'écran jusqu'à **BEST PRACTICE ANALYZER**, à droite de BEST PRACTICE ANALYZER, cliquez sur **TÂCHES**, puis cliquez sur **Commencer l'analyse BPA**.
11. Dans la boîte de dialogue **Sélection des serveurs**, cliquez sur **Rechercher**. L'analyse peut prendre entre 2 et 5 minutes.
12. Dans le Gestionnaire de serveurs, faites défiler l'écran vers la zone **PERFORMANCES**, à droite des PERFORMANCES, cliquez sur **TÂCHES**, puis sur **Configurer des alertes de performances**.
13. Dans la boîte de dialogue **Serveurs de Toronto : configurer les alertes de performance**, dans la zone **Utilisation du processeur (%)**, tapez **75**.
14. Dans la zone **Mémoire (Mo disponibles)**, tapez **100**, puis cliquez sur **Enregistrer**.
15. Dans la liste des serveurs sous le graphique des performances, cliquez avec le bouton droit sur **TOR-SS1**, puis cliquez sur **Démarrer les compteurs de performances**.

Remarque : L'affichage des données peut prendre 30 minutes ou plus. Passez à l'exercice suivant. À la fin de l'atelier pratique, vous vérifierez les données.

16. Dans le Gestionnaire de serveur, faites défiler l'écran jusqu'à **RÔLES ET FONCTIONNALITÉS**, à droite de RÔLES ET FONCTIONNALITÉS, cliquez sur **TÂCHES**, puis sur **Ajouter des rôles et fonctionnalités**.
17. Dans l'Assistant **Ajouter des rôles et fonctionnalités**, dans la page **Avant de commencer**, cliquez sur **Suivant**.
18. Dans la page **Sélectionner le type d'installation**, assurez-vous que l'option **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.
19. Dans la page **Sélectionner le serveur de destination**, cliquez sur **TOR-SS1.Adatum.com**, puis cliquez sur **Suivant**.
20. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Serveur Web (IIS)**, dans la boîte de dialogue **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
21. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
22. Dans la page **Rôle Web Server (IIS)**, cliquez sur **Suivant**.
23. Dans la page **Sélectionner des services de rôle**, cliquez sur **Suivant**.
24. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
25. Dans la page **Résultats**, patientez jusqu'à la fin de l'exécution de la tâche **Installation de fonctionnalité**, puis cliquez sur **Fermer**.

▶ Tâche 2 : Configurer un ensemble de collecteurs de données

1. Sur TOR-SVR1, dans le Gestionnaire de serveur, cliquez sur **Serveurs de Toronto**.
2. Dans la zone **SERVEURS**, cliquez avec le bouton droit sur **TOR-SVR1** et, dans la zone de liste déroulante, cliquez sur **Gestion de l'ordinateur**.
3. Dans la fenêtre **Gestion de l'ordinateur**, dans le volet gauche, développez **Performance**, puis **Ensembles de collecteurs de données**.
4. Sous **Ensembles de collecteurs de données**, développez **Définis par l'utilisateur**, puis cliquez sur **Server Manager Performance Monitor** (Analyseur de performances du Gestionnaire de serveur).
5. Cliquez sur **Définis par l'utilisateur**.
6. Dans le volet **Actions**, cliquez sur **Autres actions** et, dans la zone de liste déroulante, cliquez sur **Nouveau**, puis cliquez sur **Ensemble de collecteurs de données**.
7. Dans la page **Créer un nouvel ensemble de collecteurs de données**, dans la zone **Nom**, tapez **Ressources principales**, puis cliquez sur **Suivant**.
8. Dans la page **Quel modèle voulez-vous utiliser ?**, cliquez sur **System Performance** (Performances du système), puis sur **Suivant**.
9. Dans la page **Où enregistrer les données ?**, cliquez sur **Suivant**.
10. Dans la page **Créer l'ensemble de collecteurs de données**, cliquez sur **Terminer**.
11. Cliquez avec le bouton droit sur **Ressources principales**, puis cliquez sur **Propriétés**.
12. Cliquez sur l'onglet **Planification**, puis sur **Ajouter**.
13. Dans la boîte de dialogue **Action du dossier**, dans la zone **Heure de début**, tapez **8:00:00**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

14. Vérifiez que seuls les jours suivants sont activés, puis cliquez sur **OK**:
    - **Lundi**
    - **Mardi**
    - **Mercredi**
    - **Jeudi**
    - **Vendredi**
15. Cliquez sur l'onglet **Condition d'arrêt**, puis dans la zone **Durée globale**, tapez **10**.
16. À droite de **Durée globale**, dans la zone de liste déroulante **Unités**, cliquez sur **Heures**, et cliquez sur **OK**.
17. Cliquez sur **Ressources principales**, puis double-cliquez sur **Performance Counter** (Compteur de performance).
18. Dans la boîte de dialogue **Propriétés de : Performance Counter**, examinez les compteurs collectés, puis dans la zone **Intervalle d'échantillonnage**, vérifiez que l'intervalle est défini sur **1**.
19. Dans la zone de liste déroulante **Unités,** cliquez sur **Minutes**, puis sur **OK**.
20. Cliquez avec le bouton droit sur **NT Kernel** (Noyau NT), cliquez sur **Supprimer**, puis sur **Oui**.
21. Sous **Définis par l'utilisateur**, cliquez avec le bouton droit sur **Ressources principales** et cliquez sur **Démarrer**.
22. Patientez 10 minutes, puis cliquez avec le bouton droit sur **Ressources principales**, puis dans la zone de liste déroulante, cliquez sur **Arrêter**.

Cliquez avec le bouton droit sur **Ressources principales**, puis dans la zone de liste déroulante, cliquez sur **Dernier rapport**.

Remarque : Si le collecteur de données s'exécute toujours, un message d'état de rapport disant **Collecte des données pendant 3600 secondes...** s'affichera.

23. Dans le **Rapport de performances du système**, cliquez sur **Processeur**, sur **Processus**, puis affichez les compteurs collectés.
24. Examinez le rapport, puis fermez la gestion de l'ordinateur.

▶ Tâche 3 : Configurer un abonnement aux événements

1. Sur TOR-SVR1, cliquez sur l'écran d'accueil, puis sur **Outils d'administration**.
2. Dans la fenêtre Outils d'administration, cliquez sur **Observateur d'événements**.
3. Dans la fenêtre Observateur d'événements, cliquez sur **Abonnements**.
4. Dans la boîte de dialogue **Observateur d'événements**, cliquez sur **Oui** pour démarrer le service Collecteur d'événements.
5. Dans le volet Actions, cliquez sur **Créer un abonnement**.
6. Dans la boîte de dialogue **Propriétés de l'abonnement**, dans la zone **Nom d'abonnement**, tapez **Événements TOR-SS1**, puis cliquez sur **Sélectionner des ordinateurs...**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Dans la boîte de dialogue **Ordinateurs**, cliquez sur **Ajouter des ordi. du domaine...**.
8. Dans la boîte de dialogue **Sélectionnez un ordinateur**, dans la zone **Entrez le nom de l'objet à sélectionner (exemples) :** tapez **TOR-SS1**, cliquez sur **Vérifier les noms**, puis sur **OK**.
9. Cliquez sur **Sélectionner des événements**.
10. Dans la boîte de dialogue **Filtre de requête**, cliquez sur **Critique** et sur **Erreur**.
11. Dans la zone de liste déroulante **Journaux d'événements**, activez la case à cocher à gauche de **Journaux Windows**, puis cliquez en dehors de la liste déroulante et sur **OK**.
12. Cliquez de nouveau sur **OK**.
13. Dans le Gestionnaire de serveur, sélectionnez **TOR-SS1** pour gérer le serveur à distance. Cliquez sur **Outils**, puis dans la zone de liste déroulante, cliquez sur **Gestion de l'ordinateur**.
14. Dans Gestion de l'ordinateur, développez **Utilisateurs et groupes locaux**, puis cliquez sur **Groupes**.
15. Dans la liste des groupes, cliquez avec le bouton droit sur **Lecteurs des journaux d'événements**, puis sur **Ajouter au groupe**.
16. Dans la boîte de dialogue **Propriétés de : Lecteurs des journaux d'événements**, cliquez sur **Ajouter**.
17. Dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs, des comptes de servi...**, cliquez sur **Types d'objets**.
18. Dans la boîte de dialogue **Types d'objets**, cliquez sur **des ordinateurs**, puis cliquez sur **OK**.
19. Dans la zone **Entrez les noms des objets à sélectionner (exemples) :**, tapez **TOR-SVR1**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
20. Dans la boîte de dialogue **Propriétés de : Lecteurs des journaux d'événements**, cliquez sur **OK**.
21. Affichez les événements transférés dans l'Observateur d'événements. Le transfert des événements peut prendre plusieurs minutes.

Résultats : Après avoir terminé cet exercice, vous devriez avoir configuré l'analyse pour les serveurs à l'aide des outils disponibles dans Windows Server® 2012.

Exercice 2 : Implémentation de l'agent Microsoft System Center 2012 - Operations Manager

▶ Tâche 1 : Déployer l'agent Microsoft® System Center 2012 Operations Manager (Operations Manager) à l'aide de la détection

1. Sur LON-OM1, sur l'écran d'accueil, cliquez sur **Operations Console** (Console Opérateur).
2. Dans Operations Console, dans le volet gauche inférieur, cliquez sur **Administration**.
3. Dans l'espace de travail Administration, dans le volet central, cliquez sur **Assistant Détection**.
4. Dans l'Assistant Gestion des ordinateurs et des périphériques, dans la page **Type de détection**, vérifiez que l'option **Ordinateurs Windows** est sélectionnée, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans la page **Automatique ou avancé ?**, vérifiez que l'option **Détection avancée** est sélectionnée, puis cliquez sur **Suivant**.
6. Dans la page **Méthode de détection**, cliquez sur **Rechercher ou taper des noms d'ordinateurs**, dans la zone située au-dessous, tapez **LON-SVR1, LON-SVR2**, puis cliquez sur **Suivant**.
7. Dans la page **Compte d'administrateur**, cliquez sur **Détecter**.
8. Dans la page **Sélectionner les objets à gérer**, cliquez sur **Sélectionner tout**, puis sur **Suivant**.
9. Dans la page **Résumé**, cliquez sur **Terminer**.
10. Dans la fenêtre **État de la tâche de gestion de l'agent**, attendez la fin de la tâche, puis fermez la fenêtre.
11. Basculez vers LON-SVR1.
12. Sur l'écran d'accueil, cliquez sur **Outils d'administration**.
13. Dans la fenêtre Outils d'administration, double-cliquez sur **Services**.
14. Dans la fenêtre Services, vérifiez que le service **System Center Management** (Administration de System Center) a démarré.

▶ Tâche 2 : Déployer l'agent Operations Manager manuellement

1. Sur LON-OM1, dans la console Opérateur, cliquez sur **Administration**.
2. Dans l'espace de travail Administration, dans le volet d'administration, cliquez sur **Paramètres**, puis double-cliquez sur **Sécurité**.
3. Dans la boîte de dialogue **Paramètres globaux du serveur d'administration – Sécurité**, cliquez sur **Vérifier les nouvelles installations manuelles d'agents dans l'affichage d'administration en attente**, puis sur **OK**.
4. Basculez vers LON-DC1.
5. Cliquez sur l'écran d'accueil, tapez **Exécuter**, puis dans le volet de résultats **Applications**, cliquez sur **Exécuter**.
6. Dans la boîte de dialogue **Exécuter**, dans la zone **Ouvrir**, tapez **\\LON-OM1\c$**, puis cliquez sur **OK**.
7. Dans la fenêtre **c$**, développez **Programmes**, **System Center 2012**, **Operations Manager**, **Server**, **AgentManagement**, puis **amd64**.
8. Double-cliquez sur **MOMAgent.msi**.

 **Remarque :** Si une boîte de dialogue d'avertissement de sécurité s'affiche avec le titre **Fichier ouvert – Avertissement de sécurité**, cliquez sur **Exécuter**.

9. Dans la boîte de dialogue **System Center 2012 – Operations Manager Agent Setup** (Installation de l'agent System Center 2012 – Operations Manager), cliquez sur **Next** (Suivant).
10. Dans la page **IMPORTANT NOTICE** (Remarque importante), cliquez sur **I agree** (J'accepte).
11. Dans la page **Destination Folder** (Dossier de destination), cliquez sur **Next** (Suivant).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

12. Dans la page **Management Group Configuration** (Configuration du groupe d'administration), cliquez sur **Next** (Suivant).
13. Dans la page **Management Group Configuration** (Configuration du groupe d'administration), dans la zone **Management Group Name** (Nom du groupe d'administration), tapez **Adatum**. Dans la zone **Management Server** (Serveur d'administration), tapez **LON-OM1**, puis cliquez sur **Next** (Suivant).
14. Dans la page **Agent Action Account** (Compte d'action d'agent), vérifiez que l'option **Local System** (Système local) est sélectionnée, puis cliquez sur **Suivant**.
15. Dans la page **Microsoft Update**, cliquez sur **Next** (Suivant).
16. Dans la page **Ready to Install** (Prêt pour l'installation), cliquez sur **Install** (Installer). Attendez la fin de la tâche, puis cliquez sur **Finish** (Terminer).
17. Dans le Gestionnaire de serveur, cliquez sur **Serveur local**.
18. Faites défiler l'écran jusqu'à **SERVICES** et localisez le service **System Center Management**.

 **Remarque :** vous pourrez avoir besoin d'actualiser l'affichage pour voir le service et de trier la liste par nom de service pour le localiser plus facilement. Si vous ne voyez pas le service après actualisation, cliquez sur OUTILS dans le Gestionnaire de serveur, puis sur Services. Localisez le service dans la console de gestion Services.

19. Basculez vers LON-OM1.
20. Dans la console Opérateur, dans l'espace de travail Administration, cliquez sur **Gestion en attente**.
21. Dans la liste Installation manuelle d'un agent, cliquez sur **LON-DC1.Adatum.com**.
22. Dans le volet des tâches, cliquez sur **Approuver**.
23. Dans la boîte de dialogue **Installation manuelle d'un agent**, cliquez sur **Approuver**.
24. Dans le volet Administration, cliquez sur **Géré par agent**. Notez que LON-DC1 s'affiche désormais.

 **Remarque :** la mise à jour de l'état de LON-DC1 peut prendre entre 5 et 10 minutes.

Résultats : Après avoir terminé cet exercice, vous devriez avoir installé et vérifié l'agent Operations Manager sur les ordinateurs du centre de données de Londres.

Exercice 3 : Configuration des composants d'analyse d'Operations Manager

▶ Tâche 1 : Installer et configurer les packs d'administration

1. Sur LON-OM1, dans la console Opérateur, dans le volet gauche, cliquez sur **Administration**.
2. Dans l'espace de travail Administration, sous le nœud **Administration**, cliquez sur **Packs d'administration**.
3. Dans le volet des tâches, cliquez sur **Importer les packs d'administration**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans la boîte de dialogue **Importer les packs d'administration**, cliquez sur **Ajouter**, puis dans la zone de liste déroulante Ajouter, cliquez sur **Ajouter à partir du disque**.
5. Dans la boîte de dialogue **Connexion au catalogue en ligne**, cliquez sur **Non**.
6. Dans la boîte de dialogue **Sélectionnez les packs d'administration à importer**, développez le lecteur **C**, développez **Program Files (x86)**, développez **System Center Management Packs**, développez **System Center Monitoring Pack for SQL Server**, sélectionnez tous les fichiers de packs d'administration SQL Server, puis cliquez sur **Ouvrir**.
7. Dans la page **Sélectionner les packs d'administration**, cliquez sur **Installer**. Attendez que les packs d'administration soient importés, puis cliquez sur **Fermer**.
8. Faites défiler la liste des packs d'administration vers le bas pour localiser les nouveaux packs d'administration.
9. Dans le volet gauche inférieur, cliquez sur **Analyse**.
10. Dans l'espace de travail Analyse, développez **Microsoft SQL Server**, puis cliquez sur **Ordinateurs**. Vous devrez peut-être patienter quelques secondes avant que LON-OM1.Adatum.com ne s'affiche.
11. Dans la console Opérateur, dans le volet gauche inférieur, cliquez sur **Administration**.
12. Dans l'espace de travail Administration, dans le volet Administration, cliquez sur **Packs d'administration**.
13. Dans le volet des tâches, cliquez sur **Créer un pack d'administration**.
14. Dans la boîte de dialogue **Créer un pack d'administration**, dans la page **Propriétés générales**, dans la zone **Nom**, tapez **SQL Server 2008 (Analyse) – Remplacements**, puis cliquez sur **Suivant**.
15. Dans la page **Base de connaissances**, cliquez sur **Créer**.
16. Dans la console Opérateur, dans le volet gauche inférieur, cliquez sur **Création** pour ouvrir l'espace de travail Création.
17. Dans le volet de création, développez **Objets du pack d'administration**, puis cliquez sur **Moniteurs**.
18. Dans la barre jaune en haut du volet Analyseurs, cliquez sur **Modifier l'étendue**.
19. Dans la boîte de dialogue **Étendre les objets du pack d'administration**, cliquez sur **Effacer tout**, sur **Afficher toutes les cibles**, puis dans la zone **Rechercher**, tapez **SQL Server 2008**.
20. Dans la liste des cibles, cliquez sur **Fichier de base de données SQL Server 2008**, puis sur **OK**.
21. Développez **Fichier de base de données SQL Server 2008**, développez **Intégrité de l'entité**, développez **Performances**, puis cliquez sur **Espace du fichier de base de données**.
22. Dans le volet des tâches, cliquez sur **Remplacement**, dans la zone de liste déroulante, cliquez sur **Remplacer le Analyse**, puis sur **Pour tous les objets de la classe : Fichier de base de données SQL Server 2008**.
23. Dans la boîte de dialogue **Propriétés du remplacement**, activez la case à cocher **Seuil inférieur**, puis remplacez la **Valeur de remplacement** par **20**.
24. Activez la case **Seuil supérieur**, puis remplacez la **Valeur de remplacement** par 30.
25. Dans la zone de liste déroulante **Sélectionnez le pack d'administration de destination**, cliquez sur **SQL Server 2008 (Analyse) – Remplacements**, puis sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer les notifications

1. Dans la console Opérateur, dans le volet gauche inférieur, cliquez sur **Administration**.
2. Dans le volet Administration, sous le nœud **Notifications**, cliquez sur **Canaux**.
3. Dans le volet des tâches, cliquez sur **Nouveau**, puis dans la zone de liste déroulante, cliquez sur **Courrier électronique (SMTP)**.
4. Dans la boîte de dialogue **Canal de notification par courrier électronique**, dans la page **Description**, dans la zone **Nom du canal**, tapez **Canal de notification SMTP**, puis cliquez sur **Suivant**.
5. Dans la page **Paramètres**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Ajouter un serveur SMTP**, dans la zone **Serveur SMTP (nom de domaine complet)**, tapez **LON-SVR1.Adatum.com**, puis cliquez sur **OK**.
7. Dans la zone **Adresse de retour**, tapez **om@adatum.com**, puis cliquez sur **Suivant**.
8. Dans la page **Format**, notez les variables utilisées dans l'objet et le message du courrier électronique, puis cliquez sur **Terminer**.
9. Patientez jusqu'à la fin de la tâche, puis cliquez sur **Fermer**.
10. Dans le volet Administration, cliquez sur **Abonnés**.
11. Dans le volet des tâches, cliquez sur **Nouveau**.
12. Dans la boîte de dialogue **Assistant d'abonné aux notifications**, dans la page **Description**, dans **Nom d'abonné**, tapez **ADATUM\Administrateur**, puis cliquez sur **Suivant**.
13. Dans la page **Planifier**, cliquez sur **Envoyer des notifications uniquement dans les plages horaires spécifiées**, puis cliquez sur **Ajouter**.
14. Dans la boîte de dialogue **Spécifier la planification**, sous **Périodicité hebdomadaire**, cliquez sur **Du**, puis définissez la première heure sur **8 h 00** et la seconde sur **20 h 00**.
15. Sous **Les jours suivants de la semaine**, cliquez sur **Lundi**, **Mardi**, **Mercredi**, **Jeudi**, **Vendredi** et **Samedi**, puis cliquez sur **OK**.
16. Dans la page **Planifier**, cliquez sur **Suivant**.
17. Dans la page **Adresses**, cliquez sur **Ajouter**.
18. Dans la boîte de dialogue **Décrire l'adresse d'abonné**, dans la zone **Nom d'adresse**, tapez **ADATUM\Administrateur**, puis cliquez sur **Suivant**.
19. Dans la zone de liste déroulante **Type de canal**, cliquez sur **Courrier électronique (SMTP)**.
20. Dans la zone **Adresse de remise pour le canal sélectionné**, tapez **administrateur@adatum.com**, puis cliquez sur **Suivant**.
21. Dans la page **Planifier**, cliquez sur **Terminer**.
22. Dans la page **Adresses**, cliquez sur **Terminer**, puis sur **Fermer**.
23. Dans la console Opérateur, dans le volet gauche inférieur, cliquez sur **Administration**.
24. Dans le volet Administration, cliquez sur **Abonnements**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

25. Dans le volet des tâches, cliquez sur **Nouveau**.
26. Dans la boîte de dialogue **Création d'abonnement aux notifications**, dans la zone **Nom d'abonnement**, tapez **Alertes SQL critiques**, puis cliquez sur **Suivant**.
27. Dans la page **Critères**, dans la liste **Conditions**, cliquez sur **déclenché(e) par toute instance d'un groupe spécifique** et **de gravité spécifique**.
28. Dans la zone **Description des critères (cliquez sur la valeur soulignée pour modifier) :**, cliquez sur la première occurrence de **spécifique**.
29. Dans la boîte de dialogue **Recherche de groupes**, dans la zone **Filtrer par (facultatif)**, tapez **SQL**, puis cliquez sur **Rechercher**.
30. Dans la liste **Groupes disponibles**, cliquez sur **SQL Server 2008 Computers** (Ordinateurs SQL Server 2008), sur **Ajouter**, puis sur **OK**.
31. Dans la zone **Description des critères (cliquez sur la valeur soulignée pour modifier) :**, cliquez sur la seconde occurrence de **spécifique**.
32. Dans la boîte de dialogue **Type d'alerte**, cliquez sur **Critique**, puis cliquez sur **OK**.
33. Dans la page **Critères**, cliquez sur **Suivant**.
34. Dans la page **Abonnés**, cliquez sur **Ajouter**.
35. Dans la boîte de dialogue **Recherche d'abonnés**, cliquez sur **Rechercher**, sur **ADATUM\Administrateur**, sur **Ajouter**, puis sur **OK**.
36. Dans la page **Abonnés**, cliquez sur **Suivant**.
37. Dans la page **Canaux**, cliquez sur **Ajouter**.
38. Dans la boîte de dialogue **Recherche de canaux**, cliquez sur **Rechercher**, sur **Canal de notification SMTP**, sur **Ajouter**, puis sur **OK**.
39. Dans la page **Canaux**, cliquez sur **Suivant**.
40. Dans la page **Résumé**, cliquez sur **Terminer**, puis sur **Fermer**.

▶ Tâche 3 : Vérifier les compteurs de performance

1. Basculez vers **TOR-SVR1**, dans le Gestionnaire de serveur, cliquez sur **Serveurs de Toronto**.
2. Dans la zone **SERVEURS**, cliquez sur **TOR-SS1**.
3. Faites défiler l'écran vers la zone **PERFORMANCES**, puis affichez les données de performances sur le graphique.

 **Remarque :** L'affichage des données peut prendre 30 minutes ou plus. Si les données ne s'affichent pas encore à ce stade, laissez les ordinateurs virtuels s'exécuter pendant le cours et revérifiez plus tard.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V®.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-SVR2**, **22414B-LON-OM1**, **22414B-TOR-SS1** et **22414B-TOR-SVR1**.

Résultats : Après avoir terminé cet exercice, vous devriez avoir importé et configuré le pack d'administration Microsoft SQL Server® dans Operations Manager.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 7 : Planification et implémentation d'une haute disponibilité pour des services et des applications de fichiers

Atelier pratique : Planification et implémentation d'une haute disponibilité pour des services et des applications de fichiers

Exercice 1 : Planification d'une stratégie de haute disponibilité pour des services de fichiers

▶ Tâche 1 : Lire la documentation fournie avec le produit

1. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur la vignette du **Bureau**.
3. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
4. Accédez à **\\LON-DC1\E$\Labfiles\Module6**.
5. Ouvrez le fichier **email1.docx**.
6. À l'invite **Nom d'utilisateur**, cliquez sur **OK**. Dans la boîte de dialogue **Bienvenue dans Microsoft Office 2010**, cliquez sur **Ne pas apporter de modifications**, puis cliquez sur **OK**.
7. Consultez les informations, puis fermez le document.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

1. Sur LON-CL1, utilisez l'Explorateur de fichiers pour accéder à **\\LON-DC1\E$\Labfiles\Module6**.
2. Ouvrez le fichier **Proposal1.docx**, puis renseignez les suggestions pour traiter chacun des problèmes répertoriés.
3. Fermez le document.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

1. Sur LON-CL1, utilisez l'Explorateur de fichiers pour accéder à **\\LON-DC1\E$\Labfiles\Module6**.
2. Ouvrez le fichier **FinalProposal1.docx**, comparez vos réponses, puis présentez-les à la classe.
3. Fermez le fichier.

Résultats : Après avoir terminé cet exercice, vous devez avoir planifié une stratégie de haute disponibilité pour des serveurs de fichiers.

Les stagiaires concevront le déploiement de l'espace de stockage. La conception doit intégrer les serveurs et composants réseau qui seront déployés, ainsi que les unités de stockage. La conception doit également contenir des remarques au sujet des fonctionnalités hautement disponibles que le déploiement inclut, comme l'association de cartes d'interface réseau (NIC) sur les serveurs, Microsoft Multipath I/O (MPIO) pour le chemin d'accès réseau, et les niveaux RAID sur le compartiment de stockage.

Les stagiaires concevront également le déploiement DFS. La conception inclura les emplacements des serveurs, les espaces de noms DFS déployés et cibles DFS. La conception doit comprendre des remarques sur la configuration pour la configuration de réplication DFS.

Exercice 2 : Planification d'une stratégie de haute disponibilité pour des applications Web

▶ Tâche 1 : Lire la documentation fournie avec le produit

1. Sur LON-CL1, utilisez l'Explorateur de fichiers pour accéder à **\\LON-DC1\E$\Labfiles\Module6**.
2. Ouvrez le fichier **email2.docx**, puis analysez-le.
3. Fermez le document.

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

1. Sur LON-CL1, utilisez l'Explorateur de fichiers pour accéder à **\\LON-DC1\E$\Labfiles\Module6**.
2. Ouvrez le fichier **Proposal2.docx**, puis renseignez les suggestions pour traiter chacun des problèmes répertoriés.
3. Fermez le fichier.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

1. Sur LON-CL1, utilisez l'explorateur de fichiers pour accéder à **\\LON-DC1\E$\Labfiles\Module6**.
2. Ouvrez le fichier **FinalProposal2.docx**, comparez vos réponses, puis présentez-les à la classe.
3. Fermez le fichier.

Résultats : Après avoir terminé cet exercice, vous devez avoir planifié une stratégie de haute disponibilité pour des applications Web, y compris les éléments suivants :

- votre conception de déploiement NLB doit inclure le déploiement du serveur et la conception de stockage. Utilisez les informations de l'exercice précédent pour planifier la conception du stockage ;
- votre conception doit intégrer les règles de port NLB et la conception des paramètres réseau.

Exercice 3 : Implémentation d'une solution de haute disponibilité pour le stockage de fichiers

▶ Tâche 1 : Configurer une association de cartes d'interface réseau (NIC)

1. Connectez-vous à TOR-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Serveur local**.
3. Dans le volet PROPRIÉTÉS Pour TOR-SVR1, à droite de **Connexion au réseau local**, cliquez sur l'adresse IP répertoriée.
4. Dans la boîte de dialogue **Connexions réseau**, sélectionnez et cliquez avec le bouton droit sur **Connexion au réseau local 2**, puis cliquez sur **Activer**. Répétez cette étape en activant **Connexion au réseau local 3** et **Connexion au réseau local 4**.
5. Fermez la boîte de dialogue **Connexions réseau**.
6. Actualisez le volet PROPRIÉTÉS Pour TOR-SVR1, puis à droite de **Association de cartes réseau**, cliquez sur **Désactivé**.
7. Dans la fenêtre Association de cartes réseau, dans le volet CARTES ET INTERFACES, cliquez sur **Connexion au réseau local**. Appuyez sur la touche Ctrl et maintenez-la enfoncée, puis cliquez sur **Connexion au réseau local 2**.
8. Dans la fenêtre Association de cartes réseau, dans le volet CARTES ET INTERFACES, cliquez sur **TÂCHES**. Dans le menu déroulant, cliquez sur **Ajouter à une nouvelle équipe**.
9. Dans le champ **Nom de l'équipe**, tapez **Association d'accès iSCSI 1**, puis cliquez sur **OK**.
10. Fermez la fenêtre Association de cartes réseau.
11. Cliquez sur l'écran Accueil, sur **Panneau de configuration**, sur **Réseau et Internet**, puis sur **Centre Réseau et partage**.
12. Dans Centre Réseau et partage, cliquez sur **Modifier les paramètres de la carte**.
13. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur **Association d'accès iSCSI 1**, puis cliquez sur **Propriétés**.

UTILISATION PRIVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

14. Dans la boîte de dialogue **Propriétés de Association d'accès iSCSI 1**, double-cliquez sur **Protocole Internet version 4 (TCP/IPv4)**.
15. Cliquez sur **Utiliser l'adresse IP suivante**, puis entrez les paramètres suivants :
    - Adresse IP : **172.16.1.20**
    - Masque de sous-réseau : **255.255.0.0**
    - Passerelle par défaut : **172.16.0.1**
16. Cliquez sur **Utiliser l'adresse de serveur DNS suivante**, puis tapez **172.16.0.10** dans le champ **Serveur DNS préféré**. Cliquez sur **Oui**, puis sur **OK**.
17. Cliquez sur **OK**, puis sur **OK** pour fermer la boîte de dialogue **Propriétés de Association d'accès iSCSI 1**.
18. Fermez la fenêtre Connexions réseau.
19. Fermez la fenêtre Centre Réseau et partage.
20. Dans le Gestionnaire de serveur, cliquez sur **Serveur local**.
21. Dans le volet PROPRIÉTÉS Pour TOR-SVR1, à droit de **Association de cartes réseau**, cliquez sur **Activé**.
22. Dans la fenêtre Association de cartes réseau, dans le volet CARTES ET INTERFACES, cliquez sur **Connexion au réseau local 3**. Appuyez sur la touche Ctrl et maintenez-la enfoncée, puis cliquez sur **Connexion au réseau local 4**.
23. Dans la fenêtre Association de cartes réseau, dans le volet CARTES ET INTERFACES, cliquez sur **TÂCHES**. Dans le menu déroulant, cliquez sur **Ajouter à une nouvelle équipe**.
24. Dans la boîte de dialogue **Nom de l'équipe**, tapez **Association d'accès iSCSI 2**, puis cliquez sur **OK**.
25. Fermez la fenêtre Association de cartes réseau.
26. Sur l'écran Accueil, cliquez sur **Panneau de configuration**, sur **Réseau et Internet**, puis sur **Centre Réseau et partage**.
27. Dans Centre Réseau et partage, cliquez sur **Modifier les paramètres de la carte**.
28. Cliquez avec le bouton droit sur **Association d'accès iSCSI 2**, puis cliquez sur **Propriétés**.
29. Dans la boîte de dialogue **Propriétés de Association d'accès iSCSI 2**, double-cliquez sur **Protocole Internet version 4 (TCP/IPv4)**.
30. Cliquez sur **Utiliser l'adresse IP suivante**, puis entrez les paramètres suivants :
    - Adresse IP : **131.107.1.10**
    - Masque de sous-réseau : **255.255.0.0**
    - Passerelle par défaut : Laissez ce champ vide
31. Cliquez sur **Utiliser l'adresse de serveur DNS suivante**, puis tapez **172.16.0.10** à côté de **Serveur DNS préféré**.
32. Cliquez sur **OK**, puis sur **OK** pour fermer la boîte de dialogue **Propriétés de Association d'accès iSCSI 2**.
33. Fermez la fenêtre Connexions réseau.
34. Fermez la fenêtre Centre Réseau et partage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer des initiateurs iSCSI et MPIO

1. Connectez-vous à TOR-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**. Si le Gestionnaire de serveur n'est pas ouvert, cliquez sur l'icône **Gestionnaire de serveur** sur la barre des tâches.
2. Dans le Gestionnaire de serveur, cliquez sur **Tableau de bord**, puis sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, dans la page **Avant de commencer**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
7. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **MPIO (Multipath I/O)**, puis sur **Suivant**.
8. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
9. Une fois l'installation terminée, cliquez sur **Fermer**.
10. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis dans la liste déroulante **Outils**, cliquez sur **Initiateur iSCSI**.
11. Dans la boîte de dialogue **Microsoft iSCSI**, cliquez sur **Oui**.
12. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, dans l'onglet **Cibles**, dans la zone **Cible**, tapez **172.16.1.25**, puis cliquez sur **Connexion rapide**. Dans la section **Cibles découvertes**, vous devez maintenant voir une cible découverte avec un état **Connecté**.
13. Dans la boîte de dialogue **Connexion rapide**, cliquez sur **Terminer**.
14. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : Initiateur iSCSI**.
15. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis dans la liste déroulante **Outils**, cliquez sur **MPIO**.
16. Dans la boîte de dialogue **Propriétés de : MPIO**, cliquez sur l'onglet **Découvrir plusieurs chemins**.
17. Sous l'onglet **Découvrir plusieurs chemins**, activez la case à cocher **Ajouter la prise en charge des périphériques iSCSI**, puis cliquez sur **Ajouter**. Lorsque vous êtes invité à redémarrer l'ordinateur, cliquez sur **Oui**.
18. Lorsque l'ordinateur a démarré, ouvrez une session sur TOR-SVR1 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
19. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis dans la liste déroulante **Outils**, cliquez sur **MPIO**.
20. Dans la boîte de dialogue **Propriétés de : MPIO**, dans l'onglet **Périphériques MPIO**, notez que **ID du matériel de périphérique MSFT2005iSCSIBusType_0x9** est ajouté à la liste.
21. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : MPIO**.

▶ Tâche 3 : Configurer des espaces de stockage à l'aide des cibles iSCSI

1. Sur TOR-SVR1, Dans le Gestionnaire de serveur, dans le volet gauche, cliquez sur **Services de fichiers et de stockage**, puis dans le volet Serveurs, cliquez sur **Pools de stockage**.
2. Dans le volet POOLS DE STOCKAGE, cliquez sur **TÂCHES**, puis dans la liste déroulante **TÂCHES**, cliquez sur **Nouveau pool de stockage**.
3. Dans l'Assistant Nouveau pool de stockage, dans la page **Avant de commencer**, cliquez sur **Suivant**.
4. Dans la page **Indiquer un pool de stockage et son sous-système**, dans la zone **Nom**, tapez **iSCSIPool**, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionner les disques physiques pour le pool de stockage**, cliquez sur les disques physiques suivants, puis cliquez sur **Suivant** :
   a. **PhysicalDisk1 (TOR-SVR1)**
   b. **PhysicalDisk2 (TOR-SVR1)**
   c. **PhysicalDisk3 (TOR-SVR1)**
   d. **PhysicalDisk4 (TOR-SVR1)**
   e. **PhysicalDisk5 (TOR-SVR1)**
6. Dans la page **Confirmer les sélections**, cliquez sur **Créer**.
7. Dans la page **Afficher les résultats** attendez que les tâches soient terminées, puis cliquez sur **Fermer**.
8. Sélectionnez **iSCSIPool**, dans le volet DISQUES VIRTUELS, cliquez sur **TÂCHES**, puis cliquez sur **Nouveau disque virtuel**.
9. Dans l'Assistant Nouveau disque virtuel, dans la page **Avant de commencer**, cliquez sur **Suivant**.
10. Dans la page **Sélectionner le pool de stockage**, cliquez sur **iSCSIPool**, puis sur **Suivant**.
11. Dans la page **Spécifier le nom du disque virtuel**, dans la zone **Nom**, tapez **DFSDisk**, puis cliquez sur **Suivant**.
12. Dans la page **Sélectionner la disposition de stockage**, dans la liste **Disposition**, cliquez sur **Parity** (Parité), puis sur **Suivant**.
13. Dans la page **Spécifier le type d'approvisionnement**, cliquez sur **Fixe**, puis sur **Suivant**.
14. Dans la page **Spécifier la taille du disque virtuel**, cliquez sur **Taille maximale**, puis sur **Suivant**.
15. Dans la page **Confirmer les sélections**, cliquez sur **Créer**.
16. Dans la page **Afficher les résultats**, attendez que la tâche soit terminée. Assurez-vous que la case à cocher **Créer un volume lorsque l'Assistant se ferme** est activée, puis cliquez sur **Fermer**.
17. Dans l'Assistant Nouveau volume, dans la page **Avant de commencer**, cliquez sur **Suivant**.
18. Dans la page **Sélectionner le serveur et le disque**, dans le volet Disque, cliquez sur le disque virtuel **DFSDisk**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

19. Dans la page **Spécifier la taille du volume**, cliquez sur **Suivant** pour confirmer la sélection par défaut.
20. Dans la page **Affecter à la lettre d'un lecteur ou à un dossier**, dans la liste déroulante **Lettre du lecteur**, assurez-vous que la lettre **H** est sélectionnée, puis cliquez sur **Suivant**.
21. Dans la page **Sélectionner les paramètres du système de fichiers**, dans la liste déroulante **Système de fichiers**, cliquez sur **NTFS**, et dans la zone **Nom de volume**, tapez **Volume DFS**, puis cliquez sur **Suivant**.
22. Dans la page **Confirmer les sélections**, cliquez sur **Créer**.
23. Dans la page **Dernière étape**, attendez que la création soit terminée, puis cliquez sur **Fermer**.

▶ Tâche 4 : Valider la haute disponibilité du déploiement contre le risque de perte d'un disque

1. Sur TOR-SVR1, dans la barre des tâches, cliquez sur le bouton Windows PowerShell®.
2. Dans la fenêtre Windows PowerShell, à l'invite de commandes, tapez la commande suivante, puis appuyez sur Entrée :

```
Copy C:\windows\system32\notepad.exe H:\
```

3. Fermez la fenêtre Windows PowerShell.
4. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
5. Dans l'Explorateur de fichiers, développez **Ordinateur**, puis cliquez sur **Volume DFS (H:)**.
6. Vérifiez que notepad.exe figure dans la liste des fichiers.
7. Fermez l'Explorateur de fichiers.
8. Sur l'ordinateur hôte, dans le Gestionnaire Hyper-V®, dans le volet Ordinateurs virtuels, cliquez avec le bouton droit sur **22414B-TOR-SVR1**, puis sur **Paramètres**.
9. Dans la fenêtre Paramètres pour 22414B-TOR-SVR1 sur LON-HOST1, dans le volet Matériel, cliquez sur la première occurrence de **Carte réseau héritée**. Dans la liste déroulante **Commutateur virtuel**, cliquez sur **Non connecté**, puis cliquez sur **OK**.
10. Sur TOR-SVR1, ouvrez l'explorateur de fichiers, puis cliquez sur **Volume DFS (H:)**.
11. Vérifiez que notepad.exe figure dans la liste de fichiers, même si TOR-SVR1 n'est pas connecté au réseau.
12. Sur l'ordinateur hôte, dans le Gestionnaire Hyper-V, dans le volet Ordinateurs virtuels, cliquez avec le bouton droit sur **22414B-TOR-SVR1**, puis sur **Paramètres**.
13. Dans la fenêtre Paramètres pour 22414B-TOR-SVR1 sur LON-HOST1, dans le volet Matériel, cliquez sur la première occurrence de **Carte réseau héritée**. Dans la liste déroulante **Commutateur virtuel**, cliquez sur **Réseau externe**, puis cliquez sur **OK**.

Résultats : Après avoir terminé cet exercice, vous devez avoir implémenté une solution de haute disponibilité pour un stockage de fichiers.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 4 : Implémentation d'une solution de haute disponibilité à l'aide de l'équilibrage de charge réseau

▶ Tâche 1 : Configurer un cluster d'équilibrage de la charge réseau (NLB)

1. Connectez-vous à LON-DC1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur l'écran Accueil, puis sur l'icône **Internet Explorer**.
3. Dans la barre d'adresses de Windows Internet Explorer, tapez l'adresse **http://LON-SVR1.adatum.com**, puis appuyez sur Entrée. Si une fenêtre contextuelle s'affiche, cliquez sur **Oui**. Vérifiez que le nom du serveur s'affiche en haut de la page.
4. Dans la zone **Prénom**, tapez votre nom, puis cliquez sur **OK**. Vérifier qu'un message indiquant votre nom s'affiche.
5. Dans Internet Explorer, cliquez sur le bouton **Précédent**. Vérifiez que le message **Bienvenue *<votre nom>*** s'affiche. Si le message ne s'affiche pas, appuyez sur F5 pour actualiser la page. Cela s'explique par le fait que l'application Web conserve l'état de session.
6. Dans Internet Explorer, ouvrez un nouvel onglet, tapez **http://LON-SVR2.adatum.com** dans la barre d'adresse, puis appuyez sur Entrée. Vérifiez que le nom du serveur s'affiche en haut de la page.
7. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis dans la liste déroulante **Outils**, cliquez sur **DNS**.
8. Dans le **Gestionnaire DNS**, développez **LON-DC1**, puis développez **Zones de recherche directes**.
9. Sélectionnez **Adatum.com**, cliquez dessus avec le bouton droit, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
10. Dans la boîte de dialogue **Nouvel hôte**, dans la zone **Nom**, tapez **www**. Dans la zone **Adresse IP**, tapez **172.16.0.111**, cliquez sur **Ajouter un hôte**, sur **OK**, puis sur **Terminé**.
11. Basculez vers LON-SVR1 et connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
12. Dans le Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur **Windows PowerShell ISE**.
13. Dans la fenêtre environnement d'écriture de scripts intégré (ISE) de Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Invoke-Command -Computername LON-SVR1,LON-SVR2 -command {Install-
WindowsFeature NLB,RSAT-NLB}
```

14. Dans la fenêtre Windows PowerShell ISE, saisissez la commande suivante et appuyez sur Entrée :

```
New-NlbCluster -InterfaceName "Connexion au réseau local" -OperationMode Multicast -
ClusterPrimaryIP 172.16.0.111 -ClusterName LON-NLB
```

15. Dans la fenêtre Windows PowerShell ISE, saisissez la commande suivante et appuyez sur Entrée :

```
Add-NlbClusterNode -InterfaceName "Connexion au réseau local" -NewNodeName "LON-SVR2"
-NewNodeInterface "Connexion au réseau local"
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Dans le Gestionnaire de serveur, cliquez sur **Outils**, dans la liste déroulante **Outils**, cliquez sur **Gestionnaire d'équilibrage de la charge réseau**, puis sur **OK**.

Remarque : La configuration de NLB n'est pas encore terminée. Par conséquent, un message d'avertissement, que vous pouvez ignorer, s'affiche.

17. Dans le Gestionnaire d'équilibrage de la charge réseau, cliquez avec le bouton droit sur **LON-NLB**, puis cliquez sur **Propriétés du cluster**.
18. Dans la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.111)**, sous l'onglet **Règles de port**, cliquez sur la règle de port **Tous**, puis cliquez sur **Supprimer**.
19. Sous l'onglet **Règles de port**, cliquez sur **Ajouter**.
20. Dans la boîte de dialogue **Ajouter/Modifier une règle de port**, entrez les informations suivantes, puis cliquez sur **OK** :
    - Étendue du port : **80** à **80**
    - Protocoles : **TCP**
    - Mode de filtrage : **Hôte multiple**
    - Affinité : **Unique**
21. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.111)**.

▶ Tâche 2 : Configurer des serveurs Web pour utiliser le stockage à haute disponibilité

1. Connectez-vous à LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis, dans la liste déroulante **Outils**, cliquez sur **Gestion du système de fichiers distribués DFS**.
3. Dans la console Gestion du système de fichiers distribués DFS, développez le nœud **Espaces de noms**, puis cliquez sur l'espace de noms **\\adatum.com\website**.
4. Dans le volet du milieu, cliquez sur l'onglet **Serveurs d'espaces de noms**. Notez que trois serveurs sont en cours d'utilisation :
    - LON-SVR1
    - LON-SVR2
    - TOR-SVR1
5. Développez le nœud **Réplication**, puis cliquez sur **adatum.com\website\wwwroot**.
6. Dans le volet du milieu, cliquez sur l'onglet **Connexions**. Notez que chaque serveur se réplique sur les deux autres, formant ainsi une topologie en maille.
7. Fermez la console Gestion du système de fichiers distribués DFS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis dans la liste déroulante **Outils**, cliquez sur **Gestionnaire des services Internet (IIS)**.
9. Dans le volet Connexions**,** développez **LON-SVR1**, **Sites**, puis cliquez sur **Default Web Site** (Site Web par défaut).

Remarque : Si une boîte de dialogue contenant le message **Voulez-vous débuter avec Microsoft Web Platform pour rester connecté avec les tout derniers composants Web Platform ?** s'affiche, activez la case à cocher Ne pas afficher ce message et cliquez sur **Oui**.

10. Dans le volet Actions**,** cliquez **Paramètres de base**.
11. Dans la boîte de dialogue **Modifier le site**, dans la zone **Chemin d'accès physique**, tapez **\\adatum.com\website\wwwroot**.
12. Cliquez sur **Se connecter en tant que**.
13. Dans la boîte de dialogue **Se connecter en tant que**, cliquez sur **Utilisateur spécifique**, puis sur **Définir**.
14. Dans la boîte de dialogue **Définir les informations d'identification**, tapez **ADATUM\Administrateur** en tant que **Nom d'utilisateur**, et **Pa$$w0rd** dans les champs **Mot de passe** et **Confirmer le mot de passe**. Cliquez trois fois sur **OK**, puis fermez le Gestionnaire des services Internet (IIS).
15. Basculez vers LON-SVR2 et connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**. Répétez les étapes 8 à 14.

Remarque : N'utilisez pas le compte administrateur pour vous connecter au dossier partagé dans un environnement de production. Vous devez utiliser un compte d'utilisateur normal disposant d'autorisations limitées.

▶ Tâche 3 : Valider le déploiement

1. Basculez vers LON-CL1.
2. Sur le **Bureau**, cliquez sur l'icône **Internet Explorer** sur la barre des tâches.
3. Dans la barre d'adresses d'Internet Explorer, tapez l'adresse **http://www.adatum.com**, puis appuyez sur Entrée. Notez le nom du serveur qui s'affiche en haut de la page.
4. Dans la zone **Prénom**, tapez votre nom, puis cliquez sur **OK**. Vérifier qu'un message indiquant votre nom s'affiche.
5. Cliquez sur l'icône **Actualiser** 20 fois. Notez que le nom du serveur ne change pas, en raison de l'affinité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Basculez vers LON-SVR1.
7. Dans la console Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur **Windows PowerShell ISE**.
8. Dans la fenêtre Windows PowerShell ISE, saisissez la commande suivante et appuyez sur Entrée :

```
Stop-NlbClusterNode nom_serveur
```

   Dans cette commande, *nom_serveur* est le nom du serveur auquel vous vous êtes connecté lors des étapes précédentes.

9. Basculez vers LON-CL1.
10. Cliquez sur l'icône **Actualiser**. Vérifiez que vous vous connectez à un autre serveur et que vous perdez l'état de session.
11. Basculez vers LON-SVR1.
12. Dans la fenêtre Windows PowerShell ISE, saisissez la commande suivante et appuyez sur Entrée :

```
Start-NlbClusterNode nom_serveur
```

   Dans cette commande, *nom_serveur* est le même nom du serveur que vous avez utilisé dans la commande précédente.

13. Basculez vers LON-CL1.
14. Cliquez sur l'icône **Actualiser**. Le nom du serveur ne doit pas changer.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V®.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, et cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-SVR2**, **22414B-LON-CL1**, **22414B-TOR-SS1** et **22414B-TOR-SVR1**.

Résultats : Après avoir terminé cet exercice, vous devez avoir implémenté une solution de haute disponibilité à l'aide de NLB.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 8 : Planification et implémentation d'une infrastructure haute disponibilité à l'aide du clustering avec basculement

Atelier pratique : Planification et implémentation d'une infrastructure hautement disponible à l'aide du clustering avec basculement

Exercice 1 : Conception de rôles serveur hautement disponibles

▶ Tâche 1 : Analyser des rôles serveur devant être hautement disponibles

▶ Tâche 2 : Répondre à la question et proposer une conception hautement disponible

Réponses :

1. Pour AD DS, vous ne devez implémenter aucune technologie hautement disponible spécifique. Vous avez seulement besoin d'implémenter plusieurs contrôleurs de domaine AD DS. AD DS ne prend en charge ni le clustering avec basculement ni l'équilibrage de la charge réseau.
2. Habituellement, pour les serveurs Web, nous utilisons l'équilibrage de la charge réseau. Cependant, si les serveurs Web sont connectés à une base de données en arrière-plan, il est également possible d'implémenter le clustering avec basculement pour rendre les bases de données hautement disponibles.
3. Le service DHCP prend en charge le clustering avec basculement et vous pouvez le rendre hautement disponible en ayant recours à cette technologie. Cependant, dans Windows Server® 2012, vous pouvez également utiliser le basculement DHCP comme technologie d'implémentation sans cluster des serveurs DHCP hautement disponibles.
4. La seule solution à haut niveau de disponibilité recommandée pour SQL Server est le clustering avec basculement.
5. Le serveur de fichiers prend en charge le clustering. Cependant, en fonction de l'utilisation envisagée de votre serveur de fichiers, vous pouvez également envisager d'utiliser des technologies comme le système de fichiers distribués (DFS).
6. Le serveur Exchange Server Mailbox prend en charge le clustering avec basculement mais uniquement via l'implémentation de groupes de disponibilité de base de données (DAG). Pour le rôle serveur d'accès au client, vous devez utiliser des tableaux d'accès client et l'équilibrage de la charge réseau.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

Résultats : À la fin de cet exercice, vous aurez terminé la conception de la haute disponibilité pour différents rôles serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Implémenter la fonction Réplica Hyper-V

▶ Tâche 1 : Importer un ordinateur virtuel 22414B-LON-CORE sur l'ordinateur LON-HOST1

1. Connectez-vous à LON-HOST1 en tant que **Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-HOST1, ouvrez la console du Gestionnaire Hyper-V.
3. Dans le volet Actions, cliquez sur **Importer un ordinateur virtuel**.
4. Dans la page **Avant de commencer** de l'Assistant Importation d'ordinateur virtuel, cliquez sur **Suivant**.
5. Dans la page **Localiser le dossier**, cliquez sur **Parcourir**.
6. Accédez au dossier **E:\Programmes\Microsoft Learning\22414\Drives\22414B-LON-CORE**. Cliquez sur **Sélectionner un dossier**, puis cliquez sur **Suivant**.

Remarque : La lettre de lecteur peut être différente selon le nombre de lecteurs présents sur l'ordinateur hôte physique.

7. Dans la page **Sélectionner l'ordinateur virtuel**, sélectionnez **22414B-LON-CORE**, puis cliquez sur **Suivant**.
8. Dans la page **Choisir le type d'importation**, cliquez sur **Suivant**.
9. Dans la page **Résumé**, cliquez sur **Terminer**.

▶ Tâche 2 : Configurer un réplica sur les deux ordinateurs hôtes

1. Sur LON-HOST1, ouvrez la console du Gestionnaire Hyper-V.
2. Dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur **LON-HOST1**, puis sélectionnez **Paramètres Hyper-V**.
3. Dans Paramètres Hyper-V pour LON-HOST1, cliquez sur **Configuration de la réplication**.
4. Dans le volet Configuration de la réplication, cliquez sur **Activez ce ordinateur en tant que serveur de réplication**.
5. Dans la section Authentification et ports, sélectionnez **Utiliser Kerberos (HTTP)**.
6. Dans la section Autorisation et stockage, cliquez sur **Autoriser la réplication à partir de n'importe quel serveur authentifié**, puis cliquez sur **Parcourir**.
7. Cliquez sur **Ordinateur**, puis double-cliquez sur **Disque local (E)**, puis cliquez sur **Nouveau dossier**. Saisissez **VMReplica** pour le nom de dossier, puis appuyez sur Entrée.
8. Sélectionnez le dossier **E:\VMReplica**, puis cliquez sur **Sélectionner un dossier**. (Remarque : la lettre du lecteur peut changer en fonction de votre configuration matérielle hôte.)
9. Dans **Paramètres Hyper-V de LON-HOST1**, cliquez sur **OK**.
10. Dans la fenêtre Paramètres, lisez la notification et cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans l'écran d'**accueil**, cliquez sur **Panneau de configuration**.
12. Dans le Panneau de configuration, cliquez sur **Système et sécurité**, puis cliquez sur **Pare-feu Windows**.
13. Cliquez sur **Paramètres avancés**.
14. Cliquez sur **Règles de trafic entrant**, puis dans le volet droit, dans la liste de règles, recherchez la règle **Écouteur HTTP de réplica Hyper-V (Tcp-In)**. Cliquez avec le bouton droit sur la règle, puis cliquez sur **Activer la règle**.
15. Fermez la console Pare-feu Windows avec fonctions avancées de sécurité, puis fermez le **Pare-feu Windows**.
16. Répétez les étapes 1 à 15 sur LON-HOST2.

▶ Tâche 3 : Configurer une réplication pour l'ordinateur virtuel

1. Sur LON-HOST1, ouvrez le Gestionnaire Hyper-V. Cliquez sur **LON-HOST1**, puis cliquez avec le bouton droit sur **22414B-LON-CORE**.
2. Cliquez sur **Activer la réplication**, puis dans la page **Avant de commencer**, cliquez sur **Suivant**.
3. Dans la page **Spécifier le serveur de réplication**, cliquez sur **Parcourir**.
4. Dans la fenêtre Sélectionner l'ordinateur, saisissez **LON-HOST2**, cliquez sur **Vérifier les noms**, sur **OK**, puis sur **Suivant**.
5. Dans la page **Spécifier les paramètres de connexion**, examinez les paramètres et assurez-vous que l'option **Utiliser l'authentification Kerberos (HTTP)** est sélectionnée, puis cliquez sur **Suivant**.
6. Dans la page **Choisir les disques durs virtuels de réplication**, veillez à ce que **22414B-LON-CORE.vhd** soit sélectionné, puis cliquez sur **Suivant**.
7. Dans la page **Configurer l'historique de récupération**, sélectionnez **Uniquement le dernier point de récupération**, puis cliquez sur **Suivant**.
8. Dans la page **Choisir la méthode de réplication initiale**, cliquez sur **Envoyer la copie initiale sur le réseau**, sélectionnez **Démarrer la réplication immédiatement**, puis cliquez sur **Suivant**.
9. Dans la page **Fin de l'Assistant Activation de la réplication**, cliquez sur **Terminer**.

   Patientez 5 à 10 minutes. Vous pouvez suivre la progression de la réplication initiale dans la colonne **Statut** dans la console Gestionnaire Hyper-V sur LON-HOST1. À l'issue de la réplication (la barre de progression atteint 100 %), veillez à ce que **22414B-LON-CORE** s'affiche sur LON-HOST2 dans le Gestionnaire Hyper-V.

▶ Tâche 4 : Valider un basculement planifié vers le site de réplication

1. Sur LON-HOST2 dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22414B-LON-CORE**.
2. Sélectionnez **Réplication**, puis cliquez sur **Afficher l'intégrité de la réplication**.
3. Passez en revue le contenu de la fenêtre qui s'affiche et veillez à ce qu'il n'y ait aucune erreur.
4. Cliquez sur **Fermer**.
5. Sur LON-HOST1, ouvrez le Gestionnaire Hyper-V et vérifiez que **22414B-LON-CORE** est arrêté.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Cliquez avec le bouton droit sur **22414B-LON-CORE**, sélectionnez **Réplication**, puis cliquez sur **Basculement planifié**.
7. Dans la fenêtre Basculement planifié, assurez-vous que l'option **Démarrez l'ordinateur virtuel réplica après le basculement** est sélectionnée, puis cliquez sur **Basculement**.
8. Dans la fenêtre Basculement planifié, cliquez sur **Fermer**.
9. Sur LON-HOST2, dans le Gestionnaire Hyper-V, assurez-vous que **22414B-LON-CORE** est en cours d'exécution.
10. Sur LON-HOST1, cliquez avec le bouton droit sur **22414B-LON-CORE**, pointez sur **Réplication**, puis cliquez sur **Supprimer la réplication**.
11. Dans la boîte de dialogue **Supprimer la réplication**, cliquez sur **Supprimer la réplication**.
12. Sur LON-HOST2, cliquez avec le bouton droit sur **22414B-LON-CORE**, puis cliquez sur **Arrêter**. Dans la boîte de dialogue **Arrêter l'ordinateur**, cliquez sur **Arrêter**.

Résultats : À l'issue de cet exercice, les étudiants auront implémenté un réplica Hyper-V.

Exercice 3 : Déployer un cluster de basculement

▶ Tâche 1 : Se connecter à des cibles iSCSI à partir des deux ordinateurs hôtes

1. Sur LON-HOST1, ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis cliquez sur **Initiateur iSCSI**. À l'invite **Microsoft iSCSI**, cliquez sur **Oui**.
2. Cliquez sur l'onglet **Découverte**, sur **Découvrir un portail**, puis dans la zone **Adresse IP ou nom DNS**, tapez **172.16.0.10**, puis cliquez sur **OK**.
3. Cliquez sur l'onglet **Cibles**, sur **Actualiser**, puis dans la liste **Cibles**, sélectionnez **iqn.1991-05.com.microsoft:lon-dc1-target1-target** et cliquez sur **Connexion**.
4. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez sur **OK**.
5. Cliquez sur **OK** pour fermer les propriétés de l'initiateur iSCSI.
6. Sur LON-HOST2, ouvrez le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Initiateur iSCSI**.
7. Dans la boîte de dialogue **Microsoft iSCSI**, cliquez sur **Oui**.
8. Cliquez sur l'onglet **Découverte**.
9. Cliquez sur **Découvrir un portail**.
10. Dans la zone Adresse IP ou nom DNS, tapez **172.16.0.10**, puis cliquez sur **OK**.
11. Cliquez sur l'onglet **Cibles**.
12. Cliquez sur **Actualiser**.
13. Dans la liste **Cibles découvertes**, sélectionnez **iqn.1991-05.com.microsoft:lon-dc1-target1-target**, puis cliquez sur **Connexion**.
14. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez sur **OK**. Cliquez sur **OK** pour fermer les propriétés de l'initiateur iSCSI.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

15. Sur LON-HOST2, dans la fenêtre Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestion de l'ordinateur**.
16. Développez **Stockage**, puis cliquez sur **Gestion des disques**.
17. Cliquez avec le bouton droit sur **Disque 2**, puis cliquez sur **En ligne**.
18. Cliquez avec le bouton droit sur **Disque 2**, puis sur **Initialiser le disque**. Dans la boîte de dialogue **Initialiser le disque**, cliquez sur **OK**.
19. Cliquez avec le bouton droit sur l'espace non alloué en regard de **Disque 2**, puis cliquez sur **Nouveau volume simple**.
20. Dans la page d'**accueil**, cliquez sur **Suivant**.
21. Dans la page **Spécifier la taille du volume**, cliquez sur **Suivant**.
22. Dans la page **Attribuer une lettre de lecteur ou de chemin d'accès**, cliquez sur **Suivant**.
23. Dans la page **Formater une partition**, dans la zone **Nom de volume**, tapez **ClusterDisk**. Activez la case à cocher **Effectuer un formatage rapide**, puis cliquez sur **Suivant**.
24. Cliquez sur **Terminer**.
25. Sur LON-HOST1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestion de l'ordinateur**.
26. Développez **Stockage**, puis cliquez sur **Gestion des disques**.
27. Cliquez avec le bouton droit sur **Gestion des disques**, puis cliquez sur **Actualiser**.
28. Cliquez avec le bouton droit sur **Disque 2**, puis cliquez sur **En ligne**.

▶ Tâche 2 : Installer et configurer un clustering avec basculement sur les deux ordinateurs hôtes

1. Sur LON-HOST1, dans la barre des tâches, cliquez sur l'icône **Gestionnaire de serveur** pour ouvrir le Gestionnaire de serveur.
2. À partir du **Tableau de bord**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
7. Dans la page **Sélectionner des fonctionnalités**, dans la liste **Fonctionnalités**, cliquez sur **Clustering avec basculement**, puis cliquez sur **Ajouter des fonctionnalités** et sur **Suivant**.
8. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
9. Une fois l'installation terminée, cliquez sur **Fermer**.
10. Répétez les étapes 1 à 9 sur LON-HOST2.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Sur LON-HOST1, dans la console du Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire du cluster de basculement**.
12. Dans le Gestionnaire du cluster de basculement, dans le volet central, sous **Administration**, cliquez sur **Créer le cluster**.
13. Dans l'Assistant Création d'un cluster, dans la page **Avant de commencer**, lisez les informations qui s'affichent. Cliquez sur **Suivant**.
14. Dans la zone **Nom du serveur**, tapez **LON-HOST1**, puis cliquez sur **Ajouter**. Tapez **LON-HOST2**, puis cliquez sur **Ajouter**.
15. Vérifiez les entrées, puis cliquez sur **Suivant**.
16. Dans la page **Avertissement de validation**, cliquez sur **Non. Je n'ai pas besoin de l'assistance de Microsoft pour ce cluster**, puis cliquez sur **Suivant**.
17. Dans la page **Point d'accès pour l'administration du cluster**, dans le champ **Nom du cluster**, tapez **VMCluster**.
18. Dans la zone Nom de l'adresse IP, sous **Adresse**, tapez **172.16.0.126**, puis cliquez sur **Suivant**.
19. Dans la boîte de dialogue **Confirmation**, vérifiez les informations, désactivez la case à cocher en regard de **Ajouter la totalité du stockage disponible au cluster**, puis cliquez sur **Suivant**.
20. Dans la page **Résumé** de l'Assistant Création d'un cluster, cliquez sur **Terminer**.

▶ Tâche 3 : Configurer le cluster

1. Sur LON-HOST1, dans la console Gestionnaire du cluster de basculement, développez **VMCluster.Adatum.com**, développez **Stockage** et cliquez avec le bouton droit sur **Disques**.
2. Cliquez sur **Ajouter un disque**.
3. Dans la boîte de dialogue **Ajouter des disques à un cluster**, vérifiez que l'option **Disque du cluster 1** est sélectionnée, puis cliquez sur **OK**.
4. Vérifiez que le disque est disponible pour le stockage en cluster dans la console **Gestionnaire du cluster de basculement**.
5. Cliquez avec le bouton droit sur **VMCluster.adatum.com**, sélectionnez **Autres actions**, puis cliquez sur **Configurer les paramètres du quorum du cluster**. Cliquez sur **Suivant**.
6. Dans la page **Sélectionner l'option de configuration du quorum**, cliquez sur **Utiliser les paramètres standard**, puis sur **Suivant**.
7. Dans la page **Confirmation**, cliquez sur **Suivant**.
8. Dans la page **Résumé**, cliquez sur **Terminer**.

▶ Tâche 4 : Valider le groupe

1. Sur LON-HOST2, ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire du cluster de basculement**.
2. Cliquez sur **VMCluster.Adatum.com** dans le volet gauche, puis dans le volet **Actions**, cliquez sur **Validez le cluster**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans l'Assistant Validation d'une configuration, dans la page **Avant de commencer**, cliquez sur **Suivant**.
4. Dans la page **Options de test**, vérifiez que l'option **Exécuter tous les tests (recommandé)** est sélectionnée, puis cliquez sur **Suivant**.
5. Dans la page **Examiner le statut du stockage**, sélectionnez **Disque de cluster 1**, puis cliquez sur **Suivant**.
6. Dans la page **Confirmation**, cliquez sur **Suivant**.
7. Attendez que le test de cluster soit terminé, puis cliquez sur **Rapport**. Examinez le rapport. Certains avertissements peuvent s'afficher, mais aucune erreur.
8. Fermez Windows Internet Explorer®, puis cliquez sur **Terminer**.

Résultats : À la fin de cet exercice, vous aurez déployé un cluster de basculement.

Exercice 4 : Implémenter un serveur de fichiers avec montée en puissance parallèle

▶ Tâche 1 : Installation du rôle de serveur de fichiers et du clustering avec basculement sur LON-SVR1 et LON-SVR2

1. Sur LON-SVR1, dans **Gestionnaire de serveur**, cliquez sur **Tableau de bord**, puis sur **Ajouter des rôles et des fonctionnalités**.
2. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
3. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner des rôles de serveurs**, développez **Service de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, puis vérifiez que l'option **Services de fichiers et iSCSI (Installé)** est sélectionnée. Cliquez sur **Suivant**.
6. Dans la page **Sélectionner des fonctionnalités**, sélectionnez **Clustering avec basculement**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
7. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
8. Lorsque le message **Progression de l'installation** s'affiche, cliquez sur **Fermer**.
9. Répétez les étapes 1 à 9 sur LON-SVR2.

▶ Tâche 2 : Se connecter à la cible iSCSI des deux nœuds de cluster du serveur de fichiers

1. Sur LON-SVR1, ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Initiateur iSCSI**. À l'invite **Microsoft iSCSI**, cliquez sur **Oui**.
2. Cliquez sur l'onglet **Découverte**.
3. Cliquez sur **Découvrir un portail**, et dans la zone **Adresse IP ou nom DNS**, tapez **172.16.0.10**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Cliquez sur l'onglet **Cibles**.
5. Dans la liste **Cibles**, sélectionnez **iqn.1991-05.com.microsoft:lon-dc1-target1-target**, puis cliquez sur **Connexion**.
6. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez sur **OK**.
7. Cliquez sur **OK** pour fermer les propriétés de l'initiateur iSCSI.
8. Sur LON-SVR2, ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis cliquez sur **Initiateur iSCSI**.
9. Dans la boîte de dialogue **Microsoft iSCSI**, cliquez sur **Oui**.
10. Cliquez sur l'onglet **Découverte**.
11. Cliquez sur **Découvrir un portail**, et dans la zone **Adresse IP ou nom DNS**, tapez **172.16.0.10**, puis cliquez sur **OK**.
12. Cliquez sur l'onglet **Cibles**.
13. Dans la liste **Cibles découvertes**, sélectionnez **iqn.1991-05.com.microsoft:lon-dc1-target1-target**, puis cliquez sur **Connexion**.
14. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez sur **OK**. Cliquez sur **OK** pour fermer les propriétés de l'initiateur iSCSI.
15. Sur LON-SVR2, dans la fenêtre Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de l'ordinateur**.
16. Développez **Stockage**, puis cliquez sur **Gestion des disques**.
17. Cliquez avec le bouton droit sur **Disque 2**, puis cliquez sur **En ligne**. (Remarque : faites attention à ne pas cliquer sur Disque 1, car il s'agit du disque utilisé dans un autre cluster créé précédemment.)
18. Cliquez avec le bouton droit sur **Disque 2**, puis sur **Initialiser le disque**. Dans la boîte de dialogue **Initialiser le disque**, cliquez sur **OK**.
19. Cliquez avec le bouton droit sur l'espace non alloué en regard de **Disque 2**, puis cliquez sur **Nouveau volume simple**.
20. Dans la page d'**accueil**, cliquez sur **Suivant**.
21. Dans la page **Spécifier la taille du volume**, cliquez sur **Suivant**.
22. Dans la page **Attribuer une lettre de lecteur ou de chemin d'accès**, cliquez sur **Suivant**.
23. Dans la page **Formater une partition**, dans la zone **Nom de volume**, tapez **ClusterDisk**. Activez la case à cocher **Effectuer un formatage rapide**, puis cliquez sur **Suivant**.
24. Cliquez sur **Terminer**. Si l'invite Microsoft Windows s'affiche, cliquez sur **Annuler**.
25. Cliquez avec le bouton droit sur **Disque 3**, puis cliquez sur **En ligne**.
26. Cliquez avec le bouton droit sur **Disque 3**, puis sur **Initialiser le disque**. Dans la boîte de dialogue **Initialiser le disque**, cliquez sur **OK**.
27. Cliquez avec le bouton droit sur l'espace non alloué en regard de **Disque 3**, puis cliquez sur **Nouveau volume simple**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

28. Dans la page d'**accueil**, cliquez sur **Suivant**.
29. Dans la page **Spécifier la taille du volume**, cliquez sur **Suivant**.
30. Dans la page **Attribuer une lettre de lecteur ou de chemin d'accès**, cliquez sur **Suivant**.
31. Dans la page **Formater une partition**, dans la zone **Nom de volume**, tapez **Quorum**. Activez la case à cocher **Effectuer un formatage rapide**, puis cliquez sur **Suivant**.
32. Cliquez sur **Terminer**. Si l'invite Microsoft Windows s'affiche, cliquez sur **Annuler**.
33. Fermez Gestion de l'ordinateur.
34. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de l'ordinateur**.
35. Développez **Stockage**, puis cliquez sur **Gestion des disques**.
36. Cliquez avec le bouton droit sur **Gestion des disques**, puis cliquez sur **Actualiser**.
37. Cliquez avec le bouton droit sur **Disque 3**, puis cliquez sur **En ligne**. (Remarque : faites attention à ne pas cliquer sur Disque 2.)
38. Cliquez avec le bouton droit sur **Disque 4**, puis cliquez sur **En ligne**.

    (Remarque : LON-SVR1 a déjà deux disques, ces disques supplémentaires sont donc nommés Disque 3 et Disque 4, à la différence de LON-SVR2 où les mêmes disques sont nommés Disque 2 et Disque 3.)
39. Fermez Gestion de l'ordinateur.

▶ Tâche 3 : Configurer le serveur de fichiers avec montée en puissance parallèle

1. Sur LON-SVR1, dans la console du Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire du cluster de basculement**.
2. Dans le Gestionnaire du cluster de basculement, dans le volet central, sous **Administration**, cliquez sur **Créer le cluster**.
3. Dans l'Assistant Création d'un cluster, dans la page **Avant de commencer**, lisez les informations, puis cliquez sur **Suivant**.
4. Dans la zone **Nom du serveur**, tapez **LON-SVR1**, puis cliquez sur **Ajouter**. Tapez **LON-SVR2**, puis cliquez sur **Ajouter**.
5. Vérifiez les entrées, puis cliquez sur **Suivant**.
6. Dans la page **Avertissement de validation**, cliquez sur **Non. Je n'ai pas besoin de l'assistance de Microsoft pour ce cluster**, puis cliquez sur **Suivant**.
7. Dans la page **Point d'accès pour l'administration du cluster**, dans le champ **Nom du cluster**, tapez **FSCluster**.
8. Sous **Adresse**, tapez **172.16.0.127**, puis cliquez sur **Suivant**.
9. Dans la boîte de dialogue **Confirmation**, vérifiez les informations, désactivez la case à cocher en regard de **Ajouter la totalité du stockage disponible au cluster**, puis cliquez sur **Suivant**.
10. Dans la page **Résumé** de l'Assistant Création d'un cluster, cliquez sur **Terminer**.
11. Dans la console Gestionnaire du cluster de basculement, développez **FSCluster.Adatum.com**, puis **Stockage**, et cliquez avec le bouton droit sur **Disques**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

12. Cliquez sur **Ajouter un disque**.
13. Dans la boîte de dialogue **Ajouter des disques à un cluster**, vérifiez que les options Disque du cluster 1 et Disque du cluster 2 sont sélectionnées, puis cliquez sur **OK**.
14. Vérifiez que le disque est disponible pour le stockage en cluster dans la console **Gestionnaire du cluster de basculement**.
15. Cliquez avec le bouton droit sur **Disque de cluster 1**, puis cliquez sur **Ajouter aux volumes partagés de cluster**.
16. Cliquez avec le bouton droit sur **FSCluster.adatum.com**, sélectionnez **Autres actions**, puis cliquez sur **Configurer les paramètres du quorum du cluster**. Cliquez sur **Suivant**.
17. Dans la page **Sélectionner l'option de configuration du quorum**, cliquez sur **Utiliser les paramètres standard**, puis sur **Suivant**.
18. Dans la page **Confirmation**, cliquez sur **Suivant**.
19. Dans la page **Résumé**, cliquez sur **Terminer**.
20. Cliquez avec le bouton droit sur **Rôles**, puis sélectionnez **Configurer un rôle**.
21. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
22. Dans la page **Sélectionner un rôle**, sélectionnez **Serveur de fichiers**, puis cliquez sur **Suivant**.
23. Dans la page **Type de serveur de fichiers**, cliquez sur **Serveur de fichiers avec montée en puissance parallèle pour les données d'application**, puis sur **Suivant**.
24. Dans la page **Point d'accès client**, dans la zone **Nom**, saisissez **AdatumFS**, puis cliquez sur **Suivant**.
25. Dans la page **Confirmation**, cliquez sur **Suivant**.
26. Dans la page **Résumé**, cliquez sur **Terminer**.

▶ Tâche 4 : Créer un partage de fichiers disponible en permanence

1. Sur LON-SVR1, dans la console **Gestionnaire du cluster de basculement**, cliquez sur **Rôles**, puis dans le volet central, cliquez avec le bouton droit sur **AdatumFS**.
2. Sélectionnez **Ajouter le partage de fichiers.** (Si vous recevez un message indiquant que le point d'accès client n'est pas prêt, effectuez ces étapes sur LON-SVR2.)
3. Dans l'Assistant Nouveau partage, dans la page **Sélectionner le profil de ce partage**, sélectionnez **Partage SMB – Applications**, puis cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur et le chemin d'accès au partage**, cliquez sur **Sélectionner par volume**, puis cliquez sur **Suivant**.
5. Dans la page **Indiquer le nom de partage**, dans la zone **Nom du partage**, tapez **VMachines**, puis cliquez sur **Suivant**.
6. Dans la page **Configurer les paramètres de partage**, cliquez sur **Suivant**.
7. Dans la page **Spécifier les autorisations pour contrôler l'accès**, cliquez sur **Personnaliser les autorisations**.
8. Dans la fenêtre Paramètres de sécurité avancés pour VMachines, cliquez sur **Ajouter**.
9. Dans la fenêtre Autorisations pour VMachines, cliquez sur **Sélectionnez un principal**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Dans la fenêtre Sélectionner les utilisateurs, ordinateurs, comptes de service ou groupes, cliquez sur **Types d'objets**. Dans la fenêtre Types d'objets, sélectionnez **des ordinateurs**, puis cliquez sur **OK**.
11. Dans la zone de texte, tapez **LON-HOST1**. Cliquez sur **Vérifier les noms**, puis sur **OK**.
12. Dans la section **Autorisations de base**, sélectionnez **Contrôle total**, puis cliquez sur **OK**.
13. Répétez les étapes 8 à 12 pour attribuer les autorisations **Contrôle total** à LON-HOST2.
14. Cliquez sur **OK** pour fermer la fenêtre **Paramètres de sécurité avancés pour VMachines**.
15. Dans la page **Spécifier les autorisations pour contrôler l'accès**, vérifiez que **ADATUM\LON-HOST1$** et **ADATUM\LON-HOST2$** sont tous les deux présents dans la liste avec l'accès **Contrôle total**, puis cliquez sur **Suivant**.
16. Dans la page **Confirmer les sélections**, cliquez sur **Créer**, puis sur **Fermer**.

Résultats : À la fin de cet exercice, vous aurez configuré un serveur de fichiers à haut niveau de disponibilité.

Exercice 5 : Implémenter des ordinateurs virtuels hautement disponibles

▶ Tâche 1 : Déplacer un fichier .vhd sur le stockage hautement disponible

1. Sur LON-HOST1, ouvrez l'Explorateur de fichiers.
2. Accédez au dossier **E:\Programmes\Microsoft Learning\22414\Drives\22414B-LON-CORE\Virtual Hard Disks**.
3. Cliquez avec le bouton droit sur le fichier **22414B-LON-CORE.vhd**, puis cliquez sur **Copier**.
4. Dans la barre d'adresses de l'Explorateur de fichiers, tapez **\\AdatumFS\VMachines**, puis appuyez sur Entrée.
5. Cliquez avec le bouton droit dans un espace vide dans le dossier, sélectionnez **Nouveau**, cliquez sur **Dossier**, tapez **22414B-LON-CORE**, puis appuyez sur Entrée.
6. Double-cliquez sur le dossier **22414B-LON-CORE**, cliquez avec le bouton droit dans le dossier, puis sélectionnez **Coller**.
7. Patientez quelques minutes jusqu'à ce que le fichier .vhd soit copié dans le partage de fichiers hautement disponible.
8. Fermez l'Explorateur de fichiers.

▶ Tâche 2 : Configurer les nœuds Hyper-V de sorte qu'ils utilisent le cluster de serveurs de fichiers avec montée en puissance parallèle

1. Sur LON-HOST1, ouvrez le **Gestionnaire Hyper-V**.
2. Cliquez avec le bouton droit sur LON-HOST1, puis sélectionnez **Paramètres Hyper-V**.
3. Dans la fenêtre Paramètres Hyper-V pour LON-HOST1, sélectionnez **Disques durs virtuels** dans le volet gauche.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans le volet droit, tapez **\\adatumfs\VMachines** dans la zone de texte.
5. Cliquez sur **Ordinateurs virtuels** dans le volet gauche.
6. Dans le volet droit, tapez **\\adatumfs\VMachines** dans la zone de texte. Cliquez sur **OK** pour fermer la fenêtre Paramètres Hyper-V.
7. Répétez les étapes 1 à 6 sur LON-HOST2.

▶ Tâche 3 : Configurer l'ordinateur virtuel en tant qu'ordinateur à haut niveau de disponibilité

1. Sur LON-HOST1, ouvrez la console Gestionnaire du cluster de basculement.
2. Développez **VMCluster.Adatum.com**, puis cliquez avec le bouton droit sur **Rôles**.
3. Sélectionnez **Ordinateurs virtuels**, puis cliquez sur **Nouvel ordinateur virtuel**.
4. Dans la fenêtre Nouvel ordinateur virtuel, sélectionnez **LON-HOST1**, puis cliquez sur **OK**.
5. Dans l'Assistant Nouvel ordinateur virtuel, dans la page **Avant de commencer**, cliquez sur **Suivant**.
6. Dans la page **Spécifier le nom et l'emplacement**, tapez **22414B-LON-CORE** pour le nom et cliquez sur **Stocker l'ordinateur virtuel à un autre emplacement**. Tapez **\\AdatumFS\VMachines\22414B-LON-CORE**, puis cliquez sur **Suivant**.
7. Dans la page **Affecter la mémoire**, saisissez **768** dans la zone **Mémoire de démarrage**, puis cliquez sur **Suivant**.
8. Dans la page **Configurer la mise en réseau**, sélectionnez **Réseau externe** dans la zone de liste déroulante, puis cliquez sur **Suivant**.
9. Dans la page **Connecter un disque dur virtuel**, cliquez sur **Utiliser un disque dur virtuel existant**, puis sur **Parcourir**. Dans la zone **Nom du fichier**, tapez **\\ADatumFS\VMachines\22414B-LON-CORE**, puis appuyez sur Entrée.
10. Sélectionnez le fichier **22414B-LON-CORE.vhd**, puis cliquez sur **Ouvrir**.
11. Cliquez sur **Suivant**.
12. Dans la page **Fin de l'Assistant Nouvel ordinateur virtuel**, cliquez sur **Terminer**.
13. Dans la **Page de résumé**, vérifiez que le processus indique **Réussite**, puis cliquez sur **Terminer**.
14. Dans le **Gestionnaire de cluster de basculement**, cliquez sur **Rôles**, cliquez avec le bouton droit sur **22414B-LON-CORE**, puis sélectionnez **Redémarrer**. Assurez-vous que l'ordinateur virtuel démarre.
15. Une fois que l'ordinateur démarre, cliquez dessus avec le bouton droit, puis sélectionnez **Connecter**.
16. Dans la fenêtre Connexion à un ordinateur virtuel, cliquez sur le bouton **Ctrl+Alt+Suppr**, puis connectez-vous en tant qu' **Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.

▶ Tâche 4 : Exécuter une migration dynamique pour l'ordinateur virtuel

1. Sur LON-HOST2, ouvrez **Windows PowerShell**.
2. Dans la fenêtre Windows PowerShell, tapez **ping lon-core –t**, puis appuyez sur Entrée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Vérifiez que vous recevez les réponses de l'adresse IP LON-CORE. Laissez la fenêtre Windows PowerShell ouverte.
4. Ouvrez la console Gestionnaire du cluster de basculement et développez **VMCluster.Adatum.com**, puis cliquez sur **Rôles**.
5. Cliquez avec le bouton droit sur l'ordinateur virtuel **22414B-LON-CORE**, sélectionnez **Déplacer**, puis **Migration dynamique** et cliquez sur **Sélectionnez un nœud**.
6. Cliquez sur **LON-HOST2**, puis sur **OK**.
7. Basculez vers la fenêtre Windows PowerShell, et surveillez les paquets ICMP. Vous ne devez perdre qu'un minimum de paquets (1 ou 2) voire aucun.
8. Gardez la fenêtre Windows PowerShell ouverte.

▶ Tâche 5 : Valider la haute disponibilité en cas de défaillance du stockage

1. Sur LON-SVR1, ouvrez le **Gestionnaire du cluster de basculement**.
2. Développez **FSCluster.Adatum.com**, puis cliquez sur **Rôles**.
3. Dans le volet central, vérifiez qu'AdatumFS est en cours d'exécution. Lisez la valeur de la colonne de **Nœud propriétaire** (devrait être LON SVR1 ou LON-SVR2).
4. Ouvrez le **Gestionnaire Hyper-V** sur LON-HOST1, cliquez avec le bouton droit sur l'ordinateur virtuel propriétaire d'AdatumFS (à l'étape 3), puis cliquez sur **Paramètres**.
5. Cliquez sur **Carte réseau héritée** dans le volet gauche. Dans le volet droit, dans la zone de liste déroulante **Commutateur virtuel**, sélectionnez **Non connecté**, puis cliquez sur **OK**.
6. Revenez immédiatement au **Gestionnaire du cluster de basculement** sur le propriétaire actuel d'AdatumFS, puis vérifiez que le nœud propriétaire a été remplacé par **AdatumFS**.
7. Développez **Nœuds**, puis vérifiez qu'un nœud est en panne.
8. Basculez vers la fenêtre Windows PowerShell sur LON-HOST2, puis vérifiez qu'aucun paquet n'a été perdu.
9. Ouvrez le **Gestionnaire Hyper-V** sur LON-HOST1, cliquez avec le bouton droit sur l'ordinateur virtuel que vous avez déconnecté à l'étape 6, puis cliquez sur **Paramètres**.
10. Cliquez sur **Carte réseau héritée** dans le volet gauche. Dans le volet droit, dans la zone de liste déroulante **Commutateur virtuel**, sélectionnez **Réseau externe**, puis cliquez sur **OK**.
11. Rebasculez vers le **Gestionnaire du cluster de basculement** sur LON SVR1, puis vérifiez que les deux nœuds sont exécutés. (La console peut prendre jusqu'à minute pour actualiser l'état. Si vous ne voyez toujours pas le nœud FSCluster.Adatum.com, rouvrez le Gestionnaire du cluster de basculement.)
12. Sur LON-HOST1, dans le Gestionnaire du cluster de basculement, cliquez avec le bouton droit sur 22414B-LON-CORE, puis cliquez sur **Arrêter**.
13. Sur LON-HOST1 et LON-HOST2, fermez le Gestionnaire du cluster de basculement.

Exercice 6 : Implémenter l'intégration d'Operations Manager et de VMM

▶ Tâche 1 : Importer des packs d'administration

1. Basculez vers **LON-OM1**.
2. Ouvrez Operations Console dans la barre des tâches.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Cliquez sur l'espace de travail **Administration**.
4. Développez **Administration**, **Gestion des périphériques**, puis cliquez sur **Packs d'administration**. Attendez que la liste des packs d'administration s'affiche.
5. Cliquez sur **Importer les packs d'administration**.
6. Dans la fenêtre Importer les packs d'administration, cliquez sur **Ajouter**, puis cliquez sur **Ajouter à partir du disque**.
7. Dans la fenêtre Connexion au catalogue en ligne, cliquez sur **Non**.
8. Dans **Sélectionner les packs d'administration à importer**, tapez **\\lon-vmm1\C$** dans la zone de texte **Nom du fichier**, puis cliquez sur **Ouvrir**.
9. Accédez à **Programmes\Microsoft System Center 2012\Virtual Machine Manager\ Management Packs**.
10. Sélectionnez tous les fichiers, puis cliquez sur **Ouvrir**.
11. Dans la fenêtre Sélectionner les packs d'administration, cliquez sur **Installer**.
12. Dans la fenêtre Operations Manager, cliquez sur **Oui**. Attendez que les packs d'administration soient importés, puis cliquez sur **Fermer**.

▶ Tâche 2 : Activer l'intégration de Microsoft System Center 2012 - Virtual Machine Manager (VMM) avec Operations Manager

1. Sur **LON-VMM1**, ouvrez la console Virtual Machine Manager. (Remarque : Si la console VMM ne démarre pas, ouvrez les Services à partir des Outils d'administration et vérifiez que tous les services VMM définis pour démarrer automatiquement sont exécutés.)
2. Cliquez sur l'espace de travail **Paramètres**.
3. Cliquez sur **Paramètres de System Center**.
4. Dans le volet central, double-cliquez sur **Serveur Operations Manager**.
5. Dans la fenêtre **Ajouter Operations Manager**, dans la page **Introduction**, cliquez sur **Suivant**.
6. Dans la page **Connexion à Operations Manager**, dans la zone de texte **Nom du serveur**, tapez **lon-om1.adatum.com**. Cliquez sur **Utiliser un compte d'identification**, puis sur **Parcourir**.
7. Sélectionnez **Administrateur**, puis cliquez sur **OK**.
8. Cliquez sur **Suivant**.
9. Dans la page **Connexion à VMM**, tapez **Adatum\Administrateur** en tant que Nom d'utilisateur et **Pa$$w0rd** en tant que Mot de passe, puis cliquez sur **Suivant**.
10. Dans la page **Résumé**, cliquez sur **Terminer**.
11. Attendez la fin du travail, puis fermez la fenêtre **Travaux**. Si le travail ne s'achève pas correctement, redémarrez LON-OM1 et LON-VMM1 et refaites les étapes 1 à 10.

▶ Tâche 3 : Valider l'intégration de la fonctionnalité PRO

1. Sur **LON-OM1**, dans la console Operations Manager, cliquez sur l'espace de travail **Analyse**.
2. Dans l'espace de travail **Analyse**, développez **Analyse** et **PRO**, puis cliquez sur **État de l'objet PRO**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans le volet central, vérifiez que **LON-VMM1.adatum.com** est affiché.
4. Vérifiez que l'état est **Sain**. Si l'état est défini sur **Non surveillé**, patientez quelques minutes, puis actualisez la console.
5. Basculez sur l'ordinateur **LON-VMM1**.
6. Dans la console du Gestionnaire VMM, cliquez sur **Paramètres**.
7. Cliquez sur **Paramètres de System Center**, puis dans le volet droit, double-cliquez sur **Serveur Operations Manager**.
8. Dans la fenêtre Paramètres de Operations Manager, cliquez sur **PRO de test**.
9. Dans la fenêtre Virtual Machine Manager, cliquez sur **OK**, puis dans la fenêtre Paramètres de Operations Manager, cliquez sur **OK**.
10. Cliquez sur l'espace de travail **Travaux**, recherchez un travail nommé **Diagnostic PRO**, attendez l'état Terminé, puis fermez la boîte de dialogue PRO. Cliquez sur **Historique**, recherchez un travail appelé Diagnostic PRO, sélectionnez-le, puis cliquez sur **Détails**.
11. Assurez-vous que toutes les tâches dans ce travail se sont terminées correctement.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-SVR2**, **22414B-LON-VMM1** et **22414B-LON-OM1**.
5. Sur LON-HOST1, dans la console Gestionnaire de serveur, supprimez la fonctionnalité Clustering avec basculement.
6. Redémarrez LON-HOST1. Lorsque le serveur démarre, choisissez LON-HOST1 dans le menu de démarrage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 9 : Planification et implémentation d'une infrastructure de mise à jour de serveur

Atelier pratique : Planification et implémentation d'une infrastructure de correction de serveur

Exercice 1 : Implémenter la mise à jour hôte dans VMM

▶ Tâche 1 : Configurer l'intégration de VMM avec WSUS

1. Sur LON-VMM1, ouvrez la **Console Virtual Machine Manager**, cliquez sur **Connecter**, puis quand la console s'ouvre, cliquez sur l'espace de travail **Ensemble fibre optique**.
2. Dans le volet de navigation, développez le nœud **Serveurs** et cliquez sur **Serveur de mise à jour**.
3. Cliquez avec le bouton droit sur **Serveur de mise à jour**, puis cliquez sur **Ajouter un serveur de mise à jour**. La boîte de dialogue **Ajouter le serveur Windows Server Update Services** s'ouvre.
4. Dans la boîte de dialogue **Ajouter le serveur Windows Server Update Services**, dans le champ **Nom de l'ordinateur**, tapez **LON-WSUS**, puis dans le champ **Port TCP/IP**, tapez **8530**.
5. Sélectionnez l'option **Entrez un nom d'utilisateur et un mot de passe**. Dans le champ **Nom d'utilisateur**, tapez **ADATUM\Administrateur**, dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Ajouter**. La fenêtre Travaux s'ouvre.
6. Dans la fenêtre Travaux, sélectionnez le travail **Ajouter un serveur de mise à jour**. Sur les onglets **Résumé** et **Détails**, surveillez le statut de la tâche de configuration.
7. Une fois le travail affiché en tant que **Terminé avec des informations**, fermez la fenêtre Travaux. **Remarque :** l'état doit être **Terminé avec des informations**.
8. Sélectionnez le nœud **Serveur de mise à jour** et vérifiez que **lon-wsus.Adatum.com** s'affiche dans le volet de résultats et que la colonne **État de l'agent** affiche **Réponse en cours**.

▶ Tâche 2 : Configurer une base de référence de mise à jour logicielle dans VMM

1. Sur LON-VMM1, dans la console **Virtual Machine Manager**, cliquez sur l'espace de travail **Bibliothèque**.
2. Dans le volet de navigation, développez **Mettre à jour le catalogue et les lignes de base**, puis cliquez sur **Mettre à jour le catalogue**.
3. Dans le volet des résultats, vérifiez que les différentes mises à jour logicielles sont affichées. Ces mises à jour ont été synchronisées à partir du rôle serveur Windows Server® Update Services (WSUS). Si vous ne visualisez pas de mises à jour logicielles, cliquez avec le bouton droit sur **Mettre à jour le catalogue**, puis cliquez sur **Synchroniser le serveur de mise à jour**. Une fois la synchronisation terminée, fermez la fenêtre Travaux.
4. Dans le ruban, cliquez sur **Créer** à deux reprises, puis sur **Ligne de base**. L'Assistant Mise à jour de la ligne de base démarre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans l'Assistant Mise à jour de la ligne de base, dans la page **Général**, dans le champ **Nom**, tapez **Serveur base de référence**, et cliquez sur **Suivant**.
6. Dans la page **Mises à jour**, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Ajouter les mises à jour à la ligne de base**, cliquez sur la mise à jour suivante :
   - **Mise à jour pour Windows Server 2012 (KB2751352)**
8. Cliquez sur **Ajouter**, puis sur **Suivant**.
9. Dans la page **Étendue de l'affectation**, activez les cases à cocher correspondant aux éléments suivants, puis cliquez sur **Suivant** :
   - Serveurs de bibliothèque : **LON-VMM1.Adatum.com**
   - Serveur de mise à jour : **LON-WSUS.Adatum.com**
   - Serveur VMM : **LON-VMM1.Adatum.com**
10. Dans la page **Résumé**, cliquez sur **Terminer**.
11. Dans la fenêtre Travaux, vérifiez que la tâche de **Créer une nouvelle ligne de base** été accomplie avec succès.
12. Fermez la fenêtre Travaux.

▶ Tâche 3 : Vérifier la conformité de la base de référence

1. Sur LON-VMM1, cliquez sur l'espace de travail **Ensemble fibre optique**.
2. Dans le volet de navigation, développez **Serveurs**, et cliquez sur **Serveurs de bibliothèque**.
3. Dans le ruban, cliquez sur le bouton **Compatibilité**.
4. Dans le volet des résultats, notez la conformité et l'état opérationnel de **LON-VMM1.Adatum.com**. L'état de conformité doit être **Inconnu**, et l'état opérationnel doit être **Analyse de compatibilité en attente**.
5. Sélectionnez **LON-VMM1.Adatum.com**, puis dans le ruban, cliquez sur **Analyse**. Le contenu de la colonne État opérationnel devient **Analyse**. Après une minute environ, l'état de conformité doit devenir **Conforme**. Ceci indique que lon-vmm1.adatum.com est conforme à la base de référence que vous avez configurée dans la tâche précédente. Remarque : si l'état de conformité est indiqué comme étant **Non compatible**, cliquez avec le bouton droit sur LON-VMM1.Adatum.com, et sélectionnez **Corriger** dans la fenêtre Correction de mise à jour. En outre, activez la case à cocher **Ne pas redémarrer les serveurs après la correction**, puis cliquez sur le bouton **Corriger**. Après une minute environ, l'**État de conformité** doit devenir Conforme.
6. Fermez la console **Virtual Machine Manager**.
7. Rétablissez 22414B-LON-VMM1.

Résultats : Après avoir terminé cet exercice, vous aurez configuré la mise à jour hôte VMM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Configuration du clustering avec basculement et de la mise à jour adaptée aux clusters

▶ Tâche 1 : Implémenter un clustering avec basculement

1. Sur LON-SVR1, dans **Gestionnaire de serveur**, cliquez sur **Tableau de bord**, puis sur **Ajouter des rôles et des fonctionnalités**.
2. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
3. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner des fonctionnalités**, sélectionnez **Clustering avec basculement**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
7. Dans la page **Confirmation**, cliquez sur **Installer**.
8. Lorsque le message **Installation réussie** s'affiche, cliquez sur **Fermer**.
9. Répétez les étapes 1 à 8 sur LON-SVR2.

▶ Tâche 2 : Configurer la cible iSCSI

1. Sur LON-SVR1, ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Initiateur iSCSI**. À l'invite **Microsoft iSCSI**, cliquez sur **Oui**.
2. Cliquez sur l'onglet **Découverte**.
3. Cliquez sur **Découvrir un portail**.
4. Dans la zone **Adresse IP ou nom DNS**, tapez **172.16.0.10**, puis cliquez sur **OK**.
5. Cliquez sur l'onglet **Cibles**.
6. Cliquez sur **Actualiser**.
7. Dans la liste Cibles découvertes, sélectionnez **iqn.1991-05.com.microsoft:lon-dc1-target1-target**, puis cliquez sur **Connexion**.
8. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez sur **OK**.
9. Cliquez sur **OK** pour fermer les Propriétés de : Initiateur iSCSI.
10. Sur LON-SVR2, ouvrez le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Initiateur iSCSI**.
11. Dans la boîte de dialogue **Microsoft iSCSI**, cliquez sur **Oui**.
12. Cliquez sur l'onglet **Découverte**.
13. Cliquez sur **Découvrir un portail**.
14. Dans la zone Adresse IP ou nom DNS, tapez **172.16.0.10**, puis cliquez sur **OK**.
15. Cliquez sur l'onglet **Cibles**.
16. Cliquez sur **Actualiser**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

17. Dans la liste **Cibles découvertes**, sélectionnez **iqn.1991-05.com.microsoft:lon-dc1-target1-target**, puis cliquez sur **Connexion**.
18. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez sur **OK**. Cliquez sur **OK** pour fermer les Propriétés de : Initiateur iSCSI.
19. Sur LON-SVR2, dans la fenêtre Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de l'ordinateur**.
20. Développez **Stockage**, puis cliquez sur **Gestion des disques**.
21. Cliquez avec le bouton droit sur **Disque 2**, puis cliquez sur **En ligne**. (Remarque : Faites attention à ne pas cliquer sur Disque 1.)
22. Cliquez avec le bouton droit sur **Disque 2**, puis sur **Initialiser le disque**. Dans la boîte de dialogue **Initialiser le disque**, cliquez sur **OK**.
23. Cliquez avec le bouton droit sur l'espace non alloué en regard de **Disque 2**, puis cliquez sur **Nouveau volume simple**.
24. Cliquez sur **Suivant** dans la page d'accueil.
25. Dans la page **Spécifier la taille du volume**, cliquez sur **Suivant**.
26. Dans la page **Attribuer une lettre de lecteur ou de chemin d'accès**, cliquez sur **Suivant**.
27. Dans la page **Formater une partition**, dans la zone **Nom de volume**, tapez **ClusterDisk**. Activez la case à cocher **Effectuer un formatage rapide**, puis cliquez sur **Suivant**.
28. Cliquez sur **Terminer**. (Remarque : Si une boîte de dialogue avec une invite de formatage du disque apparaît, cliquez sur Annuler.)
29. Cliquez avec le bouton droit sur **Disque 3**, puis cliquez sur **En ligne**.
30. Cliquez avec le bouton droit sur **Disque 3**, puis sur **Initialiser le disque**. Dans la boîte de dialogue **Initialiser le disque**, cliquez sur **OK**.
31. Cliquez avec le bouton droit sur l'espace non alloué en regard de **Disque 3**, puis cliquez sur **Nouveau volume simple**.
32. Cliquez sur **Suivant** dans la page d'accueil.
33. Dans la page **Spécifier la taille du volume**, cliquez sur **Suivant**.
34. Dans la page **Attribuer une lettre de lecteur ou de chemin d'accès**, cliquez sur **Suivant**.
35. Dans la page **Formater une partition**, dans la zone **Nom de volume**, tapez **Quorum**. Activez la case à cocher **Effectuer un formatage rapide**, puis cliquez sur **Suivant**.
36. Cliquez sur **Terminer**. (Remarque : Si une boîte de dialogue avec une invite de formatage du disque apparaît, cliquez sur Annuler.)
37. Fermez Gestion de l'ordinateur.
38. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de l'ordinateur**.
39. Développez **Stockage**, puis cliquez sur **Gestion des disques**.
40. Cliquez avec le bouton droit sur **Gestion des disques**, puis cliquez sur **Actualiser**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

41. Cliquez avec le bouton droit sur **Disque 3**, puis cliquez sur **En ligne**. (Remarque : faites attention à ne pas cliquer sur Disque 2.)
42. Cliquez avec le bouton droit sur **Disque 4**, puis cliquez sur **En ligne**.

    (Remarque : LON-SVR1 a déjà deux disques, ces disques supplémentaires sont donc nommés Disque 3 et Disque 4, à la différence de LON-SVR2 où les mêmes disques sont nommés Disque 2 et Disque 3).
43. Fermez Gestion de l'ordinateur.

▶ Tâche 3 : Configurer le cluster

1. Sur LON-SVR1, dans la console du Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire du cluster de basculement**.
2. Dans le Gestionnaire du cluster de basculement, dans le volet central, sous Administration, cliquez sur **Créer le cluster**.
3. Dans l'Assistant Création d'un cluster, dans la page Avant de commencer, lisez les informations qui s'affichent. Cliquez sur **Suivant**.
4. Dans la zone **Nom du serveur**, tapez **LON-SVR1**, puis cliquez sur **Ajouter**. Tapez **LON-SVR2**, puis cliquez sur **Ajouter**.
5. Vérifiez les entrées, puis cliquez sur **Suivant**.
6. Dans la page **Avertissement de validation**, cliquez sur **Non. Je n'ai pas besoin de l'assistance de Microsoft pour ce cluster** et cliquez sur **Suivant**.
7. Dans la page **Point d'accès pour l'administration du cluster**, dans le champ **Nom du cluster**, tapez **FSCluster**.
8. Sous **Adresse**, tapez **172.16.0.127**, puis cliquez sur **Suivant**.
9. Dans la boîte de dialogue **Confirmation**, vérifiez les informations, désactivez la case à cocher en regard de **Ajouter la totalité du stockage disponible au cluster**, puis cliquez sur **Suivant**.
10. Dans la page Résumé de l'Assistant Création d'un cluster, cliquez sur **Terminer**.
11. Dans la console Gestionnaire du cluster de basculement, développez **FSCluster.Adatum.com**, puis **Stockage** et cliquez avec le bouton droit sur **Disques**.
12. Cliquez sur **Ajouter un disque**.
13. Dans la boîte de dialogue **Ajouter des disques à un cluster**, vérifiez que les options Disque du cluster 1 et Disque du cluster 2 sont sélectionnées, puis cliquez sur **OK**.
14. Développez Stockage et cliquez sur **Disques**. Vérifiez que les disques sont disponibles pour le stockage en cluster dans **Gestionnaire du cluster de basculement**.
15. Cliquez avec le bouton droit sur Disque de cluster 1 et sélectionnez **Ajouter aux volumes partagés de cluster**.
16. Cliquez avec le bouton droit sur **FSCluster.adatum.com**, sélectionnez **Autres actions**, puis cliquez sur **Configurer les paramètres du quorum du cluster**. Cliquez sur **Suivant**.
17. Dans la page **Sélectionner l'option de configuration du quorum**, cliquez sur **Utiliser les paramètres standard**, puis sur **Suivant**.
18. Dans la page **Confirmation**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

19. Dans la page **Résumé**, cliquez sur **Terminer**.
20. Cliquez avec le bouton droit sur **Rôles**, puis sélectionnez **Configurer un rôle**.
21. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
22. Dans la page **Sélectionner un rôle**, sélectionnez **Serveur de fichiers**, puis cliquez sur **Suivant**.
23. Dans la page **Type de serveur de fichiers**, cliquez sur **Serveur de fichiers avec montée en puissance parallèle pour les données d'application**, puis sur **Suivant**.
24. Dans la page **Point d'accès client**, dans la zone **Nom**, saisissez **AdatumFS**, puis cliquez sur **Suivant**.
25. Dans la page **Confirmation**, cliquez sur **Suivant**.
26. Dans la page **Résumé**, cliquez sur **Terminer**.

▶ Tâche 4 : Configurer CAU

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Dans l'Assistant **Ajout de rôles et de fonctionnalités**, dans la page **Avant de commencer**, cliquez sur **Suivant**.
3. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner des fonctionnalités**, dans la liste de fonctionnalités, cliquez sur **Clustering avec basculement**. Dans la boîte de dialogue **Ajouter les fonctionnalités requises Pour Clustering avec basculement ?**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
7. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
8. Une fois l'installation terminée, cliquez sur **Fermer**.
9. Basculez vers LON-SVR1. Ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils** et cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité**.
10. Dans la fenêtre Pare-feu Windows avec fonctions avancées de sécurité, cliquez sur **Règles de trafic entrant**.
11. Dans la liste de règles, recherchez la **Règle entrante pour l'arrêt à distance (RPC-EP entrant).** Cliquez avec le bouton droit sur la règle, puis sélectionnez **Activer la règle**.
12. Dans la liste de règles, recherchez la **Règle entrante pour l'arrêt à distance (TCP entrant).** Cliquez avec le bouton droit sur la règle, puis sélectionnez **Activer la règle**.
13. Fermez la fenêtre Pare-feu Windows avec fonctions avancées de sécurité.
14. Passez à LON-SVR2 et répétez les étapes 9 à 13.
15. Basculez vers l'ordinateur LON-WSUS.
16. Ouvrez **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Services WSUS** (Windows Server Update Services).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

17. Dans le nœud **Update Services**, développez **LON-WSUS**, puis **Mises à jour** et cliquez sur **Toutes les mises à jour**.
18. Dans le volet central, faites défiler la liste des mises à jour, sélectionnez **Mise à jour pour Windows Server 2012 (KB2771431)** puis maintenez la touche **CTRL** enfoncée, et sélectionnez **Mise à jour pour Windows Server 2012 (KB2772501)**. Cliquez avec le bouton droit sur les mises à jour sélectionnées et cliquez sur **Approuver**.
19. Dans la fenêtre **Approuver les mises à jour**, cliquez sur la zone de liste déroulante en regard de **Ordinateurs non attribués** et sélectionnez **Approuvée pour l'installation**. Cliquez sur **OK**, puis sur **Fermer**.
20. Sur LON-DC1, dans le tableau de bord **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Mise à jour adaptée aux clusters**.
21. Dans la fenêtre Mise à jour adaptée aux clusters, dans la liste déroulante **Se connecter à un cluster de basculement**, sélectionnez **FSCLUSTER**. Cliquez sur **Connecter**.
22. Dans le volet Actions de cluster, cliquez sur **Afficher un aperçu des mises à jour pour ce cluster**.
23. Dans la fenêtre FSCluster - Afficher un aperçu des mises à jour, cliquez sur **Générer la liste des aperçus de mises à jour**. Après quelques minutes, des mises à jour apparaissent dans la liste. Examinez-les, puis cliquez sur **Fermer**.

▶ Tâche 5 : Mettre à jour le cluster de basculement

1. Sur LON-DC1, dans la console **FSCluster - Mise à jour adaptée aux clusters**, cliquez sur **Appliquer les mises à jour à ce cluster**.
2. Dans la page **Mise en route**, cliquez sur **Suivant**.
3. Dans la page **Options avancées**, examinez les options de mise à jour, puis cliquez sur **Suivant**.
4. Dans la page **Options de mise à jour supplémentaires**, cliquez sur **Suivant**.
5. Dans la page **Confirmation**, cliquez sur **Mettre à jour**, puis sur **Fermer**.
6. Dans le volet Nœuds de cluster, vous pouvez examiner la progression de la mise à jour. **Remarque :** notez qu'un nœud du cluster est **En attente**, tandis que l'autre nœud redémarre une fois qu'il a été mis à jour.
7. Attendez la fin du processus. **Remarque :** Le redémarrage des deux nœuds peut être requis. Le processus est terminé lorsque deux nœuds affichent la valeur **Opération réussie** dans la colonne État de la dernière exécution.
8. Ouvrez une session sur LON-SVR1 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd,** si nécessaire.
9. Sur LON-SVR1, dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Mise à jour adaptée aux clusters**.
10. Dans la boîte de dialogue **Mise à jour adaptée aux clusters**, dans la liste déroulante **Se connecter à un cluster de basculement**, sélectionnez **FSCLUSTER**. Cliquez sur **Connecter**.
11. Cliquez sur **Configurer les options de mise à jour automatique du cluster** dans le volet **Actions de cluster**.
12. Dans la page **Mise en route**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

13. Dans la page **Ajouter le rôle en cluster de la mise à jour adaptée aux clusters avec la mise à jour automatique activée**, cliquez sur **Ajouter le rôle en cluster de la mise à jour adaptée aux clusters, avec le mode de mise à jour automatique activé, à ce cluster**, puis sur **Suivant**.
14. Dans la page **Spécifier la planification de la mise à jour automatique**, cliquez sur **Chaque semaine** et dans la zone **Heure du jour**, sélectionnez **04:00**, puis dans la zone **Jour de la semaine**, sélectionnez **dimanche**. Cliquez sur **Suivant**.
15. Dans la page **Options avancées**, cliquez sur **Suivant**.
16. Dans la page **Options de mise à jour supplémentaires**, cliquez sur **Suivant**.
17. Dans la page **Confirmation**, cliquez sur **Appliquer**.
18. Cliquez sur **Fermer** une fois que le rôle en cluster est installé.

Résultats : Après avoir terminé cet exercice, vous aurez installé la fonctionnalité de cluster de basculement et configuré la mise à jour adaptée aux clusters.

Exercice 3 : Planification d'un déploiement WSUS

▶ Tâche 1 : Lisez et analysez le scénario de l'exercice

1. Utilisez le manuel du stagiaire pour lire le scénario de l'exercice.

▶ Tâche 2 : Selon les exigences du scénario de l'exercice, proposez une conception de déploiement WSUS

1. Combien de serveurs WSUS A. Datum a-t-il en tout ?

   Réponse : Puisque chaque site doit avoir un serveur WSUS, il y en aura trois au total. Chaque site en aura un.

2. Quel type de configuration de serveur WSUS allez-vous déployer à Sydney ?

   Réponse : Sydney doit avoir un serveur WSUS distinct qui va synchroniser des mises à jour à partir d'Internet.

3. Quel type de configuration de serveur WSUS allez-vous déployer à Toronto ?

   Réponse : Le site de Toronto doit avoir un serveur WSUS en mode Réplication.

4. Comment allez-vous répondre aux exigences pour déployer les mises à jour par service ?

   Réponse : Vous pouvez effectuer des déploiements par service en créant des groupes d'ordinateurs dans WSUS pour chaque service. Vous devez ensuite utiliser le ciblage au niveau client pour placer chaque ordinateur de chaque service dans le groupe d'ordinateurs compétent sur WSUS.

5. Comment répondre aux exigences pour stocker la bande passante entre Londres et Sydney ?

   Réponse : Puisque Sydney aura un serveur WSUS indépendant, WSUS ne génère aucun trafic entre Londres et Sydney.

6. Comment répondre aux exigences pour stocker la bande passante entre Toronto et Internet ?

   Réponse : Puisque Toronto aura un serveur WSUS en mode Réplication, ce serveur synchronisera les mises à jour du serveur WSUS de Londres. Cela permet de réduire le trafic WSUS sur Internet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Comment allez-vous configurer les groupes de tests ?

   Réponse : Les groupes de tests se composeront d'ordinateurs avec des configurations similaires ou identiques à celles d'un environnement de production. Chaque configuration de production doit avoir son représentant dans le groupe de tests.

8. Y a-t-il d'autres solutions ?

   Réponse : Vous devez présenter des solutions alternatives avec la classe.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

1. Utilisez le corrigé de l'atelier pratique pour comparer votre solution avec celle fournie.
2. Comparez votre solution avec celle de la classe et de l'instructeur.

Résultats : À la fin de cet exercice, vous aurez planifié une scénario de déploiement WSUS.

Exercice 4 : Déploiement d'un serveur WSUS en mode Réplication

▶ Tâche 1 : Installer et configurer un serveur de réplication sur TOR-SVR1

1. Sur TOR-SVR1, dans la console du **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
3. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner des rôles de serveurs**, faites défiler l'écran vers le bas, sélectionnez **Services WSUS (Windows Server Update Services)**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
6. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Dans la page **Services WSUS (Windows Server Update Services)**, cliquez sur **Suivant**.
8. Dans la page **Sélectionner des services de rôle**, cliquez sur **Suivant**.
9. Dans la page **Sélection de l'emplacement du contenu**, tapez **C:\Mises à jour** dans la zone de texte et cliquez sur **Suivant**.
10. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. Une fois l'installation terminée, cliquez sur **Fermer**.
12. Dans le tableau de bord du **Gestionnaire de serveur**, cliquez sur **WSUS**.
13. Dans le volet central, cliquez sur **Autres**.
14. Dans **Détails de la tâche Tous les serveurs**, cliquez sur **Lancer les tâches de post-installation**.
15. Patientez jusqu'à la fin de la configuration. **Remarque :** Vous savez que la configuration est terminée une fois que la colonne **Étape** comprend la valeur **Terminé**. Fermez la fenêtre Détails de la tâche Tous les serveurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Dans la console **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Services WSUS (Windows Server Update Services)**.
17. Dans l'Assistant de configuration de Windows Server Update Services, dans la page **Avant de commencer**, cliquez sur **Suivant**.
18. Dans **S'inscrire au Programme d'amélioration de Microsoft Update**, cliquez sur **Suivant**.
19. Dans la page **Choisir le serveur en amont**, cliquez sur le serveur **Synchroniser à partir d'un autre serveur Windows Server Update Services**.
20. Tapez **LON-WSUS.adatum.com** dans la zone de texte **Nom du serveur**. Sélectionnez l'option **Il s'agit d'un réplica du serveur en amont**, puis cliquez sur **Suivant**.
21. Dans la page **Définir le serveur proxy**, cliquez sur **Suivant**.
22. Dans la page **Se connecter au serveur en amont**, cliquez sur **Démarrer la connexion**. Une fois la connexion établie, cliquez sur **Suivant**. Remarque : La connexion peut mettre quelques minutes pour être établie.
23. Dans la page **Choisir les langues**, cliquez sur **Suivant**.
24. Dans la page **Définir la planification de la synchronisation**, assurez-vous que **Synchroniser manuellement** est sélectionné, puis cliquez sur **Suivant**.
25. Dans la page **Terminé**, cliquez sur **Terminer**.

▶ Tâche 2 : Vérifier la réplication à partir du serveur en amont

1. Dans la console **Mettre à jour les services**, cliquez sur **TOR-SVR1**, et dans le volet central, cliquez sur **Synchroniser maintenant**. Attendez que la synchronisation atteigne 100 %, et que le **État** soit **En attente**.
2. Basculez vers **LON-WSUS**. Ouvrez **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Services WSUS (Windows Server Update Services)**.
3. Dans le nœud **Update Services** (Services de mise à jour), développez **LON-WSUS**, puis cliquez sur **Serveurs en aval**.
4. Vérifiez que **TOR-SVR1.Adatum.com** s'affiche dans le volet central, avec la valeur **Réplica** dans la colonne **Mode**.
5. Développez le nœud **Mises à jour**, puis cliquez sur **Mises à jour critiques.**
6. Dans la zone de liste déroulante **État**, cliquez sur **Toutes**, puis sur **Actualiser**.
7. Dans la liste des mises à jour, cliquez avec le bouton droit sur la mise à jour **Mise à jour pour Windows 8 pour ordinateurs à processeur x64 (KB2751352)**, puis cliquez sur **Approuver**.
8. Dans la fenêtre Approuver les mises à jour qui s'affiche, cliquez sur la flèche à côté de **Tous les ordinateurs**, sélectionnez **Approuver l'installation**, puis cliquez sur **OK**. Dans la boîte de dialogue **Progression de l'approbation**, cliquez sur **Fermer**.
9. Rebasculez vers TOR-SVR1.
10. Dans le nœud **Update Services**, développez **TOR-SVR1**, puis **Mises à jour**, puis cliquez sur **Mises à jour critiques**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans la zone de liste déroulante **État**, cliquez sur **Toutes**, puis sur **Actualiser**.
12. Vérifiez que **Mise à jour pour Windows 8 pour ordinateurs à processeur x64 (KB2751352)** a le **Statut d'approbation** défini sur **Non approuvée**. Cliquez avec le bouton droit, puis vérifiez que l'option **Approuver** est désactivée.
13. Dans le nœud **Update Services**, cliquez sur **TOR-SVR1**, puis dans le volet central, cliquez sur **Synchroniser maintenant**. Patientez jusqu'à la fin de la synchronisation.
14. Rebasculez sur le nœud **Mises à jour critiques**. Cliquez sur la zone de liste déroulante **Approbation**, sélectionnez **Approuvées**, puis cliquez sur **Actualiser**. Vérifiez que **Mise à jour pour Windows 8 pour les ordinateurs à processeur x64 (KB2751352)** apparaît dans la liste des mises à jour approuvées. (Remarque : Si la mise à jour n'apparaît pas, attendez 4-5 minutes puis répétez les étapes 13 et 14).
15. Fermez la console **Mettre à jour les services**.

▶ Tâche 3 : Configurer un objet de stratégie de groupe pour WSUS

1. Sur LON-DC1, dans la console du Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la console **Gestion de stratégie de groupe**, développez **Forêt : Adatum.com**, puis **Domaines**, puis **Adatum.com**, cliquez avec le bouton droit sur le conteneur **Objets de stratégie de groupe** et choisissez **Nouveau**.
3. Dans la fenêtre Nouvel objet GPO, dans la zone **Nom**, tapez **WSUS**, puis cliquez sur **OK**.
4. Dans le volet central, cliquez avec le bouton droit sur **WSUS**, puis cliquez sur **Modifier**.
5. Dans l'Éditeur de gestion des stratégies de groupe, dans le nœud **Configuration ordinateur**, développez **Stratégies**, puis **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local**, puis **Composants Windows**, puis cliquez sur **Windows Update**.
6. Dans le volet de droite, double-cliquez sur **Configuration du service Mises à jour automatiques**.
7. Dans la fenêtre Configuration du service Mises à jour automatiques, cliquez sur **Activé**. Dans la zone déroulante **Configuration de la mise à jour automatique**, sélectionnez **4 – Téléchargement automatique et planification des installations**.
8. Dans la zone déroulante **Jour de l'installation planifiée**, sélectionnez **1-Tous les dimanches**, puis cliquez sur **Paramètre suivant**.
9. Dans la fenêtre Spécifier l'emplacement intranet du service de mise à jour Microsoft, cliquez sur **Activé**.
10. Dans la zone de texte **Configurer le service de Mise à jour pour la détection des mises à jour**, tapez : **http://TOR-SVR1.adatum.com,** tapez la même chose dans **Configurer le serveur intranet de statistiques**, puis cliquez sur **OK**.
11. Fermez l'Éditeur de gestion des stratégies de groupe.

Résultats : À la fin de cet exercice, vous aurez déployé un serveur de réplication WSUS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 5 : Configurer les options de mise à jour du client

▶ Tâche 1 : Créer les groupes d'ordinateurs requis

1. Sur LON-WSUS, dans le nœud Mettre à jour les services, développez **LON-WSUS**, puis **Ordinateurs**, cliquez avec le bouton droit sur **Tous les ordinateurs**, puis sélectionnez **Ajouter un groupe d'ordinateurs**.
2. Dans la zone de texte **Nom**, tapez **clients ADatum**, puis cliquez sur **Ajouter**.
3. Cliquez avec le bouton droit sur **Tous les ordinateurs**, puis sélectionnez **Ajouter un groupe d'ordinateurs**.
4. Dans la zone de texte **Nom**, tapez **Serveurs ADatum**, puis cliquez sur **Ajouter**.

▶ Tâche 2 : Configurer des mises à jour automatiques

1. Sur LON-DC1, dans la console Gestion de stratégie de groupe, développez **Forêt : Adatum.com**, puis **Domaines,** puis **Adatum.com**, et cliquez sur **Objets de stratégie de groupe**.
2. Dans le volet central, cliquez avec le bouton droit sur **WSUS**, puis cliquez sur **Modifier**.
3. Dans l'Éditeur de gestion des stratégies de groupe, dans le nœud **Configuration ordinateur**, développez **Stratégies**, puis **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local**, puis **Composants Windows**, puis cliquez sur **Windows Update**.
4. Double-cliquez sur **Fréquence de détection des mises à jour automatiques**.
5. Cliquez sur **Activé**. Définissez la valeur du champ **Vérifier la présence de mises à jour à l'intervalle suivant (heures)** sur **1.** Cliquez sur **OK**
6. Double-cliquez sur **Autoriser l'installation immédiate des mises à jour automatiques**. Cliquez sur **Activé**, puis sur **OK**.
7. Double-cliquez sur **Activer les mises à jour automatiques recommandées via le service Mises à jour automatiques**. Cliquez sur **Activé**, puis sur **OK**.
8. Fermez l'Éditeur de gestion des stratégies de groupe.
9. Dans la console de gestion des stratégies de groupe, cliquez avec le bouton droit sur le domaine **Adatum.com**, puis sélectionnez **Lier un objet de stratégie de groupe existant**.
10. Dans la fenêtre Sélectionner un objet GPO, sélectionnez **WSUS**, puis cliquez sur **OK**.
11. Fermez la console Gestion de stratégie de groupe.

▶ Tâche 3 : Valider la configuration de la mise à jour

1. Ouvrez Windows PowerShell® sur l'ordinateur LON-DC1.
2. Tapez **gpupdate /force**, puis appuyez sur Entrée.
3. Fermez Windows PowerShell.
4. Ouvrez le Panneau de configuration.
5. Dans la liste déroulante **Afficher par**, sélectionnez **Grandes icônes**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Cliquez sur **Windows Update**.
7. Dans la fenêtre Windows Update, sélectionnez **Modifier les paramètres**.
8. Assurez-vous que l'option permettant de configurer les mises à jour importantes est désactivée. En outre, assurez-vous qu'il y a un message dans la zone jaune indiquant que certains paramètres sont gérés par votre administrateur système.
9. Fermez le panneau de configuration et Windows Update.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-SVR2**, **22414B-LON-WSUS**, et **22414B-TOR-SVR1**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré le serveur WSUS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 10 : Planification et implémentation d'une stratégie de continuité des activités de l'entreprise

Atelier pratique : Implémentation d'une stratégie de sauvegarde d'ordinateurs virtuels avec DPM

Exercice 1 : Configurer DPM

▶ Tâche 1 : Configurer un pool de stockage dans Microsoft® System Center® 2012 - Data Protection Manager (DPM)

1. Basculez vers LON-DM1, puis réduisez la fenêtre du Gestionnaire de serveur.
2. Sur le Bureau, double-cliquez sur **Microsoft System Center 2012 Service Pack 1 Data Protection Manager**.
3. Dans la Console Administrateur System Center 2012 Service Pack 1 DPM**,** cliquez sur l'espace de travail **Administration**, puis, dans la barre de navigation, cliquez sur le lien **Disques**.
4. Dans le ruban, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter des disques au pool de stockage** s'affiche.
5. Dans la fenêtre Ajouter des disques au pool de stockage, sélectionnez **Disque 1**, cliquez sur **Ajouter**, puis cliquez sur **OK**.
6. Vous devez voir **Disque 1 (Virtuel HD ATA Device)** (périphérique ATA HD virtuel) ajouté dans **Disques du pool de stockage DPM**, marqué d'une case à cocher verte.

▶ Tâche 2 : Déployer les agents de protection DPM

1. Basculez vers **LON-**SVR1.
2. Dans la barre des tâches, cliquez sur l'icône du **Gestionnaire de serveur**.
3. Dans le **Gestionnaire de serveur**, dans la partie supérieure droite de la fenêtre, cliquez sur **Outils**, puis sur **Propriétés de : Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local**.
4. Dans la fenêtre Pare-feu Windows avec fonctions avancées de sécurité, dans le volet de navigation, cliquez avec le bouton droit sur **Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local**, puis cliquez sur **Propriétés**.
5. Dans la fenêtre Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local, cliquez dans la liste déroulante **Connexions entrantes**, sélectionnez **Autoriser**, puis cliquez sur **OK**.
6. Fermez la fenêtre Pare-feu Windows avec fonctions avancées de sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Basculez vers **LON-HOST1.**
8. Répétez les étapes de 1 à 6 sur **LON-HOST1**.

Remarque : Dans l'environnement de production, vous pouvez personnaliser les paramètres de pare-feu sur les serveurs d'entreprise pour autoriser le trafic provenant des adresses IP et des ports nécessaires pour la communication avec DPM.

9. Basculez vers **LON-DM1.**
10. Dans la Console Administrateur DPM, cliquez sur l'espace de travail **Administration**, puis, dans la barre de navigation, cliquez sur le lien **Agents**.
11. Dans le ruban, cliquez sur **Installer**. L'Assistant Installation de l'agent de protection s'ouvre.
12. Dans la page **Sélectionnez la méthode de déploiement de l'agent**, cliquez sur **Installer des agents**, puis cliquez sur **Suivant**.
13. Dans la page **Sélectionner les ordinateurs**, sélectionnez **LON-SVR1** et **LON-HOST1** dans la liste, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
14. Dans la page **Entrer les informations d'identification**, dans la zone **Nom d'utilisateur**, tapez **Administrateur** et, dans la zone **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Suivant**.
15. Dans la page **Choisir une méthode de redémarrage**, cliquez sur **Oui**. Redémarrer les ordinateurs sélectionnés une fois les agents de protection installés (si nécessaire), puis cliquez sur **Suivant**.
16. Dans la page **Résumé**, cliquez sur **Installer**. Attendez que la colonne Résultats indique **Réussite** pour chacun des serveurs sur lesquels vous avez installé l'agent.
17. Cliquez sur **Fermer** pour fermer l'Assistant Installation de l'agent de protection.

▶ Tâche 3 : Configurer des groupes de protection

Créer un groupe de protection de données

1. Sur LON-DM1, dans la Console Administrateur DPM, cliquez sur l'espace de travail **Protection**.
2. Dans le ruban, cliquez sur **Nouveau**. L'Assistant Créer un nouveau groupe de protection s'ouvre.
3. Dans la page Bienvenue dans l'Assistant Nouveau groupe de protection, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le type de groupe de protection**, sélectionnez **Serveurs**, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionnez les membres du groupe**, sous **Membres disponibles**, développez **LON-SVR1**, développez **Tous les volumes**, développez le lecteur **C:**, activez la case à cocher du dossier **Financial Data** (Données financières), cliquez sur **OK**, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner la méthode de protection des données**, dans la zone **Nom du groupe de protection**, tapez **Dossier des données financières du groupe de protection**, assurez-vous que l'option **Je souhaite une protection à court terme à l'aide de : Disque** est sélectionnée, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Dans la page **Spécifier les objectifs à court terme**, acceptez les paramètres par défaut, puis cliquez sur **Suivant**.
8. Dans la page **Vérifier l'allocation de disque**, cliquez sur **Suivant**.
9. Dans la page **Choisir la méthode de création de réplica**, cliquez sur **Suivant**.
10. Dans la page **Options de vérification de cohérence**, cliquez sur **Suivant**.
11. Dans la page **Résumé**, cliquez sur **Créer un groupe**.
12. Dans la page **État**, vérifiez que les deux processus indiquent **Réussite** dans la colonne **Résultats**, puis cliquez sur **Fermer**.

Créer un groupe de protection d'ordinateurs virtuels

1. Sur LON-DM1, dans la Console Administrateur DPM, cliquez sur l'espace de travail **Protection**.
2. Dans le ruban, cliquez sur **Nouveau**. L'Assistant Créer un nouveau groupe de protection s'ouvre.
3. Dans la page **Bienvenue dans l'Assistant Nouveau groupe de protection**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le type de groupe de protection**, sélectionnez **Serveurs**, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionnez les membres du groupe**, sous **Membres disponibles**, développez **LON-HOST1**, développez **Hyper-V**, activez la case à cocher **Backup Using Saved State\ 22414B-LON-TEST**, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner la méthode de protection des données**, dans la zone **Nom du groupe de protection**, tapez **Groupe de protection VM**, assurez-vous que l'option **Je souhaite une protection à court terme à l'aide de : Disque** est sélectionnée, puis cliquez sur **Suivant**.
7. Dans la page **Spécifier les objectifs à court terme**, acceptez les paramètres par défaut, puis cliquez sur **Suivant**.
8. Dans la page **Vérifier l'allocation de disque**, cliquez sur **Suivant**.
9. Dans la page **Choisir la méthode de création de réplica**, cliquez sur **Suivant**.
10. Dans la page **Options de vérification de cohérence**, cliquez sur **Suivant**.
11. Dans la page **Résumé**, cliquez sur **Créer un groupe**.
12. Dans la page **État**, vérifiez que les deux processus indiquent **Réussite** dans la colonne **Résultats**, puis cliquez sur **Fermer**.

Résultats : Une fois ces tâches terminées, vous aurez :

- configuré un pool de stockage dans DPM ;
- déployé des agents de protection DPM ;
- configuré des groupes de protection.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT - - - - QUEMENT

Exercice 2 : Implémenter la sauvegarde et la récupération des données des ordinateurs virtuels

▶ Tâche 1 : Configurer Data Protection Manager pour sauvegarder les données d'ordinateur virtuel

1. Sur LON-DM1, dans la Console Administrateur DPM, cliquez sur l'espace de travail **Protection**.
2. Dans le volet d'informations, assurez-vous que l'état du **Dossier des données financières du groupe de protection** est marqué d'une case à cocher verte.
3. Dans le volet d'informations, sélectionnez puis cliquez avec le bouton droit sur **C:\Financial Data** (Données financières), puis cliquez sur **Créer un point de récupération**. La boîte de dialogue **Créer un point de récupération** s'ouvre.
4. Dans **Créer un point de récupération**, cliquez sur **OK**.
5. Dans la page **Créer un point de récupération**, vérifiez que les deux processus indiquent **Réussite** dans la colonne **Résultats**, puis cliquez sur **Fermer**.

▶ Tâche 2 : Supprimer les données

1. Basculez vers LON-SVR1.
2. Dans la barre des tâches, cliquez sur **Explorateur de fichiers**, puis cliquez sur **Disque local (C:)** dans le volet de navigation.
3. Dans l'**Explorateur de fichiers**, dans le volet d'informations, cliquez avec le bouton droit sur le dossier **Financial Data**, puis cliquez sur **Supprimer**.
4. Fermez l'Explorateur de fichiers.

▶ Tâche 3 : Restaurer les données supprimées

1. Basculez vers LON-DM1.
2. Dans la Console Administrateur DPM, cliquez sur l'espace de travail **Récupération**.
3. Dans le volet de navigation, développez **LON-SVR1**, développez **Tous les volumes protégés**, puis cliquez sur **C:**.
4. Dans le volet de résultats, sélectionnez puis cliquez avec le bouton droit sur **Financial Data**, puis cliquez sur **Récupérer**. L'Assistant Récupération s'ouvre.
5. Dans la page **Vérifier la récupération sélectionnée**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner le type de récupération**, cliquez sur **Récupérer à l'emplacement d'origine**, puis cliquez sur **Suivant**.
7. Dans la page **Spécifier les options de récupération**, cliquez sur **Suivant**.
8. Dans la page **Résumé**, cliquez sur **Récupérer**.
9. Dans la page **Statut de la récupération**, vérifiez que **Statut de la récupération** est **Réussite**, puis cliquez sur **Fermer**.
10. Cliquez sur l'espace de travail **Protection**, puis cliquez sur **Tous les groupes de protection**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans le volet d'informations, cliquez avec le bouton droit sur **C:\Financial Data** (Données financières), puis cliquez sur **Effectuer une vérification de cohérence**. Cliquez sur **Oui** dans le message qui s'affiche. Quelques instants plus tard, l'**État de la protection** doit présenter une coche verte.
12. Basculez vers LON-SVR1.
13. Sur LON-SVR1, dans la barre des tâches, cliquez sur **Explorateur de fichiers**, puis, dans le volet de navigation, cliquez sur **Disque local (C:)** , puis assurez-vous que le dossier **Financial Data** a été restauré.
14. Fermez l'Explorateur de fichiers.

Résultats : Une fois ces tâches terminées, vous aurez :

- configuré DPM pour sauvegarder les données d'ordinateur virtuel ;
- supprimé les données ;
- restauré les données.

Exercice 3 : Implémenter la sauvegarde et la restauration des ordinateurs virtuels à l'aide de Data Protection Manager

▶ Tâche 1 : Sauvegarder un ordinateur virtuel à l'aide de Data Protection Manager

1. Sur LON-DM1, dans la Console Administrateur DPM, cliquez sur l'espace de travail **Protection**, puis, dans le volet d'informations, cliquez sur **Groupe de protection : Groupe de protection VM**.
2. Dans le volet d'informations, assurez-vous que l'état du **Groupe de protection VM** est marqué d'une coche verte. Jusqu'à 10 minutes peuvent être nécessaires pour que l'état indique **OK**.
3. Dans le volet d'informations, cliquez avec le bouton droit sur **\Backup Using Saved State\ 22414B-LON-TEST**, puis cliquez sur **Créer un point de récupération**. La boîte de dialogue **Créer un point de récupération** s'ouvre.
4. Dans **Créer un point de récupération**, cliquez sur **OK**.
5. Dans la page **Créer un point de récupération**, vérifiez que la tâche indique **Réussite** dans la colonne **Résultats**, puis cliquez sur **Fermer**.

▶ Tâche 2 : Modifier une configuration sur l'ordinateur virtuel

1. Basculez vers **LON-HOST1**.
2. Dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22414B-LON-TEST**, puis cliquez sur **Paramètres**.
3. Dans **Paramètres pour 22414B-LON-TEST sur LON-HOST1**, dans le volet gauche, sous **Matériel**, cliquez sur **Mémoire**, puis dans le volet droit, à côté de **RAM de démarrage**, tapez **256**, puis cliquez sur **OK**.

Remarque : Cette modification perturbera le fonctionnement normal de LON-TEST en raison de la petite quantité de mémoire configurée. Dans la tâche suivante, vous restaurerez le paramètre initial de mémoire pour LON-TEST à partir de la sauvegarde.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Restaurer l'ordinateur virtuel

1. Basculez vers LON-DM1.
2. Dans la Console Administrateur DPM, cliquez sur l'espace de travail **Récupération**.
3. Dans le volet de navigation, développez **Données récupérables\Adatum.com\LON-HOST1**, puis cliquez sur **Toutes les données HyperV protégées**.
4. Dans le volet de résultats, sous **Élément récupérable**, sélectionnez et cliquez avec le bouton droit sur **Backup Using Saved State\22414B-LON-TEST**, puis cliquez sur **Récupérer**. L'Assistant Récupération s'ouvre.
5. Dans la page **Vérifier la récupération sélectionnée**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner le type de récupération**, cliquez sur **Récupérer sur l'instance d'origine**, puis cliquez sur **Suivant**.
7. Dans la page **Spécifier les options de récupération**, cliquez sur **Suivant.**
8. Dans la page **Résumé**, cliquez sur **Récupérer**.
9. Dans la page **Statut de la récupération**, vérifiez que **Statut de la récupération** est **Réussite**, puis cliquez sur **Fermer.**
10. Basculez vers LON-HOST1.
11. Dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22414B-LON-TEST**, puis cliquez sur **Paramètres**.
12. Dans **Paramètres pour 22414B-LON-TEST sur LON-HOST1**, dans le volet gauche, sous **Matériel**, cliquez sur **Mémoire**, puis dans le volet droit, à côté de **RAM de démarrage,** vérifiez que la valeur **1024** a été restaurée, puis cliquez sur **OK**.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1** et **22414B-LON-DM1**.

Résultats : Une fois ces tâches terminées, vous aurez :

- sauvegardé un ordinateur virtuel à l'aide de DPM ;
- modifié une configuration sur l'ordinateur virtuel ;
- restauré l'ordinateur virtuel.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 11 : Planification et implémentation d'une infrastructure à clé publique

Atelier pratique : Planification et implémentation d'une infrastructure AD CS

Exercice 1 : Planification du déploiement AD CS

▶ Tâche 1 : Lire la documentation fournie avec le produit

- Lire le scénario de l'exercice d'atelier pratique

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

Répondez à ces questions :

1. Vous pouvez satisfaire l'exigence d'isolement de l'autorité de certification racine en déployant une autorité de certification racine hors connexion.
2. Vous pouvez obtenir la haute disponibilité du rôle d'autorité de certification en déployant un cluster d'autorités de certification ou en déployant plusieurs autorités de certification pour chaque région.
3. Vous pouvez réaliser l'authentification basée sur les certificats en déployant des cartes à puce pour tous les responsables et pour tous les utilisateurs qui utilisent les applications qui requièrent une authentification basée sur les certificats. Vous pouvez aussi faire en sorte que les responsables ne se connectent qu'avec des cartes à puce, en configurant des options proposées dans leurs comptes utilisateurs des services de domaine Active Directory® (AD DS).
4. Pour configurer un certificat de serveur Web, vous dupliquerez un modèle de certificat de serveur Web existant et configurerez les options requises sur le nouveau modèle. Le nouveau modèle sera utilisé au lieu de l'ancien en configurant le remplacement.
5. Vous devrez placer tous les ordinateurs portables dans une unité d'organisation (OU) distincte. Vous devrez en outre dupliquer le modèle de certificat d'ordinateur, puis en faire un nouveau appelé Windows® 8 DirectAccess avec les options indiquées dans le scénario de l'atelier pratique. Vous configurerez une liste de contrôle d'accès discrétionnaire (DACL) sur ce modèle de certificat, de sorte que seuls les ordinateurs portables puissent s'inscrire pour ce certificat. Ensuite vous configurerez le nouvel objet de stratégie de groupe et le lierez à l'unité d'organisation des portables. Vous configurerez l'inscription automatique de certificats d'ordinateur dans cet objet de stratégie de groupe.
6. Pour réduire la bande passante utilisée pour le contrôle de révocation entre les sites, vous pouvez déployer la fonctionnalité de répondeur en ligne sur chaque site.
7. Pour activer le contrôle de révocation à partir d'Internet, vous devez configurer de nouveaux emplacements de points de distribution de liste de révocation de certificats (CDP) et d'accès aux informations de l'autorité (AIA) dans les propriétés de l'autorité de certification émettrice. Vous devez ensuite publier les fichiers des listes de révocation de certificats et d'AIA sur cet emplacement, puis rendre cet emplacement accessible depuis Internet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

Comparez votre solution avec celle exposée dans le corrigé de l'atelier pratique. Présentez des solutions alternatives et discutez-en avec la classe.

Résultats : À la fin de cet exercice, les stagiaires auront planifié un déploiement d'AD CS.

Exercice 2 : Déploiement de l'infrastructure d'autorité de certification

▶ Tâche 1 : Installer le rôle AD CS sur un serveur autonome

1. Connectez-vous à **LON-CA1** en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la console du Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner des rôles de serveurs**, sélectionnez **Services de certificats Active Directory**. Lorsque la fenêtre de l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
7. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Dans la page **Services de certificats Active Directory**, cliquez sur **Suivant**.
9. Dans la page **Sélectionner des services de rôle**, vérifiez que l'option **Autorité de certification** est sélectionnée, puis cliquez sur **Suivant**.
10. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. Dans la page **Progression de l'installation**, une fois l'installation réussie, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination**.
12. Dans l'Assistant Configuration des services de certificats Active Directory, dans la page **Informations d'identification**, cliquez sur **Suivant**.
13. Dans la page **Services de rôle**, sélectionnez **Autorité de certification**. Cliquez sur **Suivant**.
14. Dans la page **Type d'installation**, sélectionnez **Autorité de certification autonome**, puis cliquez sur **Suivant**.
15. Dans la page **Type d'autorité de certification**, vérifiez que l'option **Autorité de certification racine** est sélectionnée, puis cliquez sur **Suivant**.
16. Dans la page **Clé privée**, vérifiez que l'option **Créer une clé privée** est sélectionnée, puis cliquez sur **Suivant**.
17. Dans la page **Chiffrement pour l'autorité de certification**, conservez les sélections par défaut pour CSP et l'algorithme de hachage, mais définissez la **Longueur de la clé** sur **4096**, puis cliquez sur **Suivant**.
18. Dans la page **Nom de l'autorité de certification**, dans la zone **Nom commun de cette AC**, tapez **AdatumRootCA**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

19. Dans la page **Période de validité**, cliquez sur **Suivant**.
20. Dans la page **Base de données de l'autorité de certification**, cliquez sur **Suivant**.
21. Dans la page **Confirmation**, cliquez sur **Configurer**.
22. Dans la page **Résultats**, cliquez sur **Fermer**.
23. Dans la page **Progression de l'installation**, cliquez sur **Fermer**.

▶ Tâche 2 : Configurer la révocation de certificats pour l'AC secondaire

1. Sur LON-CA1, dans la console Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Autorité de certification**.
2. Dans la console certsrv - [Autorité de certification (Local)], cliquez avec le bouton droit sur **AdatumRootCA**, puis cliquez sur **Propriétés**.
3. Dans la fenêtre Propriétés de : AdatumRootCA, cliquez sur l'onglet **Extensions**.
4. Sous l'onglet **Extensions**, dans la liste déroulante **Sélectionner l'extension**, sélectionnez **Points de distribution de liste de révocation des certificats (CDP)**, puis cliquez sur **Ajouter**.
5. Dans la zone de texte **Emplacement**, tapez **http://lon-svr1.adatum.com/CertData/**, et dans la zone de liste déroulante **Variable**, cliquez sur **<NomAutoritéCertification>**, puis sur **Insérer**.
6. Dans la zone de liste déroulante **Variable**, cliquez sur **<SuffixeNomListeRévocationCertificats>**, puis sur **Insérer**. Dans la zone de liste déroulante **Variable**, cliquez sur **<ListeRévocationCertificatsDeltaAutorisée>**, puis sur **Insérer**.
7. Dans la zone de texte **Emplacement**, placez le curseur à la fin de l'URL, tapez **.crl** et cliquez sur **OK**.
8. Sélectionnez les options suivantes : **Inclure dans l'extension CDP des certificats émis,** et **Inclure dans les listes de révocation des certificats afin de pouvoir rechercher les listes de révocation des certificats delta.** Cliquez sur **Appliquer**. Dans la fenêtre contextuelle Autorité de certification, cliquez sur **Non**.
9. Dans la zone de liste déroulante **Sélectionner l'extension :**, cliquez sur **Accès aux informations de l'autorité (AIA)**, puis cliquez sur **Ajouter**.
10. Dans la zone de texte **Emplacement**, tapez **http://lon-svr1.adatum.com/CertData/**, puis dans la zone déroulante **Variable**, cliquez sur **<Nom du serveur DNS>**, puis sur **Insérer**.
11. Dans la zone de texte **Emplacement**, tapez un caractère de soulignement (_), puis dans la zone de liste déroulante **Variable**, cliquez sur **<NomAutoritéCertification>**, puis sur **Insérer**.
12. Dans la zone de liste déroulante **Variable**, cliquez sur **<NomCertificat>**, puis sur **Insérer**.
13. Dans la zone de texte **Emplacement**, placez le curseur à la fin de l'URL, tapez **.crt**, puis cliquez sur **OK**.
14. Activez la case à cocher **Inclure dans l'extension AIA des certificats émis**, puis cliquez sur **OK**.
15. Cliquez sur **Oui** pour redémarrer le service d'autorité de certification.
16. Dans la console Autorité de certification, développez **AdatumRootCA**, cliquez avec le bouton droit sur **Certificats révoqués**, pointez sur **Toutes les tâches**, puis cliquez sur **Publier**.
17. Dans la fenêtre Publier la liste de révocation des certificats, cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Cliquez avec le bouton droit sur **AdatumRootCA**, puis cliquez sur **Propriétés**.
19. Dans la boîte de dialogue **Propriétés de : AdatumRootCA**, cliquez sur **Afficher le certificat**.
20. Dans la fenêtre Certificat, cliquez sur l'onglet **Détails**.
21. Sous l'onglet **Détails**, cliquez sur **Copier dans un fichier**.
22. Dans l'Assistant Exportation du certificat, dans la page **Bienvenue**, cliquez sur **Suivant**.
23. Dans la page **Format du fichier d'exportation**, sélectionnez **X.509 binaire encodé DER (*.cer)**, puis cliquez sur **Suivant**.
24. Dans la page **Fichier à exporter**, cliquez sur **Parcourir**. Dans la zone de texte **Nom du fichier**, tapez **\\lon-svr1\C$**, et appuyez sur Entrée.
25. Dans la zone de texte **Nom du fichier**, tapez **RootCA**, cliquez sur **Enregistrer**, puis sur **Suivant**.
26. Cliquez sur **Terminer**, puis sur **OK** à trois reprises.
27. Ouvrez une fenêtre Explorateur de fichiers, puis accédez à **C:\Windows\System32\CertSrv\CertEnroll**.
28. Dans le dossier **Cert Enroll**, sélectionnez les deux fichiers, cliquez avec le bouton droit sur les fichiers en surbrillance et cliquez sur **Copier**.
29. Dans la barre d'adresses de l'Explorateur de fichiers, tapez **\\lon-svr1\C$**, puis appuyez sur Entrée.
30. Cliquez avec le bouton droit sur l'espace vide, puis cliquez sur **Coller**.
31. Fermez l'Explorateur de fichiers.

▶ Tâche 3 : Publier le certificat de l'autorité de certification racine dans le domaine

1. Sur LON-DC1, ouvrez **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la console Gestion de stratégie de groupe, développez **Forêt : Adatum.com**, **Domaines**, **Adatum.com**, puis cliquez avec le bouton droit sur **Stratégie de domaine par défaut**, et cliquez sur **Modifier**.
3. Dans le nœud **Configuration ordinateur**, développez **Stratégies**,**Paramètres Windows**, **Paramètres de sécurité**, **Stratégies de clé publique**, puis cliquez avec le bouton droit sur **Autorités de certification racines de confiance**, et cliquez sur **Importer**.
4. Cliquez sur **Suivant**.
5. Dans la page **Fichier à importer**, cliquez sur **Parcourir**.
6. Dans le champ de texte **Nom du fichier**, tapez **\\lon-svr1\C$**, et appuyez sur Entrée.
7. Sélectionnez le fichier **RootCA.cer**, puis cliquez sur **Ouvrir**.
8. Cliquez à deux reprises sur **Suivant**, puis cliquez sur **Terminer**.
9. Lorsque l'invite Assistant Importation du certificat s'affiche, cliquez sur **OK.**
10. Fermez l'Éditeur de gestion des stratégies de groupe.
11. Fermez la console Gestion de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer le rôle AD CS sur l'AC d'entreprise secondaire

1. Connectez-vous à LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la console du Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner des rôles de serveurs**, sélectionnez **Services de certificats Active Directory**.
7. Lorsque la fenêtre de l'Assistant Ajout de rôles et de fonctionnalités apparaît, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
8. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Dans la page **Services de certificats Active Directory**, cliquez sur **Suivant**.
10. Dans la page **Sélectionner des services de rôle**, vérifiez que l'option **Autorité de certification** est déjà sélectionnée, puis sélectionnez **Inscription de l'autorité de certification via le Web**.
11. Lorsque la fenêtre de l'Assistant Ajout de rôles et de fonctionnalités apparaît, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
12. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
13. Dans la page **Progression de l'installation**, une fois l'installation réussie, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination**.
14. Dans l'Assistant Configuration des services de certificats Active Directory, dans la page **Informations d'identification**, cliquez sur **Suivant**.
15. Dans la page **Services de rôle**, sélectionnez **Autorité de certification** et **Inscription de l'autorité de certification via le Web**, puis cliquez sur **Suivant**.
16. Dans la page **Type d'installation**, sélectionnez **Autorité de certification d'entreprise**, puis cliquez sur **Suivant**.
17. Dans la page **Type d'autorité de certification**, cliquez sur **Autorité de certification secondaire**, puis sur **Suivant**.
18. Dans la page **Clé privée**, vérifiez que l'option **Créer une clé privée** est sélectionnée, puis cliquez sur **Suivant**.
19. Dans la page **Chiffrement pour l'autorité de certification**, conservez les sélections par défaut, puis cliquez sur **Suivant**.
20. Dans la page **Nom de l'autorité de certification**, dans la zone de texte **Nom commun de cette AC**, tapez **Adatum-IssuingCA**, puis cliquez sur **Suivant**.
21. Dans la page **Demande de certificat**, vérifiez que l'option **Enregistrer une demande de certificat dans un fichier de l'ordinateur cible** est sélectionnée, puis cliquez sur **Suivant**.
22. Dans la page **Base de données de l'autorité de certification**, cliquez sur **Suivant**.
23. Dans la page **Confirmation**, cliquez sur **Configurer**.
24. Dans la page **Résultats**, cliquez sur **Fermer**.
25. Dans la page **Progression de l'installation**, cliquez sur **Fermer**.

▶ Tâche 5 : Configurer les certificats pour activer l'approbation secondaire

1. Sur LON-SVR1, ouvrez une fenêtre de l'Explorateur de fichiers et accédez au **Disque local (C:)**.
2. Cliquez avec le bouton droit sur **RootCA.cer**, puis cliquez sur **Installer le certificat**.
3. Dans l'Assistant Importation du certificat, cliquez sur **Ordinateur local**, puis sur **Suivant**.
4. Dans la page **Magasin de certificats**, cliquez sur **Placer tous les certificats dans le magasin suivant**, puis sur **Parcourir**.
5. Sélectionnez **Autorités de certification racines de confiance**, et cliquez sur **OK**.
6. Cliquez sur **Suivant**, puis sur **Terminer**. Lorsque la fenêtre Assistant Importation du certificat s'affiche, cliquez sur **OK.**
7. Dans la fenêtre de l'Explorateur de fichiers, sélectionnez les fichiers **AdatumRootCA.crl** et **LON-CA1_AdatumRootCA.crt**, cliquez avec le bouton droit sur les fichiers et cliquez sur **Copier**.
8. Double-cliquez sur **inetpub**.
9. Double-cliquez sur **wwwroot**.
10. Créez un nouveau dossier et nommez-le **CertData**.
11. Collez les deux fichiers copiés dans ce dossier.
12. Basculez vers le **Disque local (C:)**.
13. Cliquez avec le bouton droit sur le fichier **LON-SVR1.Adatum.com_Adatum- IssuingCA.req**, puis cliquez sur **Copier**.
14. Dans la barre d'adresses de l'Explorateur de fichiers, tapez **\\LON-CA1\C$**, puis appuyez sur Entrée.
15. Dans la fenêtre de l'Explorateur de fichiers, cliquez avec le bouton droit sur un espace vide, puis cliquez sur **Coller**. Vérifiez que le fichier de demande est bien copié sur LON-CA1.
16. Passez au serveur LON-CA1.
17. Dans la console Autorité de certification, cliquez avec le bouton droit sur **AdatumRootCA**, pointez sur **Toutes les tâches**, puis cliquez sur **Soumettre une nouvelle demande**.
18. Dans la fenêtre Ouvrir un fichier de demande, accédez au **Disque local (C:)**, sélectionnez le fichier **LON-SVR1.Adatum.com_Adatum- IssuingCA.req**, puis cliquez sur **Ouvrir**.
19. Dans la console **certsrv - [Autorité de certification (Local)]**, développez **AdatumRootCA**, puis cliquez sur le conteneur **Demandes en attente**. Cliquez avec le bouton droit sur **Demandes en attente**, puis cliquez sur **Actualiser**.
20. Dans le volet de droite, cliquez avec le bouton droit sur la demande (ID n°2), pointez sur **Toutes les tâches** et cliquez sur **Délivrer**.
21. Cliquez sur le conteneur **Certificats délivrés**.
22. Dans le volet de droite, double-cliquez sur le certificat, puis cliquez sur l'onglet **Détails**.
23. Cliquez sur **Copier dans un fichier**.
24. Dans l'Assistant Exportation du certificat, dans la page **Bienvenue**, cliquez sur **Suivant**.
25. Dans la page **Format du fichier d'exportation**, sélectionnez **Standard de syntaxe de message cryptographique – Certificats PKCS #7 (.P7B)**, **Inclure tous les certificats dans le chemin d'accès de certification, si possible** puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

26. Dans la page **Fichier à exporter**, cliquez sur **Parcourir**.
27. Dans la zone de texte **Nom du fichier**, tapez **\\lon-svr1\C$**, et appuyez sur Entrée.
28. Dans la zone de texte **Nom du fichier**, tapez **SubCA**, cliquez sur **Enregistrer**, puis sur **Suivant**.
29. Cliquez sur **Terminer**, puis sur **OK** à deux reprises.
30. Basculez vers **LON-SVR1**.
31. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Autorité de certification**.
32. Dans la console Autorité de certification, cliquez avec le bouton droit sur **Adatum-IssuingCA**, pointez sur **Toutes les tâches**, puis cliquez sur **Installer un certificat d'autorité de certification**.
33. Accédez au **Disque local (C:)**, cliquez sur le fichier **SubCA.p7b**, puis sur **Ouvrir**.
34. Attendez 15 à 20 secondes, puis, dans la barre d'outils, cliquez sur l'icône verte pour démarrer le service de l'autorité de certification.
35. Vérifiez que l'AC démarre correctement.

Résultats : À la fin de cet exercice, les stagiaires auront déployé une infrastructure d'AC.

Exercice 3 : Implémentation de modèles de certificats

▶ Tâche 1 : Configurer des unités d'organisation et des groupes pour les ordinateurs portables

1. Sur LON-DC1, à partir du **Gestionnaire de serveur**, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur l'objet de domaine **Adatum.com**, sélectionnez **Nouveau**, puis cliquez sur **Unité d'organisation**.
3. Dans la fenêtre Nouvel Objet – Unité d'organisation, dans la zone de texte **Nom**, tapez **Portables**, puis cliquez sur **OK**.
4. Dans la console **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur l'unité d'organisation **Portables**, sélectionnez **Nouveau**, puis cliquez sur **Groupe**.
5. Dans la fenêtre Nouvel objet – Groupe, dans la zone de texte **Nom du groupe**, tapez **Portables**, puis cliquez sur **OK**.
6. Dans la console **Utilisateurs et ordinateurs Active Directory** cliquez sur le conteneur **Computers**.
7. Cliquez avec le bouton droit sur **LON-CL1**, sélectionnez **Déplacer**, et dans la fenêtre Déplacer, sélectionnez l'unité d'organisation **Portables**, puis cliquez sur **OK**
8. Cliquez sur l'unité d'organisation **Portables** dans la console, cliquez avec le bouton droit sur l'objet ordinateur **LON-CL1**, puis sélectionnez **Propriétés**.
9. Cliquez sur l'onglet **Membre de**, cliquez sur **Ajouter**, et dans la fenêtre Sélectionnez des groupes, tapez **Portables**, puis cliquez sur **OK**.
10. Cliquez sur **OK**.
11. Fermez la console Utilisateurs et ordinateurs Active Directory.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer le modèle de certificat du serveur Web

1. Sur LON-SVR1, dans la console certsrv - [Autorité de certification (Local)], développez **Adatum-IssuingCA**, cliquez avec le bouton droit sur **Modèles de certificats**, puis sélectionnez **Gérer**.
2. Dans la Console des modèles de certificat, localisez le modèle **Serveur Web** dans la liste, cliquez dessus avec le bouton droit, puis sélectionnez **Dupliquer le modèle**.
3. Cliquez sur l'onglet **Général**.
4. Dans le champ **Nom complet du modèle**, tapez **Serveur Web d'Adatum** et définissez la **Période de validité** sur **3 années**
5. Cliquez sur l'onglet **Traitement de la demande**, sélectionnez **Autoriser l'exportation de la clé privée** et cliquez sur **OK**.
6. Fermez la Console des modèles de certificat.

▶ Tâche 3 : Configurer le modèle de certificat DirectAccess

1. Sur LON-SVR1, dans la console certsrv - [Autorité de certification (Local)], développez **Adatum-IssuingCA**, cliquez avec le bouton droit sur **Modèles de certificats**, puis sélectionnez **Gérer**.
2. Dans la console Modèles de certificat, localisez le modèle **Ordinateur** dans la liste, cliquez dessus avec le bouton droit, puis sélectionnez **Dupliquer le modèle**.
3. Cliquez sur l'onglet **Général**.
4. Dans le champ **Nom complet du modèle**, tapez **Clients DirectAccess** et définissez la **Période de validité** à **6 mois**.
5. Cliquez sur l'onglet **Sécurité**.
6. Cliquez sur **Ajouter**.
7. Dans la fenêtre Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes, tapez **Portables**, puis cliquez sur **Vérifier les noms**.
8. Cliquez sur **OK**.
9. Sélectionnez le groupe d'utilisateurs **Portables**, puis dans le volet inférieur, sélectionnez les options **Autoriser** pour **Lecture, Inscrire** et **Inscription automatique**.
10. Cliquez sur **OK**.

▶ Tâche 4 : Configurer le certificat pour les cartes à puces

1. Dans la Console des modèles de certificats, cliquez avec le bouton droit sur le modèle Certificat **Utilisateur**, puis cliquez sur **Dupliquer le modèle**.
2. Dans la boîte de dialogue **Propriétés du nouveau modèle**, cliquez sur l'onglet **Général**, puis dans la zone de texte **Nom complet du modèle**, tapez **Utilisateur de carte à puce Adatum**.
3. Sous l'onglet **Nom du sujet**, désactivez les cases à cocher **Inclure le nom de compte de messagerie dans le nom du sujet** et **Nom de messagerie électronique**.
4. Sous l'onglet **Extensions**, cliquez sur **Stratégies d'application**, puis sur **Modifier**.
5. Dans la boîte de dialogue **Modifier l'extension des stratégies d'application**, cliquez sur **Ajouter**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans la boîte de dialogue **Ajouter une stratégie d'application**, sélectionnez **Ouverture de session par carte à puce**, puis cliquez sur **OK** à deux reprises.
7. Cliquez sur l'onglet **Modèles obsolètes**, puis sur **Ajouter**.
8. Cliquez sur le modèle **Utilisateur**, puis sur **OK**.
9. Cliquez sur l'onglet **Sécurité**.
10. Cliquez sur **Ajouter**.
11. Dans la fenêtre Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes, tapez **Managers**, puis cliquez sur **Vérifier les noms**.
12. Cliquez sur **OK**.
13. Sélectionnez le groupe d'utilisateurs **Managers**, puis dans le volet inférieur, sélectionnez les options **Autoriser** pour **Lecture, Inscrire** et **Inscription automatique**.
14. Cliquez sur **OK**.
15. Fermez la Console des modèles de certificat.

▶ Tâche 5 : Émettre les modèles de certificats

1. Sur LON-SVR1, dans la console certsrv - [Autorité de certification (Local)], cliquez avec le bouton droit sur **Modèles de certificats**, pointez sur **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
2. Dans la fenêtre Activer les modèles de certificat, sélectionnez **Utilisateur de carte à puce Adatum**, **Clients DirectAccess** et **Serveur Web d'Adatum**, puis cliquez sur **OK**.

Résultats : À la fin de cet exercice, les stagiaires auront configuré des modèles de certificats répondant aux exigences de sécurité.

Exercice 4 : Implémentation de la révocation et de la distribution de certificats

▶ Tâche 1 : Configurer le contrôle de la révocation de certificats

1. Sur LON-SVR1, ouvrez le **Gestionnaire de serveur**.
2. Dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Cliquez sur **Suivant** à trois reprises.
4. Dans la page **Sélectionner des rôles de serveurs**, développez **Services de certificats Active Directory (Installé)**, puis sélectionnez **Répondeur en ligne**.
5. Cliquez sur **Ajouter des fonctionnalités**.
6. Cliquez sur **Suivant** à deux reprises, puis cliquez sur **Installer**.
7. Lorsque le message affiche que l'installation a réussi, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.
8. Dans l'Assistant Configuration des services de certificats Active Directory, cliquez sur **Suivant**.
9. Sélectionnez **Répondeur en ligne**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Cliquez sur **Configurer**, puis cliquez à deux reprises sur **Fermer**.
11. Sur **LON-SVR1**, ouvrez la console certsrv - [Autorité de certification (Local)].
12. Dans la console certsrv - [Autorité de certification (Local)], cliquez avec le bouton droit sur **Adatum-IssuingCA**, puis cliquez sur **Propriétés**.
13. Dans la boîte de dialogue **Propriétés de : Adatum-IssuingCA**, sous l'onglet **Extensions**, dans la liste **Sélectionner l'extension**, cliquez sur **Accès aux informations de l'autorité (AIA**), puis sur **Ajouter**.
14. Dans la boîte de dialogue **Ajouter un emplacement**, tapez **http://LON-SVR1/ocsp**, puis cliquez sur **OK**.
15. Activez la case à cocher **Inclure dans l'extension AIA des certificats émis**.
16. Activez la case à cocher **Inclure dans l'extension OCSP (Online Certificate Status Protocol)**, puis cliquez sur **OK**.
17. Dans la boîte de dialogue **Autorité de certification**, redémarrez AD CS en cliquant sur **Oui**.
18. Dans la console certsrv, développez **Adatum-IssuingCA**, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
19. Dans la **Console des modèles de certificats**, double-cliquez sur le modèle **Signature de réponse OCSP**.
20. Dans la boîte de dialogue **Propriétés de : Signature de réponse OCSP**, cliquez sur l'onglet **Sécurité**, et sous **Autorisations pour Utilisateurs authentifiés**, activez la case à cocher **Inscrire** puis cliquez sur **OK**.
21. Fermez la Console des modèles de certificat.
22. Dans la console certsrv - [Autorité de certification (Local)], cliquez avec le bouton droit sur le dossier **Modèles de certificats**, pointez sur **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
23. Dans la boîte de dialogue **Activer les modèles de certificat**, sélectionnez le modèle **Signature de réponse OCSP**, puis cliquez sur **OK**.
24. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des répondeurs en ligne**.
25. Dans la console ocsp - [Répondeur en ligne : LON-SVR1.Adatum.com], cliquez avec le bouton droit sur **Configuration de révocation**, puis cliquez sur **Ajouter une configuration de révocation**.
26. Dans l'Assistant Ajouter une configuration de révocation, cliquez sur **Suivant**.
27. Dans la page **Nom de la configuration de révocation**, dans la zone **Nom**, tapez **Répondeur en ligne AdatumCA**, puis cliquez sur **Suivant**.
28. Dans la page **Sélectionner un emplacement de certificat d'autorité de certification**, cliquez sur **Suivant**.
29. Dans la page **Choisir un certificat d'autorité de certification**, cliquez sur **Parcourir**, sur le certificat **Adatum-IssuingCA**, sur **OK**, puis sur **Suivant**.
30. Dans la page **Sélectionner le certificat utilisé pour la signature**, vérifiez que les options **Sélectionner automatiquement un certificat de signature** et **Inscription automatique pour un certificat de signature OCSP** sont sélectionnées, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

31. Dans la page **Fournisseur de révocation**, cliquez sur **Terminer**. L'État de configuration de révocation est **En cours de calcul**.
32. Fermez la console ocsp - [Répondeur en ligne : LON-SVR1.Adatum.com].

▶ Tâche 2 : Configurer la vérification de la révocation des certificats pour les clients DirectAccess

1. Sur LON-SVR1, dans la console Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Autorité de certification**.
2. Dans la console certsrv - [Autorité de certification (Local)], cliquez avec le bouton droit sur **Adatum-IssuingCA**, puis cliquez sur **Propriétés**.
3. Dans la fenêtre Propriétés de : Adatum-IssuingCA, cliquez sur l'onglet **Extensions**.
4. Sous l'onglet **Extensions**, dans la liste déroulante **Sélectionner l'extension**, sélectionnez **Points de distribution de liste de révocation des certificats (CDP)**, puis cliquez sur le bouton **Ajouter**.
5. Dans la zone de texte **Emplacement**, tapez **http://www.adatum.com/CertData/**_, et dans la zone de liste déroulante **Variable**, cliquez sur **<NomAutoritéCertification>**, puis sur **Insérer**.
6. Dans la zone de liste déroulante **Variable**, cliquez sur **<SuffixeNomListeRévocationCertificats>**, puis sur **Insérer**. Dans la zone de liste déroulante **Variable**, cliquez sur **<ListeRévocationCertificatsDeltaAutorisée>**, puis sur **Insérer**.
7. Dans la zone de texte **Emplacement**, placez le curseur à la fin de l'URL, tapez **.crl** et cliquez sur **OK**.
8. Activez les options **Inclure dans l'extension CDP des certificats émis** et **Inclure dans les listes de révocation des certificats afin de pouvoir rechercher les listes de révocation des certificats delta**, puis cliquez sur **Appliquer**. Dans la fenêtre contextuelle Autorité de certification, cliquez sur **Non**.
9. Dans la zone de liste déroulante **Sélectionner l'extension**, cliquez sur **Accès aux informations de l'autorité (AIA)**, puis cliquez sur **Ajouter**.
10. Dans la zone de texte **Emplacement**, tapez **http://www.adatum.com/CertData/**, et dans la zone déroulante **Variable**, cliquez sur **<Nom du serveur DNS>**, puis sur **Insérer**.
11. Dans la zone de texte **Emplacement**, tapez un caractère de soulignement (_), puis dans la zone de liste déroulante **Variable**, cliquez sur **<NomAutoritéCertification>**, puis sur **Insérer**.
12. Dans la zone de liste déroulante Variable, cliquez sur **<NomCertificat>**, puis sur **Insérer**.
13. Dans la zone de texte **Emplacement**, placez le curseur à la fin de l'URL, tapez **.crt**, puis cliquez sur **OK**.
14. Activez la case à cocher **Inclure dans l'extension AIA des certificats émis**, puis cliquez sur **OK**.
15. Cliquez sur **Oui** pour redémarrer le service d'autorité de certification.

▶ Tâche 3 : Configurer l'inscription automatique pour les certificats DirectAccess

1. Sur LON-DC1, dans **Gestionnaire de serveur**, ouvrez **Outils**, puis sélectionnez **Gestion des stratégies de groupe**.
2. Dans la console Gestion de stratégie de groupe, développez **Forêt : Adatum.com**, développez successivement **Domaines** et **Adatum.com**, cliquez avec le bouton droit sur l'unité d'organisation **Portables** et activez l'option **Créer un objet GPO dans ce domaine et le lier ici**.
3. Dans la fenêtre Nouvel objet GPO, dans la zone **Nom**, tapez **DirectAccessCert**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Cliquez sur l'unité d'organisation **Portables**, et dans le volet de droite, cliquez avec le bouton droit sur **DirectAccessCert** et sélectionnez **Modifier**
5. Dans l'**Éditeur de gestion des stratégies de groupe**, sous le nœud **Configuration ordinateur**, développez successivement **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, puis cliquez sur **Stratégies de clé publique**.
6. Dans le volet de droite, double-cliquez sur **Client des services de certificats – Inscription automatique**.
7. Dans la fenêtre Propriétés de : Client des services de certificats – Inscription automatique, dans la zone déroulante **Modèle de Configuration**, sélectionnez **Activé**.
8. Activez les cases à cocher en regard de **Renouveler les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués**, et en regard de **Mettre à jour les certificats qui utilisent les modèles de certificats**, puis cliquez sur **OK.**
9. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 4 : Valider les méthodes d'inscription des certificats

1. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur **LON-CL1**, ouvre l'invite de commandes.
3. Tapez **gpupdate /force**, puis appuyez sur Entrée.
4. Tapez **mmc.exe**, puis appuyez sur Entrée.
5. Dans la fenêtre Console1, cliquez sur **Fichier** et sélectionnez **Ajouter/Supprimer un composant logiciel enfichable**. Dans la console Ajouter ou supprimer des composants logiciels enfichables, sélectionnez **Certificats**, puis cliquez sur **Ajouter**.
6. Dans le composant logiciel enfichable **Certificats**, sélectionnez **Un compte d'ordinateur**. Cliquez sur **Suivant**, puis sur **Terminer**. Cliquez sur **OK**.
7. Dans la fenêtre Console1, développez **Certificats (ordinateur local)**, développez **Personnel**, puis cliquez sur **Certificats**.
8. Vérifiez que le certificat est publié sur LON-CL1.Adatum.com.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-CA1** et **22414B-LON-CL1**.

Résultats : Après avoir terminé cet exercice, les stagiaires auront configuré la révocation et la révocation des certificats.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 12 : Planification et implémentation d'une infrastructure de fédération d'identités

Atelier pratique : Planification et implémentation d'une infrastructure AD FS

Exercice 1 : Conception du déploiement AD FS

▶ Tâche 1 : Choisir le scénario de déploiement AD FS approprié

Selon les exigences identifiées, déterminez si un déploiement par authentification unique Web ou par authentification unique Web fédérée est requis pour qu'A. Datum conclut un partenariat avec Trey Research.

- La société A. Datum fournira initialement la fonctionnalité d'authentification unique pour les utilisateurs internes, mais créera ensuite un partenariat avec Trey Research et d'autres sociétés et clients. Par conséquent, vous déploierez une authentification unique Web fédérée.

▶ Tâche 2 : Identifier le nombre de serveurs Active Directory® Federation Services (AD FS) requis pour le déploiement, ainsi que le rôle et l'emplacement de chacun des serveurs de fédération que vous déploierez.

1. Pour le déploiement des services AD FS dans A. Datum et Trey Research, identifiez le nombre de serveurs AD FS requis pour le déploiement dans les deux sociétés.
    - Puisqu'il s'agira d'un déploiement par authentification unique Web fédérée, vous aurez besoin de deux serveurs pour ce déploiement.
2. Pour les serveurs AD FS identifiés dans l'étape 1, déterminez le rôle et l'emplacement de chacun des serveurs de fédération que vous déploierez.
    - A. Datum hébergera un serveur de fédération de ressources, tandis qu'un serveur de fédération de comptes sera présent à Trey Research.

Remarque : Trey Research n'héberge pas d'applications, par conséquent son serveur AD FS est toujours un serveur de fédération de comptes. Toutefois, notez que le serveur AD FS d'A. Datum est un serveur de fédération de ressources du point de vue de l'authentification unique Web fédérée. Mais vous pouvez également le considérer comme un serveur de fédération de comptes lorsque vous fournissez la fonctionnalité d'authentification unique aux utilisateurs d'A. Datum.

Résultats : Dans cet exercice, vous devez avoir identifié le scénario de déploiement AD FS approprié à utiliser pour répondre aux exigences définies. Vous devez également avoir identifié le nombre de serveurs AD FS requis pour le déploiement, leur emplacement et le rôle de chacun d'eux dans le déploiement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Configuration des composants prérequis pour AD FS

▶ Tâche 1 : Configurer les redirecteurs DNS (Domain Name System)

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Développez **LON-DC1**, puis cliquez sur **Redirecteurs conditionnels**.
3. Cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez sur **Nouveau redirecteur conditionnel**.
4. Dans la boîte de dialogue **Domaine DNS**, tapez **TreyResearch.net**.
5. Cliquez dans la colonne **Adresse IP**, puis tapez **172.16.10.10**. Appuyez sur Entrée, puis cliquez sur **OK**.
6. Fermez le Gestionnaire DNS.
7. Sur **PRS-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
8. Développez **PRS-DC1**, puis cliquez sur **Redirecteurs conditionnels**.
9. Cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez sur **Nouveau redirecteur conditionnel**.
10. Dans la zone **Domaine DNS**, tapez **Adatum.com**.
11. Cliquez dans la colonne **Adresse IP**, puis tapez **172.16.0.10**. Appuyez sur Entrée, puis cliquez sur **OK**.
12. Fermez le Gestionnaire DNS.

▶ Tâche 2 : Échanger les certificats racines pour activer des approbations de certificat

1. Sur LON-DC1, cliquez sur la page **Accueil**.
2. Dans la page **Accueil**, tapez **\\PRS-DC1.treyresearch.net\certenroll**, puis appuyez sur Entrée.
3. Dans la fenêtre certenroll, cliquez avec le bouton droit sur le fichier **PRS-DC1.TreyResearch.net_TreyResearch-PRS-DC1-CA.crt**, puis cliquez sur **Copier**.
4. Dans le volet gauche, cliquez sur **Documents**, puis collez le fichier dans le dossier **Documents**.
5. Sur l'**écran d'accueil** de Windows Server 2012, tapez **MMC.exe**, puis appuyez sur Entrée.
6. Dans la fenêtre Console1, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
7. Cliquez sur **Éditeur de gestion des stratégies de groupe**, puis sur **Ajouter**.
8. Dans **Objet de stratégie de groupe**, cliquez sur **Parcourir**.
9. Cliquez sur **Default Domain Policy**, puis sur **OK**.
10. Cliquez sur **Terminer**, puis sur **OK**.
11. Double-cliquez sur **Stratégie Default Domain Policy [LON-DC1.Adatum.com]**. Dans l'arborescence de la console, développez **Configuration ordinateur** > **Stratégies** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies de clé publique** > **Autorités de certification racines de confiance**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

12. Cliquez avec le bouton droit sur **Autorités de certification racines de confiance**, puis cliquez sur **Importer**.
13. Dans la page **Bienvenue dans l'Assistant Importation du certificat**, cliquez sur **Suivant**.
14. Dans la page **Fichier à importer**, cliquez sur **Parcourir**.
15. Dans la fenêtre Ouvrir, cliquez sur **PRS-DC1.TreyResearch.net_TreyResearch-PRS-DC1-CA.crt**, cliquez sur **Ouvrir**, puis sur **Suivant**.
16. Dans la page **Magasin de certificats**, vérifiez que **Placer tous les certificats dans le magasin suivant** est sélectionné, vérifiez que le magasin **Autorités de certification racines de confiance** est répertorié, puis cliquez sur **Suivant**.
17. Dans la page **Fin de l'Assistant Importation du certificat**, cliquez sur **Terminer** puis, quand l'invite de l'Assistant Importation du certificat s'affiche, cliquez sur **OK**.
18. Fermez l'Éditeur de gestion des stratégies de groupe sans enregistrer les modifications.
19. Sur PRS-DC1, cliquez sur la page **Accueil**.
20. Dans la page **Accueil**, tapez **\\LON-DC1.adatum.com\certenroll**, puis appuyez sur Entrée.
21. Dans la fenêtre certenroll, cliquez avec le bouton droit sur le fichier **LON-DC1.Adatum.com_Adatum-LON-DC1-CA.crt**, puis cliquez sur **Copier**.
22. Dans le volet gauche, cliquez sur **Documents**, puis collez le fichier dans le dossier **Documents**.
23. Ouvrez une invite de commandes Windows PowerShell, tapez **MMC**, puis appuyez sur Entrée.
24. Dans la fenêtre Console1, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
25. Cliquez sur **Certificats**, puis sur **Ajouter**.
26. Cliquez sur **Un compte d'ordinateur**, puis sur **Suivant**..
27. Vérifiez que l'ordinateur local (l'ordinateur sur lequel cette console s'exécute) est sélectionné, cliquez sur **Terminer**, puis sur **OK**.
28. Développez **Certificats**, puis cliquez sur **Autorités de certification racines de confiance**.
29. Cliquez avec le bouton droit sur **Autorités de certification racines de confiance**, pointez sur **Toutes les tâches**, puis cliquez sur **Importer**.
30. Dans la page **Bienvenue dans l'Assistant Importation du certificat**, cliquez sur **Suivant**.
31. Dans la page **Fichier à importer**, cliquez sur **Parcourir**.
32. Dans la fenêtre Ouvrir, cliquez sur **LON-DC1.Adatum.com_Adatum-LON-DC1-CA.crt**, cliquez sur **Ouvrir**, puis sur **Suivant**.
33. Dans la page **Magasin de certificats**, vérifiez que **Placer tous les certificats dans le magasin suivant** est sélectionné, vérifiez que le magasin **Autorités de certification racines de confiance** est répertorié, puis cliquez sur **Suivant**.
34. Dans la page **Fin de l'Assistant Importation du certificat**, cliquez sur **Terminer** puis, quand l'invite de l'Assistant Importation du certificat s'affiche, cliquez sur **OK**.
35. Fermez Console1 sans enregistrer les modifications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Demander et installer un certificat pour le serveur Web

1. Sur LON-SVR3, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire des services Internet (IIS)**.
2. Dans l'arborescence de la console, cliquez sur **LON-SVR3 (ADATUM\Administrateur)**.
3. Dans le volet central, double-cliquez sur **Certificats de serveur**.
4. Dans le volet Actions, cliquez sur **Créer un certificat de domaine**.
5. Dans la page **Propriétés du nom unique**, tapez les paramètres comme indiqué ci-dessous, puis cliquez sur **Suivant** :
   - Nom commun : **LON-SVR3.adatum.com**
   - Organisation : **A. Datum**
   - Unité d'organisation : **IT**
   - Ville : **London**
   - Département/région : **England**
   - Pays/région : **GB**
6. Dans la page **Autorité de certification en ligne**, dans **Indiquer une autorité de certification en ligne**, cliquez sur **Sélectionner** pour rechercher un serveur d'autorité de certification dans le domaine.
7. Sélectionnez **Adatum-LON-DC1-CA**, puis cliquez sur **OK**.
8. Dans **Nom convivial**, tapez **LON-SVR3.adatum.com**, puis cliquez sur **Terminer**.

▶ Tâche 4 : Lier le certificat à l'application prenant en charge les revendications sur le serveur Web et vérifier l'accès à l'application

1. Sur LON-SVR3, dans le Gestionnaire des services Internet (IIS), développez **Sites**, cliquez sur **Default Domain Policy**, puis dans le volet Actions, cliquez sur **Liaisons**.
2. Dans la boîte de dialogue **Liaisons de sites**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter la liaison de site**, sous **Type**, sélectionnez **https**, et sous **Port**, vérifiez que **443** est sélectionné. Dans la liste déroulante **Certificat SSL**, cliquez sur **LON-SVR3.adatum.com**, puis sur **OK**.
4. Cliquez sur **Fermer**, puis fermez le **Gestionnaire des services Internet (IIS)**.
5. Sur LON-DC1, ouvrez Windows Internet Explorer®.
6. Dans la barre d'adresses, tapez **https://lon-svr3.adatum.com/adatumtestapp**, puis appuyez sur Entrée.
7. Vérifiez que vous pouvez vous connecter au site, mais que vous recevez une erreur d'accès refusé 401. Cela est normal, car vous n'avez pas encore configuré AD FS pour l'authentification.
8. Fermez Internet Explorer.

Résultats : Dans cet exercice, vous devez avoir configuré le transfert DNS pour activer la résolution de noms entre A. Datum et Trey Research. En outre, vous devez avoir échangé des certificats racines entre les deux organisations, et installé et configuré un certificat Web sur le serveur d'applications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Déploiement des services AD FS pour les utilisateurs internes

▶ Tâche 1 : Installer et configurer le rôle de serveur AD FS

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
2. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
3. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services AD FS (Active Directory Federation Services)**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
6. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Dans la page **Services AD FS** (Active Directory Federation Services), cliquez sur **Suivant**.
8. Dans la page **Sélectionner des services de rôle**, cliquez sur **Suivant**.
9. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**, puis patientez jusqu'à la fin de l'installation. Ne fermez pas la fenêtre.
10. Lorsque l'installation est terminée, dans la page **Progression de l'installation**, cliquez sur **Exécuter le composant logiciel enfichable Gestion AD FS**.
11. Dans le volet Vue d'ensemble, cliquez sur le lien **Assistant Configuration du serveur de fédération AD FS**.
12. Dans la page **Bienvenue**, assurez-vous que l'option **Créer un service de fédération** est sélectionnée, puis cliquez sur **Suivant**.
13. Dans la page **Sélectionner un déploiement autonome ou de batterie**, cliquez sur **Serveur de fédération autonome**, puis sur **Suivant**.
14. Dans la page **Spécifier le nom du service de fédération**, vérifiez que le **Certificat SSL** sélectionné est **LON-DC1.Adatum.com**, le **Port** est **443** et que le **Nom du service de fédération** est **LON-DC1.Adatum.com**, puis cliquez sur **Suivant**..
15. Dans la page **Prêt à appliquer les paramètres**, vérifiez que les paramètres de configuration corrects sont répertoriés, puis cliquez sur **Suivant**.
16. Patientez jusqu'à la fin de la configuration, puis cliquez sur **Fermer**.
17. Sur l'ordinateur virtuel LON-DC1, dans le Gestionnaire de serveur, fermez l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Outils**, puis sur **Windows PowerShell**.
18. À l'invite Windows PowerShell, tapez set-ADFSProperties –AutoCertificateRollover $False, puis appuyez sur Entrée. Cette étape est indispensable afin de pouvoir modifier les certificats qu'utilise AD FS.
19. Fermez la fenêtre Windows PowerShell.
20. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion AD FS**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

21. Dans la console AD FS, dans le volet gauche, développez **Service**, puis cliquez sur **Certificats**.
22. Cliquez avec le bouton droit sur **Certificats**, puis cliquez sur **Ajouter un certificat de signature de jetons**.
23. Dans la boîte de dialogue **Sélectionner un certificat de signature de jetons**, cliquez sur le premier certificat nommé **LON-DC1.Adatum.com**, puis sur **Cliquez ici pour afficher les propriétés du certificat**.
24. Vérifiez que les rôles du certificat incluent **Garantit votre identité auprès d'un ordinateur distant** et **Garantit l'identité d'un ordinateur distant**, puis cliquez sur **OK**.
25. Cliquez sur **OK** pour fermer la boîte de dialogue **Sécurité de Windows**.
26. Quand la boîte de dialogue d'avertissement **Gestion AD FS** s'affiche, cliquez sur **OK**.

 **Remarque :** Vérifiez que le certificat a l'objet **CN=LON-DC1.Adatum.com**. Si aucun nom ne s'affiche sous **Objet** lorsque vous ajoutez le certificat, supprimez le certificat et ajoutez le certificat suivant dans la liste.

27. Sous **Signature de jetons**, cliquez avec le bouton droit sur le certificat ajouté récemment, puis cliquez sur **Définir en tant que certificat principal**. Lisez le message d'avertissement, puis cliquez sur **Oui**.
28. Sélectionnez le certificat qui vient d'être remplacé, cliquez avec le bouton droit sur le certificat, puis cliquez sur **Supprimer**. Cliquez sur **Oui** pour confirmer la suppression.

▶ Tâche 2 : Configurer l'approbation de fournisseur de revendications

1. Sur **LON-DC1**, dans la console AD FS, développez **Relations d'approbation**, puis cliquez sur **Approbations de fournisseur de revendications**.
2. Dans le volet central, cliquez avec le bouton droit sur **Active Directory**, puis cliquez sur **Modifier les règles de revendication**.
3. Dans la fenêtre Modifier les règles de revendication pour Active Directory, sur l'onglet **Règles de transformation d'acceptation**, cliquez sur **Ajouter une règle**.
4. Dans l'Assistant Ajout de règle de revendication de transformation, dans la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Envoyer les attributs LDAP en tant que revendications**, puis cliquez sur **Suivant**.
5. Dans la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, tapez **Règle d'attributs LDAP sortants**.
6. Dans la liste déroulante **Magasin d'attributs**, sélectionnez **Active Directory**.
7. Dans la section **Mappage des attributs LDAP aux types de revendications sortantes**, sélectionnez les valeurs suivantes pour l'Attribut LDAP et le Type de revendication sortante :
   - E-mail-Addresses = **Adresse de messagerie**
   - User-Principal-Name = **UPN**
   - Display-Name = **Nom (Sélectionnez la première occurrence de la liste)**
8. Cliquez sur **Terminer**, puis sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer l'application WIF pour approuver le déploiement AD FS

1. Sur **LON-SVR3**, cliquez sur l'**écran d'accueil**, puis sur **Windows Identity Foundation Federation Utility**.
2. Dans la page **Welcome to the Federation Utility Wizard** (Bienvenue dans l'Assistant Utilitaire de fédération), dans **Application configuration location** (Emplacement de configuration de l'application), tapez **C:\inetpub\wwwroot\AdatumTestApp\web.config** pour l'emplacement du fichier web.config de l'exemple d'application Windows Identity Foundation (WIF).
3. Dans **Application URI** (URI d'application), tapez **https://lon-svr3.adatum.com/AdatumTestApp/** pour indiquer le chemin d'accès à l'exemple d'application qui approuvera les revendications entrantes du serveur de fédération. Cliquez sur **Next** (Suivant) pour continuer.
4. Dans la page **Security Token Service** (Service d'émission de jeton de sécurité), sélectionnez **Use an existing STS** (Utiliser un STS existant), tapez **https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml** pour l'emplacement du document STS WS-Federation metadata, puis cliquez sur **Next** (Suivant) pour continuer..
5. Dans la page **Security token encryption** (Chiffrement de jeton de sécurité), sélectionnez **No encryption** (Aucun chiffrement), puis cliquez sur **Next** (Suivant).
6. Dans la page **Offered claims** (Revendications offertes), vérifiez les revendications qui seront offertes par le serveur de fédération, puis cliquez sur **Next** (Suivant).
7. Dans la page **Summary** (Résumé), vérifiez les modifications que l'Assistant Utilitaire de fédération apportera à l'exemple d'application, faites défiler les éléments pour comprendre ce que fait chaque élément, puis cliquez sur **Finish** (Terminer).
8. Cliquez sur **OK** dans la boîte de dialogue **Success** (Succès).

▶ Tâche 4 : Configurer une approbation de partie de confiance et les règles de revendications

1. Sur **LON-DC1**, dans la console de Gestion AD FS, cliquez sur **AD FS**.
2. Dans le volet central, cliquez sur **Requis : ajouter une partie de confiance approuvée**.
3. Dans l'Assistant Ajout d'approbation de partie de confiance, dans la page **Bienvenue**, cliquez sur **Démarrer**.
4. Dans la page **Sélectionner une source de données**, sélectionnez **Importer les données, publiées en ligne ou sur un réseau local, contenant la partie de confiance**, puis tapez **https://lon-svr3.adatum.com/adatumtestapp**.
5. Cliquez sur **Suivant** pour continuer. Cette action invite l'Assistant à vérifier les métadonnées de l'application que le rôle serveur Web héberge.
6. Dans la page **Entrer le nom complet**, dans la zone **Nom complet**, tapez **Adatum Test App**, puis cliquez sur **Suivant**.
7. Dans la page **Choisir les règles d'autorisation d'émission**, vérifiez que l'option **Autoriser l'accès de tous les utilisateurs à cette partie de confiance** est sélectionnée, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Dans la page **Prêt à ajouter l'approbation**, vérifiez les paramètres d'approbation de partie de confiance, puis cliquez sur **Suivant**.
9. Dans la page **Terminer**, cliquez sur **Fermer**. La fenêtre Modifier les règles de revendication pour Adatum Test App s'ouvre.
10. Dans la boîte de dialogue de propriétés **Modifier les règles de revendication pour Adatum Test App** , sur l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
11. Dans l'Assistant Ajout de règle de revendication de transformation, dans la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**. Cette action passe une revendication entrante à l'utilisateur à l'aide de l'authentification Windows intégrée.
12. Dans la page **Configurer la règle**, dans **Nom de la règle de revendication**, tapez **Passer la règle du nom de compte Windows**. Dans la liste déroulante **Type de revendication entrante**, sélectionnez **Nom de compte Windows**, puis cliquez sur **Terminer**.
13. Cliquez sur **Ajouter une règle**.
14. Dans la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
15. Dans la page **Configurer la règle**, dans **Nom de la règle de revendication**, tapez **Passer la règle d'adresse de messagerie**, dans la liste déroulante **Type de revendication entrante**, sélectionnez **Adresse de messagerie**, puis cliquez sur **Terminer**.
16. Cliquez sur **Ajouter une règle**.
17. Dans la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
18. Dans la page **Configurer la règle**, dans **Nom de la règle de revendication**, tapez **Passer la règle du nom d'utilisateur principal**, dans la liste déroulante **Type de revendication entrante**, sélectionnez **UPN**, puis cliquez sur **Terminer**.
19. Cliquez sur **Ajouter une règle**.
20. Dans la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
21. Dans la page **Configurer la règle**, dans **Nom de la règle de revendication**, tapez **Passer la règle du nom**, dans la liste déroulante **Type de revendication entrante**, sélectionnez **Nom (Sélectionnez la première occurrence de la liste)**, puis cliquez sur **Terminer**.
22. Cliquez sur **Appliquer**, puis sur **OK**.

▶ Tâche 5 : Vérifier l'accès à l'application pour les utilisateurs internes

1. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Brad** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-CL1, cliquez sur le Bureau, puis ouvrez Internet Explorer.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Connectez-vous à **https://lon-svr3.adatum.com/AdatumTestApp/**.

Remarque : Assurez-vous de saisir la barre oblique (/).

4. Si vous êtes invité à indiquer vos informations d'identification, tapez **ADATUM\Brad** et le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée. La page s'affiche et vous voyez les revendications qui ont été traitées pour permettre l'accès au site Web.
5. Fermez Internet Explorer.

Résultats : Dans cet exercice, vous devez avoir installé et configuré le rôle serveur AD FS sur LON-DC1. Vous devez également avoir configuré les approbations de fournisseur de revendications et de partie de confiance, puis avoir configuré les règles de revendication nécessaires. Enfin, vous devez avoir configuré l'application WIF pour approuver le déploiement AD FS, puis avoir vérifié que les utilisateurs internes approuvés peuvent accéder à l'application.

Exercice 4 : Déploiement des services AD FS pour une organisation partenaire

▶ Tâche 1 : Ajouter une approbation de fournisseur de revendications pour le serveur AD FS de TreyResearch.net

1. Sur **LON-DC1**, le cas échéant, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion AD FS**.
2. Dans la console AD FS, développez **Relations d'approbation**, puis cliquez sur **Approbations de fournisseur de revendications**.
3. Dans le volet Actions, cliquez sur **Ajouter une approbation de fournisseur de revendications**.
4. Dans la page **Bienvenue**, cliquez sur **Démarrer**.
5. Dans la page **Sélectionner une source de données**, sélectionnez **Importer les données publiées en ligne ou sur un réseau local concernant le fournisseur de revendications**, tapez **https://prs-dc1.treyresearch.net**, puis cliquez sur **Suivant**.
6. Dans la page **Entrer le nom complet**, cliquez sur **Suivant**.
7. Dans la page **Prêt à ajouter l'approbation**, examinez les paramètres d'approbation de fournisseur de revendications, puis cliquez sur **Suivant** pour sauvegarder la configuration.
8. Dans la page **Terminer**, cliquez sur **Fermer**.
9. Dans la boîte de dialogue de propriétés **Modifier les règles de revendication pour prs-dc1.treyresearch.net**, sur l'onglet **Règles de transformation d'acceptation**, cliquez sur **Ajouter une règle**.
10. Dans la liste **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans la zone de texte **Nom de la règle de revendication**, tapez **Passer la règle du nom de compte Windows**.
12. Dans la liste déroulante **Type de revendication entrante**, sélectionnez **Nom de compte Windows**.
13. Sélectionnez **Passer toutes les valeurs de revendication**, cliquez sur **Terminer**, puis sur **Oui**.
14. Cliquez sur **OK**, puis fermez la console AD FS.
15. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Windows PowerShell**.
16. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
Set-ADFSClaimsProviderTrust –TargetName “prs-dc1.treyresearch.net” –
SigningCertificateRevocationCheck None
```

17. Fermez la fenêtre Windows PowerShell.

▶ Tâche 2 : Configurer une approbation de partie de confiance sur PRS-DC1 pour l'application prenant en charge les revendications A. Datum

1. Sur **PRS-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion AD FS**.
2. Dans la console AD FS, dans la page **Vue d'ensemble**, cliquez sur **Requis : ajouter une partie de confiance approuvée**.
3. Dans la page **Bienvenue**, cliquez sur **Démarrer**.
4. Dans la page **Sélectionner une source de données**, sélectionnez **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confiance**, tapez **https://lon-dc1.adatum.com**, puis cliquez sur **Suivant**.
5. Dans la page **Entrer le nom complet**, dans la zone de texte **Nom complet**, tapez **Adatum TestApp**, puis cliquez sur **Suivant**.
6. Dans la page **Choisir les règles d'autorisation d'émission**, sélectionnez **Autoriser l’accès de tous les utilisateurs à cette partie de confiance**, puis cliquez sur **Suivant**.
7. Dans la page **Prêt à ajouter l'approbation**, examinez les paramètres d'approbation de la partie de confiance, puis cliquez sur **Suivant** pour enregistrer la configuration.
8. Dans la page **Terminer**, cliquez sur **Fermer**. La fenêtre Modifier les règles de revendication pour Adatum TestApp s'ouvre.
9. Dans la fenêtre Modifier les règles de revendication pour Adatum TestApp, sur l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
10. Dans la liste **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
11. Dans la zone **Nom de la règle de revendication**, tapez **Passer la règle du nom de compte Windows** et, dans la liste déroulante **Type de revendication entrante**, sélectionnez **Nom de compte Windows**.
12. Sélectionnez **Passer toutes les valeurs de revendication**, puis cliquez sur **Terminer**.
13. Cliquez sur **OK**, puis fermez la console AD FS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Vérifier l'accès à l'application de test A. Datum pour les utilisateurs de Trey Research

1. Sur PRS-DC1, ouvrez Internet Explorer, puis connectez-vous à **https://lon-svr3.adatum.com/adatumtestapp/**.

Remarque : Le processus de connexion a changé et vous devez désormais sélectionner une autorité qui peut autoriser et valider la demande d'accès. La page de **découverte du domaine d'accueil** (la page **Se connecter**) s'affiche et vous devez sélectionner une autorité.

2. Dans la page **Connexion**, sélectionnez **prs-dc1.treyresearch.com**, puis cliquez sur **Continuer la connexion**.
3. Si vous êtes invité à indiquer vos informations d'identification, tapez **TreyResearch\April** avec le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée. Vous devez pouvoir accéder à l'application.
4. Fermez Internet Explorer.
5. Ouvrez Internet Explorer, puis connectez-vous à nouveau à **https://lon-svr3.adatum.com/adatumtestapp/**.
6. Si vous êtes invité à indiquer vos informations d'identification, tapez **TreyResearch\April** avec le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée. Vous devez pouvoir accéder à l'application.
7. Fermez Internet Explorer.

Remarque : À nouveau, vous n'êtes pas invité à sélectionner un domaine d'accueil. Une fois que les utilisateurs ont sélectionné un domaine d'accueil et ont été authentifiés par une autorité du domaine, le serveur de fédération de la partie de confiance délivre un cookie _LSRealm. La durée de vie par défaut pour le cookie est de 30 jours. Par conséquent, pour vous connecter à plusieurs reprises, vous devez supprimer ce cookie après chaque tentative de connexion pour revenir à un état propre.

▶ Tâche 4 : Configurer les règles de revendication pour que l'approbation de fournisseur de revendications et l'approbation de partie de confiance autorisent l'accès à un seul groupe

1. Sur **PRS-DC1**, ouvrez la console AD FS, développez **Relations d'approbation**, puis cliquez sur **Approbations de partie de confiance**.
2. Sélectionnez **Adatum TestApp** et, dans le volet Actions, cliquez sur **Modifier les règles de revendication**.
3. Dans la fenêtre Modifier les règles de revendication pour Adatum TestApp, sur l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
4. Dans la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Envoyer l'appartenance à un groupe en tant que revendication**, puis cliquez sur **Suivant**.
5. Dans la page **Configurer la règle**, dans le champ **Nom de la règle de revendication**, saisissez **Autoriser la règle du groupe de production**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. En regard de **Groupe d'utilisateurs**, cliquez sur **Parcourir**, tapez **Production**, puis cliquez sur **OK**.
7. Sous **Type de revendication sortante**, cliquez sur **Groupe**.
8. Sous **Valeur de revendication sortante**, tapez **Production**, cliquez sur **Terminer**, puis sur **OK**.
9. Sur **LON-DC1**, si nécessaire, ouvrez la console de gestion AD FS.
10. Dans la console AD FS, développez **Relations d'approbation**, puis cliquez sur **Approbations de fournisseur de revendications**.
11. Sélectionnez **prs-dc1.treyresearch.net** et, dans le volet Actions, cliquez sur **Modifier les règles de revendication**.
12. Sur l'onglet **Règles de transformation d'acceptation**, cliquez sur **Ajouter une règle**.
13. Dans la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
14. Dans la page **Configurer la règle**, dans le champ **Nom de la règle de revendication**, saisissez **Envoyer la règle du groupe de production**.
15. Dans la liste déroulante **Type de revendication entrante**, cliquez sur **Groupe**, puis sur **Terminer**. Cliquez sur **Oui**, puis sur **OK**.
16. Dans la console AD FS, sous **Relations d'approbation**, cliquez sur **Approbations de la partie de confiance**.
17. Sélectionnez **Adatum Test App** et, dans le volet Actions, cliquez sur **Modifier les règles de revendication**.
18. Sur l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
19. Sous **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**, puis sur **Suivant**.
20. Sous **Nom de la règle de revendication**, tapez **Envoyer la règle du nom de groupe TreyResearch**.
21. Dans la liste déroulante **Type de revendication entrante**, cliquez sur **Groupe**, puis sur **Terminer**.
22. Dans la fenêtre **Modifier les règles de revendication pour Adatum Test App**, sur l'onglet **Règles d'autorisation d'émission**, sélectionnez la règle nommée **Autoriser l'accès à tous les utilisateurs**, puis cliquez sur **Supprimer une règle**. Cliquez sur **Oui** pour confirmer. Sans règle, l'accès est refusé aux utilisateurs.
23. Sur l'onglet **Règles d'autorisation d'émission** , cliquez sur **Ajouter une règle**.
24. Dans la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Autoriser ou refuser l'accès des utilisateurs en fonction d'une revendication entrante**, puis cliquez sur **Suivant**.
25. Dans la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, tapez **Autoriser la règle du groupe Production TreyResearch** et, dans la liste déroulante **Type de revendication entrante**, sélectionnez **Groupe**.
26. Dans le champ **Valeur de revendication entrante**, tapez **Production**, sélectionnez l'option **Autoriser l'accès aux utilisateurs avec cette revendication entrante**, puis cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

27. Sur l'onglet **Règles d'autorisation d'émission** , cliquez sur **Ajouter une règle**.
28. Dans la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Autoriser ou refuser l'accès des utilisateurs en fonction d'une revendication entrante**, puis cliquez sur **Suivant**.
29. Dans la page **Configurer la règle**, dans le champ **Nom de la règle de revendication**, tapez **Temp** et, dans la liste déroulante **Type de revendication entrante**, sélectionnez **UPN**.
30. Dans le champ **Valeur de revendication entrante**, tapez **@adatum.com**, sélectionnez l'option **Autoriser l'accès aux utilisateurs avec cette revendication entrante**, puis cliquez sur **Terminer**.
31. Cliquez sur la règle **Temp**, puis sur **Modifier une règle**.
32. Dans la boîte de dialogue **Modifier la règle – Temp**, cliquez sur **Afficher le langage de règle**.
33. Appuyez sur Ctrl + C pour copier le langage des règles dans le presse-papiers, puis cliquez sur **OK**.
34. Cliquez sur **Annuler**.
35. Cliquez sur la règle **Temp**, cliquez sur **Supprimer une règle**, puis sur **Oui**.
36. Sur l'onglet **Règles d'autorisation d'émission**, cliquez sur **Ajouter une règle**.
37. Dans la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Envoyer les revendications en utilisant une règle personnalisée**, puis cliquez sur **Suivant**.
38. Dans la page **Configurer la règle**, dans le champ **Nom de la règle de revendication**, saisissez **Règle d'accès utilisateur ADatum**.
39. Cliquez dans la zone **Règle personnalisée**, puis appuyez sur les touches Ctrl + V pour coller le contenu du presse-papiers dans la zone. Modifiez la première URL afin qu'elle corresponde au texte suivant, puis cliquez sur **Terminer** :

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn", Value =~
"^(?i).+@adatum\.com$"]=> issue(Type =
“http://schemas.microsoft.com/authorization/claims/permit”, Value =
“PermitUsersWithClaim”);
```

Remarque : Cette règle active l'accès à quiconque présente une revendication qui comprend le Nom d'utilisateur principal (UPN) de @adatum.com. La ligne Valeur de la première URL définit l'attribut qui peut être mis en correspondance dans la revendication. Dans cette ligne, ^ indique le début de la chaîne à faire correspondre, (?i) signifie que le texte n'est pas sensible à la casse, .+ signifie qu'un ou plusieurs caractères seront ajoutés et $ signifie la fin de la chaîne.

40. Cliquez sur **OK** pour fermer la page de propriétés et sauvegardez les modifications apportées à l'approbation de partie de confiance.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Vérifier les restrictions et l'accessibilité à l'application prenant en charge les revendications

1. Sur PRS-DC1, ouvrez Internet Explorer, puis connectez-vous à **https://lon-svr3.adatum.com/adatumtestapp/**.
2. Si vous êtes invité à indiquer vos informations d'identification, tapez **TreyResearch\April** avec le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée. April n'est pas membre du groupe Production, elle ne doit donc pas avoir accès à l'application.
3. Fermez Internet Explorer.
4. Rouvrez Internet Explorer, cliquez sur l'icône **Outils** dans le coin supérieur droit, puis sur **Options Internet**.
5. Sous **Historique de navigation**, cliquez sur **Supprimer**, cliquez à nouveau sur **Supprimer**, puis sur **OK**.
6. Connectez-vous à **https://lon-svr3.adatum.com/adatumtestapp/**.
7. Dans la page **Connexion**, cliquez sur **prs-dc1.treyresearch.net**, puis sur **Continuer la connexion**.
8. Si vous êtes invité à indiquer vos informations d'identification, tapez **TreyResearch\Morgan** avec le mot de passe **Pa$$w0rd**, puis appuyez sur Entrée. Morgan est membre du groupe Production et doit pouvoir accéder à l'application.
9. Fermez Internet Explorer.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR3**, **22414B-PRS-DC1** et **22414B-LON-CL1**.

Résultats : Dans cet exercice, vous devez avoir configuré une approbation de fournisseur de revendications pour TreyResearch sur Adatum.com ainsi qu'une approbation de partie de confiance pour Adatum sur TreyResearch. Vous devez également avoir vérifié l'accès à l'application prenant en charge les revendications d'A. Datum, puis avoir configuré l'application pour limiter l'accès à partir de TreyResearch aux groupes spécifiques. Enfin, vous devez avoir vérifié l'accès approprié.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 13 : Planification et implémentation d'une infrastructure de gestion des droits relatifs à l'information (IRM)

Atelier pratique : Planification et implémentation d'une infrastructure AD RMS

Exercice 1 : Planification du déploiement AD RMS

▶ Tâche 1 : Lire la documentation fournie avec le produit

Documentation fournie avec le produit

----- Message d'origine -----
De : Charlotte Weiss [Charlotte@contoso.com]
Envoyé : 03 fév. 2013 08:45
À : Ed@contoso.com
Objet : AD RMS

Ed,

En raison de la nature hautement confidentielle de la recherche que l'équipe Research exécute au sein d'A. Datum, l'équipe en charge de la sécurité chez A. Datum Corporation souhaite implémenter une sécurité supplémentaire pour certains documents créés par le département de recherche. En particulier, l'équipe chargée de la sécurité souhaite s'assurer que les utilisateurs à l'intérieur et en dehors de l'organisation ne puissent pas partager les documents confidentiels avec des utilisateurs non autorisés.

Vous devez organiser et implémenter une solution AD RMS qui fournira le niveau de protection exigé par l'équipe chargée de la sécurité.

Veuillez proposer un plan pour installer AD RMS chez A. Datum et chez Trey Research, et pour intégrer le reste des actions à entreprendre.

Merci !

Charlotte

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié

Répondez aux questions du document Plan IRM A. Datum : AD RMS, proposé ci-après.

Plan IRM A. Datum : AD RMS	
Numéro de référence du document : GW00612	
Auteur du document	Charlotte Weiss
Date	6 février

Présentation des exigences

- Concevez un déploiement AD RMS pour les sociétés A. Datum et Trey Research.
- L'objectif du déploiement AD RMS est de pouvoir protéger les informations, quelle que soit leur destination. Une fois que vous ajoutez la protection AD RMS à un fichier numérique, la protection demeure avec le fichier. Par défaut, seul le propriétaire du contenu peut supprimer la protection du fichier. Le propriétaire accorde aux autres utilisateurs le droit d'exécuter certaines actions sur le contenu, comme afficher, copier ou imprimer le fichier :
- Tous les documents stockés dans le dossier ConfidentialResearch doivent être automatiquement définis comme confidentiels et protégés avec AD RMS.
- Seuls les membres des groupes Research et Managers doivent pouvoir accéder aux documents.
- Configurez l'intégration du déploiement AD RMS au contrôle d'accès dynamique.
- Les employés d'A. Datum doivent pouvoir partager le contenu protégé par AD RMS avec les utilisateurs de Trey Research.
- L'équipe chargée de la sécurité chez A. Datum souhaite vérifier qu'aucun contenu protégé par AD RMS n'est sécurisé de telle façon que personne ne puisse accéder aux informations.

Informations supplémentaires

Nous devons réduire le nombre total de serveurs requis. Envisagez d'utiliser la base de données interne plutôt qu'un déploiement SQL Server complet. Le déploiement AD RMS sur les contrôleurs de domaine existants est autorisé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Plan IRM A. Datum : AD RMS
Propositions **Question** : Combien de clusters AD RMS devons-nous déployer pour répondre aux exigences de sécurité des deux sociétés ? **Réponse** : Cette région compte 300 ordinateurs. Les spécifications stipulent qu'environ 50 ordinateurs doivent être déployés dans chaque sous-réseau. Vous devez aussi planifier une croissance d'environ 25 %. Six sous-réseaux sont requis dans la région pour héberger les ordinateurs, mais vous devez planifier un sous-réseau supplémentaire pour chaque emplacement afin d'anticiper l'hébergement d'un nombre croissant d'ordinateurs. Cela signifie un total de neuf sous-réseaux. **Question** : Quelle solution de base de données devez-vous déployer ? **Réponse** : Les spécifications stipulent que vous devez déployer un maximum de 50 ordinateurs hôtes pour chaque sous-réseau. **Question** : Quels comptes de service, le cas échéant, devez-vous créer ? **Réponse** : Vous n'avez besoin que d'un seul compte qui fera office de compte de service. Nous ne pouvons pas utiliser le compte de l'administrateur, car la configuration de la console AD RMS nécessite un autre compte que celui procédant à l'installation pour activer la base de données. **Question** : Quelles sont nos exigences en termes de certificats SSL ? Comment les satisfaisons-nous dans les deux forêts ? **Réponse** : Nous pouvons utiliser des certificats auto-signés. Nous pouvons placer les certificats dans le magasin des autorités de certification approuvées de chaque ordinateur.

▶ Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique

Examinez le plan AD RMS final du corrigé de l'atelier pratique et soyez prêt à présenter vos solutions.

Corrigé de l'atelier pratique :

1. Un cluster dans la forêt A. Datum et un autre dans la forêt Trey Research
2. La base de données interne Windows, afin de réduire le nombre de serveurs déployés. Cependant, vous ne pourrez pas déployer des serveurs supplémentaires dans chaque cluster.
3. Vous n'avez besoin que d'un seul compte qui fasse office de compte de service. Vous ne pouvez pas utiliser le compte de l'administrateur, car la configuration de la console AD RMS nécessite un autre compte que celui procédant à l'installation pour activer la base de données.
4. Vous pouvez utiliser les certificats auto-signés et les placer dans le magasin des autorités de certification approuvées de chaque ordinateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Déploiement de l'infrastructure AD RMS pour les utilisateurs internes

▶ Tâche 1 : Configurer les conditions préalables AD RMS

Créer et configurer les comptes

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console, développez **Adatum.com**.
3. Sélectionnez **Users** (Utilisateurs), cliquez avec le bouton droit, pointez sur **Nouveau**, puis cliquez sur **Utilisateur**.
4. Dans la boîte de dialogue Nouvel objet – Utilisateur, tapez **ADRMSSRVC** dans les zones **Prénom** et **Nom d'ouverture de session de l'utilisateur**, puis cliquez sur **Suivant**.
5. Dans la boîte de dialogue Nouvel objet – Utilisateur, tapez **Pa$$w0rd** dans les zones **Mot de passe** et **Confirmer le mot de passe**. Désactivez la case à cocher **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**, cliquez sur **Suivant**, puis cliquez sur **Terminer**.
6. Cliquez sur **Utilisateurs**, puis cliquez avec le bouton droit sur **ADRMSSRVC**, puis cliquez sur **Ajouter à un groupe**. Tapez **Admins du domaine**, puis cliquez sur **OK**.
7. Cliquez sur **OK** pour fermer le message.

Pour ajouter des adresses de messagerie aux utilisateurs

1. Cliquez sur **l'unité d'organisation** Research. Recherchez le compte nommé **Hani Loza**, puis double-cliquez dessus.
2. Sous l'onglet **Propriétés**, **Général**, dans le champ **Adresse de messagerie**, tapez hani@adatum.com, puis cliquez sur **OK**.
3. Faites de même pour les comptes ci-après, qui se trouvent dans les UO/conteneurs suivants :

UO/Conteneur	Nom d'utilisateur	Courrier électronique
Development	Toni Poe	toni@adatum.com
Sales	Limor Henig	limor@adatum.com
Marketing	Stuart Glasson	stuart@adatum.com

Pour ajouter de nouveaux groupes à Active Directory

1. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Users** (Utilisateurs), pointez sur **Nouveau**, puis cliquez sur **Groupe**.
2. Dans la boîte de dialogue Nouvel objet – Groupe, tapez **Management** dans **Nom du groupe**, sélectionnez l'option **Universelle** pour **Étendue du groupe**, puis cliquez sur **OK**.
3. Effectuez les étapes ci-dessus 1 et 2 pour un groupe nommé **Employees**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour ajouter les adresses de messagerie aux objets de groupe

1. Dans la console Utilisateurs et ordinateurs Active Directory, sélectionnez l'unité d'organisation **Research**, puis double-cliquez sur le groupe de sécurité **Research** pour ouvrir la boîte de dialogue **Propriétés de : Research**.
2. Sous l'onglet **Général**, tapez **Research@adatum.com** dans la zone **Adresse de messagerie**, puis cliquez sur **OK**.
3. Exécutez les étapes 1 et 2 ci-dessus pour les groupes de sécurité **Management** et **Employees** situés dans le conteneur **Users**. Utilisez le format de messagerie **groupe@adatum.com**.

Pour ajouter des comptes d'utilisateurs aux groupes

1. Dans la console **Utilisateurs et ordinateurs Active Directory**, cliquez sur **Users** (Utilisateurs), puis double-cliquez sur **Employees**.
2. Cliquez sur **Membres**, puis cliquez sur **Ajouter**.
3. Tapez **limor@adatum.com;stuart@adatum.com**, cliquez sur **OK**, puis cliquez sur **OK**.
4. Exécutez les étapes 2 et 3 ci-dessus pour ajouter un membre aux groupes restants, comme suit :
   - Limor Henig : Management
   - Toni Poe : Management
5. Fermez la console Utilisateurs et ordinateurs Active Directory.

Créer les dossiers partagés sur LON-DC1

1. Sur LON-DC1, dans la barre des tâches, ouvrez l'Explorateur de fichiers, puis cliquez avec le bouton droit sur **Disque local (C:)**. Pointez sur **Nouveau**, puis cliquez sur **Dossier**.
2. Tapez **ConfidentialResearch** comme nom de dossier, puis appuyez sur Entrée.
3. Cliquez avec le bouton droit sur **ConfidentialResearch**, pointez sur **Partager avec**, puis cliquez sur **Des personnes spécifiques**. L'Assistant Partage de fichiers s'ouvre.
4. Sous **Choisir les utilisateurs pouvant accéder à votre dossier partagé**, tapez **Research**, puis cliquez sur **Ajouter**. Tapez **Management**, puis cliquez sur **Ajouter**.
5. Dans la liste, cliquez sur la flèche **Niveau d'autorisation** du groupe **Research**, puis sélectionnez **Lecture/écriture**. Répétez l'opération pour **Management**.
6. Cliquez sur **Partager**, puis sur **Terminé**.

Créer un partage sur LON-DC1 pour stocker les modèles AD RMS

1. Dans l'Explorateur de fichiers, cliquez avec le bouton droit sur **Disque local (C:)**.
2. Pointez sur **Nouveau**, puis cliquez sur **Dossier**.
3. Tapez **Public** comme nom de dossier, puis appuyez sur ENTRÉE.
4. Cliquez avec le bouton droit sur **Public**, pointez sur **Partager avec**, puis cliquez sur **Des personnes spécifiques**. L'Assistant Partage de fichiers s'ouvre.
5. Sous **Choisir les utilisateurs pouvant accéder à votre dossier partagé**, cliquez sur la flèche, sélectionnez **Tout le monde**, puis cliquez sur **Ajouter**.

6. Dans la liste, cliquez sur la flèche **Niveau d'autorisation** du groupe **Tout le monde**, puis confirmez la sélection de **Lecture**.
7. Cliquez sur **Partager**, puis sur **Terminé**.
8. Fermez l'Explorateur de fichiers.

▶ Tâche 2 : Déployer le premier serveur du cluster AD RMS

Déployer le cluster AD RMS dans Adatum.com

1. Sur LON-DC1, dans la console Tableau de bord du Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Cliquez sur **Suivant** à trois reprises pour accéder à la page **Sélectionner des rôles de serveurs**.
3. Dans la page **Sélectionner des rôles de serveurs**, sélectionnez **Services AD RMS (Active Directory Rights Management Services)**. Lorsque vous êtes invité à ajouter des fonctionnalités, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
4. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
5. Dans **Services AD RMS (Active Directory Rights Management Services)**, cliquez sur **Suivant**.
6. Dans **Sélectionner des services de rôle**, vérifiez que **Active Directory Rights Management Server** est sélectionné, puis cliquez sur **Suivant**.
7. Cliquez sur **Installer** pour ajouter le rôle. Patientez jusqu'à la fin de l'installation, puis cliquez sur **Fermer**.

Pour configurer un nouveau cluster racine AD RMS

1. Dans le Gestionnaire de serveur, cliquez sur l'icône **Notifications**.
2. Pour l'événement de tâche étiqueté **Configuration requise pour : Services AD RMS (Active Directory Rights Management Services) à LON-DC1**, cliquez sur **Effectuer une configuration supplémentaire**. L'Assistant Configuration AD RMS : LON-DC1.Adatum.com s'ouvre.
3. Dans l'Assistant Configuration AD RMS : LON-DC1.Adatum.com, dans la page **Services AD RMS (Active Directory Rights Management Services)**, cliquez sur **Suivant**.
4. Dans la page **Créer ou joindre un cluster AD RMS**, acceptez la sélection par défaut (**Créer un nouveau cluster racine AD RMS**) puis cliquez sur **Suivant**.
5. Dans la page **Sélectionner un serveur de base de données de configuration**, activez la case d'option **Utiliser la base de données interne de Windows sur ce serveur**, puis cliquez sur **Suivant**.
6. Dans Spécifier un compte de service, cliquez sur **Spécifier**, et, dans la boîte de dialogue Sécurité de Windows, tapez **ADRMSSRVC** et le mot de passe (**Pa$$w0rd**), puis cliquez sur **OK**.
7. Vérifiez que le **Compte d'utilisateur de domaine** a la valeur **ADATUM\ADRMSSRVC**, puis cliquez sur **Suivant**.
8. Pour Mode de chiffrement, acceptez la valeur par défaut (**Mode de chiffrement 2 (clés RSA 2048 bits/hachages SHA-256)**), puis cliquez sur **Suivant**.
9. Pour **Stockage de clé de cluster**, acceptez la valeur par défaut (**Utiliser le stockage de clé AD RMS géré de manière centralisée**), puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Pour **Mot de passe de clé de cluster**, tapez et confirmez (**Pa$$w0rd**), puis cliquez sur **Suivant**.
11. Pour **Site Web de cluster**, acceptez la valeur par défaut (**Default Web Site** (Site Web par défaut)), puis cliquez sur **Suivant**.
12. Pour **Adresse du cluster**, sélectionnez **Utiliser une connexion non chiffrée (http://)**), pour **Nom de domaine complet**, tapez **LON-DC1.adatum.com** (veillez à utiliser le domaine complet, pas seulement LON-DC1), puis cliquez sur **Suivant**.
13. Pour **Certificat de licence**, acceptez le nom par défaut (**LON-DC1** n'a pas besoin d'être le nom de domaine complet), puis cliquez sur **Suivant**.
14. Pour **Inscription du SCP**, acceptez la valeur par défaut (**Enregistrer le point de connexion de service maintenant**), puis cliquez sur **Suivant**.
15. Pour **Confirmation**, vérifiez vos choix d'installation, puis cliquez sur **Installer**. Cliquez sur **Fermer**.
16. Déconnectez-vous de LON-DC1, puis connectez-vous de nouveau en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd** pour mettre le jeton à jour de sécurité du compte d'utilisateur connecté.
17. Votre cluster racine AD RMS est désormais installé et configuré.

Pour ouvrir la console Services AD RMS (Active Directory Rights Management Services)

1. Dans le Gestionnaire de serveur sur LON-DC1, cliquez sur **Outils**, puis sur **Services AD RMS (Active Directory Rights Management Services)**. Vérifiez que la console s'ouvre sans aucune erreur.
2. Fermez la console Services AD RMS (Active Directory Rights Management Services).

▶ Tâche 3 : Déployer le cluster AD RMS dans la forêt Trey Research

Ajouter le compte ADRMSSRVC à PRS-DC1

1. Connectez-vous à **PRS-DC1** en tant que **TREYRESEARCH\Administrateur** à l'aide du mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
3. Dans l'arborescence de la console, développez **TreyResearch.net**. Sélectionnez **Users** (Utilisateurs), cliquez avec le bouton droit, pointez sur **Nouveau**, puis cliquez sur **Utilisateur**.
4. Dans la boîte de dialogue **Nouvel objet – Utilisateur**, tapez **ADRMSSRVC** dans les zones **Prénom** et **Nom d'ouverture de session de l'utilisateur**, puis cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Nouvel objet – Utilisateur**, tapez **Pa$$w0rd** dans les zones **Mot de passe** et **Confirmer le mot de passe**. Désactivez la case à cocher **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**, cliquez sur **Suivant**, puis cliquez sur **Terminer**.
6. Double-cliquez sur **Admins du domaine**.
7. Cliquez sur **Membres**, puis cliquez sur **Ajouter**.
8. Tapez **adrmssrvc**, cliquez sur **OK**, puis sur **OK**.
9. Fermez la console Utilisateurs et ordinateurs Active Directory.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour ajouter le rôle serveur AD RMS

1. Sur PRS-DC1, dans la console Tableau de bord du Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Cliquez sur **Suivant** à trois reprises pour accéder à la page **Sélectionner des rôles de serveurs**.
3. Dans la page **Sélectionner des rôles de serveurs**, sélectionnez **Services AD RMS (Active Directory Rights Management Services)**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
4. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
5. Dans **Services AD RMS (Active Directory Rights Management Services)**, cliquez sur **Suivant**.
6. Dans **Sélectionner des services de rôle**, vérifiez que **Active Directory Rights Management Server** est sélectionné, puis cliquez sur **Suivant**.
7. Cliquez sur **Installer** pour ajouter le rôle, puis cliquez sur **Fermer**.
8. Dans le Gestionnaire de serveur, cliquez sur le bouton **Notifications**, puis sur **Effectuer une configuration supplémentaire**.
9. Dans la fenêtre de configuration, dans la page **Services AD RMS (Active Directory Rights Management Services)**, cliquez sur **Suivant**.
10. Dans la page **Créer ou joindre un cluster AD RMS**, acceptez la sélection par défaut (**Créer un nouveau cluster racine AD RMS**) puis cliquez sur **Suivant**.
11. Dans la page **Sélectionner un serveur de base de données de configuration**, activez la case d'option **Utiliser la base de données interne de Windows sur ce serveur**, puis cliquez sur **Suivant**.
12. Dans Spécifier un compte de service, cliquez sur **Spécifier** et, dans la boîte de dialogue **Sécurité de Windows**, tapez **ADRMSSRVC** et le mot de passe (**Pa$$w0rd**), puis cliquez sur **OK**.
13. Vérifiez que le **Compte d'utilisateur de domaine** a la valeur **TREYRESEARCH\ADRMSSRVC**, puis cliquez sur **Suivant**.
14. Pour **Mode de chiffrement**, acceptez la valeur par défaut (**Mode de chiffrement 2 (clés RSA 2048 bits/hachages SHA-256)**), puis cliquez sur **Suivant**.
15. Pour **Stockage de clé de cluster**, acceptez la valeur par défaut (**Utiliser le stockage de clé AD RMS géré de manière centralisée**), puis cliquez sur **Suivant**.
16. Pour **Mot de passe de clé de cluster**, tapez et confirmez (**Pa$$w0rd**), puis cliquez sur **Suivant**.
17. Pour **Site Web de cluster**, acceptez la valeur par défaut (**Default Web Site** (Site Web par défaut)), puis cliquez sur **Suivant**.
18. Pour **Adresse du cluster**, sélectionnez **Utiliser une connexion non chiffrée (http://)**), pour **Nom de domaine complet**. Tapez **PRS-DC1.TreyResearch.net**, puis cliquez sur **Suivant**.
19. Pour **Certificat de licence**, acceptez le nom par défaut (**PRS-DC1** n'a pas besoin d'être le nom de domaine complet), puis cliquez sur **Suivant**.
20. Pour **Inscription du SCP**, acceptez la valeur par défaut (**Enregistrer le point de connexion de service maintenant**), puis cliquez sur **Suivant**.
21. Pour **Confirmation**, vérifiez vos choix d'installation, puis cliquez sur **Installer**. Cliquez sur **Fermer**.
22. Déconnectez-vous de PRS-DC1, puis connectez-vous de nouveau en tant qu'**TREYRESEARCH\Administrateur** avec le mot de passe **Pa$$w0rd** pour mettre le jeton à jour de sécurité du compte d'utilisateur connecté. Votre cluster racine AD RMS est désormais installé et configuré.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour ouvrir la console Services AD RMS (Active Directory Rights Management Services)

1. Dans le Gestionnaire de serveur sur PRS-DC1, cliquez sur **Outils**, puis cliquez sur **Services AD RMS (Active Directory Rights Management Services)**.
2. Vérifiez que la console Services AD RMS (Active Directory Rights Management Services) s'ouvre sans erreur.
3. Fermez la console Services AD RMS (Active Directory Rights Management Services).

▶ Tâche 4 : Configurer les modèles AD RMS

Pour créer un modèle de stratégie de droits AD RMS

1. Basculez vers LON-DC1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Services AD RMS (Active Directory Rights Management Services)**.
2. Dans la console Services AD RMS (Active Directory Rights Management Services), développez lon-dc1.adatum.com (Local).
3. Sélectionnez **Modèles de stratégies de droits**, cliquez avec le bouton droit, puis cliquez sur **Propriétés**.
4. Activez la case à cocher **Activer l'exportation**, tapez **\\LON-DC1\Public** dans la zone **Spécifiez un emplacement de fichier pour les modèles (UNC)**, puis cliquez sur **OK**.
5. Dans le volet Actions, cliquez sur **Créer un modèle de stratégie de droits distribué** pour démarrer l'Assistant Créer un modèle de stratégie de droits distribué.
6. Cliquez sur **Ajouter**. Dans la zone **Langue**, choisissez français (France).
7. Tapez **Adatum.com RC** dans la zone **Nom**.
8. Tapez **Confidentiel Adatum.com Research** dans la zone **Description**, puis cliquez sur **Ajouter**. Cliquez sur **Suivant**.
9. Cliquez sur **Ajouter**, tapez **Management@adatum.com** dans la zone **Adresse de messagerie d'un utilisateur ou groupe**, puis cliquez sur **OK**.
10. Activez la case à cocher **Afficher** pour accorder au groupe Management@adatum.com l'accès en lecture à tout document créé à l'aide de ce modèle de stratégie de droits AD RMS.
11. Cliquez sur **Ajouter**, tapez **research@adatum.com** dans la zone **Adresse de messagerie d'un utilisateur ou groupe**, puis cliquez sur **OK**.
12. Activez la case à cocher **Contrôle total** pour accorder au groupe research@adatum.com l'accès en contrôle total à tout document créé à l'aide de ce modèle de stratégie de droits AD RMS.
13. Cliquez sur **Terminer**, et fermez la console Services AD RMS (Active Directory Rights Management Services).

Distribuer le modèle de stratégie de droits à l'aide de la distribution des modèles de stratégie de droits AD RMS

Le client AD RMS demande les modèles de stratégies de droits du cluster AD RMS à l'aide d'une tâche planifiée, configurée pour interroger le pipeline de distribution de modèles sur le cluster AD RMS.

Deux tâches planifiées sont disponibles : automatisée ou manuelle. La tâche planifiée automatisée est configurée pour s'exécuter jusqu'à une heure après la connexion d'un utilisateur à l'ordinateur et chaque matin à 3 h 00, mais cette tâche planifiée est désactivée par défaut. Vous pouvez activer et modifier la configuration par défaut à l'aide du Panneau de configuration du Planificateur de tâches. Une fois la tâche planifiée activée, vous devez configurer une entrée du Registre afin que Microsoft Office 2010 puisse localiser le répertoire dans lequel les modèles de stratégies de droits sont stockés.

Pour activer la tâche planifiée automatisée

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur l'écran Accueil, tapez **Tâches planifiées**, cliquez sur **Paramètres**, puis appuyez sur Entrée.
3. Développez **Bibliothèque du Planificateur de tâches**, développez **Microsoft**, développez **Windows**, puis cliquez sur **Active Directory Rights Management Services Client**.
4. Cliquez avec le bouton droit sur **AD RMS Rights Policy Template Management (Automated)** (Gestion des modèles de stratégies de droits AD RMS (automatisée)), puis cliquez sur **Activer**.
5. Fermez le Planificateur de tâches.
6. Cliquez à nouveau sur l'écran Accueil, tapez **regedit.exe**, puis appuyez sur Entrée.
7. Développez la clé de Registre suivante :

   HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common
8. Cliquez avec le bouton droit sur **Common**, sélectionnez **Nouveau** puis cliquez sur **Clé**. Tapez **DRM**, puis appuyez sur Entrée.
9. Cliquez avec le bouton droit sur **DRM**, cliquez sur **Nouveau**, puis cliquez sur **Valeur de chaîne extensible**.
10. Dans la zone de texte **Nom**, tapez **AdminTemplatePath**, puis appuyez sur Entrée.
11. Double-cliquez sur la valeur du Registre **AdminTemplatePath**, tapez **%LocalAppData%\Microsoft\DRM\Templates** dans la zone **Données de la valeur**, puis cliquez sur **OK**.
12. Fermez l'Éditeur du Registre.
13. Déconnectez-vous de LON-CL1.

▶ Tâche 5 : Configurer les stratégies d'exclusion AD RMS

Adatum a fait appel à un groupe de conseil en gestion. À cet effet, Toni Poe, conseillère en gestion de ce groupe, a été équipée d'un espace de bureau et du système informatique d'Adatum Corp. pour effectuer son travail. Un compte a été créé dans Active Directory pour elle et elle a été placée dans le groupe universel Management. Cependant, nous devons exclure les autorisations en lecture sur les fichiers Research Confidential restreints auxquels le groupe Management a accès. À cet effet, nous allons créer pour elle une stratégie d'exclusion sur le cluster AD RMS.

Créer un certificat de compte de droits pour Toni Poe

1. Sur **LON-CL1**, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur l'écran Accueil, tapez **Microsoft Word**, puis appuyez sur Entrée. Cliquez sur **OK** à l'invite **Nom d'utilisateur**. Dans la boîte de dialogue **Bienvenue dans Microsoft Office 2010**, cliquez sur **Ne pas apporter de modifications**, puis cliquez sur **OK**.
3. Accédez à l'onglet **Fichier** du Ruban, puis cliquez sur **Protéger le document** dans la section **Autorisations**. Dans la liste déroulante, cliquez sur **Restreindre l'autorisation par les personnes**, puis cliquez sur **Accès restreint**. Dans la demande d'authentification, fournissez **ADATUM\Toni** avec le mot de passe **Pa$$w0rd**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans la boîte de dialogue **Autorisation**, activez la case à cocher **Restreindre l'autorisation à : document**, puis cliquez sur **OK**.
5. Enregistrez le document comme **Text.docx** dans la bibliothèque locale Documents, fermez toutes les fenêtres actives et déconnectez-vous de **LON-CL1**.

Pour exclure les certificats de compte de droits

1. Dans le Gestionnaire de serveur sur **LON-DC1**, cliquez sur **Outils**, puis sur **Services AD RMS (Active Directory Rights Management Services)**.
2. Dans la console Services AD RMS (Active Directory Rights Management Services), développez **lon-dc1.adatum.com (Local)**.
3. Développez **Stratégies d'exclusion**, puis cliquez sur **Utilisateurs**.
4. Dans le volet **Actions**, cliquez sur **Activer l'exclusion d'utilisateurs**.
5. Dans le volet **Actions**, cliquez sur **Exclure le certificat de compte de droits**.
6. Dans la page **Ajouter un certificat de compte de droits à exclure**, vérifiez que la case d'option **Utiliser cette option pour exclure les certificats de compte des droits des utilisateurs internes qui disposent d'un compte des services de domaine Active Directory** est sélectionnée. Tapez **toni@adatum.com** dans la zone **Nom d'utilisateur**. Cliquez sur **Terminer**. L'adresse de messagerie et la clé publique de Toni doivent désormais être dans le tableau de la page **Informations sur les exclusions d'utilisateurs**. Si la clé publique est manquante, cela est dû au fait que Toni n'a jamais consommé ses droits d'informations. Afin de terminer cette action, Toni doit se connecter à un ordinateur client, puis utiliser un document protégé. Fermez la console Services AD RMS (Active Directory Rights Management Services).

▶ Tâche 6 : Valider le déploiement interne

Pour vérifier les fonctionnalités du déploiement AD RMS, vous vous connecterez comme Hani Loza, puis restreindrez les autorisations sur un document Microsoft Word 2010. Les autorisations permettront aux membres du groupe Management de lire le document, mais pas de le modifier, de l'imprimer ou de le copier, alors que les membres du groupe Finance bénéficieront d'un contrôle total. Puis, vous vous connecterez en tant que Limor Henig, en vérifiant que l'autorisation appropriée de lire le document a été accordée, et elle seule.

Avant de pouvoir consommer le contenu protégé par des droits, vous devez ajouter l'URL du cluster AD RMS à la zone de sécurité Intranet local.

Ajoutez l'URL du cluster AD RMS à la zone de sécurité Intranet local pour tous les utilisateurs qui auront accès au contenu protégé par des droits.

Pour ajouter le cluster AD RMS à la zone de sécurité intranet local

1. Connectez-vous à **LON-CL1** en tant qu'Hani (**ADATUM\Hani**) avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur la vignette du **Bureau**.
3. Dans la barre des tâches, cliquez sur **Internet Explorer**.
4. Cliquez sur **Outils** (icône de roues dentées dans le coin supérieur droit), puis cliquez sur **Options Internet**.
5. Cliquez sur l'onglet **Sécurité**, sur **Intranet local**, puis sur **Sites**.
6. Cliquez sur **Avancé**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Dans la boîte de dialogue **Ajouter ce site Web à la zone**, tapez **http://LON-DC1.adatum.com**, puis cliquez sur **Ajouter**. Cliquez sur **Fermer**.
8. Cliquez sur **OK** à deux reprises, puis fermez Internet Explorer.
9. Déconnectez-vous de LON-CL1.
10. Répétez les étapes 1 à 9 pour **ADATUM\Limor**.

Pour restreindre les autorisations d'un document Microsoft Word

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Hani** avec le mot de passe **Pa$$w0rd**.
2. Sur l'écran Accueil, tapez **Microsoft Word**, puis appuyez sur Entrée. Cliquez sur **OK** à l'invite **Nom d'utilisateur**. Dans la boîte de dialogue **Bienvenue dans Microsoft Office 2010**, cliquez sur **Ne pas apporter de modifications**. Cliquez sur **OK**.
3. Dans la page de document vierge, tapez **Les employés de Management peuvent lire ce document, mais ne peuvent pas le modifier, l'imprimer ou le copier. Les membres du groupe Research ont le contrôle total**.
4. Sous l'onglet Fichier, cliquez sur **Protéger le document**, pointez sur **Restreindre l'autorisation par les personnes**, puis cliquez sur **Accès restreint**.
5. Dans la boîte de dialogue **Autorisations**, activez la case à cocher **Restreindre l'autorisation à : document**, puis dans la zone **Lire**, tapez **Management@adatum.com**. Dans la zone **Modifier** tapez **research@adatum.com**.
6. Cliquez sur **OK** pour fermer la boîte de dialogue **Autorisations**.
7. Dans le menu Fichier, cliquez sur **Enregistrer sous**, puis enregistrez le fichier sous **\\LON-DC1\ConfidentialResearch\ADRMS-TST.docx**.
8. Fermez Microsoft Word, puis déconnectez-vous de LON-CL1.

Pour afficher un document protégé par des droits

1. Connectez-vous à **LON-CL1** en tant que Limor Henig (**ADATUM\Limor**) avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur la vignette du **Bureau**.
3. Ouvrez l'Explorateur de fichiers et accédez à **\\LON-DC1\ConfidentialResearch**. Double-cliquez sur le fichier **ADRMS-TST.docx** pour l'ouvrir dans Microsoft Word 2010.
4. Cliquez sur **OK** à l'invite **Nom d'utilisateur**.
5. Notez que le message suivant s'affiche : « L'autorisation d'accès à ce document est actuellement restreinte. Microsoft Office doit se connecter à http://lon-dc1.adatum.com/_wmcs/licensing afin de vérifier vos informations d'identification et de télécharger votre autorisation ». Cliquez sur **OK**.
6. Dans la boîte de dialogue Bienvenue dans Microsoft Office 2010, cliquez sur **Ne pas apporter de modifications**. Cliquez sur **OK**.
7. Quand le document s'ouvre, notez que la barre jaune de l'Accès restreint affiche : **Autorisation actuellement restreinte. Seuls les utilisateurs spécifiés peuvent accéder à ce contenu**.
8. Cliquez sur l'onglet **Fichier**. Notez que l'option **Imprimer** n'est pas disponible.
9. Fermez Microsoft Word, puis déconnectez-vous de LON-CL1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous devez vérifier que l'accès de Toni Poe exclut ses autorisations de lecture sur les fichiers Confidentiel Recherche restreintes, même si elle se trouve dans le groupe Management qui bénéficie d'un accès en affichage.

1. Connectez-vous à **LON-CL1** en tant que **Toni** avec le mot de passe **Pa$$w0rd**.
2. Sur l'écran Accueil, tapez **Microsoft Word**, puis appuyez sur Entrée.
3. Dans le ruban, cliquez sur l'onglet **Fichier**, puis sur **Ouvrir**.
4. Dans la zone **Nom de fichier**, tapez **\\LON-DC1\ConfidentialResearch.** Cliquez sur **Ouvrir**.
5. Essayez d'ouvrir le document **ADRMS-TST.docx**.
6. Dans la zone de sécurité, tapez **ADATUM\Toni** avec le mot de passe **Pa$$w0rd**. Dans le message qui s'affiche, cliquez sur **OK**.
7. Notez que le message suivant s'affiche : « L'autorisation d'accès à ce document est actuellement restreinte. Microsoft Office doit se connecter à http://lon-dc1.adatum.com/_wmcs/licensing afin de vérifier vos informations d'identification et de télécharger votre autorisation ». Cliquez sur OK.
8. Le message Microsoft Word suivant s'affiche : « **Seuls les documents créés dans une application signée peuvent être ouverts dans une application signée**. » Cliquez sur **OK**.
9. Dans la fenêtre Sélectionner l'utilisateur, cliquez sur **Annuler**. Fermez Microsoft Word, puis déconnectez-vous de **LON-CL1**.

Résultats : Vous devez avoir un cluster AD RMS en fonctionnement dans les forêts Adatum.com et TreyResearch.net, ainsi que pouvoir protéger avec IRM les documents Microsoft Office et voir les résultats de cette protection.

Exercice 3 : Implémentation de l'intégration AD RMS au contrôle d'accès dynamique

▶ Tâche 1 : Activer les propriétés des ressources

Pour activer les propriétés des ressources

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, cliquez sur **Centre d'administration Active Directory**, puis basculez vers **Arborescence**.
2. Développez **Contrôle d'accès dynamique**, puis sélectionnez **Resource Properties** (Propriétés de ressource).
3. Faites défiler l'écran vers le bas jusqu'à la propriété **Impact** de la colonne **Nom complet**. Cliquez avec le bouton droit sur **Impact**, puis cliquez sur **Activer**.
4. Faites défiler l'écran vers le bas jusqu'à la propriété **Personally Identifiable Information** (Informations d'identification personnelle) de la colonne **Nom complet**. Cliquez avec le bouton droit sur **Personally Identifiable Information** (Informations d'identification personnelle), puis cliquez sur **Activer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Pour publier les propriétés de ressource dans **Global Resource Property List** (Liste des propriétés de ressources globales), dans le volet gauche, cliquez sur **Contrôle d'accès dynamique**, et dans le volet d'informations, double-cliquez sur **Resource Property Lists** (Listes des propriétés de ressources), puis double-cliquez sur **Global Resource Property List** (Liste des propriétés de ressources globales) (développez la fenêtre).
6. Sous Propriétés de ressources, cliquez sur **Ajouter**, puis faites dérouler l'écran vers le bas jusqu'à **Impact**, cliquez dessus et ajoutez-le à la liste avec le bouton **>>**. Procédez de même pour **Personally Identifiable Information** (Informations d'identification personnelle). Cliquez sur **OK** à deux reprises pour terminer. Notez que ces propriétés de ressources peuvent se trouver déjà dans la liste ; si tel est le cas, il se peut que le bouton OK soit grisé. Vérifiez alors simplement que les propriétés de ressources sont dans la liste, puis cliquez sur **Annuler**.

▶ Tâche 2 : Créer les règles de classification

Cette étape explique comment créer la règle de classification **Impact haut**. Cette règle explore le contenu des documents et si elle trouve la chaîne « Confidentiel Adatum », elle classe le document en comme ayant un impact haut sur l'activité. Cette classification remplace toute classification précédemment attribuée d'impact bas sur l'activité.

Vous créerez également une règle **Informations identification personnelle hautes**. Cette règle explore le contenu des documents et si elle trouve un numéro de sécurité sociale, elle classe le document comme ayant des informations d'identification personnelle élevées.

Pour créer la règle de classification à impact haut

1. Connectez-vous à **LON-SVR1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la barre des tâches, cliquez sur **Explorateur de fichiers**.
3. Dans l'Explorateur de fichiers, dans l'arborescence de la console, cliquez sur **Ordinateur**, puis cliquez sur **Disque local (C:)**.
4. Cliquez avec le bouton droit sur **Research Documents** et sélectionnez **Partager avec... Des personnes spécifiques**.
5. Dans la zone de texte vide, cliquez sur la flèche de la zone de liste déroulante et sélectionnez **Tout le monde**, puis cliquez sur **Ajouter**.
6. Dans l'entrée Tout le monde, cliquez sur la flèche de la zone de liste déroulante à côté de Lecture et remplacez par Lecture/écriture.
7. Clique sur le bouton **Partager**, puis cliquez sur **Terminé**. Fermez l'Explorateur de fichiers.

   Agrandissez le Gestionnaire de serveur, s'il ne l'est déjà. Dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
8. Cliquez sur **Suivant** à trois reprises jusqu'à ce que vous ayez atteint la page **Sélectionner des rôles de serveurs**. Développez **Service de fichiers et de stockage (Installé)**, puis **Services de fichiers et iSCSI (Installé)**. Activez la case à cocher en regard de **Gestionnaire de ressources du serveur de fichiers**. Cliquez sur **Ajouter des fonctionnalités**, cliquez à deux reprises sur **Suivant**, puis cliquez sur **Installer**. Une fois l'installation terminée, cliquez sur **Fermer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Vous devez actualiser les propriétés de ressources globales à partir d'Active Directory. Ouvrez Windows PowerShell, entrez la commande suivante à l'invite de commandes, puis appuyez sur Entrée :

```
Update-FSRMClassificationPropertyDefinition
```

10. Fermez **Windows PowerShell**.
11. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire de ressources du serveur de fichiers**.
12. Dans le volet gauche du Gestionnaire de ressources du serveur de fichiers, développez **Gestion de la classification**, puis sélectionnez **Règles de classification**. Dans le volet **Actions**, cliquez sur **Configurer la planification de la classification**. Sous l'onglet **Classification automatique**, sélectionnez **Activer la planification fixe**, sélectionnez **dimanche**, puis activez la case à cocher **Autoriser la classification continue de nouveaux fichiers**. Cliquez sur **OK**. Vous devrez peut-être patienter quelques instants pour que les propriétés de classification Impact et Personally Identifiable Information (Informations d'identification personnelle) soient entièrement renseignées. Affichez le nœud **Propriétés de classification** sous Gestion de la classification dans l'arborescence de la console.
13. Avec le nœud Règles de classification sélectionné, dans le volet **Actions**, cliquez sur **Créer une règle de classification**. La boîte de dialogue **Créer une règle de classification** s'ouvre.
14. Dans la zone **Nom de la règle**, tapez **Impact métier haut**.
15. Dans la zone **Description**, tapez **Détermine si le document a un impact métier haut en fonction de la présence de la chaîne Confidentiel Adatum**
16. Sous l'onglet **Portée**, cliquez sur **Définir les propriétés de gestion des dossiers**, sélectionnez **Usage du dossier**, cliquez sur **Ajouter**, cliquez sur **Parcourir**, puis accédez à **C:\Research Documents**, et cliquez sur **OK**.
17. Sous **Valeur** activez la case à cocher en regard de **Fichiers de groupe**, cliquez sur **OK**, puis sur **Fermer**.
18. Sous l'onglet **Portée**, sélectionnez **Fichiers de groupe**.
19. Cliquez sur l'onglet **Classification**. Sous **Choisissez une méthode pour attribuer une propriété aux fichiers**, sélectionnez **Classifieur de contenus** dans la zone de liste déroulante.
20. Sous **Choisissez une propriété à attribuer aux fichiers**, sélectionnez **Impact** dans la zone de liste déroulante.
21. Sous **Spécifier une valeur**, sélectionnez **High** (Haut) dans la zone de liste déroulante.
22. Cliquez sur **Configurer** sous **Paramètres**. Dans la boîte de dialogue **Paramètres de classification**, dans la liste **Type d'expression**, sélectionnez **Chaîne**. Dans la zone **Expression**, tapez **Confidentiel Adatum**, puis cliquez sur **OK**.
23. Cliquez sur l'onglet **Type d'évaluation**. Cliquez sur **Réévaluer les valeurs de propriété existantes**, cliquez sur **Remplacer la valeur existante**, puis cliquez sur **OK** pour terminer.

Pour créer la règle de classification Informations identification personnelle hautes

1. Dans le volet gauche du Gestionnaire de ressources du serveur de fichiers, développez **Gestion de la classification**, puis cliquez sur **Règles de classification**.
2. Dans le volet **Actions**, cliquez sur **Créer une règle de classification**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la zone **Nom de la règle**, tapez **Informations identification personnelle hautes**. Dans la zone **Description**, tapez **Détermine si le document a des informations d'identification personnelle hautes en fonction de la présence d'un numéro de sécurité sociale**.
4. Cliquez sur l'onglet **Portée**, puis activez la case à cocher **Fichiers de groupe**. Le dossier C:\Research Documents doit apparaître comme inclus dans l'étendue.
5. Cliquez sur l'onglet **Classification**. Sous **Choisissez une méthode pour attribuer une propriété aux fichiers**, sélectionnez **Classifieur de contenus** dans la zone de liste déroulante.
6. Sous **Choisissez une propriété à attribuer aux fichiers**, sélectionnez **Personally Identifiable Information** (Informations d'identification personnelle) dans la zone de liste déroulante.
7. Sous **Spécifier une valeur**, sélectionnez **High** (Haut) dans la zone de liste déroulante.
8. Cliquez sur **Configurer** sous **Paramètres**. Dans la fenêtre Paramètres de classification, dans la liste **Type d'expression**, sélectionnez **Expression régulière**. Dans la zone **Expression**, tapez l'expression suivante (remarque : Il n'y a aucun saut de ligne dans l'expression. la chaîne ne forme qu'un seul bloc), puis cliquez sur **OK** :

```
^(?!000)([0-7]\d{2}|7([0-7]\d|7[012]))([ -]?)(?!00)\d\d\3(?!0000)\d{4}$
```

Remarque : Cette expression autorise les numéros de sécurité sociale non valides. Cela nous permet d'utiliser des numéros de sécurité sociale fictifs dans l'atelier pratique.

9. Cliquez sur l'onglet **Type d'évaluation**. Sélectionnez **Réévaluer les valeurs de propriété existantes**, cliquez sur **Remplacer la valeur existante**, puis cliquez sur **OK** pour terminer.
10. Vous devriez maintenant avoir deux règles de classification :
    - Impact métier haut
    - Informations identification personnelle hautes

▶ Tâche 3 : Protéger automatiquement les documents avec AD RMS

Maintenant que vous avez créé des règles de classification automatique des documents en fonction du contenu, l'étape suivante consiste à créer une tâche de gestion des fichiers qui utilise AD RMS pour protéger automatiquement certains documents selon leur classification. Dans cette étape, vous allez créer une tâche de gestion de fichiers qui protège automatiquement tous les documents ayant des informations identification personnelle hautes. Seuls les membres du groupe Research auront accès aux documents qui contiennent des informations identification personnelle hautes.

Pour ajouter LON-DC1 à la zone de sécurité Intranet local sur LON-SVR1

1. Sur LON-SVR1, cliquez sur l'écran Accueil, puis sur **Internet Explorer**.
2. Cliquez sur **Outils** (icône de roues dentées dans le coin supérieur droit), puis cliquez sur **Options Internet**.
3. Cliquez sur l'onglet **Sécurité**, sur **Intranet local**, puis sur **Sites**.
4. Cliquez sur **Avancé**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans la boîte de dialogue **Ajouter ce site Web à la zone**, tapez **http://LON-DC1.adatum.com**, puis cliquez sur **Ajouter**. Cliquez sur **Fermer**.
6. Cliquez sur **OK** à deux reprises, puis fermez Internet Explorer.

Pour protéger les documents avec AD RMS

1. Dans le Gestionnaire de ressources du serveur de fichiers, dans le volet gauche, sélectionnez **Tâches de gestion de fichiers**. Dans le volet Actions, sélectionnez **Créer une tâche de gestion de fichiers**.
2. Dans le champ **Nom de la tâche :**, tapez **Informations identification personnelle hautes**. Dans le champ **Description**, tapez **Protection RMS automatique pour les documents aux informations d'identification personnelle hautes**.
3. Cliquez sur l'onglet **Portée**, puis activez la case à cocher **Fichiers de groupe**. L'emplacement **C:\Research Documents** doit apparaître comme faisant partie de l'étendue.
4. Cliquez sur l'onglet **Action**. Sous **Type**, sélectionnez **Chiffrement RMS**. Sélectionnez le modèle **Adatum.com RC**.
5. Cliquez sur l'onglet **Condition**, puis cliquez sur **Ajouter**. Sous **Propriété**, sélectionnez **Personally Identifiable Information** (Informations d'identification personnelle). Sous **Opérateur**, sélectionnez **Égal**. Sous **Valeur**, sélectionnez **High** (Haut). Cliquez sur **OK**.
6. Cliquez sur l'onglet **Planification**. Dans la section **Planification**, cliquez sur **Toutes les semaines**, puis sélectionnez **dimanche**. L'exécution hebdomadaire de la tâche garantit que vous interceptez tous les documents qui ont pu être ignorés suite à une panne de service ou autre événement perturbateur.
7. Dans la section **Opération continue**, sélectionnez **Exécuter en continu sur les nouveaux fichiers**, puis cliquez sur **OK**. Vous devez avoir maintenant une tâche de gestion de fichiers intitulée Informations identification personnelle hautes.

▶ Tâche 4 : Vérifier le déploiement

1. Sur LON-SVR1, ouvrez l'Explorateur de fichiers et accédez à **C:\Research Documents**.
2. Cliquez avec le bouton droit sur le document **Finance Memo**, cliquez sur **Propriétés**, cliquez sur l'onglet **Classification**, et notez que les deux propriétés n'ont actuellement aucune valeur. Cliquez sur **Annuler**.
3. Cliquez avec le bouton droit sur le document **Request for Approval to Hire**, puis sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Classification** et notez que les deux propriétés n'ont actuellement aucune valeur. Cliquez sur **Annuler**.
5. Basculez vers **LON-CL1**, et connectez-vous en tant qu'**ADATUM\Hani** avec le mot de passe **Pa$$w0rd**.
6. Dans l'écran d'Accueil, tapez **\\LON-SVR1\Research Documents**, et appuyez sur Entrée.
7. Ouvrez le document **Finance Memo**. Tapez **Confidentiel Adatum**, puis appuyez à deux reprises sur **Entrée**. Enregistrez le document, puis fermez Microsoft Word.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Ouvrez le document **Request for Approval to Hire**. Tapez **Sécurité sociale # :** Appuyez sur la touche Entrée et, sur une nouvelle ligne, tapez **777-77-7777**, puis appuyez sur Entrée à deux reprises. L'expression doit figurer sur une nouvelle ligne pour être remarquée rapidement par le contrôle d'accès dynamique. Enregistrez le document, puis fermez Microsoft Word.
9. Basculez vers **LON-SVR1**. Dans l'Explorateur de fichiers, accédez à **C:\Research Documents**.
10. Cliquez avec le bouton droit sur **Finance Memo**, puis cliquez sur **Propriétés**. Cliquez sur l'onglet **Classification**. Notez que la propriété **Impact** a maintenant la valeur **High** (Haut). Cliquez sur **Annuler**.
11. Cliquez avec le bouton droit sur le document **Request for Approval to Hire**, puis cliquez sur **Propriétés**.
12. Cliquez sur l'onglet **Classification**. Notez que la propriété **Personally Identifiable Information** (Informations d'identification personnelle) a maintenant la valeur **High** (Haute). Cliquez sur **Annuler**.
13. Si vous n'êtes dans aucun des deux cas, ouvrez le Gestionnaire de ressources du serveur de fichiers, puis sélectionnez **Tâches de gestion de fichiers**. Sélectionnez **Informations d'identification personnelles hautes** dans le volet d'informations et, dans le volet Actions, cliquez sur Exécuter maintenant une tâche de gestion de fichiers. Dans le message, sélectionnez **Exécuter la tâche en arrière-plan (recommandé)**, puis cliquez sur **OK**. La commande Exécuter une tâche de gestion de fichiers apparaît en grisé. Après quelques instants, le texte apparaît à nouveau en clair, signe que la tâche de gestion est terminée. Répétez les étapes 9 à 12 ci-dessus.
14. Sur tous les ordinateurs sauf LON-DC1, fermez toutes les fenêtres actives, puis déconnectez-vous.

Résultats : Les règles de classification du contrôle d'accès dynamique doivent être appliquées au contenu protégé par la gestion des droits relatifs à l'information (IRM).

Exercice 4 : Implémentation de l'intégration AD RMS avec des utilisateurs externes

▶ Tâche 1 : Exporter la stratégie des domaines d'utilisateurs approuvés

Exporter un domaine d'utilisateur approuvé

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Services AD RMS (Active Directory Rights Management Services)**.
2. Dans l'arborescence de la console, développez **lon-dc1.adatum.com (Local)**, développez **Stratégies d'approbation**, puis cliquez sur **Domaines d'utilisateurs approuvés**.
3. Dans le volet Actions, cliquez sur **Exporter le domaine d'utilisateur approuvé**. La boîte de dialogue **Exporter le domaine d'utilisateur approuvé en tant que** s'ouvre.
4. Dans la zone **Nom du fichier**, tapez **C:\ADRMS_LON-DC1_LicensorCert.bin**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Cliquez sur **Enregistrer** pour enregistrer le fichier avec le nom et l'emplacement que vous avez spécifiés.
6. Sur **PRS-DC1**, connectez-vous en tant que **ADATUM\Administrateur** à l'aide du mot de passe **Pa$$w0rd**, et répétez les étapes 1 à 5 sur **PRS-DC1**, mais utilisez le nom **ADRMS_PRS-DC1_LicensorCert.bin** pour le fichier .bin.

▶ Tâche 2 : Exporter la stratégie des domaines de publication approuvés

Exporter une stratégie de domaines de publication approuvés

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Services AD RMS (Active Directory Rights Management Services)**.
2. Dans l'arborescence de la console, développez **lon-dc1.adatum.com (Local)**, développez **Stratégies d'approbation**, puis cliquez sur **Domaines de publication approuvés**.
3. Dans le volet Résultats, sélectionnez **LON-DC1** et, dans le volet Actions, cliquez sur **Exporter le domaine de publication approuvé**.
4. Dans la boîte de dialogue **Exporter le domaine de publication approuvé**, cliquez sur **Enregistrer sous**, puis tapez **C:\AdatumTrustedPubDomain.xml**. Cliquez sur **Enregistrer**.
5. Dans les zones **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa$$w0rd**.
6. Cliquez sur **Terminer** pour créer le fichier du domaine de publication approuvé.
7. Répétez les étapes 1 à 6 sur **PRS-DC1**, avec le nom de fichier **C:\TreyTrustedPubDomain.xml** et le mot de passe **Pa$$word**.

▶ Tâche 3 : Importer la stratégie de domaine d'utilisateur approuvé à partir du domaine partenaire

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils** et, dans la zone de liste déroulante, cliquez sur **DNS**. Développez **LON-DC1**, sélectionnez **Redirecteurs conditionnels** et cliquez avec le bouton droit, puis cliquez sur **Nouveau redirecteur conditionnel**.
2. Sous **Domaine DNS**, tapez **TreyResearch.net**. Dans **Adresses IP des serveurs maîtres**, tapez **172.16.10.10**. Appuyez sur Entrée, puis cliquez sur **OK**. Fermez le Gestionnaire DNS.
3. Sur **PRS-DC1**, répétez les étapes 1 et 2. Utilisez le domaine DNS **Adatum.com** et **Adresses IP des serveurs maîtres 172.16.0.10**.
4. Sur **LON-DC1**, ouvrez la console Services AD RMS (Active Directory Rights Management Services), puis développez **lon-dc1.adatum.com (Local)**.
5. Dans l'arborescence de la console, développez **Stratégies d'approbation**, puis cliquez sur **Domaines d'utilisateurs approuvés**.
6. Dans le volet Actions, cliquez sur **Importer le domaine d'utilisateur approuvé**.
7. Dans la zone **Fichier de domaine d'utilisateur approuvé**, tapez **\\PRS-DC1\C$\ADRMS_PRS-DC1_LicensorCert.bin**.
8. Dans **Nom complet**, tapez **TreyResearch**. Cliquez sur **Terminer**.
9. Répétez les étapes 4 à 8 sur **PRS-DC1**, en remplaçant le nom de fichier ci-dessus par **\\LON-DC1\C$\ADRMS_LON-DC1_LicensorCert.bin** et le **Nom complet** par **Adatum.**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Importer la stratégie des domaines de publication approuvés à partir du domaine partenaire

Ajouter un domaine de publication approuvé

1. Sur **LON-DC1**, ouvrez la console Services AD RMS (Active Directory Rights Management Services) et développez **lon-dc1.adatum.com (Local)**.
2. Dans l'arborescence de la console, développez **Stratégies d'approbation**, puis cliquez sur **Domaines de publication approuvés**.
3. Dans le volet Actions, cliquez sur **Importer le domaine de publication approuvé**.
4. Dans **Fichier de domaine de publication approuvé**, tapez **\\PRS-DC1\c$\TreyTrustedPubDomain.xml**.
5. Tapez **Pa$$w0rd** dans la zone **Mot de passe**.
6. Dans **Nom complet**, tapez **Domaine TreyResearch**. Cliquez sur **Terminer**.
7. Répétez les étapes 1 à 6 sur **PRS-DC1**, avec le nom de fichier **\\LON-DC1\C$\AdatumTrustedPubDomain.xml**, avec le mot de passe **Pa$$w0rd** et le **Nom complet Domaine Adatum**.
8. Cliquez sur **Terminer**.

▶ Tâche 5 : Configurer l'accès anonyme au serveur de licences AD RMS

1. Basculez vers LON-DC1.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestionnaire des services Internet (IIS)**.
3. Dans le Gestionnaire des services Internet (IIS), développez **LON-DC1\Sites\Default Web Site_wmcs**. Si la zone de message Gestionnaire des services Internet (IIS) s'affiche, cliquez sur **Annuler**.
4. Cliquez avec le bouton droit sur **licensing**, puis cliquez sur **Basculer vers l'affichage du contenu**.
5. Cliquez avec le bouton droit sur **license.asmx**, puis cliquez sur **Basculer vers l'affichage des fonctionnalités**.
6. Double-cliquez sur **Authentification**, cliquez sur **Authentification anonyme** et, dans le volet Actions, cliquez sur **Activer**.
7. Cliquez sur **Authentification Windows**, puis cliquez sur **Désactiver**.
8. Cliquez avec le bouton droit sur **licensing**, puis cliquez sur **Basculer vers l'affichage du contenu**.
9. Cliquez avec le bouton droit sur **ServiceLocator.asmx**, puis cliquez sur **Basculer vers l'affichage des fonctionnalités**.
10. Double-cliquez sur **Authentification**, cliquez sur **Authentification anonyme** et, dans le volet Actions, cliquez sur **Activer**.
11. Cliquez sur **Authentification Windows**, puis cliquez sur **Désactiver**.
12. Fermez le Gestionnaire des services Internet (IIS).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 6 : Vérifier l'accès utilisateur au document protégé

1. Connectez-vous à **LON-CL1** en tant qu'utilisateur **ADATUM\Hani** avec le mot de passe **Pa$$w0rd**.
2. Sur l'écran Accueil, tapez **\\LON-DC1\ConfidentialResearch**, puis appuyez sur Entrée.
3. Double-cliquez sur **ADRMS-TST.docx** pour l'ouvrir. À l'invite Microsoft Word, cliquez sur **Changer d'utilisateur**, puis à l'invite **Sélectionner l'utilisateur**, cliquez sur **OK**. Dans la barre jaune **Accès restreint**, cliquez sur le bouton **Modifier l'autorisation**.
4. Dans la zone en regard de l'autorisation de lecture, placez un point-virgule après **Management@adatum.com**, puis ajoutez+ **liberty@treyresearch.net**. Cliquez sur **OK**.
5. Enregistrez le fichier **ADRMS-TST.docx**, fermez Microsoft Word, puis déconnectez-vous de LON-CL1.
6. Connectez-vous à **LON-DC1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
7. Copiez le fichier **ADRMS-TST.docx** depuis **C:\ConfidentialReseach** sur **\\PRS-DC1\Public**.
8. Connectez-vous à **PRS-CL1** en tant qu'utilisateur **TREYRESEARCH\Liberty** avec le mot de passe **Pa$$w0rd**.
9. Sur l'écran Accueil, tapez **\\PRS-DC1\Public**, puis appuyez sur Entrée.
10. Double-cliquez sur le fichier **ADRMS-TST.docx**.
11. Cliquez sur **OK** à l'invite **Nom d'utilisateur**.
12. Une fenêtre contextuelle Microsoft Word apparaît avec le message suivant : **« Vos informations utilisateurs doivent être vérifiées avant que vous puissiez continuer. Souhaitez-vous les vérifier maintenant ?** Cliquez sur **Oui**.
13. Dans la fenêtre contextuelle Sécurité de Windows, entrez **TREYRESEARCH\Liberty** comme nom d'utilisateur et **Pa$$w0rd** comme mot de passe. Cliquez sur **OK**.
14. Si une invite vous informe « **Impossible de vérifier les informations utilisateur actuellement. Voulez-vous ouvrir ce document avec un autre jeu d'informations d'identification ?**" cliquez sur **Oui**, puis à l'invite **Sélectionner l'utilisateur**, cliquez sur **OK**.
15. À l'invite qui indique « **L'autorisation d'accès à ce document est actuellement restreinte.** », cliquez sur **OK**, puis cliquez sur **Oui**. Dans la boîte de dialogue **Bienvenue sur Microsoft Office 2010**, cliquez sur **Ne pas apporter de modifications**, puis cliquez sur **OK**.
16. Fermez toutes les fenêtres, puis déconnectez-vous de tous les ordinateurs virtuels.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22414B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22414B-LON-SVR1**, **22414B-LON-CL1**, **22414B-PRS-DC1** et **22414B-PRS-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT