Microsoft

PRODUIT OFFICIEL DE FORMATION MICROSOFT

22411B

Administration de Windows Server® 2012

Les informations contenues dans ce document, notamment les URL et les autres références aux sites Web, 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 la permission 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 sur 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 : 22411B

Numéro de référence : X18-86874

Date de publication : 3/2013

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.

Andrew J. Warren – Développeur de contenu

Andrew Warren a plus de 25 années d'expérience dans le secteur de l'informatique, parmi lesquelles de nombreuses années passées à enseigner et écrire. Il a été impliqué en tant qu'expert technique dans la conception de plusieurs cours sur Windows Server® 2008 et a été le responsable technique de plusieurs autres cours. Il a également été impliqué dans le développement de sessions TechNet sur Microsoft® Exchange Server 2007. Basé au Royaume-Uni, Andrew a son propre cabinet d'enseignement et de formation en informatique.

Jason Kellington – Développeur de contenu

Jason Kellington (MCT (Microsoft Certified Trainer), MCITP (Microsoft Certified IT Professional) et MCSE (Microsoft Certified Solutions Expert) est consultant, instructeur et auteur. Il bénéficie d'une solide expérience dans un large éventail de technologies Microsoft, et plus particulièrement dans le domaine de l'infrastructure réseau d'entreprise. Jason exerce différentes fonctions chez Microsoft. Il est à la fois développeur de contenu pour les cours Formation Microsoft, responsable rédacteur technique pour Microsoft IT Showcase et auteur pour Microsoft Press®.

Brian Desmond – Réviseur technique

Brian Desmond est consultant et membre du programme Microsoft MVP (Most Valuable Professional). Il est basé près de Chicago, Illinois. Brian se concentre sur les projets de gestion des identités, Exchange Server et Active Directory pour les entreprises globales. Il est l'auteur d'Active Directory, 4ème édition (O'Reilly) et de nombreux articles dans les principales publications du secteur, telles que le magazine Windows IT Pro. Grand voyageur, vous pouvez habituellement rencontrer Brian lors de ses interventions à des conférences et de ses déplacements chez des clients.

David Susemiehl – Développeur de contenu

David Susemiehl travaille comme consultant, instructeur, et développeur de support pédagogique depuis 1996. David possède une grande expérience de consultant sur Microsoft Systems Management Server et Microsoft System Center Configuration Manager 2007, aussi bien que sur les déploiements de Terminal Server/Citrix, Active Directory et Exchange Server. David a développé des supports pédagogiques pour Microsoft et Hewlett-Packard, et a animé ces cours avec succès en Europe, en Amérique Centrale et à travers toute l'Amérique du Nord. Depuis quelques années, David écrit des supports pédagogiques pour Formation Microsoft et travaille comme consultant en transitions d'infrastructure dans le Michigan.

Sommaire

Module 1 : Déploiement et maintenance des images de serveur

Leçon 1 : Vue d'ensemble des services de déploiement Windows **1-2**
Leçon 2 : Implémentation d'un déploiement avec les services de déploiement Windows **1-9**
Leçon 3 : Administration des services de déploiement Windows **1-16**
Atelier pratique : Utilisation des services de déploiement Windows pour déployer Windows Server 2012 **1-23**

Module 2 : Configuration et résolution des problèmes du système DNS

Leçon 1 : Installation du rôle de serveur DNS **2-2**
Leçon 2 : Configuration du rôle de serveur DNS **2-9**
Leçon 3 : Configuration des zones DNS **2-16**
Leçon 4 : Configuration des transferts de zone DNS **2-22**
Leçon 5 : Gestion et dépannage du système DNS **2-25**
Atelier pratique : Configuration et résolution des problèmes du système DNS **2-34**

Module 3 : Gestion des services de domaine Active Directory

Leçon 1 : Vue d'ensemble d'AD DS **3-2**
Leçon 2 : Implémentation des contrôleurs de domaine virtualisés **3-8**
Leçon 3 : Implémentation des contrôleurs de domaine en lecture seule **3-13**
Leçon 4 : Administration d'AD DS **3-18**
Leçon 5 : Gestion de la base de données AD DS **3-18**
Atelier pratique : Gestion d'AD DS **3-37**

Module 4 : Gestion des comptes d'utilisateurs et de service

Leçon 1 : Automatisation de la gestion des comptes d'utilisateurs **4-2**
Leçon 2 : Configuration des paramètres de stratégie de mot de passe et de verrouillage de compte d'utilisateur **4-8**
Leçon 3 : Configuration des comptes de service gérés **4-15**
Atelier pratique : Gestion des comptes d'utilisateurs et de service **4-22**

Module 5 : Implémentation d'une infrastructure de stratégie de groupe

Leçon 1 : Présentation de la stratégie de groupe **5-2**
Leçon 2 : Implémentation et administration des objets de stratégie de groupe **5-12**
Leçon 3 : Étendue de la stratégie de groupe et traitement de la stratégie de groupe **5-20**
Leçon 4 : Dépanner l'application des objets de stratégie de groupe **5-39**
Atelier pratique : Implémentation d'une infrastructure de stratégie de groupe **5-46**

Module 6 : Gestion des bureaux des utilisateurs avec la stratégie de groupe

Leçon 1 : Implémentation des modèles d'administration **6-2**
Leçon 2 : Configuration de la redirection de dossiers et des scripts **6-12**
Leçon 3 : Configuration des préférences de stratégies de groupe **6-20**
Leçon 4 : Gestion des logiciels à l'aide de la stratégie de groupe **6-39**
Atelier pratique : Gestion des bureaux des utilisateurs avec la stratégie de groupe **6-46**

Module 7 : Configuration et résolution des problèmes d'accès à distance

Leçon 1 : Configuration de l'accès réseau **7-2**
Leçon 2 : Configuration de l'accès VPN **7-11**
Leçon 3 : Vue d'ensemble des stratégies réseau **7-22**
Leçon 4 : Résolution des problèmes du service de routage et d'accès à distance **7-29**
Atelier pratique A : Configuration de l'accès à distance **7-36**
Leçon 5 : Configuration de DirectAccess **7-41**
Atelier pratique B : Configuration de DirectAccess **7-56**

Module 8 : Installation, configuration et résolution des problèmes du rôle de serveur NPS

Leçon 1 : Installation et configuration d'un serveur NPS **8-2**
Leçon 2 : Configuration de clients et de serveurs RADIUS **8-7**
Leçon 3 : Méthodes d'authentification NPS **8-14**
Leçon 4 : Analyse et résolution des problèmes d'un serveur NPS **8-24**
Atelier pratique : Installation et configuration d'un serveur NPS **8-30**

Module 9 : Implémentation de la protection d'accès réseau

Leçon 1 : Vue d'ensemble de la protection d'accès réseau **9-2**
Leçon 2 : Vue d'ensemble des processus de contrainte de mise en conformité NAP **9-8**
Leçon 3 : Configuration de NAP **9-16**
Leçon 4 : Analyse et résolution des problèmes du système NAP **9-22**
Atelier pratique : Implémentation de la protection d'accès réseau **9-27**

Module 10 : Optimisation des services de fichiers

Leçon 1 : Vue d'ensemble de FSRM **10-3**
Leçon 2 : Utilisation de FSRM pour gérer les quotas, les filtres de fichiers et les rapports de stockage **10-10**
Leçon 3 : Implémentation des tâches de classification et de gestion de fichiers **10-21**
Atelier pratique A : Configuration des quotas et du filtrage des fichiers à l'aide de FSRM **10-28**
Leçon 4 : Vue d'ensemble de DFS **10-32**
Leçon 5 : Configuration des espaces de noms DFS **10-41**
Leçon 6 : Configuration et résolution des problèmes de la réplication DFS **10-46**
Atelier pratique B : Implémentation de DFS **10**-50

Module 11 : Configuration du chiffrement et de l'audit avancé

Leçon 1 : Chiffrement des fichiers à l'aide du système EFS (Encrypting File System) **11-2**
Leçon 2 : Configuration de l'audit avancé **11-6**
Atelier pratique : Configuration du chiffrement et de l'audit avancé **11-14**

Module 12 : Implémentation de la gestion des mises à jour

Leçon 1 : Vue d'ensemble de WSUS **12-2**
Leçon 2 : Déploiement des mises à jour avec WSUS **12-5**
Atelier pratique : Implémentation de la gestion des mises à jour **12-9**

Module 13 : Surveillance de Windows Server 2012

Leçon 1 : Outils d'analyse **13-2**
Leçon 2 : Utilisation de l'Analyseur de performances **13-9**
Leçon 3 : Analyse des journaux d'événements **13-18**
Atelier pratique : Surveillance de Windows Server 2012 **13-21**

Corrigés des ateliers pratiques

Atelier pratique du module 1 : Utilisation des services de déploiement Windows pour déployer Windows Server 2012 **L1-1**
Atelier pratique du module 2 : Configuration et résolution des problèmes du système DNS **L2-7**
Atelier pratique du module 3 : Gestion d'AD DS **L3-13**
Atelier pratique du module 4 : Gestion des comptes d'utilisateurs et de service **L4-21**
Atelier pratique du module 5 : Implémentation d'une infrastructure de stratégie de groupe **L5-25**
Atelier pratique du module 6 : Gestion des bureaux des utilisateurs avec la stratégie de groupe **L6-35**

Atelier pratique A du module 7 : Configuration de l'accès à distance **L7-41**
Atelier pratique B du module 7 : Configuration de DirectAccess **L7-48**
Atelier pratique du module 8 : Installation et configuration d'un serveur NPS **L8-63**
Atelier pratique du module 9 : Implémentation de la protection d'accès réseau **L9-69**
Atelier pratique A du module 10 : Configuration des quotas et du filtrage des fichiers à l'aide de FSRM **L10-79**
Atelier pratique B du module 10 : Implémentation de DFS **L10-84**
Atelier pratique du module 11 : Configuration du chiffrement et de l'audit avancé **L11-89**
Atelier pratique du module 12 : Implémentation de la gestion des mises à jour **L12-93**
Atelier pratique du module 13 : Surveillance de Windows Server 2012 **L13-99**

À propos de ce cours

Cette section décrit brièvement le cours « *22411B : Administration de Windows Server® 2012* » et le public visé, les connaissances préalables requises, ainsi que les objectifs.

Description du cours

Le principal objectif de ce cours consiste à configurer et assurer la maintenance des services d'infrastructure centrale dans un environnement d'entreprise Windows Server 2012. Ce cours s'adresse principalement aux professionnels des technologies de l'information qui ont implémenté un serveur Microsoft® Windows Server 2008, soit dans une infrastructure d'entreprise existante, soit comme installation autonome, et qui souhaitent acquérir les compétences et les connaissances nécessaires pour élargir cette implémentation de façon à gérer et assurer la maintenance de l'infrastructure centrale requise pour un environnement Windows Server 2008. Les candidats doivent également posséder les connaissances correspondant aux sujets abordés dans le cours *Windows Server 2012 Enterprise Core 1*, étant donné que ce cours se basera sur ces connaissances.

Public visé

Ce cours a pour objectif principal d'élargir le déploiement initial des services présenté dans Core 1 et de fournir les qualifications nécessaires pour gérer et assurer la maintenance d'une infrastructure Windows Server 2012 basée sur un domaine. Les candidats sont généralement des administrateurs système et doivent posséder une expérience d'au moins un an dans un environnement Windows Server 2012 ou Windows® 8. Ce cours peut s'adresser en second lieu à des candidats qui souhaitent obtenir la certification MCSA (Microsoft Certified Solutions Associate) en tant que telle, ou poursuivre leur formation afin d'acquérir la certification MCSE (Microsoft Certified Solutions Expert), pour laquelle ce cours est une condition préalable.

Connaissances préalables des stagiaires

Pour suivre ce cours, vous devez posséder les connaissances préalables nécessaires pour :

- installer et configurer Windows Server 2012 dans les environnements d'entreprise existants ou en tant qu'installations autonomes ;
- configurer le stockage local ;
- configurer les rôles et les fonctionnalités ;
- configurer les fichiers et les services d'impression ;
- configurer les serveurs Windows Server 2012 pour l'administration locale et distante ;
- configurer les adresses IPv4 et IPv6 ;
- configurer les services DNS (Domain Name System) et DHCP (Dynamic Host Configuration Protocol) ;
- installer les contrôleurs de domaine ;
- créer et configurer les utilisateurs, les groupes, les ordinateurs et les unités d'organisation ;
- créer et gérer les stratégies de groupe ;
- configurer les stratégies de sécurité locales.

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 :

- déployer, gérer et maintenir les serveurs ;
- configurer les fichiers et les services d'impression ;
- configurer les services et l'accès réseau ;
- configurer une infrastructure de serveur de stratégie réseau ;
- configurer et gérer les services de domaine Active Directory® (AD DS) ;
- configurer et gérer la stratégie de groupe.

Plan du cours

Le plan du cours est le suivant :

Module 1, « Déploiement et maintenance des images de serveur »

Module 2, « Configuration et résolution des problèmes du système DNS »

Module 3, « Gestion des services de domaine Active Directory »

Module 4, « Gestion des comptes d'utilisateurs et de service »

Module 5, « Implémentation d'une infrastructure de stratégie de groupe »

Module 6, « Gestion des bureaux des utilisateurs avec la stratégie de groupe »

Module 7, « Configuration et résolution des problèmes d'accès à distance »

Module 8, « Installation, configuration et résolution des problèmes du rôle de serveur NPS »

Module 9, « Implémentation de la protection d'accès réseau »

Module 10, « Optimisation des services de fichiers »

Module 11, « Configuration du chiffrement et de l'audit avancé »

Module 12, « Implémentation de la gestion des mises à jour »

Module 13, « Surveillance de Windows Server 2012 »

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Mappage d'examen/de cours

Ce cours, *22411B : Administration de Windows Server® 2012*, mappe directement son contenu aux objectifs de l'examen Microsoft *70-411 : Administration de Windows Server® 2012*.

Le tableau suivant est fourni sous la forme d'une aide d'étude pour vous aider à préparer cet examen et vous montrer la manière dont s'imbriquent les objectifs de l'examen et le contenu du cours. Le cours n'est pas conçu exclusivement en vue de l'examen, mais fournit plutôt des connaissances et compétences plus larges pour permettre une implémentation en situation réelle de cette technologie particulière. Le cours contient également du contenu qui n'est pas directement lié à l'examen et qui utilisera l'expérience et les compétences uniques de votre instructeur certifié Microsoft.

Remarque : Les objectifs de l'examen sont disponibles en ligne à l'aide de l'URL suivante : http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-411#tab2 (*Certains de ces sites adressées dans ce cours sont en anglais*).

Examen 70-411 : Administration de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Déployer, gérer et maintenir les serveurs (17 %)		**Module**	**Leçon**	**Atelier pratique**
Déployer et gérer les images de serveur.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : installer le rôle des services de déploiement Windows (WDS), configurer et gérer le démarrage, installer et découvrir des images, mettre à jour des images avec des correctifs, des correctifs logiciels et des pilotes, installer des fonctionnalités pour des images hors connexion	Mod 1	Leçons 1/2/3	Mod 1 Ex 1/2/3/4
Implémenter la gestion des correctifs.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : installer et configurer le rôle Windows Server Update Services (WSUS), configurer les stratégies de groupe pour les mises à jour, configurer le ciblage côté client, configurer la synchronisation WSUS, configurer les groupes WSUS	Mod 12	Leçon 1/2	Mod 12 Ex 1/2/3
Surveiller les serveurs.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer les ensembles de collecteurs de données (DCS), configurer les alertes, analyser les performances en temps réel, surveiller les ordinateurs virtuels, surveiller les événements, configurer les abonnements aux événements, configurer le contrôle de réseau	Mod 13	Leçons 1/2/3	Mod 13 Ex 1/2/3

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Examen 70-411 : Administration de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer les fichiers et les services d'impression (15 %)				
Configurer le système de fichiers DFS.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : installer et configurer les espaces de noms DFS, configurer les cibles de réplication DFS, configurer la planification de la réplication, configurer les paramètres de compression différentielle à distance, configurer le transit, configurer la tolérance de pannes	Mod 10	Leçons 4/5/6	Mod 10 Atelier B Ex 1/2/3
Configurer le Gestionnaire de ressources du serveur de fichiers (FSRM).	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : installer le rôle Gestionnaire de ressources du serveur de fichiers, configurer les quotas, configurer les filtres de fichiers, configurer les rapports	Mod 10	Leçons 1 /2/3	Mod 10 Atelier A Ex 1/2
Configurer le chiffrement de disques et de fichiers	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer le chiffrement Bitlocker, configurer la fonctionnalité de déverrouillage réseau, configurer les stratégies de Bitlocker, configurer l'agent de récupération EFS, gérer les certificats EFS et Bitlocker comprenant la sauvegarde et la restauration	Mod 11	Leçon 1	Mod 11 Ex 1
Configurer les stratégies d'audit avancées.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : implémenter l'audit à l'aide de la stratégie de groupe et d'AuditPol.exe, créer des stratégies d'audit basées sur des expressions, créer les stratégies d'audit des périphériques amovibles	Mod 11	Leçon 2	Mod 11 Ex 2

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Examen 70-411 : Administration de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer les services et l'accès réseau (17 %)				
Configurer des zones DNS.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer les zones principales et secondaires, configurer les zones de stub, configurer le transfert conditionnel, configurer le stockage de transfert conditionnel et de zone dans Active Directory, configurer la délégation de zone, configurer les paramètres de transfert de zone, configurer les paramètres de notification	Mod 2	Leçons 1/3/4	Mod 2 Ex 2/4
Configurer les enregistrements DNS.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : créer et configurer les enregistrements de ressource DNS (notamment les enregistrements A, AAAA, PTR, SOA, NS, SRV, CNAME et MX), configurer le nettoyage de zone, configurer les options d'enregistrement (notamment la durée de vie (TTL) et le poids), configurer le tourniquet, configurer les mises à jour dynamiques sécurisées	Mod 2	Leçons 2/5	Mod 2 Ex 1/3
Configurer l'accès VPN et le routage.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : installer et configurer le rôle d'accès à distance, implémenter la traduction d'adresses réseau (NAT), configurer les paramètres VPN, configurer les paramètres d'accès à distance pour les utilisateurs, configurer le routage	Mod 7	Leçons 1/2/3/4	Mod 7 Atelier A Ex 1/2
Configurer DirectAccess.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : implémenter la configuration requise des serveurs, implémenter la configuration des clients, configurer le DNS pour l'accès direct, configurer les certificats pour l'accès direct	Mod 7	Leçon 5	Mod 7 Atelier B Ex 1/2/3

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Examen 70-411 : Administration de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer une infrastructure de serveur de stratégie (14 %)				
Configurer le serveur NPS (Network Policy Server).	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer plusieurs infrastructures de serveur RADIUS, configurer les clients RADIUS, gérer les modèles RADIUS, configurer la gestion de comptes RADIUS, configurer les certificats	Mod 8	Leçons 3/4	Mod 8 Ex 2
Configurer les stratégies NPS	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer les stratégies de demande de connexion, configurer les stratégies réseau pour les clients VPN (allocation de liaisons multiples et de bande passante, filtres IP, chiffrement, adressage IP), gérer les modèles NPS, importer et exporter les stratégies NPS	Mod 6	Leçon 2	
		Mod 8	Leçon 1/2	Mod 8 Ex 1
Configurer la protection d'accès réseau (NAP).	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer les programmes de validation d'intégrité système (SHV), configurer les stratégies de contrôle d'intégrité, configurer la contrainte de mise en conformité NAP à l'aide des protocoles DHCP et VPN, configurer l'isolement et la mise à jour des ordinateurs non compatibles à l'aide des protocoles DHCP et VPN, configurer les paramètres de client NAP	Mod 9	Leçons 1/2/3/4	Mod 9 Ex 1/2/3

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Examen 70-411 : Administration de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer et gérer Active Directory (19 %)				
Configurer l'authentification de service.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : créer et configurer les comptes de service, créer et configurer les comptes de service gérés de groupe, créer et configurer les comptes de service gérés, configurer la délégation Kerberos, gérer les noms de principal de service (SPN)	Mod 4	Leçons 1/2/3	Mod 4 Ex 1/2
Configurer les contrôleurs de domaine.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer la mise en cache de l'appartenance au groupe universel (UGMC), transférer et prendre les maîtres d'opérations, installer et configurer un contrôleur de domaine en lecture seule (RODC), configurer le clonage de contrôleur de domaine	Mod 3	Leçons 1/2/3	Mod 3 Ex 1/2
Maintenir Active Directory.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : sauvegarder Active Directory et SYSVOL, gérer Active Directory hors connexion, optimiser une base de données Active Directory, nettoyer les métadonnées, configurer les instantanés Active Directory, exécuter la récupération de niveau d'objet et de conteneur, effectuer la restauration d'Active Directory	Mod 3	Leçons 1/3/4/5	Mod 3 Ex 2/3
Configurer les stratégies de compte.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer la stratégie de mot de passe d'utilisateur du domaine, configurer et appliquer les objets de paramètres de mot de passe (PSO), déléguer la gestion des paramètres de mot de passe, configurer la stratégie de mot de passe de l'utilisateur local, configurer les paramètres de verrouillage de compte	Mod 4	Leçons 1/2/3	Mod 4 Ex 1

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Examen 70-411 : Administration de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer et gérer la stratégie de groupe (18 %)				
Configurer le traitement de la stratégie de groupe.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer l'ordre et la priorité de traitement, configurer le blocage de l'héritage, configurer les stratégies appliquées, configurer le filtrage de la sécurité et le filtrage WMI, configurer le traitement par boucle, configurer et gérer le traitement des liaisons lentes, configurer le comportement de l'extension côté client (CSE)	Mod 5	Leçons 1/3/4	Mod 5 Ex 1/2
Configurer les paramètres de stratégie de groupe.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer les paramètres (notamment les paramètres d'installation des logiciels, de redirection de dossiers, de scripts et les paramètres de modèles d'administration), importer les modèles de sécurité, importer le fichier de modèles d'administration personnalisés, convertir les modèles d'administration à l'aide de l'outil de migration ADMX, configurer les filtres de propriété pour les modèles d'administration	Mod 6	Leçon 1/2/4	Mod 6 Ex 2
Gérer les objets de stratégie de groupe.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : sauvegarder, importer, copier et restaurer les objets de stratégie de groupe, créer et configurer la table de migration, réinitialiser les objets de stratégie de groupe par défaut, déléguer la gestion des stratégies de groupe	Mod 5	Leçon 2	Mod 5 Ex 4

Examen 70-411 : Administration de Windows Server® 2012				
Objectifs de l'examen		**Contenu du cours**		
Configurer les préférences de stratégie de groupe.	Cet objectif peut inclure, mais n'est pas limité aux éléments suivants : configurer les paramètres de préférences de stratégie de groupe, notamment les paramètres des imprimantes, des mappages de lecteur réseau, des options d'alimentation, les paramètres de Registre personnalisé, les paramètres du panneau de configuration, les paramètres d'Internet Explorer, le déploiement des fichiers et dossiers, et le déploiement des raccourcis, configurer le ciblage au niveau de l'élément	Mod 6	Leçons 1/2/3	Mod 6 Ex 1

Important : suivre ce cours ne vous préparera pas à passer les examens de certification associés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Suivre ce cours ne garantit pas que vous réussirez automatiquement n'importe quel examen de certification. En plus de suivre ce cours, vous devez également :

- posséder une expérience réelle et pratique de l'administration, de la gestion et de la maintenance d'une infrastructure Windows Server 2012 ;
- suivre des études supplémentaires extérieures au contenu du présent manuel.

Il se peut que des ressources d'étude et de préparation supplémentaires soient également disponibles pour vous permettre de préparer cet examen. Vous trouverez plus de détails à ce sujet à l'adresse suivante : http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-411#tab3

Vous devez vous familiariser avec le profil des stagiaires et les connaissances requises pour l'examen afin d'être suffisamment préparé pour cet examen de certification. Le profil complet des stagiaires pour cet examen est disponible à l'adresse URL suivante : http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-411#tab1

Le tableau de mappage examen/cours présenté ci-dessus est exact au moment de l'impression, toutefois il pourra faire l'objet de modifications à tout moment et la société Microsoft ne pourra pas être tenue pour responsable d'éventuelles incohérences entre la version publiée ici et la version accessible en ligne, et ne donnera aucune notification quant à de telles modifications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Documents de cours

Votre kit de cours contient les documents suivants :

- ***Manuel du cours*** 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** : vous guident dans les objectifs de formation et fournissent les points clés essentiels pour un apprentissage en classe réussi.
  - **Ateliers pratiques** : fournissent une plateforme qui vous permettra de mettre en application les connaissances et compétences acquises dans le module.
  - **Contrôles des acquis et éléments à retenir** : fournissent une documentation de référence pratique qui favorise la mémorisation des connaissances et compétences.
  - **Corrigés des ateliers pratiques** : fournissent des instructions pas à pas que vous pourrez consulter à tout moment au cours d'un atelier pratique.



Contenu d'accompagnement du cours sur le site http://www.microsoft.com/learning/companionmoc : Contenu numérique facile à parcourir et dans lequel il est possible d'effectuer des recherches, qui comprend de précieuses ressources en ligne intégrées, proposées en complément du Manuel du cours.

- **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 contrôle des acquis des ateliers pratiques, ainsi que des sections sur les contrôles des acquis et éléments à retenir, contenant les questions et réponses de contrôle des acquis, les méthodes conseillées, des astuces et réponses sur les problèmes courants et la résolution des problèmes, des scénarios et problèmes concrets et leurs réponses.
- **Ressources** : incluent des ressources supplémentaires présentées par catégories qui vous donnent un accès immédiat à du contenu utile et à jour disponible sur TechNet, MSDN® et Microsoft Press®.



Fichiers de cours destinés aux stagiaires à l'adresse http://www.microsoft.com/france/formation/companionmocc *:* incluent le fichier exécutable à extraction automatique Allfiles.exe, lequel contient les fichiers requis pour les ateliers pratiques et démonstrations.

- ***Évaluation du cours*** À la fin du cours, vous aurez l'occasion de remplir une fiche d'évaluation en ligne pour faire part de vos commentaires sur le cours, le centre de formation et l'instructeur.
  - Pour adresser d'autres commentaires ou remarques sur le cours, envoyez 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'ordinateurs virtuels

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

Configuration des ordinateurs virtuels

Dans ce cours, vous utiliserez Hyper-V® pour effectuer les ateliers pratiques.

Important À la fin de chaque atelier pratique, vous devez fermer l'ordinateur virtuel et vous ne devez enregistrer aucune modification. 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 montre le rôle de chaque ordinateur virtuel utilisé dans ce cours.

Ordinateur virtuel	Rôle
22411B-LON-DC1	Contrôleur de domaine Windows Server 2012 pour le domaine Adatum.com
22411B-LON-CL1	Ordinateur client Windows 8 et dans le domaine Adatum.com
22411B-LON-CL2	Ordinateur client Windows 8 et dans le domaine Adatum.com
22411B-LON-SVR1	Windows Server 2012 dans le domaine Adatum.com
22411B-LON-SVR3	Aucun système d'exploitation installé
22411B-LON-SVR4	Ordinateur serveur Windows Server 2012 dans le domaine Adatum.com
22411B-LON-RTR	Ordinateur serveur Windows Server 2012 dans le domaine Adatum.com



Configuration logicielle

Les logiciels suivants sont installés sur chaque ordinateur virtuel :

- Le Moniteur réseau 3.4 est installé sur LON-SVR2.

Fichiers du cours

Des fichiers d'ateliers pratiques sont associés aux ateliers pratiques de ce cours. Ces fichiers se trouvent dans le dossier E:\FichiersAtelier\AtelierXX sur NYC-DC1.

Configuration de la classe

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

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Niveau des éléments matériels du cours

Pour garantir une expérience 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.

- Niveau matériel 6 avec 8 gigaoctets (Go) de mémoire vive (RAM)

Navigation dans Windows Server 2012

Si vous n'êtes pas familier de l'interface utilisateur de Windows Server 2012 ou Windows 8, les informations suivantes vous aideront à vous orienter dans la nouvelle interface.

- Se connecter et Se déconnecter remplacent Connexion et Déconnexion.
- Les outils d'administration sont accessibles à partir du menu Outils du Gestionnaire de serveur.
- Déplacez la souris dans l'angle inférieur droit du bureau pour ouvrir un menu comportant :
    - Paramètres : comprend le Panneau de configuration et Alimentation
    - Menu Démarrer : permet d'accéder à des applications
    - Rechercher : permet de rechercher des applications, des paramètres et des fichiers

Les touches de raccourci suivantes vous seront peut-être également utiles :

- Windows : ouvre le menu Démarrer
- Windows+C : ouvre le même menu que le déplacement de la souris dans l'angle inférieur droit
- Windows+I : ouvre Paramètres
- Windows+R : ouvre la fenêtre Exécuter

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 1

Déploiement et maintenance des images de serveur

Table des matières :

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

Leçon 1 : Vue d'ensemble des services de déploiement Windows **1-2**

Leçon 2 : Implémentation d'un déploiement avec les services de déploiement Windows **1-9**

Leçon 3 : Administration des services de déploiement Windows **1-16**

Atelier pratique : Utilisation des services de déploiement Windows pour déployer Windows Server 2012 **1-23**

Contrôle des acquis et éléments à retenir **1-29**

Vue d'ensemble du module

Les organisations de plus grande taille ont besoin de technologies de déploiement qui puissent réduire ou éliminer l'intervention de l'utilisateur pendant le processus de déploiement. Vous pouvez utiliser le rôle Services de déploiement dans Windows Server® 2012 et Windows Server 2008 pour prendre en charge les déploiements à volume élevé de type Lite Touch et Zero Touch. Ce module explore les fonctionnalités des services de déploiement Windows et explique comment les utiliser pour effectuer des déploiements de type Lite Touch.

Objectifs

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

- Décrire les principales fonctionnalités et caractéristiques des services de déploiement Windows.
- Configurer les services de déploiement Windows dans Windows Server 2012.
- Exécuter des déploiements avec les services de déploiement Windows.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble des services de déploiement Windows

Les services de déploiement Windows vous permettent de déployer des systèmes d'exploitation Windows®. Pour déployer ces systèmes d'exploitation sur de nouveaux ordinateurs, vous pouvez utiliser une installation des services de déploiement Windows à partir du réseau. Cela signifie qu'il n'est pas nécessaire d'être physiquement présent sur chaque ordinateur. En outre, il n'est pas nécessaire d'installer chaque système d'exploitation depuis un support local. Les services de déploiement Windows répondent donc parfaitement aux besoins de déploiement des grandes organisations.

Objectifs de la leçon

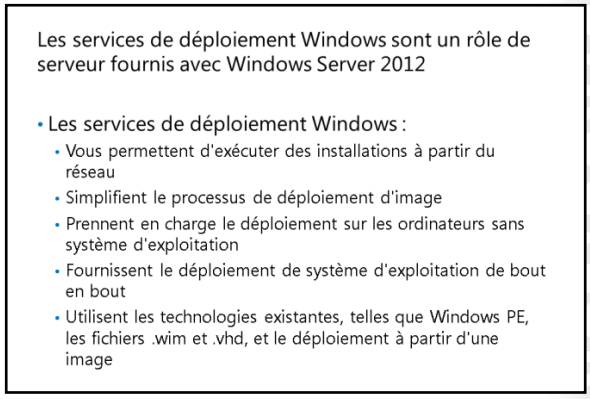
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire le fonctionnement des services de déploiement Windows ;
- décrire les composants des services de déploiement Windows ;
- décrire les avantages des services de déploiement Windows ;
- déterminer comment utiliser les services de déploiement Windows pour prendre en charge divers scénarios de déploiement.

Que sont les services de déploiement Windows ?

Les services de déploiement Windows sont un rôle serveur fourni avec Windows Server 2012. Leurs fonctions sont les suivantes :

- Ils vous permettent d'exécuter des installations à partir du réseau.
- Ils simplifient le processus de déploiement d'image.
- Ils prennent en charge le déploiement sur les ordinateurs sans système d'exploitation.
- Ils fournissent des solutions de déploiement de bout en bout pour les ordinateurs client et serveur.
- Ils utilisent des technologies existantes, telles que l'Environnement de préinstallation Windows (Windows PE), un fichier d'image système Windows (.wim), des fichiers d'image virtuelle de disque dur (.vhd) et le déploiement basé sur des images.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les services de déploiement Windows permettent le déploiement automatisé de systèmes d'exploitation Windows. Vous pouvez complètement automatiser le déploiement des systèmes d'exploitation suivants :

- Windows XP
- Windows Server 2003
- Windows Vista® avec Service Pack 1 (SP1)
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows Server 2012

Les services de déploiement Windows permettent de créer, stocker et déployer des images d'installation des systèmes d'exploitation pris en charge, et prennent en charge les fichiers image .wim et .vhd. Le déploiement peut désormais être en monodiffusion ou en multidiffusion. La multidiffusion offre une gestion plus efficace du trafic réseau que consomme le processus de déploiement. Cela peut accélérer le déploiement sans affecter défavorablement d'autres services réseau.

Systèmes d'exploitation avec composants

Les services de déploiement Windows s'intègrent étroitement avec Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8 et Windows Server 2012. Un parfait exemple de cette intégration est la conception de ces systèmes d'exploitation avec des composants. Ces systèmes d'exploitation consistent en éléments autodescriptifs, appelés composants. L'autodescription se rapporte au fait que les éléments contiennent un manifeste qui répertorie les différentes options de configuration que vous pouvez définir pour chaque composant. Vous pouvez voir les fonctionnalités et les configurations pour chaque composant. Les mises à jour, les Service Packs et les modules linguistiques sont des composants qui sont appliqués sur les systèmes d'exploitation qui peuvent être divisés.

Les pilotes sont également considérés comme des composants distincts et configurables. Le principal avantage de ces composants est de pouvoir installer des pilotes, tels que des correctifs logiciels ou des Service Packs, sur un système d'exploitation hors connexion. Au lieu de mettre à jour des images complètes chaque fois qu'une nouvelle mise à jour, un nouveau Service Pack ou un nouveau pilote est disponible, vous pouvez installer ces composants dans l'image hors connexion pour que Windows les applique quand vous déployez l'image.

Lors du déploiement des images sur le disque dur d'un nouvel ordinateur, le système reçoit l'image disque de base avec chacun des composants ajoutés, et ce avant que le système ne démarre pour la première fois.

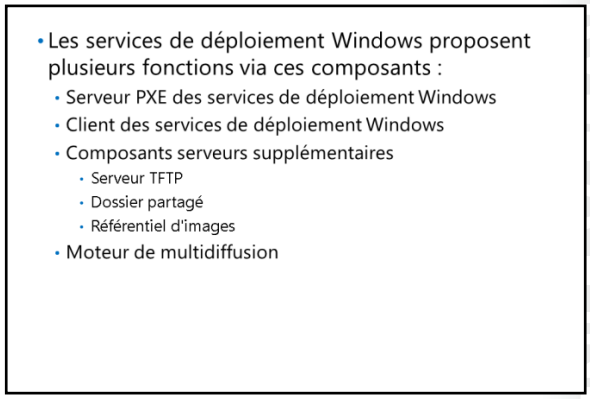
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si votre organisation est multilingue ou internationale, vous pouvez utiliser la nature indépendante de la langue des systèmes d'exploitation Windows les plus récents. Le nombre d'images à maintenir est encore réduit parce qu'il n'y a plus de versions localisées. Certaines versions de systèmes d'exploitation Windows sont limitées au nombre de modules linguistiques. Vous pouvez à tout moment ajouter ou supprimer des modules linguistiques d'un système en fonction de vos besoins, et ce sans modifier autrement l'installation.

Si vous devez prendre en charge plusieurs langues, ajoutez tous les modules linguistiques nécessaires à votre fichier de déploiement .wim puis activez-les selon vos besoins, sur tous les ordinateurs ou certains seulement.

Composants des services de déploiement Windows

Les services de déploiement Windows fournissent un certain nombre de fonctions distinctes via des composants identifiables.



Serveur PXE (Pre-Boot Execution Environment) des services de déploiement Windows

Le serveur PXE (Pre-Boot Execution Environment) fournit les fonctions suivantes :

- Il se lie aux interfaces réseau.
- Il détecte les requêtes PXE entrantes.
- Il formate les paquets de réponse du protocole DHCP (Dynamic Host Configuration Protocol).

Client des services de déploiement Windows

Le client des services de déploiement Windows fournit une interface graphique basée sur l'interface graphique d'installation de Windows Server. Elle établit un canal de communication avec le serveur des services de déploiement Windows et récupère une liste d'images d'installation sur ce serveur. En outre, le client des services de déploiement Windows fournit des informations d'état de l'ordinateur cible pendant le déploiement.

Composants serveur

Les composants serveurs supplémentaires comprennent un serveur TFTP (Trivial File Transfer Protocol) qui permet aux clients effectuant le démarrage à partir du réseau de charger une image de démarrage dans la mémoire. S'y ajoutent : un référentiel d'images contenant des images de démarrage, des images d'installation et les fichiers nécessaire à la prise en charge du démarrage réseau, ainsi qu'un dossier partagé pour héberger les images d'installation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Moteur de multidiffusion

Avec les services de déploiement Windows, la transmission d'images de système d'exploitation volumineuses sur le réseau est plus efficace. Le transfert de fichiers de plusieurs gigaoctets sur le réseau crée toutefois un trafic réseau important. Avec la nouvelle fonctionnalité de multidiffusion, vous pouvez encore réduire le coût réseau de l'utilisation des services de déploiement Windows.

Avec la multidiffusion, le serveur envoie les données en une seule fois, et plusieurs cibles reçoivent les mêmes données. Si vous déployez une image sur plusieurs cibles, cette méthode peut réduire le trafic réseau à une fraction du nombre équivalent de plusieurs transmissions en monodiffusion. Les services de déploiement Windows fournissent deux types de multidiffusion :

- La diffusion planifiée. Il existe deux façons de configurer une diffusion planifiée :
  - Nombre de clients. Lorsque vous spécifiez un nombre de clients, le serveur attend que le nombre défini de clients connectés soit atteint, puis il commence à envoyer les informations.
  - Limite dans le temps. Lorsque vous spécifiez une limite dans le temps, le serveur attend jusqu'au moment spécifié puis commence le déploiement vers les ordinateurs client connectés.

  Bien que la diffusion planifiée offre une utilisation plus efficace du réseau, elle nécessite néanmoins un certain travail, chaque ordinateur cible devant être connecté, mis en marche et mis en file d'attente.
- Diffusion automatique. Une cible peut rejoindre une diffusion automatique à tout moment, et le serveur répète la transmission tant que des cibles sont connectées. Si la cible commence recevoir l'image en cours de transmission, ou s'il lui manque une certaine partie de l'image, elle demeure connectée et rassemble les parties manquantes du fichier quand le serveur redémarre la transmission.

  Question : Quel est l'avantage de la multidiffusion sur la monodiffusion dans les scénarios de déploiements importants ?

Pourquoi utiliser les services de déploiement Windows ?

N'importe quelle organisation qui souhaite réduire les interventions requise de la part de l'administrateur pendant le déploiement de Windows Server devrait utiliser les services de déploiement Windows. En raison de leur capacité à prendre en charge le déploiement via le réseau, potentiellement sans intervention de l'utilisateur, les services de déploiement Windows permettent aux organisations de créer un environnement plus autonome et plus efficace pour installer Windows. Prenez les scénarios suivants :

Prenez les scénarios suivants :

1. Dans un petit réseau se composant d'un serveur unique et d'environ 25 ordinateurs de Windows XP, vous souhaitez accélérer le processus de mise à niveau des ordinateurs client vers Windows 8

2. Une organisation moyenne souhaite déployer plusieurs serveurs dans des filiales géographiquement dispersées. Envoyer du personnel informatique expérimenté sur chaque site pour déployer les serveurs s'avérerait long et coûteux

Scénario 1

Dans un petit réseau constitué d'un serveur unique et d'environ 25 ordinateurs sous Windows XP, vous pourriez utiliser les services de déploiement Windows pour accélérer le processus de mise à niveau des ordinateurs client vers Windows 8. Une fois que vous avez installé et configuré le rôle serveur des services de déploiement Windows sur le serveur unique, vous pouvez utiliser les services de déploiement Windows pour effectuer les tâches suivantes :

1. Ajouter boot.wim (à partir du dossier de sources sur le support de Windows Server 2012) comme image de démarrage dans les services de déploiement Windows.
2. Ajouter install.wim (à partir du dossier de sources sur le support de Windows 8) comme image d'installation.
3. Créer une image de capture à partir de l'image de démarrage que vous avez précédemment ajoutée.

Remarque : Une image de capture est une image de démarrage modifiée qui contient les éléments nécessaires pour capturer une image de fichier WIM à partir d'un ordinateur de référence configuré.

4. Démarrer votre ordinateur de référence à partir du réseau en utilisant l'environnement PXE.
5. Exécuter une installation standard de Windows 8 à partir de l'image install.wim.
6. Installer les applications de productivité et les applications personnalisées de la manière prescrite sur l'ordinateur de référence.
7. Généraliser l'ordinateur de référence avec l'outil de préparation système (Sysprep).
8. Redémarrer l'ordinateur de référence à partir du réseau en utilisant l'environnement PXE.
9. Vous connecter à l'image de capture que vous avez créée, l'utiliser pour capturer le système d'exploitation local et le télécharger à nouveau sur le serveur des services de déploiement Windows.
10. Démarrer chacun des ordinateurs cibles existants à partir du réseau en utilisant l'environnement PXE, et les connecter à l'image de démarrage appropriée.
11. Sélectionner l'image d'installation personnalisée.
12. Le déploiement commence.

Dans ce scénario, les avantages pour l'organisation sont les suivants :

- Une image d'ordinateur de bureau standardisée.
- Un déploiement rapide de chaque ordinateur avec une intervention limitée de l'installateur.

Cette solution ne serait toutefois pas adaptée à de plus grands déploiements, car il faut que l'installateur commence le déploiement sur l'ordinateur cible. En outre, l'installateur est requis pour sélectionner une partition de disque sur laquelle installer l'image d'installation sélectionnée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Scénario 2

Dans le deuxième scénario, une organisation de taille moyenne à importante souhaite déployer plusieurs serveurs dans des filiales géographiquement dispersées. Envoyer du personnel informatique expérimenté sur chaque site pour déployer les serveurs s'avérerait long et coûteux.

Grâce aux services de déploiement Windows, le personnel informatique peut solutionner ce problème :

1. Ajouter boot.wim (à partir du support de Windows Server 2012) comme image de démarrage dans les services de déploiement Windows.
2. Ajouter install.wim (à partir du support de Windows Server 2012) comme image d'installation.
3. Créer une image de capture.
4. Démarrer l'ordinateur de référence à partir du réseau.
5. Exécuter une installation standard de Windows Server 2012 à partir de l'image install.wim.
6. Personnaliser l'ordinateur de référence selon les besoins.
7. Généraliser l'ordinateur de référence.
8. Redémarrer l'ordinateur de référence.
9. Capturer le système d'exploitation Windows de référence et le télécharger à nouveau sur le serveur des services de déploiement Windows.
10. Configurer les comptes d'utilisateur AD DS (Active Directory® Domain Services) ; Il s'agit de la préconfiguration des comptes d'ordinateur.
11. Utiliser l'Assistant Gestion d'installation (SIM) dans le Kit d'installation automatisée Windows (Windows ADK) pour créer un fichier de réponses sans assistance.
12. Configurer le fichier de réponses pour l'utiliser avec l'image d'installation capturée sur les services de déploiement Windows.
13. Configurer une stratégie de format de nom personnalisée dans les services de déploiement Windows, de sorte que chaque ordinateur serveur reçoive un nom d'ordinateur approprié pendant le déploiement.
14. Configurer les services de déploiement Windows pour utiliser une image de démarrage par défaut.
15. Configurer les services de déploiement Windows pour répondre aux requêtes PXE et lancer le déploiement de l'image d'installation automatiquement.
16. Démarrer chacun des ordinateurs cibles à partir du réseau.

Remarque : Pour éviter une boucle de démarrage, il est recommandé de configurer le système BIOS de l'ordinateur pour commencer à partir du disque dur puis du réseau. Pour plus d'informations sur comment éviter une boucle de démarrage, reportez-vous au guide de déploiement des services de déploiement Windows.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

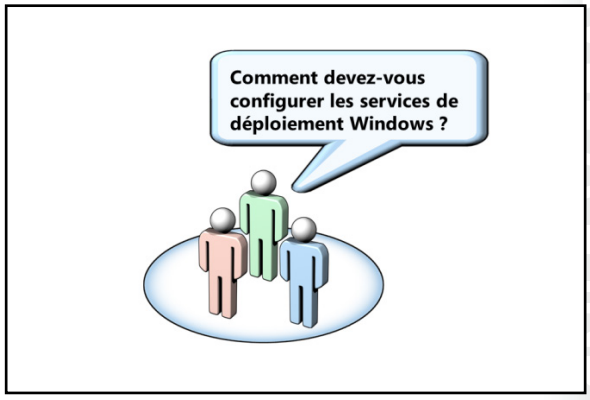
Dans ce scénario, les avantages pour l'organisation sont les suivants :

- Des versions de serveur standardisées.
- Une connexion automatique au domaine après le déploiement.
- L'attribution automatique de noms aux ordinateurs.
- Peu ou pas d'interventions de l'installateur.

La solution n'implémente pas des transmissions par multidiffusion et n'utilise pas la référence PXE. Ces technologies pourraient également être utilisées pour aider à gérer le trafic réseau pendant le déploiement.

Discussion : Procédure d'utilisation des services de déploiement Windows

Les services de déploiement Windows peuvent être utiles pour beaucoup de scénarios de déploiement impliquant des systèmes d'exploitation Windows.



Question : Le personnel informatique de la société A. Datum Corporation est sur le point de déployer Windows Server 2012 dans diverses filiales. Les informations suivantes ont été fournies au personnel informatique par la direction :

- La configuration des serveurs des différentes filiales doit être assez cohérente.
- Il n'est pas nécessaire de mettre à niveau les paramètres des serveurs existants, car ce sont de nouvelles succursales sans infrastructure informatique en place.
- L'automatisation du processus de déploiement est importante, car il y a beaucoup de serveurs à déployer.

Comment utiliseriez-vous les services de déploiement Windows pour optimiser le déploiement ?

Question : La société A. Datum Corporation souhaite déployer plusieurs douzaines de nouveaux serveurs à son siège social. Ces serveurs seront installés avec Windows Server 2012. Les informations suivantes ont été fournies au personnel informatique par la direction :

- La configuration des divers serveurs peut varier légèrement ; il y a deux configurations de serveur de base : installation serveur complète et installation serveur minimale.
- La gestion du trafic réseau est cruciale, car le réseau est presque à pleine capacité.

Comment recommanderiez-vous au personnel de chez A. Datum de procéder pour le déploiement ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2

Implémentation d'un déploiement avec les services de déploiement Windows

Bien que les services de déploiement Windows ne sont pas compliqués à installer et configurer, il est important que vous compreniez la constitution de leurs composants et comment les configurer correctement. Ce faisant, vous veillerez à ce qu'ils fournissent le niveau approprié d'automatisation du déploiement et qu'ils répondent aux besoins de déploiement de votre organisation. Une fois que vous installez et configurez les services de déploiement Windows, vous devez comprendre comment les utiliser et utiliser les outils associés pour créer, gérer et déployer des images sur des ordinateurs dans votre organisation.

Objectifs de la leçon

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

- Décrivez les composants des services de déploiement Windows.
- Expliquez comment installer et configurer les services de déploiement Windows.
- Expliquez le processus d'utilisation des services de déploiement Windows pour déployer Windows Server.

Fonctionnement des composants des services de déploiement Windows

Lorsque vous déployez le rôle serveur des services de déploiement Windows, vous pouvez choisir entre deux options de configuration. Vous pouvez choisir la configuration par défaut, qui déploie les services pour les rôles du serveur de déploiement et du serveur de transport, ou vous pouvez choisir de déployer seulement le service pour le rôle du serveur de transport. Dans ce deuxième scénario, le service pour le rôle du serveur de déploiement fournit le serveur d'image ; le serveur de transport ne fournit pas la fonctionnalité d'acquisition d'images.

Les conditions préalables à l'installation des services de déploiement Windows incluent :

- AD DS
- DHCP
- DNS
- Volume NTFS

Utilisez le kit de déploiement automatisé Windows pour créer des fichiers de réponse pour le déploiement automatisé

Le serveur de déploiement active une solution de déploiement de bout en bout, alors que le serveur de transport fournit une plateforme que vous utilisez pour créer une solution de déploiement personnalisée multidiffusion.

Le tableau suivant compare les deux services de rôle.

Composant Serveur	Serveur de déploiement	Serveur de transport
Configuration requise	AD DS, DHCP et DNS (Domain Name System)	Pas d'impératifs d'infrastructure
PXE	Utilise le fournisseur PXE par défaut	Vous devez créer un fournisseur PXE
Serveur d'image	Inclut le serveur d'image des services de déploiement Windows	Aucun
Transmission	Monodiffusion et multidiffusion	Multidiffusion seulement
Gestion	Les outils de ligne de commande WDSutil.exe et le composant logiciel enfichable MMC (Microsoft® Management Console) des services de déploiement Windows	WDSutil.exe seulement
Ordinateur cible.	Utilise le client des services de déploiement Windows ou l'outil Wdsmcast.exe	Wdsmcast.exe seulement

Fonctionnalité du serveur de transport

Vous pouvez utiliser le serveur de transport pour fournir les fonctionnalités suivantes :

- Démarrage à partir du réseau. Le serveur de transport fournit seulement un auditeur PXE ; c'est le composant qui écoute et accepte le trafic entrant. Vous devez écrire un fournisseur PXE personnalisé pour utiliser un serveur de transport pour démarrer un ordinateur à partir du réseau.
- Multidiffusion. Dans les services de déploiement Windows, le serveur de multidiffusion consiste en un fournisseur de multidiffusion et en un fournisseur de contenu :
    - Fournisseur de multidiffusion. Transmet les données sur le réseau.
    - Fournisseur de contenu. Interprète les données et les transmet au fournisseur de multidiffusion. Le fournisseur de contenu est installé avec les serveurs de transport et le serveur de déploiement, et peut être utilisé pour transférer n'importe quel type de fichier, bien qu'il ait une connaissance spécifique du format de fichier image .wim.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration requise pour l'installation des services de déploiement Windows

La configuration requise spécifique à l'installation du rôle des services de déploiement Windows dépend de si vous déployez un serveur de déploiement ou seulement un serveur de transport.

Pour installer un serveur de déploiement, votre réseau et serveur cible doivent répondre aux exigences suivantes.

- AD DS. Votre serveur des services de déploiement Windows doit être soit membre d'un domaine AD DS, soit un contrôleur de domaine pour un domaine AD DS.

Remarque : Le domaine et les niveaux fonctionnels de la forêt AD DS ne sont pas pertinents ; toutes les configurations de domaine et de forêt prennent en charge les services de déploiement Windows.

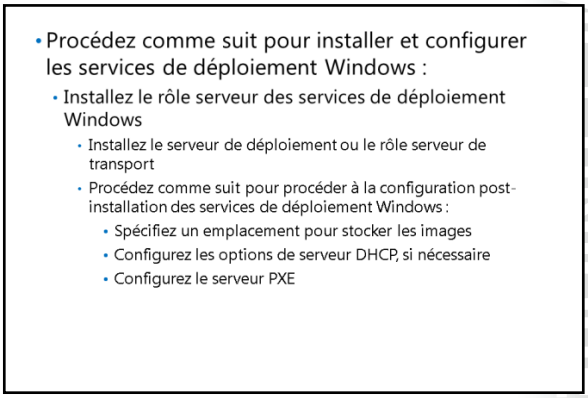
- DHCP. Vous devez avoir un serveur DHCP fonctionnel avec une étendue active sur le réseau. C'est parce que les services de déploiement Windows utilisent l'environnement PXE, qui dépend du protocole DHCP pour allouer les configurations IP.
- DNS. Vous devez avoir un serveur DNS actif sur le réseau, de sorte que les ordinateurs client puissent localiser les services requis pour le déploiement.
- Volume de système de fichiers NTFS. Le serveur qui exécute les services de déploiement Windows requiert un volume NTFS pour la banque d'images. Les services de déploiement Windows accèdent à la banque d'image dans le contexte de l'utilisateur qui a ouvert une session. Par conséquent, les comptes d'utilisateur de déploiement doivent avoir des autorisations suffisantes sur les fichiers image.

Bien qu'il ne s'agisse pas d'une configuration requise, Windows ADK vous permet de simplifier le processus de création de fichiers de réponses (unattend.xml) pour une utilisation avec les déploiements automatisés des services de déploiement Windows.

Remarque : Pour installer le rôle des services de déploiement Windows, vous devez être membre du groupe Administrateurs locaux sur le serveur. Pour initialiser le serveur, vous devez être membre du groupe Utilisateurs du domaine.

Installation et configuration des services de déploiement Windows

Une fois que votre infrastructure réseau satisfait aux conditions requises, vous pouvez installer le rôle serveur des services de déploiement Windows.



Installation du rôle serveur des services de déploiement Windows

Utilisez les étapes générales suivantes pour fournir de l'aide sur l'installation du rôle.

1. Ouvrez le Gestionnaire de serveurs, puis ajoutez le rôle serveur des services de déploiement Windows.

2. Choisissez si vous le souhaitez d'installer le service pour le rôle du serveur de déploiement (qui inclut le rôle du serveur de transport) ou juste le service pour le rôle du serveur de transport.
3. Suivez l'Assistant pour installer le rôle requis.

Configuration initiale des services de déploiement Windows

Une fois les services de déploiement Windows installés, ouvrez-les à partir des outils d'administration, puis utilisez l'aide générale suivante pour les configurer.

1. Sélectionnez votre serveur dans la console des services de déploiement Windows et lancez l'Assistant de configuration.
2. Spécifiez un emplacement pour enregistrer les images. Cet emplacement :
   - Doit être une partition NTFS.
   - Doit être assez grand pour accueillir les images de déploiement que vous prévoyez utiliser.
   - Devrait être un disque physique distinct de celui sur lequel est installé le système d'exploitation afin d'optimiser les performances.
3. Si le rôle du serveur DHCP est hébergé sur le serveur des services de déploiement Windows avec d'autres services, vous devez :
   - Empêcher le serveur PXE d'écouter sur le port 67 du protocole UDP (User Datagram Protocol) ; ce port est utilisé par le protocole DHCP.
   - Configurer l'option DHCP 60 sur PXEClient ; cela permet au client PXE de localiser le port du serveur des services de déploiement Windows.

 **Remarque :** Si vous déployez les services de déploiement Windows sur un serveur qui exécute déjà le rôle du serveur DHCP, ces modifications sont faites automatiquement. Si vous ajoutez ultérieurement le rôle du serveur DHCP à un serveur de déploiement Windows, vous devez vous assurer d'apporter lesdites modifications.

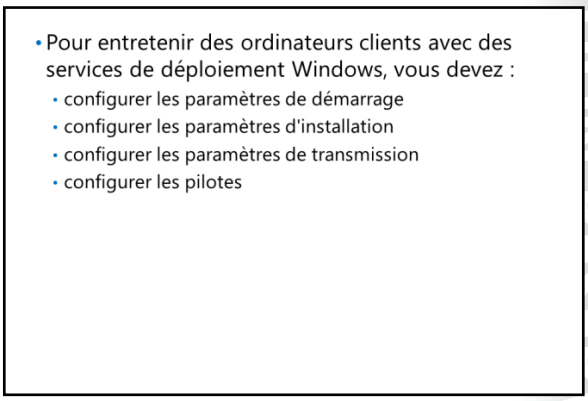
4. Déterminez comment vous souhaitez que le serveur PXE réponde aux clients :
   - Par défaut, le serveur PXE ne répond à aucun client ; c'est utile quand vous effectuez la configuration initiale des services de déploiement Windows, car vous n'avez encore aucune image disponible pour des clients.
   - Alternativement, vous pouvez choisir de configurer le serveur PXE pour :
     - Répondre aux ordinateurs client connus ; ce sont des ordinateurs que vous avez préconfigurés.
     - Répondre à tous les ordinateurs client, que vous les ayez préconfigurés ou non ; si vous sélectionnez cette option, vous pouvez en outre définir qu'une approbation d'administrateur soit requise pour les ordinateurs inconnus. Tout en attendant l'approbation, les ordinateurs client sont maintenus dans une file d'attente.

 **Remarque :** S'il y a lieu, vous pouvez reconfigurer ces paramètres après avoir terminé la configuration initiale.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion des déploiements avec les services de déploiement Windows

Une fois que vous avez installé et configuré les services de déploiement Windows, vous pouvez les préparer pour s'occuper des déploiements clients, ce qui implique les procédures suivantes.



Configuration des paramètres de démarrage

Vous devez exécuter plusieurs tâches de configuration pour configurer les paramètres de démarrage sur le serveur qui héberge les services de déploiement Windows.

- Ajoutez des images de démarrage. Une image de démarrage est une image Windows PE que vous utilisez pour démarrer un ordinateur et installer l'image d'installation. En général, vous utilisez le fichier boot.wim sur le DVD de Windows Server 2012, dans le dossier \sources. Vous pouvez également décider de créer une image de capture, qui est un type spécifique d'image de démarrage que vous pouvez utiliser pour capturer un système d'exploitation actuellement installé sur un ordinateur de référence.
- Configurez la stratégie de démarrage PXE pour les clients connus et inconnus. Cette stratégie détermine le comportement requis de l'installateur pendant la partie initiale du déploiement. Par défaut, tant la stratégie pour les ordinateurs connus que celle pour les ordinateurs inconnus exigent de l'installateur qu'il appuie sur F12 pour se connecter au serveur d'image des services de déploiement Windows. S'il ne le fait pas, l'ordinateur utilise les paramètres du BIOS pour déterminer une autre méthode de démarrage, par exemple via le disque dur ou un CD-ROM. Au lieu de cette valeur par défaut, vous pouvez configurer les options suivantes :
    - Toujours continuer le démarrage PXE. Cette option permet à l'ordinateur de poursuivre le processus de déploiement sans intervention de l'installateur.
    - Continuer le démarrage PXE sauf si l'utilisateur appuie sur Échap. Cette option donne à l'installateur la possibilité d'annuler le déploiement.
- Configurez une image de démarrage par défaut. Si vous avez plusieurs images de démarrage, par exemple pour prendre en charge plusieurs plates-formes,vous pouvez configurer une image de démarrage par défaut pour chacune d'elles. Cette image est sélectionnée après un délai d'expiration sur l'ordinateur client PXE.
- Associez un fichier de réponses pour l'installation. Vous pouvez définir un fichier de réponses associé pour chaque architecture cliente. Ce fichier de réponses fournit les informations qui sont utilisées pendant la phase d'installation initiale et permet au serveur d'image des services de déploiement Windows de sélectionner l'image d'installation appropriée pour le client, sans intervention de l'installateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Créez les images de découverte. Tous les ordinateurs ne prennent pas en charge le démarrage réseau PXE. Pour ceux qui ne le font pas, vous pouvez créer une image de découverte basée sur une image de démarrage et l'exporter vers un périphérique de stockage amovible. Pour créer une image de découverte, spécifiez :
  - Le nom et la description de l'image.
  - L'image de démarrage sur laquelle elle est basée.
  - Un nom de fichier avec lequel enregistrer l'image.
  - Le nom du serveur des services de déploiement Windows qui sera utilisé pour le déploiement.

Configuration des paramètres d'installation

Vous devez configurer les paramètres d'installation supplémentaires des services de déploiement Windows.

- Ajoutez des images d'installation. C'est l'image du système d'exploitation que vous utilisez pour installer Windows Server. En général, vous commencez par l'image d'installation install.wim, dans le dossier \sources du DVD de Windows Server 2012. Ensuite, vous pouvez choisir de créer des images personnalisées pour des groupes d'ordinateurs qui ont des configurations similaires.

 **Remarque :** Avant de pouvoir créer des images d'installation, vous devez définir un groupe d'images d'installation dans lequel consolider les images associées. Si vous ne procédez pas ainsi, le programme d'administration des services de déploiement Windows crée un groupe générique.

- Associez un fichier de réponses à une image d'installation. Si vous avez créé un fichier de réponses, par exemple à l'aide de Windows ADK, vous pouvez l'associer à une installation pour fournir les informations nécessaires pour terminer le déploiement de l'ordinateur sans l'interaction de l'installateur.
- Configurez une stratégie de format de nom du client. Vous pouvez utiliser une stratégie de format de nom du client pour définir le nom des ordinateurs inconnus pendant le déploiement. La stratégie utilise un certain nombre de variables pour créer un nom unique :
  a. %First. Le prénom de l'installateur. Mettre un chiffre après le signe % indique le nombre de caractères à utiliser dans le nom. Par exemple, %3First utilise les trois premiers caractères du prénom de l'installateur.
  b. %Last. Le nom de famille de l'installateur. Vous pouvez également définir le nombre de caractères à utiliser.
  c. %Username. Le nom d'utilisateur de l'installateur. De nouveau, vous pouvez limiter le nombre de caractères en indiquant un chiffre après le signe %.
  d. %MAC. L'adresse MAC (Media Access Control).
  e. %[n]#. Vous pouvez utiliser cette séquence pour attribuer un numéro séquentiel d'identification unique contenant *n* chiffres au nom d'ordinateur. Si vous souhaitez utiliser un numéro à plusieurs chiffres, complétez la variable avec des zéros non significatifs après le signe %. Par exemple, %2# a comme conséquence les numéros séquentiels 1, 2, 3 et ainsi de suite. %02# donne 01, 02 et 03.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Spécifiez l'emplacement AD DS pour les comptes d'ordinateur. Par défaut, le même domaine AD DS que le serveur des services de déploiement Windows est utilisé. Alternativement, vous pouvez sélectionner :
  - Le même domaine que l'utilisateur effectuant le déploiement.
  - La même unité d'organisation (OU) que l'utilisateur effectuant le déploiement.
  - Un emplacement AD DS spécifié.

 **Remarque :** L'ordinateur des services de déploiement Windows requiert les autorisations Créer un objet Ordinateur et Écrire toutes les propriétés pour le conteneur AD DS que vous spécifiez.

Configuration des paramètres de transmission

Configurez les transmissions par multidiffusion. La transmission par monodiffusion est activée par défaut ; c'est-à-dire que vous n'avez rien besoin de faire d'autre et que vous pouvez déployer des clients en utilisant la monodiffusion. Cependant, pour activer la transmission par multidiffusion, vous devez spécifier :

- Le nom de la transmission par multidiffusion.
- Une image d'installation à laquelle la transmission est associée.
- Une méthode de transmission par multidiffusion. Choisissez entre Diffusion automatique et Diffusion planifiée. Si vous choisissez la diffusion planifiée, vous pouvez définir un seuil minimal de clients avant le début de la transmission, ainsi que la date et l'heure de début.

Configuration des pilotes

Dans Windows Server 2012, les services de déploiement Windows vous permettent d'ajouter et configurer des packages de pilotes sur le serveur, puis de les déployer sur les ordinateurs client pendant les installations en fonction de leur matériel.

Utilisez les étapes générales suivantes pour configurer les pilotes :

1. Obtenez les pilotes dont vous avez besoin. Ceux-ci doivent être sous la forme d'un fichier .inf plutôt que .msi ou .exe.
2. Configurez au besoin des filtres sur le groupe de pilotes. Ces filtres déterminent quels ordinateurs client reçoivent les pilotes en fonction de leurs caractéristiques matérielles. Par exemple, vous pouvez créer un filtre qui applique seulement les pilotes aux ordinateurs qui ont un BIOS fabriqué par A. Datum.
3. Ajoutez les pilotes comme package de pilotes. Les packages de pilotes doivent être associés à un groupe de pilotes. Si vous associez le package de pilotes à un groupe non filtré, tous les ordinateurs reçoivent le pilote.

Vous pouvez utiliser les services de déploiement Windows pour ajouter des packages de pilotes à vos images de démarrage de Windows 8 et Windows Server 2012 ; par conséquent, il n'est pas nécessaire d'exporter l'image. Utilisez les outils de Windows ADK pour ajouter manuellement des packages de pilotes, puis ajoutez l'image de démarrage mise à jour.

Question : Quel est l'avantage de définir une stratégie de format de nom pour les clients ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Administration des services de déploiement Windows

Après avoir terminé la configuration des services de déploiement Windows, vous devez créer et administrer des images de démarrage, les installer et éventuellement capturer et découvrir des images. En outre, vous devez rendre ces images disponibles aux ordinateurs client avec le niveau désiré d'automatisation, en utilisant un mécanisme de transmission approprié.

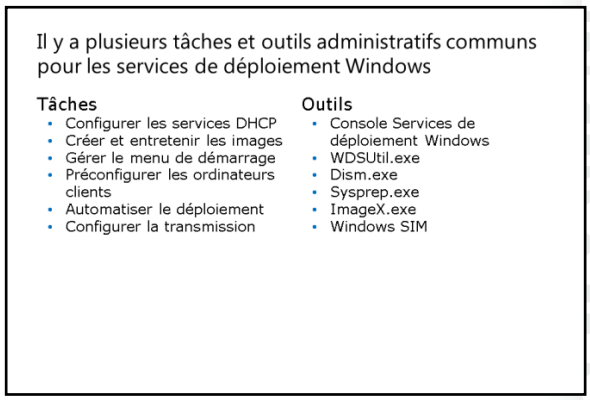
Objectifs de la leçon

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

- Décrivez les tâches d'administration communes.
- Expliquez comment ajouter et configurer des images de démarrage, de capture, de découverte et d'installation.
- Expliquez comment automatiser des déploiements.
- Expliquez comment configurer la transmission par multidiffusion pour déployer vos images.

Tâches d'administration courantes

Pour configurer efficacement les services de déploiement Windows, vous devez exécuter un certain nombre de tâches d'administration courantes. Pour vous aider à exécuter ces tâches, les services de déploiement Windows fournissent un certain nombre d'outils. Les tâches d'administration que vous devez exécuter comprennent ce qui suit :



- Configuration de DHCP
- Création et maintenance des images
- Gestion du menu de démarrage
- Préconfiguration des ordinateurs client
- Automatisation du déploiement
- Configuration de la transmission

Configuration de DHCP

Les clients qui démarrent en utilisant l'environnement PXE ont besoin d'une configuration IPv4 allouée de façon dynamique. À cet effet, vous devez créer et configurer une étendue DHCP appropriée. En outre, si le protocole DHCP et les rôles serveur des services de déploiement Windows sont hébergés conjointement, vous devez configurer la façon dont le serveur PXE écoute les demandes des clients ; il y a en effet un conflit inhérent car le protocole DHCP et les services de déploiement Windows utilisent tous les deux le port UDP 67. Pour créer et gérer les étendues DHCP, vous pouvez utiliser le composant logiciel enfichable DHCP ou l'outil de ligne de commande Netsh.exe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Création et maintenance des images

Vous pouvez créer et maintenir des images avec le composant logiciel enfichable des services de déploiement Windows, Windows SIM, l'outil de ligne de commande WDSutil.exe ou l'outil de ligne de commande Dism.exe.

Par exemple, pour ajouter une image de démarrage, utilisez la commande suivante :

```
WDSUTIL /Verbose /Progress /Add-Image /ImageFile:<chemin d'accès> /ImageType:Boot
```

Pour créer une image de capture, utilisez la commande suivante :

```
WDSUTIL /New-CaptureImage /Image:<nom de l'image de démarrage source>
/Architecture:{x86|ia64|x64} /DestinationImage /FilePath:<chemin d'accès au fichier>
```

Pour ajouter une image d'installation, utilisez les deux commandes suivantes, en appuyant sur Entrée après chaque ligne :

```
WDSUTIL /Add-ImageGroup /ImageGroup:<nom du groupe d'images>
WDSUTIL /Verbose /Progress /Add-Image /ImageFile:<chemin d'accès au fichier .wim>
/ImageType:Install
```

Remarque : Vous pouvez également effectuer ces tâches de gestion en utilisant la console de gestion des services de déploiement Windows, accessible dans le Gestionnaire de serveurs.

Gestion du menu de démarrage

L'environnement de démarrage pour Windows Server 2012 repose sur la banque de données de configuration de démarrage (BCD). Cette banque définit comment le menu de démarrage est configuré. Vous pouvez personnaliser la banque en utilisant Bcdedit.exe.

Remarque : Quand vous personnalisez la banque BCD, vous devez la forcer à être recréée pour que vos modifications prennent effet. Pour ce faire, exécutez les deux commandes WDSutil.exe suivantes (en appuyant sur Entrée après chaque ligne), afin d'arrêter puis de redémarrer le serveur des services de déploiement Windows :
wdsutil /stop-server
wdsutil /start-server

Ce qui suit est une liste de limitations pour l'interface utilisateur du menu de démarrage :

- Taille de l'écran. Seules 13 images peuvent être affichées dans le menu. Si vous en avez plus, l'installateur doit les faire défiler vers le bas pour les voir.
- Souris. Il n'y a pas de pointeur.
- Clavier. Aucun clavier autre que ceux pris en charge par le BIOS n'est pris en charge.
- Localisation. Aucune localisation autre que celles prises en charge par le BIOS n'est prise en charge.
- Accessibilité. La prise en charge des fonctionnalités d'accessibilité est limitée.

Préconfiguration des ordinateurs client

Les services de déploiement Windows prennent en charge les déploiements vers des clients inconnus. Vous pouvez exercer un certain contrôle des clients inconnus en configurant l'approbation d'administrateur. Cela permet de veiller à ce que les clients qui tentent de se déployer avec les services de déploiement Windows sont bien placés dans une file d'attente en attendant votre approbation. Vous pouvez également configurer le nom d'ordinateur client pendant l'approbation.

Cependant, si vous souhaitez un contrôle plus spécifique des déploiements, vous pouvez préconfigurer les ordinateurs dans AD DS ; cela vous permet de configurer le client :

- Commencez à partir d'un serveur différent du serveur des services de déploiement Windows.
- Utilisez un programme différent de démarrage réseau.
- Utilisez un fichier d'installation sans assistance spécifique.
- Utilisez une image de démarrage spécifique.
- Joignez un domaine AD DS spécifique.

Pour préconfigurer les ordinateurs, vous pouvez utiliser la commande suivante de l'outil de ligne de commande WDSutil.exe :

```
WDSUTIL /Add-Device /Device:<nom> /ID:<GUIDorMACAddress>
```

Dans cet exemple, <GUIDorMACAddress> est l'identificateur du nouvel ordinateur.

Automatisation du déploiement

Vous pouvez automatiser de bout en bout les déploiements des services de déploiement Windows. Pour exécuter ces tâches, vous pouvez utiliser le composant logiciel enfichable des services de déploiement Windows et Windows SIM.

Configuration de la transmission

La multidiffusion vous permet de déployer une image sur un grand nombre d'ordinateurs client sans consommer une bande passante réseau excessive.

Envisagez d'activer les transmissions par multidiffusion si votre organisation :

- Anticipe beaucoup de déploiements simultanés.
- Dispose de routeurs qui prennent en charge la propagation des multidiffusions ; c'est-à-dire qui prennent en charge le protocole IGMP (Internet Group Management Protocol).

Pour gérer la transmission par multidiffusion, vous pouvez utiliser le composant logiciel enfichable des services de déploiement Windows ou l'outil de ligne de commande WDSutil.exe. Par exemple, pour créer une transmission par multidiffusion avec diffusion automatique, utilisez la commande suivante :

```
WDSUTIL /New-MulticastTransmission /Image:<nom de l'image> /FriendlyName:<nom convivial>
/ImageType:Install /ImageGroup:<nom du groupe d'images> /TransmissionType:AutoCast
```

Pour créer une transmission de diffusion planifiée, utilisez la commande suivante :

```
WDSUTIL /New-MulticastTransmission /Image:<nom de l'image> /FriendlyName:<nom convivial>
/ImageType:Install /ImageGroup:<nom du groupe d'images> /TransmissionType:ScheduledCast
[/Time:<aaaa/mm/jj:hh:mm>][/Clients:<nb de clients>]
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Procédure d'administration des images

Cette démonstration montre comment administrer des images. Dans cette démonstration, le processus sera décomposé en quatre étapes, décrites ci-dessous :

- Installation et configuration du rôle des services de déploiement Windows.
- Ajout d'image de démarrage.
- Création d'image de capture.
- Ajout d'image d'installation.

Procédure de démonstration

Installer et configurer le rôle des services de déploiement Windows

1. Basculez vers l'ordinateur **LON-SVR1**.
2. Ouvrez le **Gestionnaire de serveur**.
3. Installez le **rôle serveur des services de déploiement Windows** avec les deux services de rôle.
4. Dans la console **Services de déploiement Windows**, cliquez avec le bouton droit sur **LON-SVR1.Adatum.com**, puis cliquez sur **Configurer le serveur**.
5. Utilisez les informations suivantes pour terminer la configuration :
    - Intégrez les services de déploiement Windows à Active Directory.
    - Sur la page **Emplacement du dossier d'installation à distance**, acceptez les valeurs par défaut.
    - Acceptez le message **Avertissement du volume système**.
    - Sur la page **Paramètres initiaux du serveur PXE**, sélectionnez l'option **Répondre à tous les ordinateurs clients (connus et inconnus)**.
    - Lorsque vous y êtes invité, choisissez de ne pas ajouter d'images au serveur.

Ajouter une image de démarrage

1. Basculez vers LON-SVR1.
2. S'il y a lieu, ouvrez la console **Services de déploiement Windows**.
3. Ajoutez une nouvelle image de démarrage en utilisant les informations suivantes pour terminer la procédure :
    a. Sur la page **Fichier image**, utilisez le nom de fichier : **D:\sources\boot.wim**.
    b. Acceptez les valeurs par défaut sur la page **Métadonnées d'image**.
    c. Acceptez les valeurs par défaut sur la page **Résumé**.
4. Sur la page **Progression de la tâche**, cliquez sur **Terminer**.

Ajouter une image d'installation

1. S'il y a lieu, ouvrez la console **Services de déploiement Windows**.
2. Ajoutez un nouveau **Groupe d'images** avec le nom de groupe **Windows Server 2012**.
3. Utilisez l'Assistant Ajout d'images pour ajouter une nouvelle image d'installation à ce groupe. Utilisez les informations suivantes pour terminer le processus :
   a. Sur la page **Fichier image**, utilisez le nom de fichier suivant : **D:\sources\install.wim**
   b. Sur la page **Images disponibles**, désactivez toutes les cases à cocher excepté **Windows Server 2012 SERVERSTANDARDCORE**.
   c. Acceptez les valeurs par défaut sur la page **Résumé**.
   d. Sur la page **Progression de la tâche**, cliquez sur **Terminer**.
4. Réduisez la fenêtre Services de déploiement Windows.

Automatisation des déploiements

Il y a quatre phases que vous pouvez automatiser pendant le processus de déploiement des services de déploiement Windows. Ces applications sont les suivantes :

Pour automatiser le processus de configuration de Windows :
1. créez le fichier UUnattend.xml
2. copiez le fichier sur le serveur des services de déploiement Windows
3. affichez les propriétés de l'image d'installation appropriée
4. activez le mode sans assistance et sélectionnez le fichier de réponse

- Stratégie de démarrage PXE. Vous pouvez déterminer la façon dont le serveur PXE répond aux clients et si l'installateur est requis pour appuyer sur la touche F12 afin d'établir la connexion avec le serveur des services de déploiement Windows et de sélectionner une image de démarrage. Par exemple, l'option **Toujours continuer le démarrage PXE** permet à l'ordinateur de poursuivre le processus de déploiement sans intervention de l'installateur.
- L'image de démarrage par défaut. Si vous configurez une image de démarrage par défaut, l'installateur ne sera pas invité à faire une sélection.
- Les écrans de la console Services de déploiement Windows. Quand l'ordinateur client utilise le protocole TFTP pour se connecter au serveur des services de déploiement Windows et sélectionner une image de démarrage, l'installateur doit alors fournir les informations d'identification et sélectionner une image du système d'exploitation à installer. Vous pouvez créer un fichier de réponses Unattend.xml pour automatiser cette phase.
- Installation de Windows. Vous pouvez personnaliser le programme d'installation de sorte que, une fois l'image d'installation sélectionnée (automatiquement ou manuellement), le programme d'installation termine la procédure d'installation sans intervention de l'installateur. C'est le même type d'automatisation que vous utilisez pour automatiser des installations avec Windows ADKADK.

Utilisez Windows SIM pour créer les deux types de fichiers de réponses, puis utilisez le composant logiciel enfichable des services de déploiement Windows pour associer les fichiers de réponses à la phase de déploiement requise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Automatisation de l'installation sans assistance client

Utilisez la procédure suivante pour associer un fichier de réponses à la phase de déploiement d'une installation sans assistance client :

1. Créez le fichier Unattend.xml dans Windows ADK avec des paramètres appropriés aux services de déploiement Windows.
2. Copiez le fichier sur le serveur des services de déploiement Windows et collez-le dans un dossier sous **\RemoteInstall**.
3. Ouvrez la console des **services de déploiement Windows**.
4. Affichez la boîte de dialogue **Propriétés** pour le serveur des services de déploiement Windows.
5. Sur l'onglet **Client**, activez l'installation sans assistance, puis sélectionnez le fichier de réponses que vous avez créé plus tôt.

Exemple de fichier de réponses Unattend pour l'installation sans assistance client des services de déploiement Windows

Ce qui suit est un exemple partiel de fichier de réponses pour l'automatisation de la phase d'installation sans assistance client des services de déploiement Windows :

```
<WindowsDeploymentServices>
            <Login>
               <WillShowUI>OnError</WillShowUI>
               <Credentials>
                     <Username>Installer</Username>
                     <Domain>Adatum.com</Domain>
                     <Password>Pa$$w0rd</Password>
                </Credentials>
            </Login>
            <ImageSelection>
               <WillShowUI>OnError</WillShowUI>
               <InstallImage>
                  <ImageName>Windows Server 2021</ImageName>
                  <ImageGroup>Adatum Server Images</ImageGroup>
                  <Filename>Install.wim</Filename>
               </InstallImage>
               <InstallTo>
                  <DiskID>0</DiskID>
                  <PartitionID>1</PartitionID>
               </InstallTo>
            </ImageSelection>
</WindowsDeploymentServices>
```

Automatisation de l'installation de Windows

Pour automatiser le processus d'installation de Windows, utilisez les étapes suivantes :

1. Créez le fichier **unattend.xml** dans Windows ADK, avec des paramètres appropriés à l'installation de Windows.
2. Copiez le fichier à un emplacement approprié sur le serveur des services de déploiement Windows.
3. Dans la console Services de déploiement Windows, affichez les propriétés de l'image d'installation appropriée.
4. Activez l'option **Autoriser l'image à s'installer en mode sans assistance**, puis sélectionnez le fichier de réponses que vous avez créé plus tôt.

Démonstration : Procédure de configuration de la transmission par multidiffusion

Cette démonstration montre comment configurer la transmission par multidiffusion.

Procédure de démonstration

1. Ouvrez la console Services de déploiement Windows sur LON-SVR1.
2. Créez une nouvelle transmission par multidiffusion en utilisant les informations suivantes :
   - Nom de la transmission : **Windows Server 2012 Branch Servers**
   - Groupe d'images : **Windows Server 2012**
   - Image : **Windows Server 2012 SERVERENTERPRISECORE**
   - Type de multidiffusion : **diffusion automatique**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Utilisation des services de déploiement Windows pour déployer Windows Server 2012

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à Londres pour s'occuper du siège social et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

A. Datum déploie des serveurs dans ses filiales dans l'ensemble de la zone pour le service Recherche. Vous avez été chargé d'aider à automatiser ce déploiement. Vous suggérez d'utiliser les services de déploiement Windows pour déployer Windows Server 2012 dans les succursales. Des instructions relatives au déploiement vous ont été envoyées par courrier électronique. Vous devez lire ces instructions, puis installer et configurer les services de déploiement Windows pour prendre en charge le déploiement.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- Installer et configurer les services de déploiement Windows.
- Créer les images du système d'exploitation en utilisant les services de déploiement Windows.
- Configurer le format de nom personnaliser des ordinateurs.
- Déployer les images avec les services de déploiement Windows.

Configuration de l'atelier pratique

Durée approximative : 75 minutes

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-SVR1 22411B-LON-SVR3
Nom d'utilisateur	**Administrateur**
Mot de passe	**Pa$$w0rd**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Ouvrez une session en utilisant les informations d'authentification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Effectuez les étapes 2 à 4 pour **22411B-LON-SVR1**. Ne démarrez pas 22411B-LON-SVR3 tant que vous n'avez pas été invité à le faire.

Exercice 1 : Installation et configuration des services de deployment Windows

Scénario

Pour vous aider dans le processus de configuration des services de déploiement Windows, vous avez reçu un courrier électronique avec les informations de configuration appropriées.

Guide de déploiement dans les succursales
Présentation de la configuration requise Afin de configurer les services de déploiement de Microsoft Windows pour faciliter le déploiement des serveurs dans les succursales.
Informations supplémentaires Méthode de déploiement : déploiements standards automatisés d'image
• Informations sur la configuration : o LON-SVR1 doit être utilisé pour héberger les services de déploiement Windows. o Configurez la transmission par multidiffusion pour qu'elle utilise la diffusion automatique. o Configurez l'attribution automatique de noms pour identifier les serveurs des succursales. o Placez les serveurs des succursales dans l'unité de l'organisation (OU) Research. o Le système d'exploitation devrait être Windows Server 2012 Enterprise Edition. o Une installation minimale doit être effectuée.

Les tâches principales de cet exercice sont les suivantes :

1. Lisez la documentation fournie avec le produit.
2. Installez le rôle des services de déploiement Windows
3. Configurer les services de déploiement Windows

▶ Tâche 1 : Lisez la documentation fournie avec le produit.

- Lisez la documentation fournie dans le scénario d'exercice pour connaître les détails du déploiement.

▶ Tâche 2 : Installez le rôle des services de déploiement Windows

1. Basculez vers l'ordinateur **LON-SVR1**.
2. Ouvrez le **Gestionnaire de serveur**.
3. Installez le rôle serveur des **services de déploiement Windows** avec les deux services de rôle.
4. Fermez le **Gestionnaire de serveur**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer les services de déploiement Windows

1. Ouvrez la console **Services de déploiement Windows**.
2. Cliquez avec le bouton droit sur **LON-SVR1.Adatum.com**, puis cliquez sur **Configurer le serveur**.
3. Utilisez les informations suivantes pour terminer la configuration :
   a. Intégrez les services de déploiement Windows à Active Directory.
   b. Sur la page **Emplacement du dossier d'installation à distance**, acceptez les valeurs par défaut.
   c. Acceptez le message **Avertissement du volume système**.
   d. Sur la page **Paramètres initiaux du serveur PXE**, sélectionnez l'option **Répondre à tous les ordinateurs clients (connus et inconnus)**.
   e. Lorsque vous y êtes invité, choisissez de ne pas ajouter d'images au serveur.

Résultats : Après avoir terminé cet exercice, vous aurez installé et configuré les services de déploiement Windows.

Exercice 2 : Création d'images du système d'exploitation avec les services de déploiement Windows

Scénario

Les services de déploiement Windows ont été installés et configurés avec succès. Vous devez maintenant créer plusieurs images du système d'exploitation pour le déploiement.

Les principales tâches de cet exercice sont les suivantes :

1. Insérer le support d'installation de Windows Server 2012 dans LON-SVR1.
2. Ajouter une image de démarrage.
3. Ajouter une image d'installation.

▶ Tâche 1 : Insérer le support d'installation de Windows Server 2012 dans LON-SVR1

1. Sur l'ordinateur hôte, ouvrez le **Gestionnaire Hyper-V®**.
2. Ouvrez la page **Paramètres** pour 22411B-LON-SVR1.
3. Sélectionnez le Lecteur de DVD et joignez le fichier ISO (International Organization for Standardization) situé sous **C:\Programmes\Microsoft Learning\22411\Drives\ WIndows2012_RTM_FR.ISO**.

▶ Tâche 2 : Ajouter une image de démarrage

1. Basculez vers LON-SVR1.
2. S'il y a lieu, ouvrez la console **Services de déploiement Windows**.
3. Ajoutez une nouvelle image de démarrage en utilisant les informations suivantes pour terminer la procédure :
   - Sur la page **Fichier image**, utilisez le nom de fichier : **D:\sources\boot.wim**.
   - Acceptez les valeurs par défaut sur la page **Métadonnées d'image**.
   - Acceptez les valeurs par défaut sur la page **Résumé**.
4. Sur la page **Progression de la tâche**, cliquez sur **Terminer**.

▶ Tâche 3 : Ajouter une image d'installation

1. S'il y a lieu, ouvrez la console **Services de déploiement Windows**.
2. Ajoutez un nouveau **Groupe d'images** avec le nom de groupe **Windows Server 2012**.
3. Utilisez l'Assistant Ajout d'images pour ajouter une nouvelle image d'installation à ce groupe. Utilisez les informations suivantes pour terminer le processus :
   a. Sur la page **Fichier image**, utilisez le nom de fichier suivant : **D:\sources\install.wim**
   b. Sur la page **Images disponibles**, désactivez toutes les cases à cocher excepté **Windows Server 2012 SERVERSTANDARDCORE**.
   c. Acceptez les valeurs par défaut sur la page **Résumé**.
   d. Sur la page **Progression de la tâche**, cliquez sur **Terminer**.
4. Réduisez la fenêtre Services de déploiement Windows.

Résultats : Après avoir terminé cet exercice, vous allez créer une image du système d'exploitation avec les services de déploiement Windows.

Exercice 3 : Configuration d'un format de nom personnalisé des ordinateurs

Scénario

Pour automatiser l'attribution de noms aux ordinateurs, vous devez configurer les propriétés de format de nom personnalisé pour les services de déploiement Windows selon le document qui vous a été envoyé. Cela implique également de configurer la délégation sur les unités de l'organisation Active Directory qui contiendront les comptes d'ordinateur. L'approbation d'administrateur étant requise, vous devez également la configurer.

Les principales tâches de cet exercice sont les suivantes :

1. Configurer l'attribution automatique de noms.
2. Configurer l'approbation d'administrateur.
3. Configurer les autorisations AD DS.

▶ Tâche 1 : Configurer l'attribution automatique de noms

1. Dans la console Services de déploiement Windows, affichez les propriétés de **LON-SVR1.Adatum.com**.
2. Sous l'onglet **AD DS**, utilisez les informations suivantes pour configurer le format de nom automatique :
   - Format : **BRANCH-SVR-%02#**
   - Emplacement du compte d'ordinateurs : **Adatum Research OU**

▶ Tâche 2 : Configurer l'approbation d'administrateur

1. Dans la console Services de déploiement Windows, affichez les propriétés de **LON-SVR1.Adatum.com**.
2. Sous l'onglet **Réponse PXE**, sélectionnez **Exiger l'approbation administrateur pour les ordinateurs inconnus** et modifiez le **Délai de réponse PXE** sur **3 secondes**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Ouvrez **Windows PowerShell®**, puis saisissez la commande suivante pour créer un message à afficher à l'installateur en attendant l'approbation administrateur :

```
WDSUTIL /Set-Server /AutoAddPolicy /Message: "L'administrateur d'Adatum autorise
cette demande. Veuillez patienter."
```

4. Fermez la fenêtre d'invite de commandes.

▶ Tâche 3 : Configurer les autorisations des services de domaine Active Directory (AD DS)

1. Basculez vers l'ordinateur LON-DC1 et ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Cliquez avec le bouton droit sur l'unité de l'organisation (OU) **Research** et utilisez l'assistant Délégation de contrôle pour donner au compte d'ordinateur **LON-SVR1** la capacité de créer des objets Ordinateur dans l'unité de l'organisation. Utilisez les informations suivantes :
   a. Tâches à déléguer : **créez une tâche personnalisée à déléguer**
   b. Sur la page **Type d'objet Active Directory**, cliquez sur **Seulement des objets suivants dans le dossier**, activez la case à cocher **Objets Ordinateur**, puis sélectionnez **Créer les objets sélectionnés dans ce dossier**.
   c. Sur la page **Autorisations**, dans la Liste des Autorisations, activez la case à cocher **Contrôle total**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré le format de nom personnalisé des ordinateurs.

Exercice 4 : Déploiement d'images avec les services de déploiement Windows

Scénario

Vous avez fourni des instructions pour qu'un superviseur de succursale lance la procédure d'installation sur le serveur de la succursale. L'installation va maintenant se faire.

Les principales tâches de cet exercice sont les suivantes :

1. Configurer un serveur des services de déploiement Windows pour la transmission par multidiffusion.
2. Configurer le client pour le démarrage PXE (Pre-Boot Execution Environment).

▶ Tâche 1 : Configurer un serveur des services de déploiement Windows pour la transmission par multidiffusion

1. Basculez vers l'ordinateur LON-SVR1.
2. Créez une nouvelle transmission par multidiffusion en utilisant les informations suivantes :
   - Nom de la transmission : **Windows Server 2012 Branch Servers**
   - Groupe d'images : **Windows Server 2012**
   - Image : **Windows Server 2012 SERVERSTANDARDCORE**
   - Type de multidiffusion : **diffusion automatique**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer le client pour le démarrage PXE (Pre-Boot Execution Environment)

1. Sur l'ordinateur hôte, basculez vers le **Gestionnaire Hyper-V**.
2. Dans la liste Ordinateurs virtuels, faites un clic droit sur **22411B-LON-SVR3**, puis cliquez sur **Paramètres**.
3. Dans la boîte de dialogue **Paramètres pour 22411B-LON-SVR3**, cliquez sur **BIOS**.
4. Dans le volet des résultats, cliquez sur **Carte réseau héritée**.
5. Utilisez les flèches pour déplacer la **Carte réseau héritée** en haut de la liste, puis cliquez sur **OK**.
6. Dans le Gestionnaire Hyper-V, cliquez sur **22411B-LON-SVR3**, puis sur Accueil dans le volet Actions.
7. Dans le volet **Actions**, cliquez sur **Se connecter**.
8. Quand l'ordinateur redémarre, notez le message du protocole DHCP (Dynamic Host Configuration Protocol) PXE. Lorsque vous y êtes invité, appuyez sur **F12** pour le démarrage réseau.

   Question : Voyez-vous le message d'approbation administrateur ?
9. Basculez vers l'ordinateur LON-SVR1.
10. Dans la console Services de déploiement Windows, cliquez sur **Périphériques en attente**.
11. Cliquez avec le bouton droit sur la **demande en attente**, puis cliquez sur **Approuver**.
12. Dans la boîte de dialogue **Périphérique en attente**, cliquez sur **OK**.
13. Basculez vers l'ordinateur LON-SVR3.

    Question : Quelle est l'image par défaut ?

    Question : L'installation démarre-t-elle ?
14. Vous n'êtes pas obligé de continuer l'installation.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Faites un clic droit sur **22411B-LON-DC1** dans la liste **Ordinateurs virtuels**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez ces étapes pour **22411B-LON-SVR3** et **22411B-LON-SVR1**.

Résultats : Après avoir terminé cet exercice, vous aurez déployé une image avec les services de déploiement Windows.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Outils

Outil	À quoi sert-il ?	Emplacement
Console Services de déploiement Windows	Administration des services de déploiement Windows	Gestionnaire de serveur - Outils
WDSutil.exe	Gestion des lignes de commande des services de déploiement Windows	Ligne de commande
Windows ADK	Gestion des fichiers image et création de fichiers de réponses	Téléchargement depuis Microsoft.com
Dism.exe	Entretien des images hors connexion et en ligne	Windows ADK
Netsh.exe	Outil de ligne de commande pour gérer les paramètres liés au réseau	Ligne de commande

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 2

Configuration et résolution des problèmes du système DNS

Table des matières :

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

Leçon 1 : Installation du rôle de serveur DNS **2-2**

Leçon 2 : Configuration du rôle de serveur DNS **2-9**

Leçon 3 : Configuration des zones DNS **2-16**

Leçon 4 : Configuration des transferts de zone DNS **2-22**

Leçon 5 : Gestion et dépannage du système DNS **2-25**

Atelier pratique : Configuration et résolution des problèmes du système DNS **2-34**

Contrôle des acquis et éléments à retenir **2-40**

Vue d'ensemble du module

Le système de nom de domaine (DNS, Domain Name System) est le service de nom de base dans Windows Server® 2022. Il fournit la résolution de noms et permet aux clients DNS de localiser des services réseau, tels que les contrôleurs de domaine AD DS (Active Directory® Domain Services), les serveurs de catalogue global et les serveurs de messagerie. Si vous configurez mal votre infrastructure DNS ou que celle-ci ne fonctionne pas correctement, ces services réseau importants seront inaccessibles à vos serveurs réseau et clients. Par conséquent, il est essentiel que vous compreniez comment déployer, configurer, gérer et dépanner ce service critique.

Objectifs

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

- installer le rôle de serveur DNS ;
- configurer le rôle de serveur DNS ;
- créer et configurer des zones DNS ;
- configurer les transferts de zone ;
- gérer et dépanner le système DNS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Installation du rôle de serveur DNS

Pour prendre en charge les services réseau sous-jacents dans votre organisation, vous devez pouvoir installer et configurer le rôle de serveur DNS de Windows Server 2022. Avant d'installer le rôle de serveur DNS, vous devez comprendre les besoins de l'infrastructure réseau de votre organisation et décider d'utiliser ou non un système DNS de déconnexion calleuse. Vous devez également considérer l'emplacement du rôle serveur DNS ainsi que le nombre de clients et de zones DNS que vous utiliserez. Cette leçon décrit le processus d'installation d'un rôle de serveur DNS.

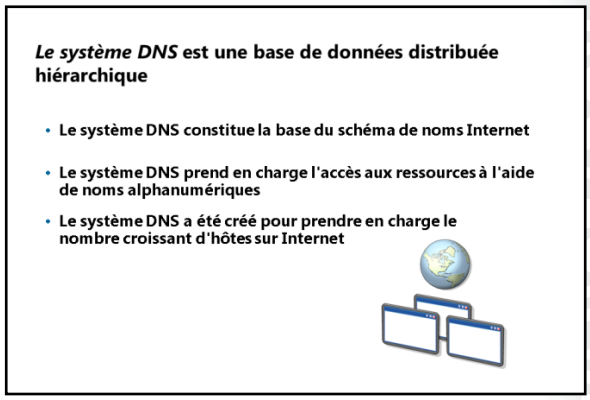
Objectifs de la leçon

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

- expliquer le rôle et les avantages du système DNS dans l'infrastructure réseau ;
- définir un espace de noms DNS ;
- décrire comment intégrer le système DNS dans les services de domaine Active Directory ;
- expliquer l'utilisation du système DNS de déconnexion calleuse ;
- expliquer comment installer le rôle de serveur DNS ;
- présenter les considérations relatives au déploiement d'un serveur DNS.

Vue d'ensemble du rôle DNS

L'acronyme DNS (Domain Name System) désigne un service de résolution de noms qui permet de résoudre des noms en adresses IP. Le service DNS est une base de données distribuée hiérarchique séparée de manière logique, ce qui permet à de nombreux serveurs différents d'héberger une base de données mondiale des noms DNS.



Comment le système DNS prend en charge les bases du schéma de noms Internet

Le système DNS est un service international qui vous permet de saisir un nom de domaine (par exemple, Microsoft.com), que votre ordinateur résout en adresse IP. Un avantage du système DNS est que les adresses IPv4 peuvent être longues et difficiles à retenir, par exemple *232.207.0.32*. Cependant, il est généralement plus facile de retenir un nom de domaine. Par ailleurs, vous pouvez utiliser des noms d'hôte qui ne changent pas ou modifier les adresses IP sous-jacentes en fonction des besoins de votre organisation.

Avec l'adoption de la norme IPv6, le service DNS sera encore plus critique puisque les adresses IPv6 sont encore plus complexes que les adresses IPv4. Exemple d'adresse IPv6 : *2002:db8:4236:e38c:384f:3764:b59c:3d97*.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

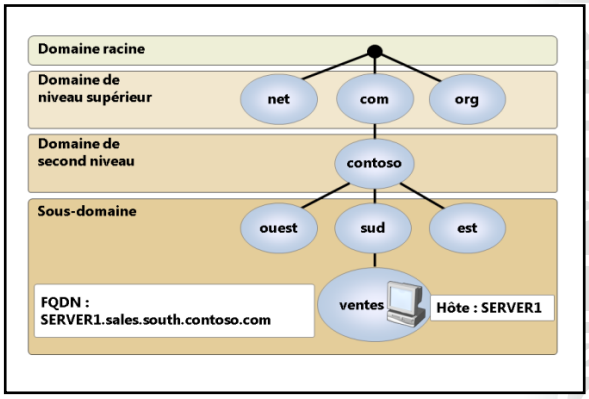
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comment le service DNS prend en charge les bases du schéma de noms de domaine Active Directory d'une organisation

Le système DNS est chargé de résoudre les ressources dans un domaine des services de domaine Active Directory (AD DS). Le rôle DNS est nécessaire à l'installation des services de domaine Active Directory. Le système DNS fournit des informations aux clients de station de travail pour leur permettre de se connecter au réseau. Il résout les ressources du domaine, telles que les serveurs, les stations de travail, les imprimantes et les dossiers partagés. Si vous configurez un serveur DNS de manière incorrecte, cela peut être à l'origine de nombreux problèmes des services de domaine Active Directory.

Vue d'ensemble de l'espace de noms DNS

L'espace de noms DNS facilite la manière dont un résolveur DNS localise un ordinateur. L'espace de noms est organisé de manière hiérarchique afin de distribuer des informations au moyen de nombreux serveurs.



Domaine racine

Un point (.) représente le domaine racine et ne se saisit pas dans un navigateur Web. Le point (.) est utilisé par défaut. La prochaine fois que vous saisirez une adresse sur un ordinateur, essayez d'ajouter le point à la fin (par exemple, www.microsoft.com.). Il existe 23 serveurs de domaines racines universels.

Remarque : Lors d'un dépannage du système DNS, il est habituel d'inclure le point final.

Domaine de niveau supérieur

Le domaine de niveau supérieur (TLD) est le premier niveau de l'espace de noms DNS. Les domaines TLD sur Internet incluent, par exemple, Internet .com, .net, .org, .biz et .ca. Les domaines les plus reconnus sont .com, .net, .org et .gov, qui sont dédiés au gouvernement des États-Unis. Les domaines associés à ce niveau sont plus nombreux et un domaine TLD est dédié à chaque pays. Par exemple, celui du Canada est .ca et celui du Royaume-Uni est .uk. L'organisation qui réglemente les noms de domaine, appelée « ICANN » (Internet Corporation for Assigned Names and Numbers), ajoute de nouveaux domaines TLD de temps en temps.

Domaine de second niveau

Le nom de domaine de second niveau correspond à la partie du nom de domaine qui apparaît avant le domaine de niveau supérieur. Par exemple, *microsoft* dans le domaine www.microsoft.com correspond au nom de domaine de second niveau. Les organisations qui enregistrent des noms de domaine de second niveau les contrôlent. N'importe qui peut enregistrer un nom de domaine de second niveau au moyen d'un service d'enregistrement Internet. De nombreux domaines de second niveau sont régis par des règles spéciales qui stipulent quelles organisations ou personnes peuvent enregistrer un nom de domaine. Par exemple, seules les associations à but non lucratif peuvent utiliser .org.

Sous-domaine

Le sous-domaine est répertorié avant les domaines de second niveau et de niveau supérieur. Par exemple, *www* désigne un sous-domaine dans le nom de domaine www.microsoft.com. Les sous-domaines sont définis dans le serveur DNS de l'organisation qui détient le serveur DNS de second niveau.

Nom de domaine complet

Un nom de domaine complet (FQDN, fully qualified domain name) est le nom DNS explicite qui comprend le nom de l'ordinateur et les sous-domaines du domaine racine. Par exemple, si l'ordinateur est désigné en tant que Server2 dans le domaine sales.south.contoso.com, le nom de domaine complet de cet ordinateur est server2.sales.south.contoso.com.

Conventions d'appellation standard DNS

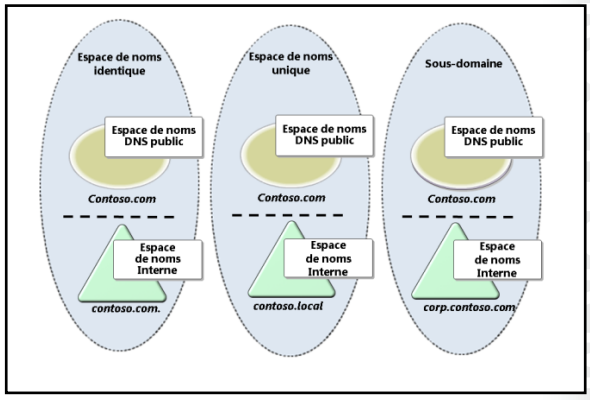
Les caractères suivants sont valides dans les noms DNS :

- majuscules de A à Z ;
- minuscules de a à z ;
- chiffres de 0 à 9 ;
- Trait d'union (-)

Remarque : Le trait de soulignement (_) est un caractère réservé.

Intégration d'AD DS et de DNS

Quand vous commencez à planifier votre espace de noms DNS, vous devez tenir compte à la fois des espaces de noms internes et externes. L'espace de noms interne est celui que les clients et serveurs internes utilisent dans votre réseau privé. L'espace de noms externe est celui par lequel votre organisation est référencée sur Internet. Il n'est pas nécessaire que les noms de domaines DNS interne et externe soient identiques.



Quand vous implémentez les services de domaine Active Directory (AD DS), vous devez utiliser un espace de noms DNS pour héberger des enregistrements AD DS.

Remarque : Examinez soigneusement vos options avant de sélectionner un conception d'espace de noms pour les services de domaine Active Directory. Bien qu'il soit possible de modifier un espace de noms après l'implémentation des services de domaine Active Directory, ce processus est long et complexe et compte de nombreuses limitations.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

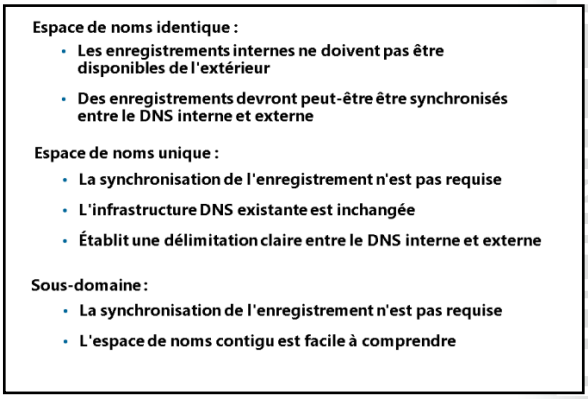
Pour déterminer un espace de noms DNS pour votre environnement AD DS, choisissez parmi les scénarios suivants :

- Rendre l'espace de noms interne identique à l'espace de noms public. Dans ce scénario, les espaces de noms internes et publics sont identiques, mais leurs enregistrements sont différents. Bien que ce scénario soit simple, ce qui en fait un choix idéal pour les petites organisations, il peut être difficile à gérer pour les réseaux plus grands.
- Rendre l'espace de noms interne différent de l'espace de noms public. Dans ce scénario, les espaces de noms internes et publics sont totalement différents. Ils n'ont aucun lien entre eux. Ce scénario permet une séparation évidente dans l'espace de noms. Dans les réseaux complexes comprenant de nombreuses applications avec accès par Internet, l'utilisation d'un nom différent présente de la clarté lors de la configuration de ces applications. Par exemple, les serveurs Edge qui sont placés sur un réseau de périmètre ont souvent besoin de plusieurs cartes d'interface réseau : une connectée au réseau privé et une destinée à la maintenance des demandes provenant du réseau public. Si chaque carte d'interface réseau a un nom de domaine différent, il est souvent plus facile de terminer la configuration de ce serveur.
- Faire de l'espace de noms interne un sous-domaine de l'espace de noms public. Dans ce scénario, l'espace de noms interne est lié à l'espace de noms public, mais il n'y a aucune superposition entre eux. Ceci fournit une approche hybride. Le nom interne est différent, ce qui permet la séparation de l'espace de noms. Cependant, le nom interne est également lié au nom public, ce qui offre de la simplicité. Cette approche est la plus simple à implémenter et à gérer. Cependant, si vous ne pouvez pas utiliser un sous-domaine de l'espace de noms public pour les services de domaine Active Directory, utilisez des espaces de noms uniques.

Remarque : Dans la plupart des situations, les ordinateurs inclus dans un domaine AD DS ont un suffixe DNS principal qui correspond au nom de domaine DNS. Il est parfois nécessaire que ces noms soient différents, par exemple, à la suite d'une fusion ou pendant une acquisition. Quand les noms diffèrent, l'espace de noms est dit disjoint. Un scénario d'espace de noms disjoint est un scénario dans lequel le suffixe DNS principal d'un ordinateur ne correspond pas au nom de domaine DNS où réside cet ordinateur. L'ordinateur dont le suffixe DNS principal ne correspond pas est dit *disjoint*. Un autre scénario d'espace de noms disjoint se produit si le nom de domaine NetBIOS d'un contrôleur de domaine ne correspond pas au nom de domaine DNS.

Choix d'utilisation d'une configuration DNS mixte

L'utilisation du même espace de noms en interne et en externe simplifie l'accès aux ressources du point de vue des utilisateurs, mais elle augmente également la complexité de gestion. Vous ne devez pas rendre les enregistrements DNS internes disponibles en externe. En revanche, la synchronisation des enregistrements pour les ressources externes est généralement requise. Par exemple, vos espaces de noms internes et externes peuvent utiliser le nom *Contoso.com*.



L'utilisation des espaces de noms uniques pour les espaces de noms internes et publics fournit une définition claire entre le système DNS interne et externe, et supprimer la nécessité de synchroniser des enregistrements entre les espaces de noms. Cependant, dans certains cas, avoir plusieurs espaces de noms peut semer la confusion des utilisateurs. Par exemple, vous pouvez choisir l'espace de noms externe de Contoso.com et l'espace de noms interne de Contoso.local. Notez que si vous implémentez une configuration d'espace de noms unique, vous n'êtes plus tenu d'utiliser des noms de domaine enregistrés.

L'utilisation d'un sous-domaine de l'espace de noms public pour les services de domaine Active Directory supprime la nécessité de synchroniser des enregistrements entre les serveurs DNS internes et externes. Puisque les espaces de noms sont liés, les utilisateurs trouvent en général cette structure facile à comprendre. Par exemple, si votre espace de noms public est Contoso.com, vous pouvez choisir d'implémenter votre espace de noms interne comme sous-domaine Active Directory ou AD.Contoso.com.

Examen de la configuration DNS mixte

Le fait que les espaces de noms DNS interne et externe correspondent peut poser certains problèmes. Cependant, la configuration DNS mixte peut résoudre ces problèmes. La configuration DNS mixte est une configuration où votre domaine a deux zones de serveur racine qui contiennent les informations d'enregistrement du nom de domaine. Vos hôtes de réseau interne sont dirigés vers une zone, alors que les hôtes externes sont dirigés vers une autre pour la résolution de noms. Par exemple, dans le cas d'une configuration DNS non mixte pour le domaine Contoso.com, vous pouvez avoir une zone DNS qui ressemble à l'exemple présenté dans le tableau suivant.

Hôte	Type d'enregistrement	Adresse IP
www	A	232.207.2.200
Relais	A	232.207.2.202
Webserver2	A	292.268.2.200
Exchange2	A	292.268.0.202

Quand un ordinateur client sur Internet souhaite accéder au relais SMTP à l'aide du nom publié de relay.contoso.com, il interroge le serveur DNS qui renvoie le résultat 232.207.2.202. Le client établit alors une connexion via SMTP à cette adresse IP.

Cependant, les ordinateurs clients sur le réseau intranet de l'entreprise utilisent également le nom publié de relay.contoso.com. Le serveur DNS renvoie le même résultat : une adresse IP publique correspondant à 232.207.2.202. Le client tente à présent d'établir une connexion à l'adresse IP retournée à l'aide de l'interface externe de l'ordinateur de publication. Selon la configuration du client, l'opération peut aboutir ou ne pas aboutir.

Pour éviter ce problème, configurez deux zones pour le même nom de domaine : une sur chacun des deux serveurs DNS.

La zone interne pour adatum.com ressemblerait aux informations figurant dans le tableau suivant.

Hôte	Type d'enregistrement	Adresse IP
www	CNAME	Webserver2.contoso.com
Relais	CNAME	Exchange2.contoso.com
Webserver2	A	292.268.2.200
Exchange2	A	292.268.0.202

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La zone externe pour adatum.com ressemblerait aux informations figurant dans le tableau suivant.

Hôte	Type d'enregistrement	Adresse IP
www	A	232.207.2.200
Relais	A	232.207.2.202
	MX	Relay.contoso.com

Les ordinateurs clients dans les réseaux internes et externes peuvent désormais résoudre le nom relay.contoso.com à l'adresse IP interne ou externe appropriée.

Démonstration : Installation du rôle de serveur DNS

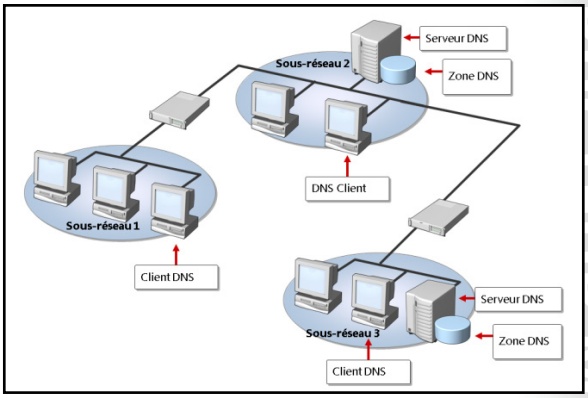
La démonstration suivante montre comment installer le rôle de serveur DNS.

Procédure de démonstration

1. Basculez vers LON-SVR2, puis connectez-vous avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Utilisez le **Gestionnaire de serveur** pour installer le rôle **Serveur DNS**.

Considérations liées au déploiement du rôle serveur DNS

Si vous envisagez de déployer le système DNS, vous devez prendre en compte plusieurs points. Vous devez notamment vous poser les questions suivantes :



- Combien de zones DNS configurerez-vous sur le serveur et combien d'enregistrements DNS chaque zone contiendra-elle ? En général, les zones sont mappées sur une base linéaire avec des domaines dans votre espace de noms. Quand vous avez un grand nombre d'enregistrements, il peut être judicieux de fractionner les enregistrements en plusieurs zones.
- Combien de clients DNS communiqueront avec le serveur sur lequel vous configurez le rôle DNS ? Plus les résolveurs clients sont nombreux, plus la charge placée sur le serveur est importante. Quand vous anticipez la charge supplémentaire, pensez à déployer des serveurs DNS supplémentaires.
- Où allez-vous placer les serveurs DNS ? Allez-vous, par exemple, centraliser les serveurs DNS dans un même endroit ou est-il préférable de les placer dans des succursales ? S'il y a peu de clients dans une succursale, vous pouvez satisfaire la plupart des requêtes DNS à l'aide d'un serveur DNS central ou en implémentant un serveur réservé à la mise en cache. Un grand nombre d'utilisateurs dans une succursale peuvent bénéficier d'un serveur DNS local avec des données de la zone appropriées.

Vos réponses aux questions précédentes détermineront le nombre de serveurs DNS que vous devez déployer et leur emplacement.

Intégration d'Active Directory

Le rôle DNS de Windows Server 2022 peut enregistrer la base de données DNS de deux manières différentes, comme indiqué dans le tableau suivant.

Méthode de stockage	Description
Fichier texte	Le rôle de serveur DNS stocke les entrées DNS dans un fichier texte que vous pouvez modifier à l'aide d'un éditeur de texte.
Active Directory	Le rôle de serveur DNS enregistre les entrées DNS dans la base de données Active Directory, qui les réplique à d'autres contrôleurs de domaine, même s'ils n'exécutent pas le rôle DNS de Windows Server 2008. Vous ne pouvez pas utiliser un éditeur de texte pour modifier les données DNS que stocke Active Directory.

Les zones intégrées à Active Directory sont plus faciles à gérer que les zones traditionnelles de type texte et elles sont plus sécurisées. La réplication des données de zone a lieu dans le cadre de la réplication Active Directory.

Placement des serveurs DNS

En général, le rôle DNS est déployé sur tous les contrôleurs de domaine. Si vous décidez d'implémenter une autre stratégie, posez-vous les questions suivantes et gardez les réponses à l'esprit :

- Comment les ordinateurs clients résoudront-ils des noms si leur serveur DNS habituel n'est plus disponible ?
- Quelle sera l'incidence sur le trafic réseau si les ordinateurs clients commencent à utiliser un autre serveur DNS, peut-être situé à distance ?
- Comment comptez-vous implémenter des transferts de zone ? Les zones intégrées à Active Directory utilisent la réplication Active Directory pour transférer la zone vers tous les autres contrôleurs de domaine. Si vous implémentez des zones non intégrées à Active Directory, vous devez organiser vous-même le mécanisme de transfert de zone.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration du rôle de serveur DNS

L'infrastructure DNS sert de base à la résolution de noms sur Internet et dans des domaines AD DS selon Windows Server 2022. Cette leçon fournit des conseils et des informations au sujet des conditions requises pour configurer le rôle de serveur DNS et explique les fonctions de base d'un serveur DNS.

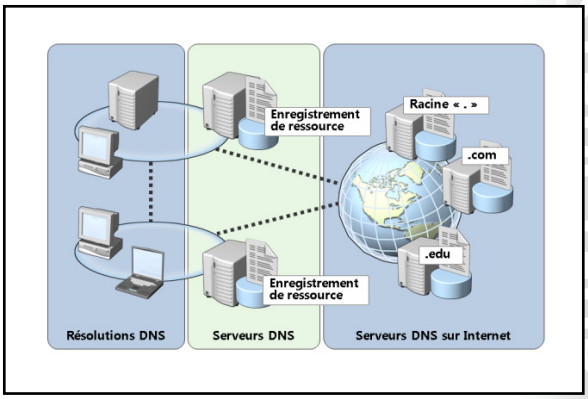
Objectifs de la leçon

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

- dresser la liste des composants d'une solution DNS ;
- décrire le fonctionnement des différents types de requêtes DNS ;
- décrire les enregistrements de ressource DNS ;
- expliquer le fonctionnement des indications de racine ;
- expliquer le fonctionnement de la redirection et de la redirection conditionnelle ;
- expliquer le fonctionnement de la mise en cache du serveur DNS ;
- expliquer comment configurer les propriétés du rôle serveur DNS.

Quels sont les composants d'une solution DNS ?

Les composants d'une solution DNS incluent les serveurs DNS, les serveurs DNS sur Internet et les résolveurs ou clients DNS.



Serveurs DNS

Un serveur DNS répond aux requêtes DNS récursives et itératives. Les serveurs DNS peuvent également héberger une ou plusieurs zones d'un domaine particulier. Les zones contiennent différents enregistrements de ressource. Les serveurs DNS peuvent également mettre en cache des recherches afin de gagner du temps pour les requêtes communes.

Serveurs DNS sur Internet

Les serveurs DNS sur Internet sont accessibles au public. Ils hébergent des informations de zones publiques et le serveur racine, ainsi que d'autres domaines de niveau supérieur courants tels que .com, .net et .edu.

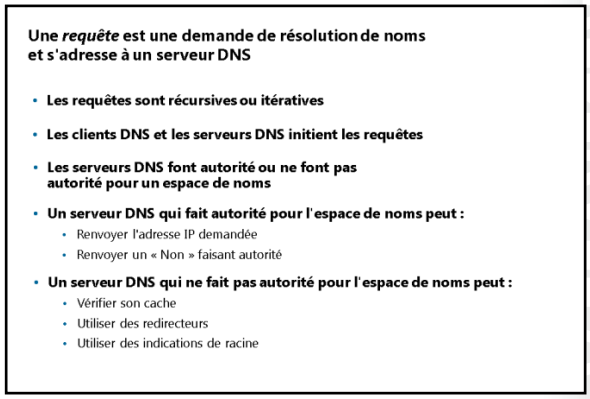
Remarque : Ne confondez pas ces serveurs avec les serveurs DNS de votre organisation qui hébergent votre espace de noms public. Ceux-ci sont situés physiquement sur votre réseau de périmètre.

Résolutions DNS

Le résolveur DNS génère et envoie des requêtes itératives ou récursives au serveur DNS. Un résolveur DNS peut être tout ordinateur exécutant une recherche DNS qui requiert une interaction avec le serveur DNS. Les serveurs DNS peuvent également publier des demandes DNS sur d'autres serveurs DNS.

Qu'est-ce qu'une requête en mode DNS ?

Une requête DNS correspond à la méthode que vous utilisez pour demander une résolution de nom et implique une requête envoyée à un serveur DNS. Il existe deux types de réponses aux requêtes DNS : celles faisant autorité et celles ne faisant pas autorité.



Il est important de noter que les serveurs DNS peuvent également servir de résolveurs DNS et envoyer des requêtes DNS à d'autres serveurs DNS.

Un serveur DNS peut faire autorité ou ne pas faire autorité pour l'espace de noms de la requête. Un serveur DNS *fait autorité* lorsqu'il héberge une copie principale ou secondaire d'une zone DNS. Les deux types de requêtes sont les suivants :

- Une requête faisant autorité est une requête pour laquelle le serveur peut renvoyer une réponse qu'il juge correcte parce que la demande est adressée au serveur faisant autorité qui gère le domaine.
- Un serveur DNS qui contient dans son cache le domaine demandé répond à une requête ne faisant pas autorité en utilisant des redirecteurs ou des indications de racine. Toutefois, la réponse fournie risque de ne pas être exacte parce que seul le serveur DNS faisant autorité pour le domaine donné peut publier cette information.

Si le serveur DNS fait autorité pour l'espace de noms de la requête, il vérifie la zone, puis réagit de l'une des manières suivantes :

- Il renvoie l'adresse demandée.
- Il renvoie une réponse de type « Non, ce nom n'existe pas » faisant autorité.

Remarque : Une réponse faisant autorité peut être donnée uniquement par le serveur faisant autorité directe pour le nom demandé.

S'il *ne fait pas autorité* pour l'espace de noms de la requête, le serveur DNS local réagit de l'une des manières suivantes :

- Il vérifie son cache et renvoie une réponse mise en cache.
- Il transmet la requête qu'il ne sait pas résoudre à un serveur spécifique appelé redirecteur.
- Il utilise les adresses connues de plusieurs serveurs racines pour rechercher un serveur DNS faisant autorité afin de résoudre la requête. Ce processus utilise des indications de racine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Requêtes récursives

Une requête récursive peut avoir deux résultats possibles :

- Elle renvoie l'adresse IP de l'hôte demandé.
- Le serveur DNS ne peut pas résoudre une adresse IP.

Pour des raisons de sécurité, il est parfois nécessaire de désactiver les requêtes récursives sur un serveur DNS. Ceci empêche le serveur DNS en question de transférer ses requêtes DNS à un autre serveur. Cette désactivation peut s'avérer utile lorsque vous ne souhaitez pas qu'un serveur DNS particulier communique à l'extérieur de son réseau local.

Requêtes itératives

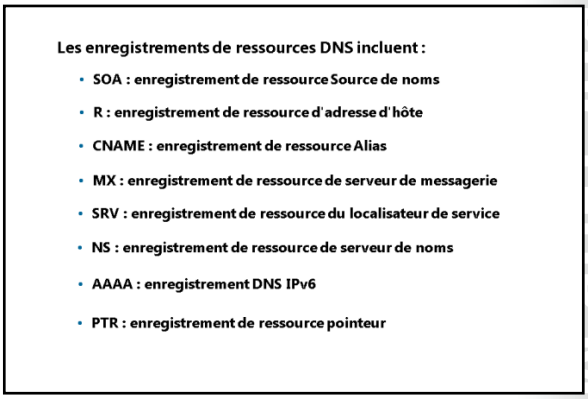
Les requêtes itératives fournissent un mécanisme d'accès aux informations de noms de domaine qui se trouvent dans tout le système DNS et permettent aux serveurs de résoudre rapidement et efficacement des noms sur de nombreux serveurs.

Lorsqu'un serveur DNS reçoit une demande à laquelle il ne peut pas répondre en utilisant ses informations locales ou ses recherches mises en cache, il fait la même demande à un autre serveur DNS en utilisant une requête itérative.

Lorsqu'un serveur DNS reçoit une requête itérative, il peut répondre soit en indiquant l'adresse IP du nom de domaine (s'il la connaît), soit en adressant la demande aux serveurs DNS responsables du domaine sur lequel porte la requête.

Enregistrements de ressources DNS

Le fichier de zone DNS stocke les enregistrements de ressources. Les enregistrements de ressources spécifient un type de ressource et l'adresse IP permettant de localiser la ressource. L'enregistrement de ressource le plus courant est un enregistrement de ressource **A**. Il s'agit d'un enregistrement simple qui résout un nom d'hôte en une adresse IP. L'hôte peut être une station de travail, un serveur ou un autre périphérique réseau, tel qu'un routeur.



Les enregistrements de ressources facilitent également la recherche de ressources pour un domaine particulier. Par exemple, quand un serveur Exchange doit rechercher le serveur qui est chargé de livrer le courrier à un autre domaine, il demande l'enregistrement MX (Mail Exchanger) de ce domaine, qui pointe vers l'enregistrement *A* de l'hôte qui exécute le service de messagerie SMTP.

Les enregistrements de ressources peuvent également contenir des attributs personnalisés. Les enregistrements MX, par exemple, comportent un attribut de préférence, qui s'avère utile si une organisation possède plusieurs serveurs de messagerie. En effet, cet attribut indique au serveur d'envoi le serveur de messagerie que l'organisation réceptrice préfère. Les enregistrements du localisateur de service (SRV) contiennent également des informations sur le port que le service écoute et le protocole que vous devez suivre pour communiquer avec le service.

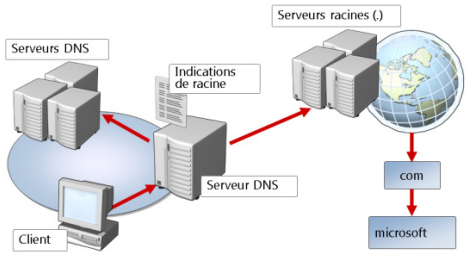
Le tableau suivant décrit les enregistrements de ressources les plus courants.

Enregistrements de ressources DNS	Description
Enregistrement de ressource SOA (Source de noms)	L'enregistrement identifie le serveur de noms principal pour une zone DNS, ainsi que d'autres détails, comme Durée de vie (TTL) et les actualise.
Enregistrement de ressource d'adresse d'hôte (A)	L'enregistrement principal qui résout un nom d'hôte en une adresse IPv4.
Enregistrement de ressource de nom canonique (CNAME)	Un type d'enregistrement d'alias qui mappe un nom à un autre (par exemple, www.microsoft.com est un CNAME de l'enregistrement *A* de microsoft.com).
Enregistrement de ressource MX	L'enregistrement est utilisé pour spécifier un serveur de messagerie électronique pour un domaine particulier.
Enregistrement de ressource SRV	L'enregistrement identifie un service qui est disponible dans le domaine. Active Directory utilise ces enregistrements de manière intensive.
Enregistrement de ressource de serveur de noms (NS)	L'enregistrement identifie un serveur de noms pour un domaine.
AAAA	L'enregistrement principal qui résout un nom d'hôte en une adresse IPv6.
Enregistrement de ressource pointeur (PTR)	L'enregistrement est utilisé pour rechercher une adresse IP et la mapper à un nom de domaine. La zone de recherche inversée stocke les noms.

Qu'est-ce que les indications de racine ?

Les indications de racine correspondent à la liste des serveurs sur Internet que votre serveur DNS utilise s'il ne parvient pas à résoudre une requête DNS en utilisant un redirecteur DNS ou son propre cache. Les indications de racine correspondent aux serveurs les plus élevés dans la hiérarchie DNS et peuvent fournir les informations nécessaires à un serveur DNS pour qu'il exécute une requête itérative sur la couche inférieure suivante de l'espace de noms DNS.

***Les indications de racine* contiennent les adresses IP des serveurs DNS racines**



Les serveurs racines sont automatiquement installés lorsque vous installez le rôle DNS. Ils sont copiés à partir du fichier cache.dns inclus dans les fichiers d'installation du rôle DNS.

Vous pouvez également ajouter des indications de racine à un serveur DNS pour prendre en charge des recherches de domaines non contigus dans une forêt.

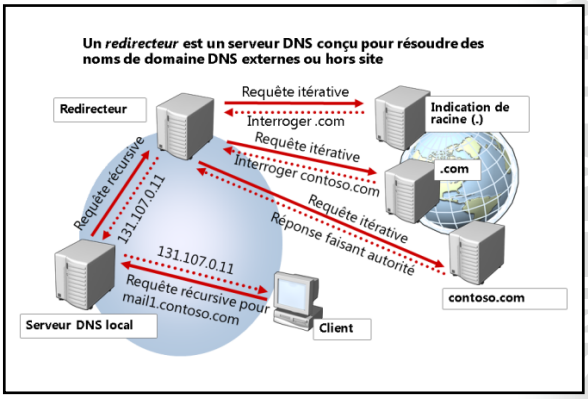
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsqu'un serveur DNS communique avec un serveur d'indications de racine, il utilise uniquement une requête itérative. Si vous sélectionnez l'option **Ne pas utiliser la récursivité pour ce domaine**, le serveur ne sera pas en mesure d'exécuter des requêtes sur les indications de racine. Si vous configurez le serveur pour utiliser un redirecteur, il essaiera d'envoyer une requête récursive à son serveur de redirection. Si le serveur de redirection ne répond pas à cette requête, le serveur répondra que l'hôte est introuvable.

Il est important de comprendre que la récursivité sur un serveur DNS et les requêtes récursives sont deux choses différentes. La récursivité sur un serveur signifie que le serveur utilise ses indications de racine pour essayer de résoudre une requête DNS. La rubrique suivante décrit les requêtes itératives et récursives de manière plus approfondie.

Qu'est-ce que le transfert ?

Un redirecteur est un paramètre de configuration de serveur DNS qui transfère des requêtes DNS de noms DNS externes aux serveurs DNS situés à l'extérieur de ce réseau. Vous pouvez également utiliser des redirecteurs conditionnels pour transférer des requêtes en fonction de noms de domaine spécifiques.



Un serveur DNS de réseau est appelé redirecteur lorsque d'autres serveurs DNS de ce réseau lui transfèrent les demandes qu'ils ne savent pas résoudre localement. En utilisant un redirecteur, vous pouvez gérer la résolution des noms situés à l'extérieur de votre réseau, tels que des noms sur Internet, et améliorer l'efficacité de la résolution de noms pour les ordinateurs de votre réseau.

Le serveur qui transfère les demandes sur le réseau doit être capable de communiquer avec le serveur DNS situé sur Internet. Cela signifie que soit vous le configurez afin de transférer les demandes à un autre serveur DNS, soit il utilise des indications de racine pour communiquer.

Méthode conseillée

Utilisez un serveur DNS de redirection central pour la résolution de noms Internet. Il permet d'améliorer les performances, de simplifier la résolution des problèmes et constitue une méthode conseillée pour assurer la sécurité. Vous pouvez isoler le serveur DNS de redirection dans un réseau de périmètre, lequel garantit qu'aucun serveur au sein du réseau ne communique directement avec Internet.

Redirection conditionnelle

Un redirecteur conditionnel est un paramètre de configuration du serveur DNS qui redirige des requêtes DNS en fonction du nom du domaine DNS contenu dans les requêtes. Par exemple, vous pouvez configurer un serveur DNS afin qu'il transfère toutes les requêtes qu'il reçoit concernant des noms se terminant par corp.contoso.com à l'adresse IP d'un serveur DNS spécifique ou aux adresses IP de plusieurs serveurs DNS. Ce transfert peut s'avérer utile lorsque vous avez plusieurs espaces de noms DNS dans une forêt.

Méthodes conseillées pour la redirection conditionnelle

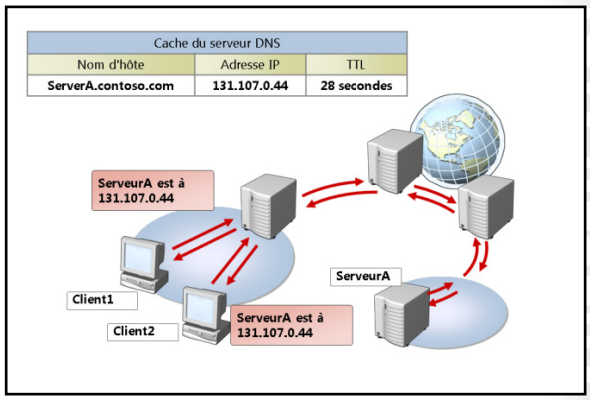
Utilisez des redirecteurs conditionnels si vous avez plusieurs espaces de noms internes. Ainsi, la résolution de noms est plus rapide.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fonctionnement de la mise en cache du serveur DNS

La mise en cache DNS augmente les performances du système DNS d'une organisation en accélérant les recherches DNS.

Lorsqu'un serveur DNS résout correctement un nom DNS, il ajoute ce nom à son cache. Au fur et à mesure, il génère un cache des noms de domaine et de leurs adresses IP associées pour les domaines les plus courants que l'organisation utilise ou auxquels elle accède.



Remarque : Le délai par défaut de mise en cache des données DNS s'élève à une heure. Pour configurer ce paramètre, modifiez l'enregistrement SOA pour la zone DNS appropriée.

Un serveur cache uniquement n'héberge pas des données de zone DNS ; il répond seulement aux recherches des clients DNS. Il s'agit du type idéal de serveur DNS à utiliser en tant que redirecteur.

Le cache client DNS est un cache DNS que le service Client DNS enregistre sur l'ordinateur local. Pour afficher le cache côté client actuel, exécutez la commande **ipconfig /displaydns** dans l'invite de commandes. Si vous devez désactiver le cache local, par exemple lorsque vous dépannez la résolution de noms, utilisez la commande **ipconfig /flushdns**.

Remarque : Vous pouvez également utiliser les applets de commande Windows PowerShell® suivants :

- **clear-DnsClientCache** pour supprimer le cache de résolution DNS
- **get-DnsClientCache** pour afficher le cache de résolution

Démonstration : Configuration du rôle de serveur DNS

Cette démonstration montre comment configurer les propriétés du serveur DNS.

Procédure de démonstration

Configurer les propriétés du serveur DNS

1. Basculez vers LON-DC2, puis si nécessaire, connectez-vous avec le nom **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Ouvrez la console DNS .

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Examinez les propriétés du serveur LON-DC2 :
    a. Dans l'onglet **Redirecteurs**, vous pouvez configurer le transfert.
    b. Dans l'onglet **Avancé**, vous pouvez configurer des options comme sécuriser le cache contre la pollution et DNSSEC.
    c. Dans l'onglet **Indications de racine**, vous pouvez voir la configuration des serveurs d'indications de racine.
    d. Dans l'onglet **Enregistrement de débogage**, vous pouvez configurer les options d'enregistrement de débogage.
    e. Dans l'onglet **Enregistrement des événements**, vous pouvez configurer le niveau d'enregistrement des événements.
    f. Dans l'onglet **Analyse**, vous pouvez réaliser des essais simples et récursifs par rapport au serveur.
    g. Dans l'onglet **Sécurité**, vous pouvez définir des autorisations sur l'infrastructure DNS.

Configurer la redirection conditionnelle

- À partir du nœud **Redirecteurs conditionnels**, vous pouvez configurer la redirection conditionnelle :
    a. Dans la boîte de dialogue **Nouveau redirecteur conditionnel**, dans la zone **Domaine DNS**, saisissez **contoso.com**.
    b. Cliquez sur la zone **<Cliquez ici pour ajouter un adresse IP ou un nom DNS>**. Saisissez **232.207.2.2**, puis appuyez sur Entrée. La validation échouera puisqu'il s'agit simplement d'un exemple de configuration.

Effacer le cache DNS

- Dans le volet de navigation, cliquez avec le bouton droit sur **LON-DC2**, puis cliquez sur **Effacer le cache**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Configuration des zones DNS

Les zones DNS constituent un important concept dans l'infrastructure DNS, car elles vous permettent de séparer et de gérer les domaines DNS de manière logique. Cette leçon fournit des informations de base permettant de comprendre les relations entre les zones et les domaines DNS ainsi que des informations sur les différents types de zones DNS disponibles dans le rôle DNS de Windows Server 2022.

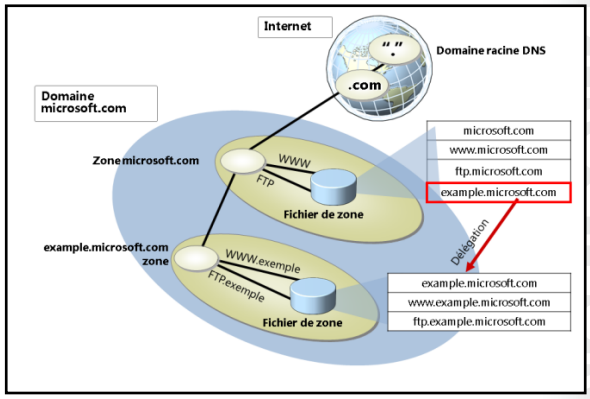
Objectifs de la leçon

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

- expliquer une zone DNS ;
- expliquer les différents types de zone DNS disponibles dans Windows Server 2022 ;
- expliquer la fonction des zones de recherche directe et inversée ;
- expliquer l'objectif des zones de stub ;
- expliquer comment créer des zones ;
- expliquer comment utiliser la délégation de zone DNS.

Qu'est-ce qu'une zone DNS ?

Une zone DNS héberge l'intégralité ou une partie d'un domaine et ses sous-domaines. La diapositive illustre la manière dont les sous-domaines peuvent appartenir à la même zone que leurs parents ou être délégués à une autre zone. Le domaine microsoft.com est séparé en deux zones. La première zone héberge les enregistrements de www.microsoft.com et de ftp.microsoft.com. Example.microsoft.com est délégué à une nouvelle zone, laquelle héberge le sous-domaine example.microsoft.com et ses enregistrements (ftp.example.microsoft.com et www.example.microsoft.com).



Remarque : La zone qui héberge une racine du domaine (microsoft.com) doit déléguer le sous-domaine (example.microsoft.com) à la deuxième zone. Dans le cas contraire, example.microsoft.com sera traité comme s'il faisait partie de la première zone.

Les données de zone peuvent être répliquées sur plusieurs serveurs. Cette réplication ajoute de la redondance à une zone parce que les informations nécessaires pour rechercher des ressources dans la zone existent désormais sur deux serveurs ou plus. Le niveau de redondance nécessaire constitue une raison de créer des zones. Si vous avez une zone qui héberge des enregistrements de ressources de serveurs critiques, il est probable que cette zone possède un niveau de redondance plus élevé qu'une zone dans laquelle des périphériques non critiques sont définis.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Caractéristiques d'une zone DNS

Les données d'une zone sont gérées sur un serveur DNS et peuvent être stockées de deux manières :

- dans un fichier de zone plat qui contient des listes de correspondance ;
- intégrées dans Active Directory.

Un serveur DNS fait autorité pour une zone s'il héberge les enregistrements de ressources correspondant aux noms et aux adresses que les clients demandent dans le fichier de zone.

Quels sont les types de zones DNS ?

Les quatre types de zones DNS sont :

- Principale
- Secondaire
- Stub
- Intégrée à Active Directory

Zones	Description
Principale	Copie en lecture/écriture d'une base de données DNS
Secondaire	Copie en lecture seule d'une base de données DNS
Stub	Copie d'une zone contenant uniquement des enregistrements utilisés pour localiser des serveurs de noms
Intégrée à Active Directory	Données de zone stockées dans Active Directory plutôt que dans des fichiers de zone

Zone principale

Lorsqu'une zone hébergée par un serveur DNS est une zone principale, le serveur DNS est la source principale d'informations sur cette zone et il stocke la copie originale des données de la zone dans un fichier local ou dans les services de domaine Active Directory (AD DS). Lorsque le serveur DNS stocke la zone dans un fichier, le fichier de la zone principale est, par défaut, nommé zone_name.dns et se trouve dans le dossier %windir%\System32\Dns du serveur. Lorsque la zone n'est pas stockée dans Active Directory, le serveur DNS hébergeant la zone principale est le seul serveur DNS qui a une copie accessible en écriture du fichier de zone.

Zone secondaire

Lorsqu'une zone hébergée par un serveur DNS est une zone secondaire, le serveur DNS est une source secondaire pour les informations de cette zone. La zone au niveau de ce serveur doit être obtenue à partir d'un autre serveur DNS distant qui l'héberge également. Ce serveur DNS doit avoir un accès réseau au serveur DNS distant pour recevoir les informations mises à jour de la zone. Étant donné qu'une zone secondaire est une copie d'une zone principale qu'un autre serveur héberge, elle ne peut pas être stockée dans AD DS. Les zones secondaires peuvent être utiles si vous répliquez des données à partir des zones DNS qui ne sont pas sur Windows ou si vous exécutez le système DNS sur les serveurs qui ne sont pas des contrôleurs de domaine AD DS.

Zone de stub

Windows Server 2003 a introduit les zones de stub, qui permettent de résoudre plusieurs problèmes liés aux grands espaces de noms DNS et aux forêts multi-arborescentes. Une forêt multi-arborescente est une forêt Active Directory qui contient deux noms de domaine de niveau supérieur différents.

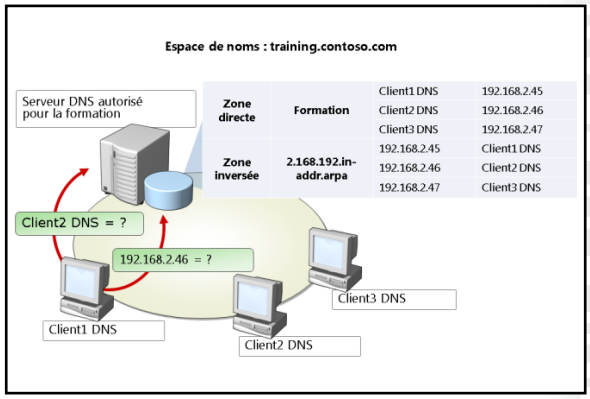
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Zone intégrée à Active Directory

Si Active Directory stocke la zone, le serveur DNS peut tirer parti du modèle de réplication multimaître pour répliquer la zone principale. Cela vous permet de modifier des données de zone sur tout serveur DNS. Windows Server 2008 a introduit un nouveau concept appelé contrôleur de domaine en lecture seule (RODC, read-only domain controller). Les données d'une zone intégrée à Active Directory peuvent être répliquées sur des contrôleurs de domaine, même si le rôle DNS n'est pas installé sur le contrôleur de domaine. Si le serveur est un contrôleur de domaine en lecture seule, un processus local ne peut pas écrire dans les données.

Qu'est-ce que les zones de recherche directe et inversée ?

Les zones peuvent être directes ou inversées. Les zones inversées sont parfois appelées zones inverses.



Zone de recherche directe

La zone de recherche directe résout des noms d'hôte en adresses IP et héberge les enregistrements de ressources courants suivants : A, CNAME, SRV, MX, SOA, TXT et NS.

Zone de recherche inversée

La zone de recherche inversée résout une adresse IP en nom de domaine et héberge les enregistrements SOA, NS et PTR.

Une zone inversée fonctionne de la même manière qu'une zone directe, mais l'adresse IP est la partie de la requête et le nom d'hôte correspond aux informations renvoyées. Les zones inversées ne sont pas toujours configurées, mais vous devez les configurer pour réduire le nombre de messages d'avertissement et d'erreur. De nombreux protocoles Internet standard se fient aux données de recherche des zones inversées pour valider les informations des zones directes. Par exemple, si la recherche directe indique que training.contoso.com est résolu en 292.268.2.45, vous pouvez utiliser une recherche inversée pour confirmer que 292.268.2.45 est associé à training.contoso.com.

Il est important d'avoir une zone inversée si vous possédez des applications recherchent des hôtes par leurs adresses IP. De nombreuses applications consignent ces informations dans des journaux de sécurité ou des événements. Si vous observez une activité suspecte à partir d'une adresse IP particulière, vous pouvez résoudre l'hôte à l'aide des informations de la zone inversée.

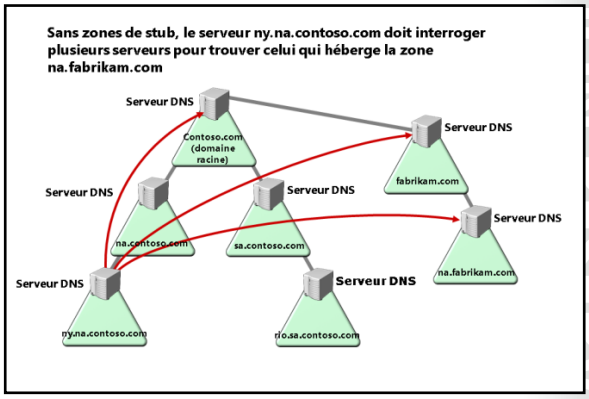
De nombreuses passerelles de sécurité de messagerie électronique utilisent des recherches inversées pour confirmer qu'une adresse IP qui envoie des messages est associée à un domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des zones de stub

Une zone de stub est une copie répliquée d'une zone qui contient uniquement les enregistrements de ressources nécessaires à l'identification des serveurs DNS faisant autorité pour la zone en question. Une zone de stub résout les noms entre des espaces de noms DNS distincts, lesquels peuvent s'avérer nécessaires lorsqu'une fusion d'entreprises a besoin que les serveurs DNS de deux espaces de noms DNS distincts résolvent les noms des clients dans les deux espaces de noms.



Une zone de stub comprend ce qui suit :

- l'enregistrement de ressource Source de noms (SOA, Start Of Authority), les enregistrements de ressources Serveur de noms (NS, Name Server) et les enregistrements de ressources de type « A » de la zone déléguée ;
- l'adresse IP d'un ou de plusieurs serveurs maîtres que vous pouvez utiliser pour mettre à jour la zone de stub.

Les serveurs maîtres d'une zone de stub correspondent à un ou plusieurs serveurs DNS faisant autorité pour la zone enfant, généralement le serveur DNS hébergeant la zone principale pour le nom de domaine délégué.

Résolution d'une zone de stub

Lorsqu'un résolveur DNS effectue une opération de requête récursive sur un serveur DNS hébergeant une zone de stub, ce serveur utilise les enregistrements de ressources de la zone de stub pour résoudre la requête. Le serveur DNS envoie une requête itérative aux serveurs DNS faisant autorité que spécifient les enregistrements de ressources NS de la zone de stub, comme s'il utilisait les enregistrements de ressources NS de sa mémoire cache. S'il ne trouve pas les serveurs DNS faisant autorité dans sa zone de stub, le serveur DNS qui héberge la zone de stub essaie la récursivité standard à l'aide d'indications de racine.

Le serveur DNS stockera les enregistrements de ressources qu'il reçoit des serveurs DNS faisant autorité qu'une zone de stub répertorie dans son cache, mais il ne stockera pas les enregistrements de ressources dans la zone de stub elle-même. Seuls les enregistrements SOA, NS et A envoyés en réponse à la requête sont stockés dans la zone de stub. Les enregistrements de ressources stockés dans le cache sont conservés conformément à la durée de vie (TTL) indiquée dans chaque enregistrement de ressource. Les enregistrements de ressources SOA, NS et A, qui ne sont pas écrits dans le cache, expirent conformément à l'intervalle d'expiration que l'enregistrement SOA de la zone de stub spécifie. Pendant la création de la zone de stub, l'enregistrement SOA est créé. Les mises à jour des enregistrements SOA se produisent pendant les transferts de la zone principale d'origine à la zone de stub.

Si la requête est itérative, le serveur DNS renvoie une référence contenant les serveurs spécifiés par la zone de stub.

Communication entre des serveurs DNS qui hébergent des zones parents et enfants

Un serveur DNS qui délègue un domaine à une zone enfant sur un serveur DNS différent est informé des nouveaux serveurs DNS faisant autorité pour la zone enfant uniquement lorsque les enregistrements de ressources qui les concernent sont ajoutés à la zone parent que le serveur DNS héberge. Il s'agit d'un processus manuel qui requiert que les administrateurs des différents serveurs DNS communiquent souvent. Les zones de stub permettent à un serveur DNS qui héberge une zone de stub pour l'un de ses domaines délégués d'obtenir des mises à jour des serveurs DNS faisant autorité pour la zone enfant lorsque la zone de stub est mise à jour. La mise à jour est effectuée depuis le serveur DNS qui héberge la zone de stub et l'administrateur du serveur DNS qui héberge la zone enfant n'a pas besoin d'être contacté.

Différence entre les zones de stub et les redirecteurs conditionnels

Il peut exister une certaine confusion au sujet de l'opportunité d'utiliser les redirecteurs conditionnels plutôt que des zones de stub. Cela est dû au fait que les deux fonctionnalités de DNS permettent à un serveur DNS de répondre à une requête avec une référence à un autre serveur DNS ou en la transférant à un autre serveur DNS. Pourtant, ces paramètres ont des objectifs différents :

- Un paramètre de redirecteur conditionnel configure le serveur DNS afin qu'il transfère une requête qu'il reçoit à un serveur DNS, en fonction du nom DNS contenu dans la requête.
- Une zone de stub maintient le serveur DNS qui héberge une zone parent informé de tous les serveurs DNS faisant autorité sur une zone enfant.

Quand utiliser les redirecteurs conditionnels

Si vous souhaitez que les clients DNS de réseaux distincts résolvent leurs noms respectifs sans avoir à interroger les serveurs DNS sur Internet, notamment dans le cas d'une fusion d'entreprises, vous devez configurer les serveurs DNS de chaque réseau pour qu'ils redirigent les requêtes de noms de l'autre réseau. Les serveurs DNS d'un réseau redirigent les noms des clients de l'autre réseau vers un serveur DNS spécifique qui crée un cache volumineux contenant les informations relatives à l'autre réseau. Cela vous permet de créer un point de contact direct entre les serveurs DNS des deux réseaux, ce qui réduit le besoin de récursivité.

Toutefois, les zones de stub n'apportent pas le même avantage de serveur à serveur. La raison est qu'un serveur DNS hébergeant une zone de stub dans un réseau répond aux requêtes de noms de l'autre réseau par la liste de tous les serveurs DNS qui font autorité sur la zone contenant ce nom, plutôt que les serveurs DNS spécifiques que vous avez désignés pour traiter ce trafic. Cette configuration complique tous les paramètres de sécurité que vous voulez établir entre les serveurs DNS spécifiques qui s'exécutent dans chacun des réseaux.

Quand utiliser des zones de stub

Utilisez les zones de stub quand vous souhaitez qu'un serveur DNS reste informé des serveurs DNS faisant autorité pour une zone étrangère.

Un redirecteur conditionnel ne constitue pas une méthode efficace pour maintenir un serveur DNS hébergeant une zone parente informé des serveurs DNS faisant autorité sur une zone enfant. En effet, dès que les serveurs DNS faisant autorité pour la zone enfant changent, vous devez configurer le paramètre du redirecteur conditionnel manuellement sur le serveur DNS qui héberge la zone parente. Plus précisément, vous devez mettre l'adresse IP à jour pour chaque nouveau serveur DNS faisant autorité pour la zone enfant.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Création des zones

Cette démonstration montre comment :

- créer une zone de recherche inversée ;
- créer une zone de recherche directe.

Procédure de démonstration

Créer une zone de recherche inversée

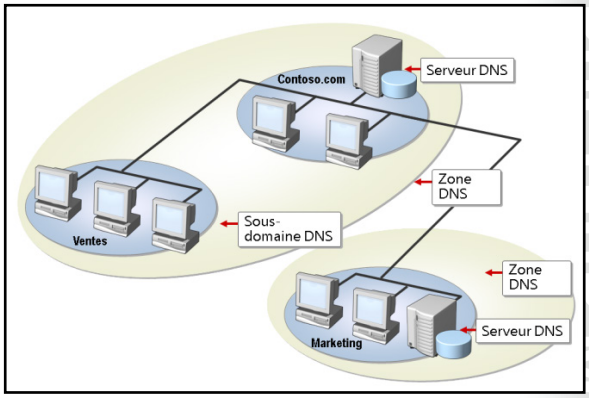
1. Basculez vers LON-DC2, puis créez une nouvelle zone de recherche inversée pour le sous-réseau IPv4 **272.26.0.0**.
2. Activez les mises à niveau dynamiques sur la zone.

Créer une zone de recherche directe

4. Basculez vers LON-SVR2, puis ouvrez la console DNS.
5. Créez une nouvelle zone de recherche directe.
3. Configurez le type comme secondaire, puis définissez **LON-DC2** en tant que serveur **Maître** pour cette zone.

Délégation de zone DNS

Le système DNS est hiérarchique et la délégation de zone relie les couches DNS entre elles. Une délégation de zone pointe vers le niveau hiérarchique inférieur suivant et identifie les serveurs de noms responsables du domaine de niveau inférieur.



Lorsque vous déterminez s'il est nécessaire de diviser l'espace de noms DNS pour ajouter des zones supplémentaires, considérez les raisons suivantes d'utiliser des zones supplémentaires :

- Vous avez besoin de déléguer la gestion d'une partie de l'espace de noms DNS à un autre emplacement ou département de votre organisation.
- Vous devez diviser une grande zone en zones plus petites afin de distribuer les charges de trafic entre plusieurs serveurs. Cela améliore les performances de résolution de nom DNS et crée un environnement DNS qui tolère mieux les pannes.
- Vous avez besoin d'étendre l'espace de noms en ajoutant de nombreux sous-domaines immédiatement pour prendre en charge l'ouverture d'une nouvelle filiale ou d'un nouveau site.

Leçon 4
Configuration des transferts de zone DNS

Les transferts de zone DNS déterminent la manière dont l'infrastructure DNS déplace les informations de zone DNS d'un serveur vers un autre. Sans transferts de zone, les différents serveurs de noms dans votre organisation gèrent des copies disparates des données de la zone. Vous devez également considérer que la zone contient des données sensibles et la protection des transferts de zone est importante. Cette leçon décrit les différentes méthodes que le rôle de serveur DNS utilise lors du transfert de zones.

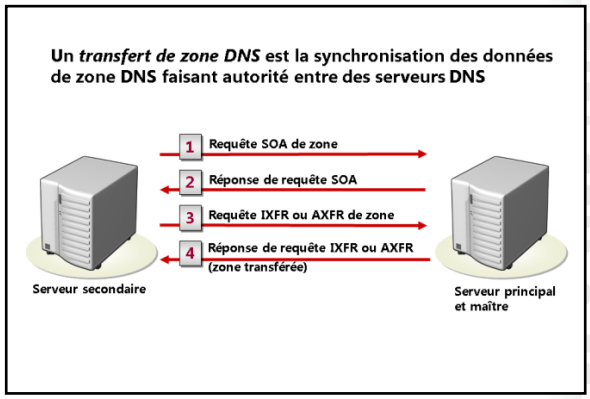
Objectifs de la leçon

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

- décrire le fonctionnement des transferts de zone DNS ;
- expliquer la manière de configurer la sécurité de transfert de zone ;
- expliquer la manière de configurer des transferts de zone DNS.

Qu'est-ce qu'un transfert de zone DNS ?

Un transfert de zone se produit lorsque vous répliquez la zone DNS située sur un serveur sur un autre serveur DNS.



Les transferts de zone synchronisent les zones de serveur DNS principales et secondaires. C'est ainsi que le système DNS constitue sa résilience sur Internet. Il est important que les zones DNS restent à jour sur les serveurs principaux et secondaires. Les divergences dans les zones principales et secondaires peuvent provoquer des défaillances du service et une résolution incorrecte des noms d'hôte.

Les transferts de zone peuvent se produire de l'une des trois façons suivantes :

- *Transfert de zone intégral*. Un transfert de zone complet se produit lorsque vous copiez la zone entière d'un serveur DNS vers un autre. Un transfert de zone complet est appelé AXFR (All Zone Transfer).
- *Transfert de zone incrémentiel*. Un transfert de zone incrémentiel se produit lorsqu'une mise à jour du serveur DNS est effectuée et que seuls les enregistrements de ressources modifiés sont répliqués sur l'autre serveur. Il s'agit d'un transfert de zone incrémentiel (IXFR, Incremental Zone Transfer).
- *Transfert rapide*. Les serveurs DNS Windows effectuent également des *transferts rapides*, qui correspondent à un type de transfert de zone qui utilise la compression et envoie plusieurs enregistrements de ressources dans chaque transmission.

Toutes les implémentations de serveurs DNS ne prennent pas en charge les transferts de zone incrémentiels et rapides. Lors de l'intégration d'un serveur DNS Windows 2022 avec un serveur DNS BIND (Berkeley Internet Name Domain), vous devez vérifier que les fonctionnalités dont vous avez besoin sont prises en charge par la version BIND installée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le tableau suivant répertorie les fonctionnalités que les différents serveurs DNS prennent en charge.

Serveur DNS	Transfert de zone complet (AXFR)	Transfert de zone incrémentiel (IXFR)	Transfert rapide
BIND antérieur à 4.9.4	Pris en charge	Non pris en charge	Non pris en charge
BIND versions 4.9.4 à 8.2	Pris en charge	Non pris en charge	Pris en charge
BIND 8.2	Pris en charge	Pris en charge	Pris en charge
Windows 2000 Service Pack 3 (SP3)	Pris en charge	Pris en charge	Pris en charge
Windows 2003 (R2)	Pris en charge	Pris en charge	Pris en charge
Windows 2008 et R2	Pris en charge	Pris en charge	Pris en charge
Windows 2022	Pris en charge	Pris en charge	Pris en charge

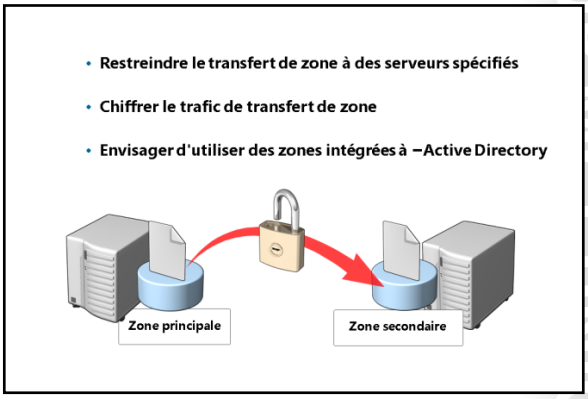
Les zones intégrées à Active Directory répliquent les informations à l'aide de la réplication des services de domaine Active Directory multimaîtres au lieu du processus de transfert de zone. Cela signifie que tout contrôleur de domaine standard qui détient également le rôle DNS peut mettre à jour les informations de zone DNS, qui se répliquent ensuite sur tous les serveurs DNS qui hébergent la zone DNS.

DNS Notify

DNS Notify est utilisé par un serveur maître pour avertir ses serveurs secondaires configurés que des mises à jour de zone sont disponibles. Les serveurs secondaires interrogent alors leur maître pour obtenir les mises à jour. DNS Notify est une mise à jour de la spécification d'origine du protocole DNS qui permet d'informer les serveurs secondaires lorsqu'une zone est modifiée. Cette mise à jour s'avère utile dans un environnement où le temps est crucial et où l'exactitude des données est importante.

Configuration de la sécurité du transfert de zone

Les informations de zone fournissent des données d'entreprise. Vous devez donc prendre des précautions pour vérifier qu'elles sont protégées contre tout accès d'utilisateur malintentionné et qu'il n'est pas possible de les remplacer par des données erronées (ce processus est appelé *empoisonnement DNS*). Une façon de protéger l'infrastructure DNS est de sécuriser les transferts de zone.



Dans l'onglet **Transferts de zone** de la boîte de dialogue **Propriétés de la zone**, vous pouvez spécifier la liste des serveurs DNS autorisés. Vous pouvez également utiliser ces options pour rejeter le transfert de zone. Par défaut, les transferts de zone sont désactivés.

Bien que l'option spécifiant les serveurs autorisés à demander des données de zone garantisse leur sécurité en limitant les destinataires de ces données, elle ne sécurise pas ces données pendant leur transmission. Si les informations de zone sont hautement confidentielles, nous vous recommandons d'utiliser une stratégie de sécurité du protocole Internet (IPsec, Internet Protocol Security) pour sécuriser la transmission ou de répliquer les données de zone sur un tunnel de réseau privé virtuel (VPN, Virtual Private Network). Ainsi, vous empêchez les détecteurs de paquet d'identifier des informations contenues dans la transmission des données.

L'utilisation de zones intégrées à Active Directory permet de répliquer les données de zone dans le cadre de réplications AD DS normales. Le transfert de zone est alors sécurisé lors de la réplication des services de domaine Active Directory.

Démonstration : Configuration des transferts de zone DNS

Cette démonstration vous explique comment :

- activer les transferts de zone DNS ;
- mettre la zone secondaire à jour depuis le serveur maître ;
- mettre la zone principale à jour et vérifier ensuite les modifications sur la zone secondaire.

Procédure de démonstration

Activer les transferts de zone DNS

1. Sur LON-DC2, activez les transferts de zone en configurant l'option **Autoriser les transferts de zone**.
2. Configurez les transferts de zone à **Uniquement vers les serveurs listés dans l'onglet Serveurs de noms**.
3. Configurez la notification sur **Uniquement vers les serveurs listés dans l'onglet Serveurs de noms**.
4. Ajoutez **LON-SVR2.adatum.com** en tant que serveur de noms répertorié pour recevoir des transferts.

Mettre la zone secondaire à jour depuis le serveur maître

- Basculez vers LON-SVR2 et dans le Gestionnaire DNS, sélectionnez **Transfert à partir du maître**. Il est parfois nécessaire d'effectuer cette étape un certain nombre de fois avant les transferts de zone. Notez également que le transfert peut se produire automatiquement à tout moment.

Mettre la zone principale à jour et vérifier ensuite les modifications sur la zone secondaire

1. Revenez à LON-DC2, puis créez un enregistrement d'alias.
2. Revenez à LON-SVR2, puis vérifiez que le nouvel enregistrement est présent dans la zone secondaire. Cela peut nécessiter un **Transfert à partir du maître** manuel et une actualisation de l'écran avant que l'enregistrement soit visible.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR UNIQUEMENT

Leçon 5
Gestion et dépannage du système DNS

Le service DNS est crucial dans l'infrastructure Active Directory. Lorsque le service DNS rencontre des problèmes, il est important de savoir comment les résoudre et de savoir identifier les problèmes courants pouvant se produire dans une infrastructure DNS. Cette leçon décrit les problèmes courants qui se produisent dans le service DNS, les sources d'informations DNS courantes et les outils que vous pouvez utiliser pour résoudre les problèmes.

Objectifs de la leçon

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

- expliquer en quoi la durée de vie, le vieillissement et le nettoyage facilitent la gestion des enregistrements DNS ;
- expliquer comment gérer la durée de vie, le vieillissement et le nettoyage des enregistrements DNS ;
- expliquer comment identifier des problèmes liés à DNS à l'aide des outils DNS ;
- décrire comment dépanner le système DNS à l'aide des outils DNS ;
- expliquer comment analyser le système DNS à l'aide du journal des événements DNS et de l'enregistrement de débogage.

Qu'est-ce qu'est la durée de vie, le vieillissement et le nettoyage ?

La durée de vie (TTL, Time to Live), le vieillissement et le nettoyage facilitent la gestion des enregistrements de ressources DNS dans les fichiers de zone. Les fichiers de zone peuvent changer au fil du temps ; par conséquent, il doit exister un moyen de gérer les enregistrements DNS mis à jour ou non valides parce que les hôtes qu'ils représentent ne se trouvent plus sur le réseau.

Le tableau suivant décrit les outils DNS qui permettent de gérer une base de données DNS.

Fonctionnalité	Description
TTL	Indique la durée de validité d'un enregistrement DNS
Vieillissement	Se produit lorsque les enregistrements insérés dans le serveur DNS atteignent leur date d'expiration et sont supprimés
Nettoyage	Exécute le nettoyage des anciens enregistrements de ressources de serveurs DNS dans le système DNS

Outil	Description
TTL	Indique la durée pendant laquelle un enregistrement DNS demeure valide et inéligible au nettoyage.
Vieillissement	Se produit lorsque les enregistrements insérés dans le serveur DNS atteignent leur date d'expiration et sont supprimés. Le vieillissement permet de maintenir l'exactitude de la base de données de zone. Dans le cadre d'un fonctionnement normal, le vieillissement doit gérer les enregistrements de ressources DNS obsolètes.
Nettoyage	Exécute le nettoyage des anciens enregistrements de ressources de serveurs DNS dans le système DNS. Si des enregistrements de ressources n'ont pas subi de vieillissement, un administrateur peut débarrasser la base de données de zone des enregistrements obsolètes qu'elle contient en forçant le nettoyage de la base de données.

Si elle n'est pas gérée, la présence d'enregistrements de ressources obsolètes dans les données de zone peut engendrer des problèmes. Par exemple :

- Si un grand nombre d'enregistrements de ressources obsolètes restent dans les zones du serveur, ils peuvent finir par occuper l'espace disque du serveur et provoquer des transferts de zone inutilement longs.
- Un serveur DNS qui charge les zones avec des enregistrements de ressources obsolètes risque d'utiliser des informations obsolètes pour répondre aux requêtes des clients, ce qui risque d'amener les ordinateurs clients à rencontrer des problèmes de résolution de noms ou de connectivité sur le réseau.
- L'accumulation d'enregistrements de ressources obsolètes sur le serveur DNS risque de dégrader ses performances et sa réactivité.
- Dans certains cas, la présence d'un enregistrement de ressource obsolète dans une zone peut empêcher un autre ordinateur ou périphérique d'hôte d'utiliser un nom de domaine DNS.

Pour résoudre ces problèmes, le service de serveur DNS comporte les fonctionnalités suivantes :

- Horodatage, selon la date et l'heure du jour définies sur le serveur, pour tous les enregistrements de ressources ajoutés dynamiquement aux zones de type principal. En outre, les horodatages sont enregistrés dans les zones principales standard pour lesquelles vous activez le vieillissement et le nettoyage.
- Pour les enregistrements de ressources que vous ajoutez manuellement, vous utilisez une valeur d'horodatage égale à zéro pour indiquer que le processus de vieillissement n'affecte pas ces enregistrements et qu'ils peuvent rester définitivement dans les données de zone, sauf si vous modifiez leur horodatage ou si vous les supprimez.
- Vieillissement des enregistrements de ressources dans les données locales, en fonction d'une période d'actualisation spécifiée, pour toutes zones éligibles.
- Seules les zones de type principal que le service de serveur DNS charge peuvent participer à ce processus.
- Nettoyage de tous les enregistrements de ressources conservés au-delà de la période d'actualisation spécifiée.

Lorsqu'un serveur DNS exécute une opération de nettoyage, il peut déterminer que les enregistrements de ressources ont vieilli au point d'être devenus obsolètes et les supprimer ensuite des données de zone. Vous pouvez configurer des serveurs afin qu'ils exécutent automatiquement des opérations de nettoyage récurrentes, ou vous pouvez initialiser une opération de nettoyage immédiate au niveau du serveur.

 **Remarque :** Par défaut, le mécanisme de vieillissement et de nettoyage du service de serveur DNS est désactivé. Vous devez l'activer uniquement lorsque vous comprenez entièrement tous les paramètres. Sinon, vous risquez de configurer le serveur afin qu'il supprime accidentellement des enregistrements qui ne devraient pas être supprimés. Si un enregistrement est supprimé accidentellement, non seulement les utilisateurs ne pourront pas résoudre les requêtes le concernant, mais ils pourront créer cet enregistrement et en devenir propriétaire, même sur les zones que vous configurez à des fins de mise à jour dynamique sécurisée. Cela présente un risque important pour la sécurité.

Le serveur utilise le contenu de chaque horodatage propre aux enregistrements de ressources, ainsi que d'autres propriétés de vieillissement et de nettoyage que vous pouvez ajuster ou configurer, pour déterminer le moment auquel il nettoie les enregistrements.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Conditions préalables pour le vieillissement et le nettoyage

Avant de pouvoir utiliser les fonctionnalités de vieillissement et de nettoyage du système DNS, plusieurs conditions doivent être remplies :

- Vous devez activer les fonctionnalités de nettoyage et de vieillissement sur le serveur DNS et la zone. Par défaut, le vieillissement et le nettoyage des enregistrements de ressources est désactivé.
- Vous devez ajouter des enregistrements de ressources dynamiquement ou les modifier manuellement afin de les utiliser dans des opérations de vieillissement et de nettoyage.

En général, seuls les enregistrements de ressources que vous ajoutez dynamiquement à l'aide du protocole de mise à jour dynamique DNS peuvent faire l'objet d'un vieillissement et d'un nettoyage.

Pour les enregistrements que vous ajoutez aux zones en chargeant un fichier de zone de type texte depuis un autre serveur DNS ou en les ajoutant manuellement à une zone, un horodatage égal à zéro est défini. Cet horodatage rend ces enregistrements inéligibles à une utilisation dans des opérations de vieillissement et de nettoyage.

Pour modifier cette valeur par défaut, vous pouvez administrer individuellement ces enregistrements, les réinitialiser et les autoriser à utiliser une valeur d'horodatage actuelle (différente de zéro). Celle-ci permet à ces enregistrements de vieillir et d'être nettoyés.

Démonstration : Gestion des enregistrements DNS

Cette démonstration montre comment :

- configurer la durée de vie ;
- activer et configurer le nettoyage et le vieillissement.

Procédure de démonstration

Configurer la durée de vie

1. Basculez vers LON-DC2, puis ouvrez les propriétés de la zone **Adatum.com**.
2. Dans l'onglet **Source de noms**, configurez la valeur **Durée de vie minimale (par défaut)** à **2** heures.

Activer et configurer le nettoyage et le vieillissement

1. Cliquez avec le bouton droit sur **LON-DC2**, puis sélectionnez l'option **Vieillissement de serveur/Propriétés de nettoyage** pour configurer les options de vieillissement et de nettoyage.
2. Activez **Nettoyer les enregistrements de ressources obsolètes**, puis utilisez les valeurs par défaut.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Test de la configuration du serveur DNS

Des problèmes peuvent se produire lorsque vous ne configurez pas le serveur DNS, ainsi que ses zones et ses enregistrements de ressources, correctement. Lorsque des enregistrements de ressources provoquent des problèmes, il peut s'avérer parfois plus difficile d'identifier le vrai problème parce que les problèmes de configuration ne sont pas toujours évidents.

Le tableau suivant répertorie les problèmes de configuration susceptibles de provoquer des problèmes de serveur DNS.

Problème	Result
Enregistrements manquants	Les enregistrements pour un hôte ne se trouvent pas sur le serveur DNS. Ils ont peut-être été nettoyés prématurément. Cela peut empêcher des stations de travail de se connecter.
Enregistrements incomplets	Les enregistrements auxquels il manque des informations requises pour localiser la ressource qu'ils représentent peuvent amener des clients qui demandent la ressource à utiliser des informations non valides. Par exemple, un enregistrement de service qui ne contient pas l'adresse de port requise est un exemple d'enregistrement incomplet.
Enregistrements mal configurés	Les enregistrements qui pointent vers une adresse IP non valide ou qui comportent des informations non valides dans leur configuration provoquent des problèmes lorsque des clients DNS essaient de rechercher des ressources.

Les outils utilisés pour résoudre ces problèmes et d'autres problèmes de configuration sont les suivants :

- *Nslookup*. Utilisez cet outil pour interroger des informations DNS. Il s'agit d'un outil flexible, capable de fournir des informations précieuses à propos de l'état du serveur DNS. Vous pouvez également l'utiliser pour rechercher des enregistrements de ressources et valider leur configuration. Vous pouvez, en outre, tester des transferts de zone, des options de sécurité et la résolution des enregistrements MX.

 **Remarque :** Vous pouvez utiliser l'applet de commande Windows PowerShell **Resolve-DnsName** pour remplir des fonctions similaires à Nslookup en résolvant les problèmes liés au système DNS.

- *Windows PowerShell*. Vous pouvez utiliser les applets de commande Windows PowerShell pour configurer et dépanner différents aspects du système DNS.
- *Dnscmd*. Gérez le service de serveur DNS à l'aide de cette interface de ligne de commande. Cet utilitaire permet de créer des scripts dans des fichiers de commandes dans le but d'automatiser des tâches de gestion DNS de routine ou de procéder à un simple travail d'installation et de configuration sans assistance de nouveaux serveurs DNS sur votre réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *IPconfig*. Utilisez cette commande pour afficher et modifier les détails de la configuration IP que l'ordinateur utilise. Cet utilitaire inclut des options de ligne de commande supplémentaires que vous pouvez utiliser pour dépanner les clients DNS et les prendre en charge. Vous pouvez consulter le cache DNS local d'un client à l'aide de la commande **ipconfig /displaydns** et vous pouvez effacer le cache local à l'aide de la commande **ipconfig /flushdns**.

Remarque : Vous pouvez également utiliser les applets de commande Windows PowerShell suivants :

  - **clear-DnsClientCache** pour supprimer le cache de résolution DNS
  - **get-DnsClientCache** pour afficher le cache de résolution

- *Onglet Analyse sur le serveur DNS*. Sous l'onglet Analyse du serveur DNS, vous pouvez configurer un test qui permet au serveur DNS de déterminer s'il peut résoudre des requêtes locales simples et exécuter une requête récursive dans le but de vérifier que le serveur peut communiquer avec des serveurs en amont. Vous pouvez également planifier ces tests pour qu'ils s'exécutent de manière régulière.

  Ce sont des tests de base, mais ils constituent un bon point de départ pour dépanner le service DNS. Les causes possibles de l'échec d'un test incluent les suivantes :

  - Le service de serveur DNS a échoué.
  - Le serveur en amont n'est pas disponible sur le réseau.

Cette démonstration montre comment utiliser Nslookup.exe pour tester la configuration du serveur DNS.

Procédure de démonstration

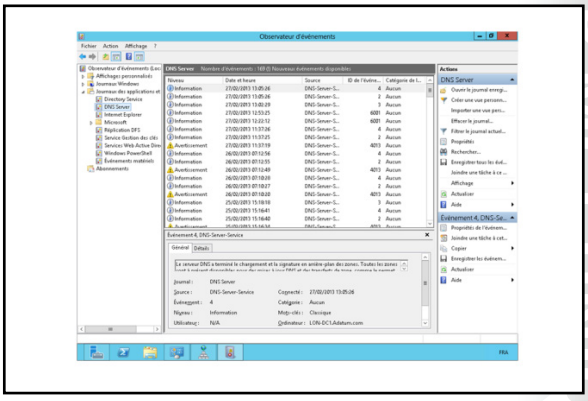
1. Ouvrez une invite de commandes, puis exécutez la commande suivante :

```
nslookup – d2 LON-svr2.Adatum.com
```

2. Examinez les informations fournies par nslookup.

Analyse du système DNS à l'aide du journal des événements DNS

Le serveur DNS possède sa propre catégorie dans le journal des événements. Comme avec tout journal des événements de l'Observateur d'événements Windows®, vous devez consulter régulièrement le journal des événements.



Événements DNS courants

Le tableau suivant décrit les événements DNS courants.

ID d'événement	Description
2	Le serveur DNS a démarré. Ce message apparaît généralement au démarrage lorsque vous démarrez soit le serveur, soit le service de serveur DNS.
3	Le serveur DNS a été arrêté. Ce message apparaît généralement lorsque le serveur est arrêté ou lorsque vous arrêtez le service de serveur DNS manuellement.
408	Le serveur DNS n'a pas pu ouvrir le socket pour l'adresse [IPaddress]. Vérifiez qu'il s'agit d'une adresse IP valide pour le serveur. Pour corriger le problème, vous pouvez effectuer les opérations suivantes : 1. Si l'adresse IP spécifiée n'est pas valide, supprimez-la de la liste des interfaces restreintes du serveur et redémarrez le serveur. 2. Si l'adresse IP spécifiée n'est plus valide et qu'elle était la seule adresse activée que le serveur DNS pouvait utiliser, le serveur risque de ne pas avoir démarré en raison de cette erreur de configuration. Pour corriger ce problème, supprimez la valeur suivante du Registre et redémarrez le serveur DNS : HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DNS\Parameters\ListenAddress 3. Si l'adresse IP du serveur est valide, vérifiez qu'aucune autre application susceptible d'utiliser le même port de serveur DNS (telle qu'une autre application de serveur DNS) ne s'exécute. Par défaut, le serveur DNS utilise le port TCP 53.
423	• Le serveur DNS envoie des demandes à d'autres serveurs DNS sur un port autre que son port par défaut (port TCP 53). • Ce serveur DNS est multirésident et a été configuré afin de restreindre le service de serveur DNS à quelques-unes de ses adresses IP configurées uniquement. C'est pourquoi il n'existe aucune garantie que les requêtes DNS soumises par ce serveur à d'autres serveurs DNS distants seront envoyées à l'aide de l'une des adresses IP activées pour le serveur DNS. • Cela risque d'empêcher les réponses aux requêtes renvoyées par ces serveurs d'être reçues sur le port DNS que le serveur est configuré pour utiliser. Pour éviter ce problème, le serveur DNS envoie des requêtes à d'autres serveurs DNS à l'aide d'un port non-DNS arbitraire, puis la réponse est reçue indépendamment de l'adresse IP utilisée. • Si vous souhaitez que le serveur DNS utilise uniquement son port DNS configuré pour envoyer des requêtes à d'autres serveurs DNS, utilisez la console DNS pour effectuer l'une des modifications suivantes dans la configuration des propriétés du serveur sous l'onglet **Interfaces** : o Sélectionnez Toutes les adresses IP pour permettre au serveur DNS d'écouter sur toutes les adresses IP du serveur configurées. o Sélectionnez Uniquement les adresses IP suivantes pour limiter la liste des adresses IP à une seule adresse IP du serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

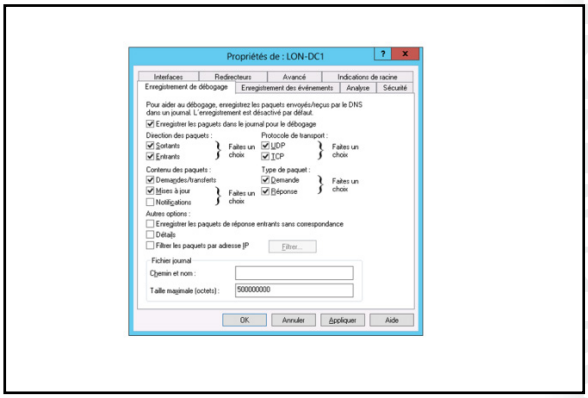
(suite)

ID d'événement	Description
424	Le serveur ne possède actuellement aucun suffixe DNS principal configuré. Son nom DNS est actuellement un nom d'hôte en une partie. Par exemple, son nom configuré est *host* plutôt que *host.example.microsoft.com* ou un autre nom de domaine complet. Bien que le serveur DNS possède un nom en une partie, les enregistrements de ressources par défaut créés pour ses zones configurées utilisent uniquement ce nom en une partie pour faire correspondre le nom d'hôte de ce serveur DNS. Cela peut générer des références incorrectes et erronées lorsque les clients et d'autres serveurs DNS utilisent ces enregistrements pour localiser ce serveur par son nom. En général, vous devez reconfigurer le serveur DNS avec un nom d'ordinateur DNS complet approprié pour son domaine ou groupe de travail sur votre réseau.
708	Le serveur DNS n'a pas détecté de zones de type principal ou secondaire. Il s'exécutera en tant que serveur cache uniquement, mais ne fera autorité sur aucune zone.
3250	Le serveur DNS a écrit une nouvelle version de la zone [zonename] dans le fichier [filename]. Vous pouvez consulter le nouveau numéro de version en cliquant sur l'onglet **Données d'enregistrement**. Cet événement doit apparaître uniquement si vous configurez le serveur DNS en tant que serveur racine.
6527	La zone [*zonename*] a expiré avant la fin du transfert de zone ou de la mise à jour à partir d'un serveur maître agissant comme source pour la zone. La zone a été fermée. Cet ID d'événement peut apparaître lorsque vous configurez le serveur DNS afin d'héberger une copie secondaire de la zone à partir d'un autre serveur DNS qui lui sert de source ou de serveur maître. Vérifiez que ce serveur possède une connectivité réseau à son serveur maître configuré. Si le problème persiste, considérez une ou plusieurs des options suivantes : 1. Supprimez la zone et recréez-la, en spécifiant soit un serveur maître différent, soit une adresse IP mise à jour et corrigée du même serveur maître. 2. Si l'expiration de zone continue, envisagez d'ajuster l'intervalle d'expiration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Analyse du serveur DNS à l'aide de l'enregistrement de débogage

Parfois, il peut être nécessaire d'obtenir davantage de détails sur un problème DNS que ceux que l'Observateur d'événements fournit. Le cas échéant, vous pouvez utiliser l'enregistrement de débogage pour obtenir des informations supplémentaires.



Les options d'enregistrement de débogage DNS suivantes sont disponibles :

- *Direction des paquets*. Cette option comporte les paramètres suivants :
  - *Envoi*. Le fichier journal du serveur DNS enregistre les paquets que le serveur DNS envoie.
  - *Réception*. Le fichier journal enregistre les paquets que le serveur DNS reçoit.
- *Contenu des paquets*. Cette option comporte les paramètres suivants :
  - *Requête standard*. Indique que des paquets contenant des requêtes standard, conformément au document RFC (Request for Comments) 2034, sont enregistrés dans le fichier journal du serveur DNS.
  - *Mises à jour*. Indique que des paquets contenant des requêtes dynamiques, conformément au document RFC 2236, sont enregistrés dans le fichier journal du serveur DNS.
  - *Notifications*. Indique que des paquets contenant des notifications, conformément au document RFC 2996, sont enregistrés dans le fichier journal du serveur DNS.
- *Protocole de transport*. Cette option comporte les paramètres suivants :
  - *UDP*. Indique que des paquets envoyés et reçus via le protocole de datagramme utilisateur (UDP, User Datagram Protocol) sont enregistrés dans le fichier journal du serveur DNS
  - *TCP*. Indique que des paquets envoyés et reçus via le protocole TCP sont enregistrés dans le fichier journal du serveur DNS
- *Type de paquet*. Cette option comporte les paramètres suivants :
  - *Requête*. Enregistre des informations sur les paquets de demande dans le fichier journal du serveur DNS. Un paquet de requête est caractérisé par un bit de requête/réponse (QR) défini à zéro dans l'en-tête du message DNS.

    Un bit QR est un champ à un bit qui spécifie si ce message est une requête (0) ou une réponse.
  - *Réponse*. Enregistre des informations sur les paquets de réponse dans le fichier journal du serveur DNS. Un paquet de réponse est caractérisé par un bit QR défini à 2 dans l'en-tête du message DNS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Filtrer les paquets par adresse IP*. Cette option fournit d'autres options de filtrage des paquets enregistrés dans le fichier journal du serveur DNS. Cette option permet d'enregistrer dans le journal des informations sur les paquets envoyés à partir d'adresses IP spécifiques vers un serveur DNS ou inversement.
- Taille maximale (octets). Cette option vous permet de définir la taille de fichier maximale du fichier journal du serveur DNS. Lorsque le fichier journal du serveur DNS atteint sa taille maximale spécifiée, le serveur DNS remplace les informations des paquets les plus anciens par les nouvelles informations.

  Si vous ne spécifiez pas de taille de fichier journal maximale, le fichier journal du serveur DNS peut occuper une grande quantité d'espace disque.

Par défaut, toutes les options d'enregistrement de débogage sont désactivées. Lorsque vous les activez de manière sélective, le service de serveur DNS peut exécuter un enregistrement supplémentaire au niveau du suivi des types sélectionnés d'événements ou de messages pour le dépannage général et le débogage du serveur.

L'enregistrement de débogage DNS peut utiliser les ressources de manière intense, ce qui risque de nuire aux performances générales du serveur et consomme de l'espace disque. Par conséquent, vous devez l'utiliser uniquement de manière temporaire, lorsque vous avez besoin d'informations plus détaillées sur les performances du serveur.

 **Remarque :** Dns.log contient l'activité d'enregistrement de débogage. Par défaut, ce fichier se trouve dans le dossier %systemroot%\System32\Dns.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Configuration et résolution des problèmes du système DNS

Scénario

A. Datum est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2022.

Vous avez été invité à ajouter plusieurs nouveaux enregistrements de ressource au service DNS installé sur LON-DC2. Les enregistrements comprennent un nouvel enregistrement MX pour Exchange Server 2020 et un enregistrement SRV pour un déploiement Microsoft Lync® en cours.

A. Datum travaille avec une organisation partenaire, Contoso, Ltd. Vous avez été invité à configurer la résolution de nom interne entre ces deux organisations. Une petite succursale a signalé que les performances de résolution de noms sont faibles. La succursale est équipée d'un serveur Windows Server 2022 qui assume plusieurs rôles. Cependant, aucun plan n'a été établi en vue d'implémenter un contrôleur de domaine supplémentaire. Vous avez été invité à installer le rôle de serveur DNS dans la succursale et à créer une zone secondaire d'Adatum.com. Pour garantir la sécurité, vous avez été chargé de configurer le serveur de la succursale pour qu'il figure sur la liste de notification des transferts de zone Adatum.com. Vous devez aussi mettre à jour tous les clients de la succursale pour qu'ils utilisent le nouveau serveur de noms dans la succursale.

Vous devez configurer le nouveau rôle de serveur DNS pour exécuter le nettoyage et le vieillissement standard selon les besoins et conformément à la stratégie d'entreprise. Après l'implémentation du nouveau serveur, vous devez tester et vérifier la configuration à l'aide des outils standard de dépannage du système DNS.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- configurer les enregistrements de ressource DNS ;
- configurer la redirection conditionnelle DNS ;
- installer et configurer les zones DNS ;
- dépanner le système DNS.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22422B-LON-DC2 22422B-LON-SVR2 22422B-LON-CL2
Nom d'utilisateur	**ADATUM\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'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur 22422B-LON-DC2 et dans le volet Actions, cliquez sur **Accueil**.
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 22422B-LON-SVR2 et 22422B-LON-CL2.

Exercice 2 : Configuration des enregistrements de ressource DNS

Scénario

Vous avez été invité à ajouter plusieurs nouveaux enregistrements de ressource au service DNS installé sur LON-DC2. Les enregistrements comprennent un nouvel enregistrement MX pour Exchange Server 2020 et un enregistrement SRV requis pour un déploiement Lync en cours. Vous avez été également invité à configurer une zone de recherche inversée pour le domaine.

Les tâches principales de cet exercice sont les suivantes :

1. Ajouter l'enregistrement MX requis
2. Ajouter les enregistrements de serveur Lync requis
3. Créer la zone de recherche inversée

▶ Tâche 2 : Ajouter l'enregistrement MX requis

1. Basculez vers LON-DC2, puis connectez-vous avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Ouvrez la console du **Gestionnaire DNS**.
3. Créez un enregistrement d'hôte présentant les propriétés suivantes :
   - Zone : **Adatum.com**
   - Nom : **Mail2**
   - Adresse IP : **272.26.0.250**
4. Dans la zone **Adatum.com**, ajoutez un nouvel enregistrement avec les informations suivantes :
   - Type : **Nouveau serveur de messagerie (MX)**
   - Nom de domaine complet (FQDN) du serveur de messagerie : **Mail2.Adatum.com**.

▶ Tâche 2 : Ajouter les enregistrements de serveur Lync requis

1. Créez un enregistrement d'hôte présentant les propriétés suivantes :
   - Zone : **Adatum.com**
   - Nom : **Lync-svr2**
   - Adresse IP : **272.26.0.252**
2. Dans la zone **Adatum.com**, ajoutez un nouvel enregistrement :
   - Type : **Emplacement du service (SRV)**
   - Service : **_sipinternaltls**
   - Protocole : **_tcp**
   - Numéro de port : **5062**
   - Hôte offrant ce service : **Lync-svr2.adatum.com**.

▶ Tâche 3 : Créer la zone de recherche inversée

- Créez une nouvelle zone de recherche inversée avec les propriétés suivantes :
  - Type de zone : **Zone principale**
  - Étendue de la zone de réplication de Active Directory : Valeur par défaut
  - Nom de la zone de recherche inversée : **Zone de recherche inversée IPv4**
  - Nom de la zone de recherche inversée : **272.26.0**
  - Mise à jour dynamique : Valeur par défaut

Résultats : À la fin de cet exercice, vous aurez configuré les enregistrements de service de messagerie requis et la zone de recherche inversée.

Exercice 2 : Configuration de la redirection conditionnelle DNS

Scénario

Vous avez été invité à configurer la résolution de nom interne entre A. Datum Corporation et son organisation partenaire, Contoso Ltd.

Les tâches principales de cet exercice sont les suivantes :

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Ajouter l'enregistrement de redirection conditionnelle pour contoso.com

- À partir du nœud **Redirecteurs conditionnels**, configurez la redirection conditionnelle pour Contoso.com :

  a. Dans la boîte de dialogue **Nouveau redirecteur conditionnel**, dans la zone **Domaine DNS**, saisissez **contoso.com**.

  b. Cliquez sur la zone **<Cliquez ici pour ajouter une adresse IP ou un nom DNS>**. Saisissez **232.207.2.2**, puis appuyez sur Entrée. La validation échouera puisque le serveur ne peut pas être contacté.

  c. Activez **Stocker ce redirecteur conditionnel dans Active Directory, et le répliquer comme suit**.

Résultats : À la fin de cet exercice, vous aurez configuré avec succès la redirection conditionnelle.

Exercice 3 : Installer et configurer des zones DNS

Scénario

Une petite succursale a signalé que les performances de résolution de noms sont faibles. La succursale est équipée d'un serveur Windows Server 2022 qui assume plusieurs rôles. Cependant, aucun plan n'a été établi en vue d'implémenter un contrôleur de domaine supplémentaire. Vous avez été invité à installer le rôle de serveur DNS dans la succursale et à créer ensuite une zone secondaire d'Adatum.com. Pour garantir la sécurité, vous avez également été chargé de configurer le serveur de la succursale pour qu'il figure sur la liste de notification des transferts de zone Adatum.com. Vous devez aussi mettre à jour tous les clients de la succursale pour qu'ils utilisent le nouveau serveur de noms dans la succursale, puis configurer le nouveau rôle de serveur DNS pour exécuter le nettoyage et le vieillissement standard selon les besoins et conformément à la stratégie d'entreprise.

Les tâches principales de cet exercice sont les suivantes :

1. Installer le rôle de serveur DNS sur LON-SVR2
2. Créer les zones secondaires requises sur LON-SVR2
3. Activer et configurer les transferts de zone
4. Configurer la durée de vie, le vieillissement et le nettoyage
5. Configurer les clients pour qu'ils utilisent le nouveau nom de serveur

▶ Tâche 2 : Installer le rôle de serveur DNS sur LON-SVR2

1. Basculez vers LON-SVR2, puis connectez-vous avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Utilisez le **Gestionnaire de serveur** pour installer le rôle **Serveur DNS**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer les zones secondaires requises sur LON-SVR2

1. Ouvrez une invite de commandes.
2. Saisissez la commande suivante pour créer la zone secondaire requise :

```
Dnscmd.exe /zoneadd Adatum.com /secondary 272.26.0.20
```

3. Ouvrez le Gestionnaire DNS, puis vérifiez la présence de la nouvelle zone de recherche directe secondaire *Adatum.com*.

▶ Tâche 3 : Activer et configurer les transferts de zone

1. Basculez vers LON-DC2.
2. Ouvrez une invite de commandes, puis exécutez la commande suivante pour configurer des transferts de zone pour la zone Adatum.com :

```
Dnscmd.exe /zoneresetsecondaries Adatum.com /notifylist 272.26.0.22
```

3. Dans le Gestionnaire DNS, vérifiez les modifications des paramètres de transferts de zone :
   a. Dans le volet de navigation, cliquez sur **Adatum.com**, puis dans la barre d'outils, cliquez sur **Actualiser**.
   b. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Propriétés**.
   c. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur l'onglet **Transferts de zone**.
   d. Cliquez sur **Notifier** et vérifiez que le serveur **272.26.0.22** est listé. Cliquez sur **Annuler**.
   e. Fermez la boîte de dialogue **Propriétés de : Adatum.com**.

▶ Tâche 4 : Configurer la durée de vie, le vieillissement et le nettoyage

1. Sur LON-DC2, ouvrez les propriétés de la zone **Adatum.com**.
2. Dans l'onglet **Source de noms**, configurez la valeur **Durée de vie minimale (par défaut)** à **2** heures.
3. Cliquez avec le bouton droit sur **LON-DC2**, puis sélectionnez l'option **Définir le vieillissement/nettoyage pour toutes les zones…** pour configurer les options de vieillissement et de nettoyage.
4. Activez **Nettoyer les enregistrements de ressources obsolètes**, puis utilisez les valeurs par défaut.

▶ Tâche 5 : Configurer les clients pour qu'ils utilisent le nouveau nom de serveur

1. Connectez-vous à l'ordinateur virtuel LON-CL2 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Utilisez le Centre Réseau et partage pour afficher les propriétés de la connexion au réseau local.
3. Reconfigurez **Protocole Internet version 4 (TCP/IPv4)** comme suit :
   - Modifiez le serveur DNS préféré : **272.26.0.22**.

Résultats : À la fin de cet exercice, vous aurez installé et configuré avec succès DNS sur LON-SVR2.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 4 : Dépannage du système DNS

Scénario

Après l'implémentation du nouveau serveur, vous devez tester et vérifier la configuration à l'aide des outils standard de dépannage du système DNS.

Les tâches principales de cet exercice sont les suivantes :

1. Tester les requêtes simples et récursives
2. Vérifier les enregistrements de ressource de source de noms (SOA) avec Windows PowerShell®

▶ Tâche 2 : Tester les requêtes simples et récursives

1. Sur LON-DC2, dans le Gestionnaire DNS, ouvrez les propriétés de **LON-DC2**.
2. Sous l'onglet **Analyse**, exécutez une requête simple sur un serveur DNS. L'opération réussit.
3. Exécutez des requêtes simples et récursives sur le serveur concerné ainsi que sur d'autres serveurs DNS. Le test récursif échoue, car aucun redirecteur n'est configuré.
4. Arrêtez le service DNS, puis répétez les tests précédents. Ils échouent parce qu'aucun serveur DNS n'est disponible.
5. Redémarrez le service DNS, puis répétez les tests. Le test simple est réussi.
6. Fermez la boîte de dialogue **Propriétés de LON-DC2**.

▶ Tâche 2 : Vérifier les enregistrements de ressource de source de noms (SOA) avec Windows PowerShell®

1. Ouvrez Windows PowerShell LON-DC2.
2. Saisissez la commande suivante, puis appuyez sur Entrée :

```
resolve-dnsname –name Adatum.com –type SOA
```

3. Affichez les résultats, puis fermez l'invite Windows PowerShell.

Résultats : À la fin de cet exercice, vous aurez testé et vérifié le système DNS avec succès.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, 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 **22422B-LON-DC2**, 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 **22422B-LON-SVR2** et **22422B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Vous déployez des serveurs DNS dans un domaine Active Directory et votre client a besoin que l'infrastructure résiste aux points uniques de défaillance. Que devez-vous prendre en compte lors de la planification de la configuration DNS ?

Question : Quelle différence existe-t-il entre les requêtes récursives et itératives ?

Question : Que devez-vous configurer avant de pouvoir transférer une zone DNS vers un serveur DNS secondaire ?

Question : Vous êtes l'administrateur d'un environnement DNS Windows Server 2022. Votre société vient d'acquérir une autre société. Vous souhaitez répliquer sa zone DNS principale. La société acquise utilise Bind 4.9.4 pour héberger ses zones DNS principales. Vous remarquez une quantité significative de trafic entre le serveur DNS Windows Server 2022 et le serveur Bind. Pourquoi ?

Question : Vous devez automatiser un processus de configuration de serveur DNS afin de pouvoir automatiser le déploiement de Windows Server 2022. Quel outil DNS pouvez-vous utiliser ?

Outils

Outil	Utilisation	Emplacement
Dnscmd.exe	Configurer le rôle de serveur DNS	Ligne de commande
Dnslint.exe	Tester le serveur DNS	Téléchargez à partir du site Web de Microsoft et utilisez ensuite la ligne de commande
Nslookup.exe	Tester la résolution de noms DNS	Ligne de commande
Ping.exe	Test simple de résolution de nom DNS	Ligne de commande
Ipconfig.exe	Vérifier et tester la fonctionnalité IP et afficher ou effacer le cache de résolution du client DNS	Ligne de commande

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 3

Gestion des services de domaine Active Directory

Table des matières :

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

Leçon 1 : Vue d'ensemble d'AD DS **3-2**

Leçon 2 : Implémentation des contrôleurs de domaine virtualisés **3-8**

Leçon 3 : Implémentation des contrôleurs de domaine en lecture seule **3-13**

Leçon 4 : Administration d'AD DS **3-18**

Leçon 5 : Gestion de la base de données AD DS **3-18**

Atelier pratique : Gestion d'AD DS **3-37**

Contrôle des acquis et éléments à retenir **3-43**

Vue d'ensemble du module

Les services de domaine Active Directory® (AD DS) représentent le composant le plus critique d'un réseau Windows Server® 2012 basé sur un domaine. AD DS contient des informations importantes sur l'authentification, l'autorisation et les ressources dans votre environnement. Ce module explique pourquoi vous implémentez des fonctionnalités spécifiques d'AD DS, comment les composants importants s'intègrent les uns aux autres et comment vous pouvez vérifier que votre réseau basé sur un domaine fonctionne correctement.

Vous découvrirez de nouvelles fonctionnalités, telles que le clonage virtualisé de contrôleur de domaine, des fonctionnalités récentes comme les contrôleurs de domaine en lecture seule (RODC) et bien d'autres fonctionnalités et outils que vous pouvez utiliser dans l'environnement d'AD DS.

Objectifs

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

- Expliquer la structure générale d'AD DS.
- Implémenter des contrôleurs de domaine virtualisés.
- Implémenter des contrôleurs de domaine en lecture seule.
- Administrer AD DS.
- Gérer la base de données AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble d'AD DS

La base de données AD DS stocke des informations sur l'identité de l'utilisateur, les ordinateurs, les groupes, les services et les ressources. Les contrôleurs de domaine AD DS hébergent également le service qui authentifie les comptes d'utilisateur et informatiques quand ils se connectent au domaine. AD DS stocke des informations sur tous les objets du domaine, et tous les utilisateurs et ordinateurs doivent se connecter aux contrôleurs de domaine Active Directory DS quand ils se connectent au réseau. Par conséquent, AD DS est la méthode principale par laquelle vous pouvez configurer et gérer les comptes d'utilisateur et d'ordinateur sur votre réseau.

Cette leçon couvre les composants logiques de base d'un déploiement d'Active Directory DS.

Objectifs de la leçon

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

- Décrire les composants AD DS.
- Expliquer la structure de la forêt et schématique d'AD DS.
- Expliquer la structure de domaine d'AD DS.

Vue d'ensemble des composants AD DS

AD DS se compose à la fois de composants physiques et logiques. Vous devez comprendre la manière dont les composants d'Active Directory DS fonctionnent ensemble de sorte à pouvoir maintenir efficacement votre environnement AD DS.

AD DS se compose à la fois de composants physiques et logiques

Composants physiques	Composants logiques
• Magasin de données	• Partitions
• Contrôleurs de domaine	• Schéma
• Serveur de catalogue global	• Domaines
• Contrôleurs de domaine en lecture seule	• Arborescences de domaine
	• Forêts
	• Sites
	• Unités d'organisation

Composants physiques

Les informations relatives à AD DS sont stockées dans un fichier unique sur le disque dur de chaque contrôleur de domaine. Le tableau suivant présente quelques composants physiques et leurs emplacements de stockage.

Composant physique	Description
Contrôleurs de domaine	Contient des copies de la base de données AD DS.
Magasin de données	Fichier sur chaque contrôleur de domaine qui stocke les informations AD DS.
Serveurs de catalogue global	Hébergent le *catalogue global*, lequel est une copie partielle, en lecture seule, de tous les objets dans la forêt. Un catalogue global accélère les recherches d'objets susceptibles d'être stockés sur des contrôleurs de domaine d'un domaine différent de la forêt.
Contrôleurs de domaine en lecture seule (RODC)	Une installation AD DS spéciale au format lecture seule. Vous utilisez cela en général dans les filiales où la sécurité et le support technique peuvent être moins avancées que dans les centres d'affaires principaux d'une entreprise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

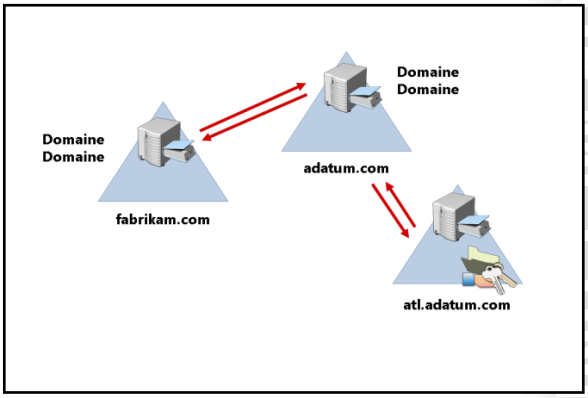
Composants logiques

Les composants logiques AD DS sont des structures utilisées pour l'implémentation d'une conception Active Directory appropriée à une organisation. Le tableau suivant décrit certains types de structures logiques qu'une base de données Active Directory peut contenir.

Composant logique	Description
Partition	Une section de la base de données AD DS. Bien que la base de données soit réellement juste un fichier nommé NTDS.DIT, les utilisateurs l'affichent, le gèrent et le répliquent comme s'il se composait de sections ou d'instances distinctes. Il s'agit de *partitions* ou de *contextes de nommage*.
Schéma	Définit la liste des types d'objets et d'attributs que tous les objets AD DS peuvent avoir.
Domaine	Limite d'administration logique pour les utilisateurs et les ordinateurs.
Arborescence de domaine	Collection des domaines qui partagent un domaine racine commun et un espace de noms du système de noms de domaine (DNS).
Forêt	Une collection des domaines qui partagent un service AD DS commun.
Site	Une collection d'utilisateurs, de groupes et d'ordinateurs, qui sont définis par leurs emplacements physiques. Les sites sont utiles dans des tâches d'administration de la planification telles que la réplication des modifications vers la base de données AD DS.
Unité d'organisation	Les unités d'organisation (OU) sont des conteneurs dans AD DS qui fournissent une infrastructure pour déléguer des droits administratifs et pour lier des objets de stratégie de groupe (GPO).

Présentation de la structure de la forêt et schématique d'AD DS

Dans AD DS, la structure de forêt et schématique sont importantes pour la définition de la fonctionnalité et de l'étendue de votre environnement.



Structure des forêts d'AD DS

Une *forêt* est une collection d'une ou plusieurs arbres de domaines. Une *forêt* est une collection d'une ou de plusieurs arborescences de domaine. Le premier domaine qui est créé dans la forêt est appelé le *domaine racine de la forêt*. Le *domaine racine de la forêt* contient quelques objets qui n'existent pas dans d'autres domaines de la forêt. Par exemple, le domaine racine de la forêt contient deux rôles spéciaux, le contrôleur de schéma et le maître d'attribution de noms de domaine. En outre, le groupe Administrateurs de l'entreprise et le groupe Administrateurs du schéma existent seulement dans le domaine racine de forêt. Le groupe Administrateurs de l'entreprise a le contrôle total sur chaque domaine de la forêt.

La forêt AD DS est une limite de sécurité. Ceci signifie que, par défaut, aucun utilisateur provenant de l'extérieur de la forêt ne peut accéder aux ressources situées à l'intérieur de la forêt. Cela signifie également que des administrateurs provenant de l'extérieur de la forêt n'ont aucun accès d'administration à l'intérieur de la forêt. Une des raisons principales pour lesquelles les organisations déploient plusieurs forêts est qu'elles doivent isoler des autorisations administratives entre différentes parties de l'organisation.

La forêt AD DS est également la limite de réplication pour les partitions de configuration et de schéma dans la base de données des services AD DS. Ceci signifie que tous les contrôleurs de domaine de la forêt doivent partager le même schéma. Une deuxième raison pour laquelle les organisations déploient plusieurs forêts est qu'elles doivent déployer des schémas incompatibles dans deux parties de l'organisation.

La forêt AD DS est également la limite de réplication du catalogue global. Ceci facilite la plupart des formulaires de collaboration entre les utilisateurs de différents domaines. Par exemple, tous les destinataires Microsoft® Exchange Server 2010 sont listés dans le catalogue global, ce qui facilite l'envoi de courrier électronique aux utilisateurs de la forêt, même ces utilisateurs dans des domaines différents.

Par défaut, tous les domaines d'une forêt approuvent automatiquement les autres domaines dans la forêt. Ceci facilite l'activation de l'accès aux ressources telles que des partages de fichiers et des sites Web pour tous les utilisateurs dans une forêt, indépendamment du domaine dans lequel le compte d'utilisateur est situé.

Structure schématique des services AD DS

Le *schéma AD DS* est le composant AD DS qui définit tous les types d'objets et attributs qu'AD DS utilise pour stocker des données. Il est parfois désigné en tant que modèle pour AD DS.

AD DS stocke et récupère les informations d'une grande variété d'applications et de services. Le service AD DS normalise la manière dont les données sont stockées de sorte qu'il puisse enregistrer et répliquer des données à partir de ces diverses sources. En normalisant la manière dont les données sont stockées, AD DS peut récupérer, mettre à jour et répliquer des données, tout en vérifiant que l'intégrité des données est maintenue.

AD DS utilise des objets comme unités de stockage. Tous les types d'objets sont définis dans le schéma. Chaque fois que le répertoire traite des données, le répertoire interroge le schéma pour une définition appropriée de l'objet. Selon la définition de l'objet dans le schéma, le répertoire crée l'objet et stocke les données.

Les définitions de l'objet contrôlent les types de données que les objets peuvent stocker et la syntaxe des données. En utilisant ces informations, le schéma vérifie que tous les objets se conforment à leurs définitions standard. En conséquence, AD DS peut stocker, récupérer et valider les données qu'il gère, indépendamment de l'application qui est la source d'origine des données. Seules des données qui ont une définition existante de l'objet dans le schéma peuvent être stockées dans le répertoire. Si un nouveau type de données doit être stocké, une nouvelle définition d'objet pour les données doit d'abord être créée dans le schéma.

Dans AD DS, le schéma définit ce qui suit :

- les objets qui sont utilisés pour stocker des données dans le répertoire ;
- les règles qui définissent quels types d'objets vous pouvez créer, quels attributs doivent être définis (obligatoire) quand vous créez l'objet et quels attributs sont facultatifs ;
- la structure et le contenu du répertoire elle-même.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez utiliser un compte qui est un membre des administrateurs de schéma pour modifier les composants de schéma sous forme de graphique. Les exemples des objets qui sont définis dans le schéma comprennent l'utilisateur, l'ordinateur, le groupe et le site. Parmi les nombreux attributs sont compris les suivants : **emplacement**, **accountExpires**, **buildingName**, **société**, **gestionnaire** et **displayName**.

Le contrôleur de schéma est l'un des contrôleurs de domaine des opérations à maître unique dans AD DS. Puisque c'est un maître unique, vous devez apporter des modifications au schéma en ciblant le contrôleur de domaine qui détient le rôle des opérations du contrôleur de schéma.

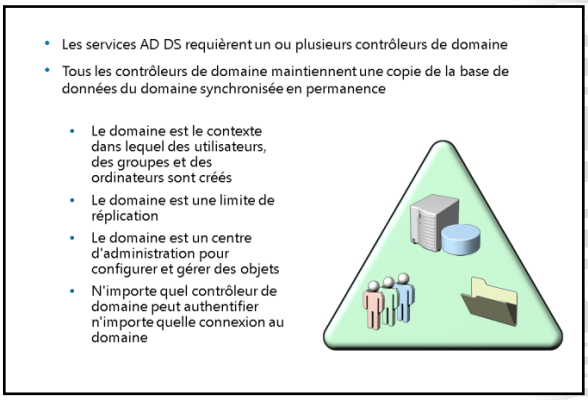
Le schéma est répliqué sur tous les contrôleurs de domaine de la forêt. Tout changement qui est apporté au schéma est répliqué à chaque contrôleur de domaine de la forêt à partir du titulaire du rôle du maître d'opérations de schéma, en général le premier contrôleur de domaine de la forêt.

Puisque le schéma dicte la manière dont les informations sont stockées et puisque toute modification apportée au schéma affecte chaque contrôleur de domaine, les modifications apportées au schéma doivent être réalisées seulement si nécessaire. Avant d'apporter des modifications, vous devez examiner les modifications au moyen d'un processus bien contrôlé, puis implémentez-les seulement après avoir réalisé le test pour vérifier que les modifications ne compromettront pas le reste de la forêt ni aucune application qui utilise AD DS.

Bien que vous ne puissiez pas apporter de modification au schéma directement, quelques applications apportent des modifications au schéma pour prendre en charge des fonctionnalités supplémentaires. Par exemple, quand vous installez Exchange Server 2010 dans votre forêt AD DS, le programme d'installation étend le schéma pour prendre en charge de nouveaux types d'objets et attributs.

Présentation de la structure de domaine AD DS

Un domaine AD DS est un regroupement logique d'utilisateur, ordinateur et objets collectifs pour des raisons de gestion et de sécurité. Tous ces objets sont enregistrés dans la base de données AD DS, et une copie de cette base de donnée est enregistrée sur chaque contrôleur de domaine dans le domaine AD DS.



Il y a plusieurs types d'objets qui peuvent être stockés dans la base de données AD DS, y compris des comptes d'utilisateur. Les comptes d'utilisateur fournissent un mécanisme que vous pouvez utiliser pour authentifier puis autoriser des utilisateurs à accéder à des ressources sur le réseau. Chacun ordinateur ayant un domaine joint doit avoir un compte dans AD DS. Ceci permet à des administrateurs de domaine d'utiliser les stratégies qui sont définies dans le domaine pour gérer les ordinateurs. Le domaine enregistre également des groupes, qui sont le mécanisme de regroupement des objets pour des raisons administratives ou de sécurité ; par exemple, des comptes d'utilisateur et des comptes d'ordinateur.

Le domaine AD DS est également une limite de réplication. Quand des modifications sont apportées à n'importe quel objet du domaine, cette modification est répliquée automatiquement à tous les autres contrôleurs de domaine du domaine.

Un domaine AD DS est un centre d'administration. Il contient un compte Administrateur et un groupe Administrateurs du domaine ; chacun a le contrôle total sur chaque objet du domaine. À moins qu'ils ne soient dans le domaine racine de forêt, leur plage de contrôle est toutefois limitée au domaine. Des règles de mot de passe et de compte sont gérées au niveau du domaine par défaut. Le domaine AD DS fournit également un centre d'authentification. Tous les comptes d'utilisateur et comptes d'ordinateur dans le domaine sont enregistrés dans la base de données du domaine et les utilisateurs et les ordinateurs doivent se connecter à un contrôleur de domaine pour s'authentifier.

Un domaine unique peut contenir plus de 1 million d'objets, ainsi la plupart des organisations doivent déployer un seul domaine. Les organisations qui ont décentralisé les structures administratives, ou qui sont distribués à travers plusieurs emplacements, pourraient plutôt implémenter plusieurs domaines dans la même forêt.

Contrôleurs de domaine

Un contrôleur de domaine est un serveur que vous pouvez configurer pour stocker une copie de la base de données d'annuaire AD DS (NTDS.DIT) et une copie du dossier SYSVOL (System Volume). Tous les contrôleurs de domaine, excepté les contrôleurs de domaine en lecture seule, enregistrent une copie en lecture/écriture de NTDS.DIT et du dossier SYSVOL. NTDS.DIT est la base de données elle-même et le dossier SYSVOL contient tous les paramètres de modèle des GPO.

Des modifications portant sur la base de données des services AD DS peuvent être initialisées sur n'importe quel contrôleur de domaine d'un domaine, hormis pour les contrôleurs de domaine en lecture seule. Le service de réplication AD DS synchronise alors les modifications et les mises à jour de la base de données AD DS vers tous autres contrôleurs de domaine du domaine. En outre, le service de réplication de fichiers (FRS) ou la réplication de système de fichiers distribués la plus récente (DFS-R) réplique les dossiers SYSVOL.

Un domaine AD DS doit toujours avoir un minimum de deux contrôleurs de domaine. De cette façon, si l'un des contrôleurs de domaine échoue, il y a une sauvegarde pour garantir la continuité des services de domaine AD DS. Quand vous décidez d'ajouter plus de deux contrôleurs de domaine, considérez la taille de votre organisation et des impératifs en matière de performances.

Unités d'organisation

Une unité d'organisation est un objet conteneur dans un domaine que vous pouvez utiliser pour consolider des utilisateurs, des groupes, des ordinateurs et d'autres objets. Il y a deux raisons de créer des unités d'organisation :

- pour configurer des objets contenus dans l'unité d'organisation. Vous pouvez attribuer des GPO à l'unité d'organisation et les paramètres s'appliquent à tous les objets dans l'unité d'organisation. Les GPO sont des stratégies que les administrateurs créent pour gérer et configurer les comptes d'ordinateurs et d'utilisateurs. La manière la plus commune de déployer ces stratégies est de les lier aux unités d'organisation.
- Pour déléguer le contrôle administratif d'objets présents dans l'unité d'organisation. Vous pouvez attribuer des autorisations de gestion sur une unité d'organisation, déléguant de ce fait le contrôle de cette unité d'organisation à un utilisateur ou à un groupe dans AD DS autre que l'administrateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez utiliser des unités d'organisation pour représenter les structures hiérarchiques et logiques au sein de votre organisation. Par exemple, vous pouvez créer des unités d'organisation qui représentent les services de votre organisation, les régions géographiques de votre organisation ou une combinaison des régions départementales et géographiques. Vous pouvez utiliser des unités d'organisation pour gérer la configuration et l'utilisation des comptes d'utilisateur, de groupe et d'ordinateur en fonction de votre modèle d'organisation.

Chaque domaine AD DS contient un jeu standard de conteneurs et d'unités d'organisation qui sont créés quand vous installez AD DS, y compris ce qui suit :

- un conteneur de domaine. Sert de conteneur racine à la hiérarchie.
- conteneur Users. L'emplacement par défaut pour les nouveaux comptes d'utilisateur et groupes que vous créez dans le domaine. Le conteneur Users contient également les comptes d'administrateur et d'invité du domaine, et quelques groupes par défaut.
- conteneur Computer. L'emplacement par défaut pour les nouveaux comptes d'ordinateur que vous créez dans le domaine.
- unité d'organisation Domain Controllers. L'emplacement par défaut des comptes d'ordinateur pour les comptes d'ordinateur du contrôleur de domaine. C'est la seule unité d'organisation qui est présente dans une nouvelle installation d'AD DS.

 **Remarque :** Aucun des conteneurs par défaut dans le domaine AD DS ne peut avoir des GPO liés à eux, excepté pour les unités d'organisation Contrôleurs de domaine par défaut et le domaine lui-même. Tous les autres conteneurs sont juste des dossiers. Pour lier des GPO afin d'appliquer des configurations et des restrictions, créez une hiérarchie des unités d'organisation, puis reliez-les aux GPO.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Implémentation des contrôleurs de domaine virtualisés

La virtualisation est une pratique commune des services informatiques. Les avantages de consolidation et de performances que la virtualisation fournit sont de grands atouts pour n'importe quelle organisation. Les services AD DS Windows Server 2012 et les contrôleurs de domaine connaissent désormais mieux la virtualisation. Dans cette leçon, vous découvrirez les éléments à prendre en compte concernant à l'implémentation de contrôleurs de domaine virtualisés dans Windows Server 2012 et la manière de déployer et de gérer ces contrôleurs de domaine dans l'environnement AD DS.

Objectifs de la leçon

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

- Identifier les éléments à prendre en compte concernant l'implémentation des contrôleurs de domaine virtualisés clonés.
- Expliquer comment déployer un contrôleur de domaine virtualisé cloné.
- Décrire comment gérer les instantanés de contrôleur de domaine virtualisés.

Présentation des contrôleurs de domaine virtualisés clonés

Windows Server 2012 fournit les fonctionnalités suivantes pour les contrôleurs de domaine virtualisés :
- Clonage sûr
- Restauration sûre depuis une capture d'écran

La mise en place des contrôleurs de domaine virtualisés offre les avantages suivants :
- Déploiement rapide des contrôleurs de domaine
- Mise en service évolutive des contrôleurs de domaine
- Remplacement ou récupération rapide des contrôleurs de domaine
- Approvisionnement facile des environnements de test

Windows Server 2012 présente le clonage de contrôleur de domaine virtualisé. Dans les versions précédentes de Windows Server, les contrôleurs de domaine qui s'exécutaient dans un ordinateur virtuel ne connaissaient pas leur état virtuel. Cela rendait potentiellement dangereux l'exécution de processus comme le clonage et la restauration d'instantanés d'ordinateur virtuel, car les modifications pouvaient se produire sur l'environnement du système d'exploitation non prévu par le contrôleur de domaine. Par exemple, deux contrôleurs de domaine ne peuvent pas coexister dans la même forêt avec le même nom, identificateur d'invocation et identificateur global unique (GUID) d'agent de système de répertoire (DSA). Dans des versions précédentes de Windows antérieures à Windows Server 2012, vous créiez des contrôleurs de domaine virtualisés en déployant une image de serveur de base Sysprepped, puis en la promouvant manuellement pour être un contrôleur de domaine. Windows Server 2012 fournit des fonctions spécifiques de virtualisation aux contrôleurs de domaine virtualisés (VDC) AD DS pour résoudre ces problèmes.

Les VDC Windows Server 2012 fournissent deux avantages importants :

- vous pouvez cloner des contrôleurs de domaine sans risque pour déployer une capacité supplémentaire et gagner du temps de configuration.
- La restauration accidentelle des instantanés de contrôleur de domaine ne perturbe pas l'environnement AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Clonage des VDC dans Windows Server 2012

Dans Windows Server 2012, cloner des ordinateurs virtuels qui agissent en tant que contrôleurs de domaine donne la possibilité de déployer rapidement des contrôleurs de domaine dans votre environnement. Par exemple, vous pouvez devoir augmenter les contrôleurs de domaine de votre environnement pour prendre en charge l'utilisation augmentée d'AD DS. Vous pouvez déployer rapidement des contrôleurs de domaine supplémentaires avec le processus suivant :

1. exécutez l'opération de clonage sur un VDC existant.
2. Arrêtez le VDC existant, puis utilisez Hyper-V pour exporter les fichiers de l'ordinateur virtuel.
3. Démarrez le VDC existant (s'il doit continuer dans l'utilisation de production).
4. Utilisez Hyper-V pour importer les fichiers de l'ordinateur virtuel en tant que nouvel ordinateur virtuel, puis mettez en marche l'ordinateur virtuel, qui contient maintenant le nouveau contrôleur de domaine.

Le clonage de contrôleur de domaine virtuel fournit les avantages suivants dans Windows Server 2012 :

- déploiement rapide du contrôleur de domaine dans une nouvelle forêt ou un nouveau domaine ;
- mise en service progressive des contrôleurs de domaine pour gérer la charge accrue ;
- remplacement ou récupération rapide des contrôleurs de domaine pour la continuité d'affaires ;
- mise en service rapide des environnements de test.

Clonage sûr

Les contrôleurs de domaine ont des caractéristiques uniques qui rendent le clonage non géré préjudiciable au processus de réplication de la base de données AD DS. Les contrôleurs de domaine simplement clonés terminent avec le même nom, ce qui n'est pas pris en charge dans le même domaine ou la même forêt. Dans les versions précédentes de Windows Server, vous deviez préparer un contrôleur de domaine au clonage à l'aide de **sysprep**. Après le processus de clonage, vous deviez alors promouvoir le nouveau serveur vers un contrôleur de domaine manuellement.

Avec le clonage sûr dans Windows Server 2012, un contrôleur de domaine cloné exécute automatiquement un sous-ensemble de processus **sysprep** et réalise la promotion avec les données existantes AD DS locales comme support d'installation.

Sauvegarde et restauration sûres

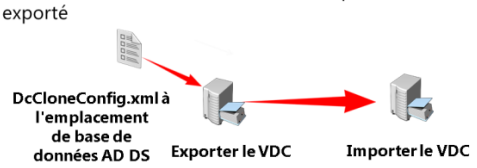
La restauration d'un ancien instantané d'un VDC est problématique car AD DS utilise la réplication à plusieurs maîtres qui se fonde sur des transactions ayant des valeurs numériques attribuées appelées des nombres de séquences de mise à jour (USN). Le VDC essaye d'attribuer des USN aux transactions antérieures qui ont déjà été attribuées aux transactions valides. Ceci provoque des incohérences dans la base de données AD DS. Windows Server 2003 et les versions plus récentes implémentent un processus qui est appelé la protection de la restauration des USN. Avec ceci en place, le VDC ne réplique pas, et vous devez le rétrograder de force ou le restaurer manuellement.

Windows Server 2012 détecte maintenant l'état instantané d'un contrôleur de domaine et synchronise ou réplique le delta des modifications, entre un contrôleur de domaine et ses partenaires pour AD DS et le SYSVOL. Vous pouvez maintenant utiliser des instantanés sans risque de désactiver de manière permanente des contrôleurs de domaine et de requérir manuellement la rétrogradation, le nettoyage de métadonnées et la repromotion forcés.

Déployer un contrôleur de domaine virtualisé cloné

Vous pouvez copier un contrôleur de domaine virtuel existant en toute sécurité en procédant comme suit :

1. créez un fichier DcCloneConfig.xml et enregistrez-le dans l'emplacement de base de données AD DS
2. prenez le VDC hors ligne et exportez-le
3. créez un nouvel ordinateur virtuel en important le VDC exporté



Lors du déploiement d'un VDC, considérez ce qui suit concernant l'installation :

- Tous les ordinateurs Windows Server 2012 prennent automatiquement en charge le clonage de VDC.
- Les exigences suivantes doivent être satisfaites pour prendre en charge le clonage des VDC :
  - Le rôle FSMO de l'émulateur du contrôleur de domaine principal (PDC) doit être situé sur un contrôleur de domaine Windows Server 2012.
  - Le contrôleur de domaine hébergeant le rôle d'opérations à maître unique flottant (FSMO) d'émulateur PDC doit être disponible pendant les opérations de clonage.
- Les exigences suivantes doivent être satisfaites pour prendre en charge le clonage des VDC et la restauration sûre :
  - les ordinateurs virtuels invités doivent exécuter Windows Server 2012 ;
  - la plateforme hôte de virtualisation doit prendre en charge l'identification de génération d'ordinateur virtuel (VM GENID). Ceci comprend Windows Server 2012 Hyper-V®.

Création d'un clone VDC

Pour créer un clone VDC dans Windows Server 2012, procédez comme suit :

1. Créer un fichier DcCloneConfig.xml qui contient la configuration du serveur unique.
2. Copier ce fichier dans l'emplacement de la base de données AD DS sur le contrôleur de domaine source (C:\Windows\NTDS par défaut). Ce fichier peut également être enregistré sur le support amovible, s'il y a lieu.
3. Prendre le VDC source hors connexion et l'exporter ou le copier.
4. Créer un nouvel ordinateur virtuel en important celui exporté. Cet ordinateur virtuel est promu automatiquement comme contrôleur de domaine unique.

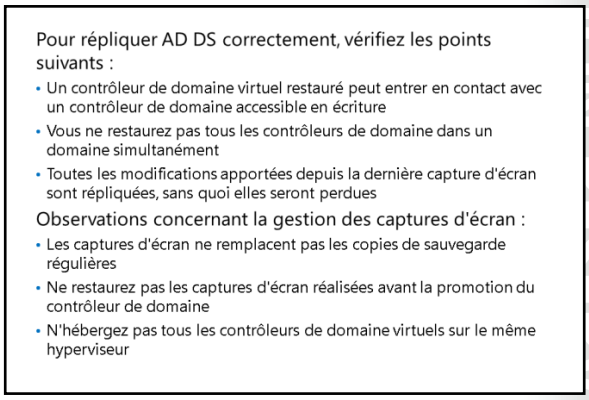
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion des contrôleurs de domaine virtualisés

La fonction de restauration sûre de Windows Server 2012 active les VDC qui exécutent Windows Server 2012 pour participer en douceur à la topologie de réplication d'AD DS, après que vous appliquiez un instantané dans Hyper-V à l'ordinateur virtuel qui héberge le contrôleur de domaine.

La prise et l'application d'instantanés d'un VDC dans Hyper-V requièrent des éléments à prendre en compte et des étapes spécifiques.



Validation d'une réplication AD DS

Quand un instantané d'ordinateur virtuel est appliqué à un VDC, le processus de restauration sûre lance la réplication entrante des modifications dans AD DS entre le contrôleur de domaine virtuel et le reste de l'environnement AD DS. Le pool d'identificateurs relatifs (RID) est libéré et un nouveau est demandé, pour empêcher d'avoir des SID dupliqués dans AD DS. Cela initialise également une réplication ne faisant pas autorité du dossier SYSVOL. Ce processus vérifie que la nouvelle version instantanée appliquée du contrôleur de domaine virtuel connaît tous les objets d'AD DS, entièrement à jour et est entièrement fonctionnelle.

Pour garantir que ce processus peut s'achever avec succès, les éléments suivants de la réplication AD DS doivent être considérés :

- Un contrôleur de domaine virtuel récupéré à partir d'un instantané Hyper-V doit pouvoir entrer en contact avec un contrôleur de domaine accessible en écriture.
- Vous ne pouvez pas restaurer tous les contrôleurs de domaine dans un domaine simultanément. Si tous les contrôleurs de domaine sont restaurés simultanément, la réplication SYSVOL s'arrêtera et tous les partenaires de la synchronisation seront considérés comme ne faisant pas autorité. C'est une considération importante pour les situations de restauration complète d'un environnement qui peuvent se produire fréquemment dans un environnement de test.
- Des modifications lancées sur un contrôleur de domaine virtuel restauré qui n'ont pas répliqué depuis que l'instantané a été pris sont perdues. Pour cette raison, vous devez vérifier que toute réplication sortante sur un contrôleur de domaine est terminée avant de prendre un instantané de l'ordinateur virtuel.

Utilisation de Windows PowerShell pour la gestion des instantanés Hyper-V

Vous pouvez utiliser les applets de commande Windows PowerShell® suivants pour effectuer la gestion des instantanés dans Windows Server 2012 :

- Checkpoint-VM
- Export-VMSnapshot
- Get-VMSnapshot
- Remove-VMSnapshot
- Rename-VMSnapshot
- Restore-VMSnapshot

Éléments à prendre en compte concernant la gestion des instantanés de contrôleur de domaine virtuel

Considérez ce qui suit lors de la gestion des instantanés de contrôleur de domaine virtuel dans Windows Server 2012 :

- N'utilisez pas les instantanés pour remplacer les sauvegardes régulières d'état du système. Dans un environnement AD DS changeant fréquemment, les instantanés ne contiennent pas toujours le contenu complet des objets AD DS, en raison des modifications de la réplication.
- Ne restaurez pas un instantané d'un contrôleur de domaine réalisée avant la promotion de ce dernier. Faire ainsi nécessitera de promouvoir de nouveau le serveur manuellement après avoir appliqué l'instantané et la survenue du nettoyage de métadonnées.
- N'hébergez pas tous les contrôleurs de domaine virtuels sur le même hyperviseur ou serveur. Cela présente un seul point de défaillance dans l'infrastructure d'AD DS et contourne plusieurs des avantages que la virtualisation de votre infrastructure de contrôleur de domaine fournit.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Implémentation des contrôleurs de domaine en lecture seule

Les contrôleurs de domaine en lecture seule fournissent une alternative à un contrôleur de domaine entièrement accessible en écriture. Dans beaucoup de scénarios, comme une filiale distante ou un emplacement où un serveur ne peut pas être placé dans un environnement physique sécurisé, les contrôleurs de domaine en lecture seule peuvent fournir la fonctionnalité d'un contrôleur de domaine sans exposer potentiellement votre environnement AD DS à des risques inutiles. Cette leçon vous aidera à mieux comprendre les méthodes et les recommandations que vous pouvez utiliser pour gérer des contrôleurs de domaine en lecture seule dans l'environnement Windows Server 2012.

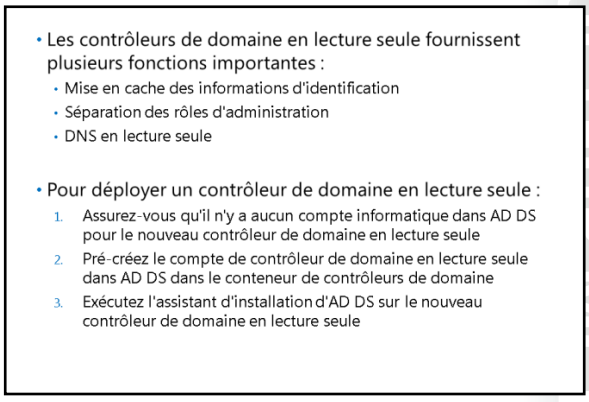
Objectifs de la leçon

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

- Expliquer les éléments à prendre en compte concernant l'implémentation des contrôleurs de domaine en lecture seule.
- Décrire comment gérer la mise en cache des informations d'identification des contrôleurs de domaine en lecture seule.
- Identifier les aspects importants de la gestion de l'administration locale des contrôleurs de domaine en lecture seule.

Éléments à prendre en compte pour implémenter les contrôleurs de domaine en lecteur seule

Un contrôleur de domaine en lecture seule a une copie en lecture seule d'un domaine Active Directory, qui contient tous les objets du domaine, mais pas tous leurs attributs. Les attributs importants du système, tels que les mots de passe, ne se répliquent pas vers un contrôleur de domaine en lecture seule, car il n'est pas considéré comme sûr. Vous pouvez empêcher des attributs supplémentaires d'être répliqués vers des contrôleurs de domaine en lecture seule en marquant l'attribut comme étant confidentiel et en l'ajoutant à le jeu d'attributs filtrés (FAS).



Présentation de la fonctionnalité RODC

Vous ne pouvez pas apporter de modifications à la base de données de domaine sur le contrôleur de domaine en lecture seule, car la base de données AD DS sur le RODC n'accepte pas de requêtes de modification des clients et des applications. Toutes les demandes de modifications sont transférées à un contrôleur de domaine accessible en écriture. Puisqu'aucune modification ne se produit sur le contrôleur de domaine en lecture seule, la réplication des modifications d'Active Directory ne passe qu'entre des contrôleurs de domaine accessibles en écriture vers le contrôleur de domaine en lecture seule.

Mise en cache des informations d'identification

Les informations d'identification d'utilisateur et d'ordinateur ne sont pas répliquées vers un contrôleur de domaine en lecture seule par défaut. Pour utiliser un contrôleur de domaine en lecture seule afin d'améliorer l'ouverture de session utilisateur, vous devez configurer une stratégie de réplication de mot de passe (PRP) qui définit quelles informations d'identification de l'utilisateur peuvent être mises en cache. Limiter les informations d'identification mises en cache sur le contrôleur de domaine en lecture seule réduit les risques en termes de sécurité. Si le contrôleur de domaine en lecture seule est volé, seuls les mots de passe pour les comptes d'utilisateur et d'ordinateur mis en cache doivent être réinitialisés.

Si les informations d'identification d'utilisateur et d'ordinateur ne sont pas répliquées vers un contrôleur de domaine en lecture seule, un contrôleur de domaine accessible en écriture doit alors être contacté pendant la procédure d'authentification. En général (dans un scénario de filiale), les informations d'identification des utilisateurs et des ordinateurs locaux sont mis en cache sur un contrôleur de domaine en lecture seule. Quand des contrôleurs de domaine en lecture seule sont placés dans un réseau de périmètre, les informations d'identification des utilisateurs et des ordinateurs ne sont généralement pas mises en cache.

Séparation des rôles d'administration

Pour gérer un contrôleur de domaine accessible en écriture, vous devez être un membre du groupe Administrateurs local du domaine. Tout utilisateur placé dans le groupe Administrateurs local du domaine obtient des autorisations pour gérer tous les contrôleurs de domaine présents dans le domaine. Ceci pose des problèmes pour l'administration de bureaux à distance avec un contrôleur de domaine accessible en écriture car l'administrateur d'un bureau distant ne doit pas obtenir l'accès à d'autres contrôleurs de domaine de l'organisation.

Ceci donne à l'administrateur d'un bureau distant l'autorisation de gérer seulement ce contrôleur de domaine en lecture seule, qui peut également être configuré pour fournir d'autres services tels que les partages et l'impression de fichiers.

DNS en lecture seule

Le DNS est une ressource critique d'un réseau Windows. Si vous configurez un contrôleur de domaine en lecture seule en tant que serveur DNS, vous pouvez alors répliquer des zones DNS via AD DS vers le contrôleur de domaine en lecture seule. Le DNS sur le contrôleur de domaine en lecture seule est en lecture seule. Les demandes de mise à jour du DNS sont adressées à une copie accessible en écriture de DNS.

Déploiement des contrôleurs de domaine en lecture seule

Pour déployer un contrôleur de domaine en lecture seule, assurez-vous que les activités suivantes sont exercées :

- Vérifier que le niveau fonctionnel de la forêt est Windows Server 2003 ou une version plus récente. Cela signifie que tous les contrôleurs de domaine doivent être de la version Windows Server 2003 ou plus récente et que chaque domaine dans la forêt doit être au niveau fonctionnel de domaine de la version Windows Server 2003 ou plus récente.
- Exécuter ADPrep/RODCPrep. Ceci configure des autorisations sur des partitions de répertoire d'applications DNS pour permettre de les répliquer vers des contrôleurs de domaine en lecture seule. Ceci est requis seulement si la forêt Active Directory a été mise à niveau.
- Assurez-vous qu'il y a un contrôleur de domaine accessible en écriture qui exécute Windows Server 2008 ou une version plus récente. Un contrôleur de domaine en lecture seule réplique la partition de domaine seulement à partir de ces contrôleurs de domaine. Par conséquent, chaque domaine comprenant des contrôleurs de domaine en lecture seule doit avoir au moins un contrôleur de domaine de version Windows Server 2008 ou plus récente. Vous pouvez répliquer les partitions de schéma et de configuration à partir de Windows Server 2003.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

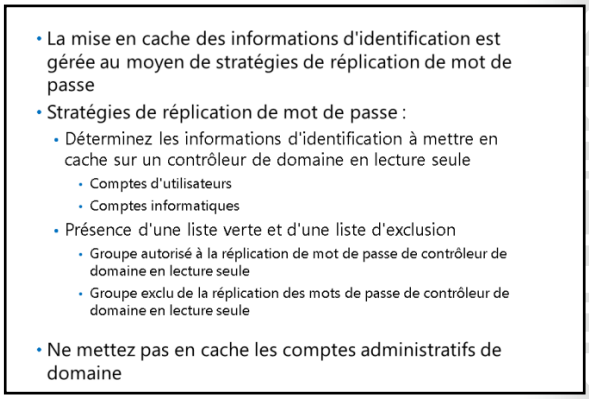
Installation du service RODC

Comme avec un contrôleur de domaine accessible en écriture, vous pouvez installer un contrôleur de domaine en lecture seule à l'aide d'une installation avec ou sans assistance. Si vous exécutez une installation avec assistance à l'aide de l'interface graphique, vous sélectionnez le contrôleur de domaine en lecture seule en tant qu'une des options supplémentaires du contrôleur de domaine.

Vous pouvez également déléguer l'installation du RODC à l'administrateur du bureau distant à l'aide d'une installation intermédiaire. Dans le cadre d'une installation intermédiaire, vous devez procéder comme suit :

1. Garantir que le serveur à configurer en tant que contrôleur de domaine en lecture seule n'est pas un membre du domaine.
2. Un administrateur de domaine utilise des utilisateurs et des ordinateurs Active Directory pour créer au préalable le compte du RODC dans l'unité d'organisation (OU) Contrôleurs de domaine. L'assistant servant à effectuer ce processus envoie une invite pour obtenir les informations nécessaires, y compris l'utilisateur ou le groupe qui est autorisé à joindre le contrôleur de domaine en lecture seule au domaine.
3. L'administrateur du bureau distant exécute l'assistant d'installation de services de domaine Active Directory et suit les étapes de l'assistant pour joindre le domaine comme compte du RODC créé au préalable.

Gestion de la mise en cache des informations d'identification d'un contrôleur de domaine en lecture seule



Les contrôleurs de domaine en lecture seule donnent la possibilité d'enregistrer uniquement un sous-ensemble d'informations d'identification pour des comptes dans AD DS via l'implémentation de la mise en cache de ces informations. Avec la mise en cache des informations d'identification, une stratégie de réplication de mot de passe (PRP) détermine quelles informations d'identification d'utilisateur et d'ordinateur peuvent être mises en cache sur un contrôleur de domaine en lecture seule spécifique. Si PRP permet à un RODC de mettre les informations d'identification d'un compte en cache, des activités d'authentification et de ticket de service de ce compte peuvent être traitées localement par le contrôleur de domaine en lecture seule. Si les informations d'identification d'un compte ne peuvent pas être mises en cache sur le contrôleur de domaine en lecture seule ou si elles ne sont pas mises en cache sur le RODC, des activités d'authentification et de ticket de service sont chaînées par le RODC à un contrôleur de domaine accessible en écriture.

Composants de la stratégie de réplication de mot de passe

Le PRP d'un contrôleur de domaine en lecture seule contient une liste approuvée et une liste refusée. Chaque liste peut contenir des comptes ou des groupes spécifiques. Un compte doit être sur la liste approuvée pour que les informations d'identification soient mises en cache. Si un groupe est sur la liste approuvée et un membre de ce groupe est sur la liste refusée, la mise en cache n'est pas autorisée pour ce membre.

Il y a deux groupes locaux de domaine que vous pouvez utiliser pour autoriser ou refuser globalement la mise en cache à tous les contrôleurs de domaine en lecture seule dans un domaine :

- Le groupe de réplication de mot de passe de contrôleur de domaine en lecture seule autorisé est ajouté à la liste approuvée de tous les RODC. Ce groupe ne comprend pas de membres par défaut.
- Le groupe de réplication de mot de passe de contrôleur de domaine en lecture seule refusé est ajouté à la liste refusée de tous les RODC. Par défaut, les Administrateurs du domaine, les administrateurs de l'entreprise et les propriétaires créateurs de la stratégie de groupe sont les membres de ce groupe.

Vous pouvez configurer la liste approuvée et la liste refusée de chaque contrôleur de domaine en lecture seule. La liste approuvée contient seulement le groupe de réplication de mot de passe de contrôleur de domaine en lecture seule autorisé. L'appartenance par défaut à la liste refusée comprend des administrateurs, des opérateurs de serveur et des opérateurs de compte.

Dans la plupart des cas, vous souhaiterez ajouter des comptes séparément à chaque contrôleur de domaine en lecture seule ou ajouter des groupes globaux contenant des comptes plutôt que de permettre globalement la mise en cache de mot de passe. Ceci vous permet de limiter le nombre d'informations d'identification mises en cache à ces seuls comptes présents généralement à cet emplacement. Les comptes d'administrateur de domaine ne doivent pas être mis en cache sur des contrôleurs de domaine en lecture seule de bureaux distants. Vous devez mettre des comptes d'ordinateur en cache pour accélérer l'authentification des comptes d'ordinateur pendant le démarrage du système. En outre, vous devez mettre les comptes de service en cache pour les services qui s'exécutent au niveau du bureau distant.

Recommandations pour la mise en cache des informations d'identification

Les recommandations suivantes doivent être observées pour garantir l'utilisation la plus efficace des informations d'identification mises en cache :

- Créer des groupes globaux AD DS distincts pour chaque contrôleur de domaine en lecture seule.
- Ne pas mettre les mots de passe en cache pour des comptes d'administrateur appliqués à l'ensemble du domaine.

Gestion de l'administration locale des contrôleurs de domaine en lecture seule

La gestion des contrôleurs de domaine en lecture seule est séparée des autres contrôleurs de domaine. Par conséquent, vous pouvez déléguer l'administration des RODC aux administrateurs locaux présents dans des bureaux distants, sans leur donner accès aux contrôleurs de domaine accessibles en écriture.

- Déléguez l'administration du contrôleur de domaine en lecture seule aux administrateurs locaux
- Définissez un principal de sécurité unique en tant qu'administrateur
  - Utilisateur
  - Groupe
- Activez à l'aide des méthodes suivantes :
  - Géré par l'onglet du contrôleur de domaine en lecture seule
  - dsmgmt
  - ntsdutil
- Mettez en cache les informations d'identification des administrateurs délégués

Vous pouvez déléguer l'administration d'un contrôleur de domaine en lecture seule dans les propriétés du compte d'ordinateur du RODC sur l'onglet Géré par. Vous devez suivre cette méthode pour déléguer l'administration d'un contrôleur de domaine en lecture seule car vous pouvez le gérer de manière centralisée et facilement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez spécifier une seule entité de sécurité sur l'onglet Géré par d'un compte d'ordinateur de contrôleur de domaine en lecture seule. Spécifiez un groupe de sorte que vous puissiez déléguer des autorisations de gestion à plusieurs utilisateurs en les faisant devenir membres du groupe.

Vous pouvez également déléguer l'administration d'un contrôleur de domaine en lecture seule à l'aide des commandes **ntdsutil** ou **dsmgmt** avec l'option des rôles locaux, comme le montre l'exemple suivant :

```
C:\>dsmgmt
Dsmgmt: local roles
local roles: add ADATUM\Research
```

Vous devez mettre le mot de passe en cache pour les administrateurs délégués pour être sûr de pouvoir effectuer la maintenance du système quand un contrôleur de domaine accessible en écriture n'est pas disponible.

 **Remarque :** Vous ne devez jamais accéder au contrôleur de domaine en lecture seule avec un compte qui a des autorisations similaires aux Administrateurs du domaine. Les ordinateurs à contrôleur de domaine en lecture seule sont considérés comme étant *compromis par défaut*, par conséquent, vous devez supposer qu'en ouvrant une session sur le contrôleur de domaine en lecture seule, vous abandonnez les informations d'identification d'admin de domaine. Ainsi les administrateurs de domaine doivent avoir un compte de type *admin serveur* distinct qui dispose d'un accès de gestion délégué au contrôleur de domaine en lecture seule.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Administration d'AD DS

La gestion d'AD DS se produit sous de très nombreuses formes. L'environnement d'AD DS contient un grand nombre d'outils de gestion qui vous permettent de surveiller et de modifier AD DS, pour vérifier que l'infrastructure du domaine de votre organisation atteint son objectif et fonctionne correctement. Windows Server 2012 comprend un jeu plus large d'outils pour travailler dans AD DS que les versions précédentes de Windows incluses. Les améliorations apportées au centre d'administration Active Directory et l'ajout de plusieurs applets de commande au module Active Directory pour Windows PowerShell permettent un meilleur contrôle de votre domaine AD DS.

Objectifs de la leçon

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

- Décrire les composants logiciels enfichables d'administration d'Active Directory.
- Décrire le centre d'administration d'Active Directory.
- Expliquer comment gérer AD DS à l'aide des outils de gestion.
- Décrire le module Active Directory pour Windows PowerShell.
- Expliquer comment gérer des rôles de maître d'opérations.
- Expliquer comment gérer la sauvegarde et la récupération du service de domaine Active Directory (AD DS).

Vue d'ensemble des composants logiciels enfichables d'administration d'Active Directory

En général, vous exécuterez la majorité de l'administration d'Active Directory à l'aide des composants logiciels enfichables et des consoles suivants :

- Les composants logiciels enfichables de l'administration d'Active Directory sont composés de quatre consoles différentes de MMC :
  - Utilisateurs et ordinateurs Active Directory
  - Sites et services Active Directory
  - Domaines et approbations Active Directory
  - Schéma Active Directory

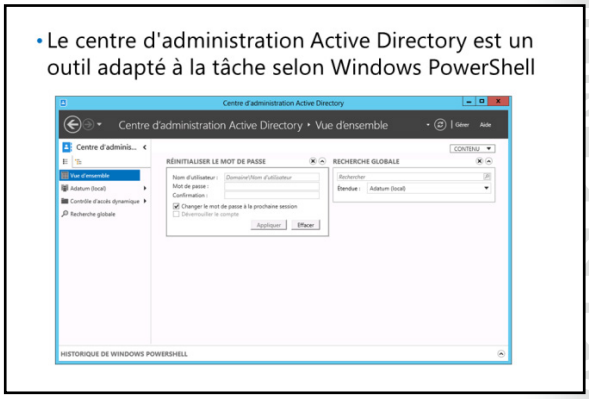
- Utilisateurs et ordinateurs Active Directory. Ce composant logiciel enfichable gère la plupart des ressources quotidiennes communes, y compris des utilisateurs, des groupes, et des ordinateurs. Il s'agit probablement du composant logiciel enfichable le plus largement utilisé pour un administrateur d'Active Directory.
- Sites et services Active Directory. Cela gère la réplication, la topologie du réseau et les services connexes.
- Domaines et approbations Active Directory. Cela configure et maintient les relations d'approbation ainsi que le niveau fonctionnel du domaine et de la forêt.
- Schéma Active Directory. Ce schéma examine et modifie la définition des attributs et des classes d'objets d'Active Directory. Le schéma est le *modèle* pour Active Directory et, en général, vous ne l'affichez pas ou ne le modifiez pas très souvent. Par conséquent, le composant logiciel enfichable Schéma Active Directory n'est pas entièrement installé, par défaut.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble du centre d'administration d'Active Directory

Windows Server 2012 fournit une autre option pour gérer des objets AD DS. Le centre d'administration Active Directory fournit une interface utilisateur graphique (GUI) créée sur Windows PowerShell. Cette interface améliorée vous permet d'effectuer la gestion d'objets Active Directory à l'aide de la navigation orientée vers les tâches. Les tâches que vous pouvez effectuer à l'aide du centre d'administration Active Directory comprennent :



- Création et gestion des comptes d'utilisateur, d'ordinateurs et de groupes.
- Création et gestion des unités d'organisation.
- Connexion et gestion de plusieurs domaines dans une instance unique du centre d'administration Active Directory.
- Recherche et filtrage des données d'Active Directory en générant des requêtes.
- Création et gestion de stratégies de mot de passe affinées.
- Récupération d'objets à partir de la corbeille d'Active Directory.

Configuration requise pour l'installation

Vous pouvez installer le centre d'administration Active Directory seulement sur des ordinateurs qui exécutent Windows Server 2008 R2, Windows Server 2012, Windows® 7 ou Windows 8. Vous pouvez installer le centre d'administration Active Directory en :

- Installation du rôle de serveur AD DS par le Gestionnaire de serveur.
- Installation des outils d'administration de serveur distant (RSAT) sur un serveur Windows Server 2012 ou sur Windows 8.

Remarque : Le centre d'administration Active Directory repose sur les services Web Active Directory (ADWS), que vous devez installer sur au moins un contrôleur de domaine dans le domaine. Le service exige également que le port 9389 soit ouvert sur le contrôleur de domaine sur lequel ADWS s'exécute.

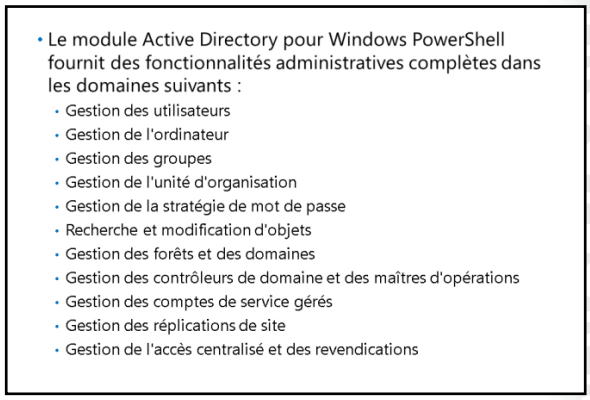
Nouvelles fonctionnalités du centre d'administration Active Directory dans Windows Server 2012

Le centre d'administration Active Directory contient plusieurs nouvelles fonctionnalités dans Windows Server 2012 qui activent la gestion graphique de la fonctionnalité AD DS :

- Corbeille Active Directory. Le centre d'administration Active Directory propose maintenant une gestion complète de la corbeille Active Directory. Les administrateurs peuvent utiliser le centre d'administration Active Directory pour afficher et localiser des objets supprimés et gérer et restaurer ces objets vers leur emplacement d'origine ou désiré.
- Stratégies de mot de passe affinées. Le centre d'administration Active Directory fournit également une interface utilisateur graphique pour la création et la gestion des objets de paramètres de mot de passe afin d'implémenter des stratégies de mot de passe affinées dans un domaine AD DS.
- Visionneuse d'historique Windows PowerShell. La fonctionnalité du centre d'administration Active Directory est établie sur Windows PowerShell. Toute commande ou action que vous exécutez dans l'interface du centre d'administration Active Directory est effectuée dans Windows Server 2012 au moyen des applets de commande Windows PowerShell. Quand un administrateur effectue une tâche dans l'interface du centre d'administration Active Directory, la visionneuse d'historique Windows PowerShell montre les commandes Windows PowerShell qui ont été émises pour la tâche. Cela permet à des administrateurs de réutiliser le code pour créer des scripts réutilisables et leur permet de se familiariser avec la syntaxe et l'utilisation de Windows PowerShell.

Vue d'ensemble du module Active Directory pour Windows PowerShell

Le module Active Directory pour Windows PowerShell dans Windows Server 2012 consolide un groupe d'applets de commande que vous pouvez utiliser pour gérer vos domaines Active Directory. Windows Server 2012 génère sur la base établie dans le module Active Directory pour Windows PowerShell initialement présenté dans Windows Server 2008 R2, en ajoutant 60 applets de commande supplémentaires qui étendent les domaines préexistants des fonctions de Windows PowerShell et ajoutent de nouvelles fonctions dans les domaines de la réplication et du contrôle de l'accès aux ressources.



Le module Active Directory pour Windows PowerShell active la gestion d'AD DS dans les domaines suivants :

1. Gestion des utilisateurs
2. Gestion de l'ordinateur
3. Gestion des groupes
4. Gestion de l'unité d'organisation
5. Gestion de la stratégie de mot de passe

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Recherche et modification d'objets
7. Gestion des forêts et des domaines
8. Gestion du contrôleur de domaine et des maîtres d'opérations
9. Gestion des comptes de service gérés
10. Gestion des réplications de site
11. Gestion de l'accès centralisé et des revendications

Exemples d'applets de commande

- **New-ADComputer** crée un nouvel objet ordinateur dans AD DS.
- **Remove-ADGroup** supprime un groupe Active Directory.
- **Set-ADDomainMode** définit le niveau fonctionnel du domaine pour un domaine Active Directory.

Installation

Vous pouvez installer le module Active Directory à l'aide de l'une des méthodes suivantes :

- Par défaut, sur un serveur Windows Server 2008 R2 ou Windows Server 2012, quand vous installez les rôles de serveur des services AD DS ou AD LDS (Active Directory Lightweight Directory Services).
- Par défaut, quand vous faites d'un serveur Windows Server 2008 R2 ou Windows Server 2012 un contrôleur de domaine.
- Dans le cadre de la fonctionnalité RSAT sur un ordinateur Windows Server 2008 R2, Windows Server 2012, Windows 7 ou Windows 8.

Démonstration : Gestion d'AD DS à l'aide des outils de gestion

Les divers outils de gestion d'AD DS ont chacun un objectif dans le cadre de l'administration de l'ensemble de l'environnement AD DS. Cette démonstration vous montrera les principaux outils que vous pouvez utiliser pour gérer AD DS et une tâche que vous effectuez en général avec l'outil.

Cette démonstration montre comment :

- Créer des objets dans Utilisateurs et ordinateurs Active Directory.
- Rechercher des attributs d'objets dans Utilisateurs et ordinateurs Active Directory.
- Naviguer dans le centre d'administration Active Directory.
- Effectuer une tâche administrative dans le centre d'administration Active Directory.
- Utiliser la visionneuse de Windows PowerShell dans le centre d'administration Active Directory.
- Gérer les objets d'Active Directory DS avec Windows PowerShell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

Utilisateurs et ordinateurs Active Directory

Afficher des objets

1. Sur LON-DC1, ouvrez Utilisateurs et ordinateurs Active Directory.
2. Naviguez dans l'arborescence de domaine Adatum.com, en affichant les objets **Conteneurs, Unités d'organisation (OU)** et **Ordinateur, Utilisateur et Groupe**.

Actualisez l'affichage

- Actualisez l'affichage dans la console Utilisateurs et ordinateurs Active Directory.

Créer des objets

1. Créez un nouvel objet ordinateur nommé LON-CL4 dans le conteneur Computer.
2. Pour créer un objet dans Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur un domaine ou un conteneur (tel que des utilisateurs ou des ordinateurs), ou sur une unité d'organisation, pointez sur **Nouveau**, puis cliquez sur le type d'objet que vous souhaitez créer.
3. Quand vous créez un objet, vous êtes invité à configurer plusieurs des propriétés les plus fondamentales de l'objet, y compris les propriétés que l'objet requiert.

Configurer des attributs d'objet

1. Dans Utilisateurs et ordinateurs Active Directory, ouvrez la page Propriétés pour LON-CL4.
2. Ajoutez LON-CL4 au groupe Adatum/Research.

Afficher tous les attributs d'objet

1. Activez la vue Fonctionnalités avancées dans Utilisateurs et ordinateurs Active Directory.
2. Ouvrez la page **Propriétés** pour LON-CL4, puis affichez les attributs AD DS.

Centre d'administration Active Directory

Navigation

1. Sur LON-DC1, ouvrez le Centre d'administration Active Directory.
2. Dans le centre d'administration Active Directory, cliquez sur les nœuds de navigation.
3. Basculez vers l'affichage d'arborescence.
4. Développez Adatum.com.

Effectuer des tâches d'administration

1. Naviguez jusqu'à l'affichage Vue d'ensemble.
2. Réinitialisez le mot de passe pour **ADATUM\Adam** sur **Pa$$w0rd**, sans exiger de l'utilisateur qu'il modifie le mot de passe à l'ouverture de session suivante.
3. Utilisez la section Recherche globale pour rechercher tous les objets qui correspondent à la chaîne de recherche Rex.

Utiliser la visionneuse d'historique Windows PowerShell

1. Ouvrez le volet Historique Windows PowerShell.
2. Affichez l'applet de commande Windows PowerShell que vous avez utilisé pour effectuer la tâche la plus récente.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Windows PowerShell

Création d'un groupe

1. Ouvrez le module Active Directory pour Windows PowerShell.
2. Créez un nouveau groupe appelé **SalesManagers** à l'aide de la commande suivante :

```
New-ADGroup –Name “SalesManagers”–GroupCategory Security –GroupScope Global –
DisplayName “Sales Managers” –Path ”CN=Users,DC=Adatum,DC=com”
```

3. Ouvrez le centre d'administration Active Directory et confirmez que le groupe **SalesManagers** est présent dans le conteneur **Users**.

Déplacer un objet vers une nouvelle unité d'organisation (OU)

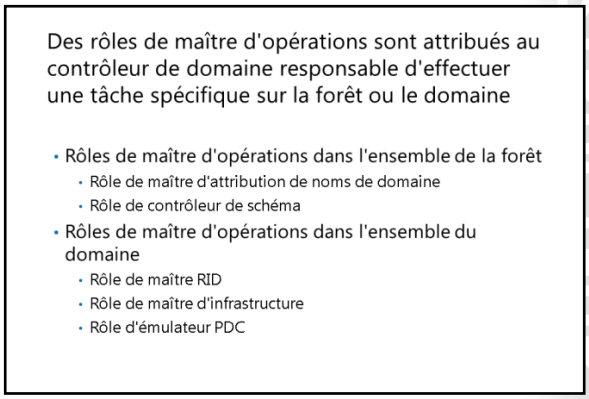
1. À l'invite PowerShell, déplacez **SalesManagers** vers l'unité d'organisation Sales à l'aide de la commande suivante :

```
Move-ADObject “CN=SalesManagers,CN=Users,DC=Adatum,DC=com” –TargetPath
“OU=Sales,DC=Adatum,DC=com”
```

2. Basculez vers le centre d'administration Active Directory, puis confirmez que le groupe **SalesManagers** a été déplacé vers l'unité d'organisation **Sales**.

Gestion des rôles des maîtres d'opérations

Dans un environnement AD DS, une réplication à plusieurs maîtres signifie que tous les contrôleurs de domaine ont les mêmes fonctions et priorités générales lors de la modification de la base de données AD DS. Cependant, certaines opérations doivent être exécutées par un seul système. Dans AD DS, les maîtres d'opération sont des contrôleurs de domaine qui remplissent une fonction spécifique dans l'environnement de domaine.



Rôles de maître d'opérations dans l'ensemble de la forêt

Le contrôleur de schéma et le maître d'opérations des noms de domaine doivent être uniques dans la forêt. Chaque rôle est effectué par un seul contrôleur de domaine dans la forêt entière.

Rôle de maître d'attribution de noms de domaine

Le rôle d'attribution de noms de domaine est utilisé lors de l'ajout ou de la suppression de domaines et de partitions d'application dans la forêt. Quand vous ajoutez ou supprimez une partition de domaine ou d'application, le maître d'attribution de noms de domaine doit être accessible ou l'opération échouera.

Rôle de contrôleur de schéma

Le contrôleur de domaine détenant le rôle de contrôleur de schéma est responsable de toutes les modifications à apporter sur le schéma de la forêt. Tous les autres contrôleurs de domaine maintiennent les réplicas en lecture seule du schéma. Quand vous devez modifier le schéma, les modifications doivent être envoyées au contrôleur de domaine qui héberge le rôle de contrôleur de schéma.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Rôles de maître d'opérations dans l'ensemble du domaine

Chaque domaine maintient trois opérations à maître unique : le maître des identificateurs relatifs (RID), le maître d'infrastructure et l'émulateur du contrôleur de domaine principal (PDC). Chaque rôle est effectué par un seul contrôleur de domaine dans le domaine.

Rôle de maître RID

Le maître RID fait partie intégrante de la génération d'identificateurs de sécurité (SID) pour des entités de sécurité telles que des utilisateurs, des groupes et des ordinateurs. Le SID d'une entité de sécurité doit être unique. Puisque n'importe quel contrôleur de domaine peut créer des comptes, et donc des SID, un mécanisme est nécessaire pour vérifier que les SID générés par un contrôleur de domaine sont uniques. Les contrôleurs de domaine Active Directory génèrent des SID en ajoutant un RID unique au SID du domaine. Le maître RID du domaine alloue des pools de RID uniques à chaque contrôleur de domaine dans le domaine. Par conséquent, chaque contrôleur de domaine peut être sûr que les SID qu'il génère sont uniques.

Rôle de maître d'infrastructure

Dans un environnement comprenant plusieurs domaines, il est courant pour un objet de faire référence à des objets situés dans d'autres domaines. Par exemple, un groupe peut inclure des membres d'un autre domaine. Son attribut membre à valeurs multiples contient les noms uniques de chaque membre. Si le membre dans l'autre domaine est déplacé ou renommé, le maître d'infrastructure du domaine du groupe met à jour les références à l'objet.

Rôle d'émulateur PDC

Le rôle d'émulateur PDC effectue plusieurs fonctions cruciales pour un domaine :

- Participe à la gestion des mises à jour spéciales de mot de passe pour le domaine. Quand le mot de passe d'un utilisateur est réinitialisé ou modifié, le contrôleur de domaine qui apporte la modification réplique immédiatement la modification vers l'émulateur PDC. Cette réplication spéciale garantit que les contrôleurs de domaine connaissent le nouveau mot de passe aussi rapidement que possible.
- Gère des mises à jour de stratégies de groupe dans un domaine. Si vous modifiez un GPO sur deux contrôleurs de domaine quasiment au même moment, il peut y avoir des conflits entre les deux versions qui ne pourraient pas être rapprochées comme répliques d'objet Stratégie de groupe. Pour éviter cette situation, l'émulateur PDC agit en tant que point focal par défaut pour toutes les modifications de la stratégie de groupe.
- Fournit une source de temps de base pour le domaine. Beaucoup de composants et de technologies Windows reposent sur des horodatages, ainsi la synchronisation du temps à travers tous les systèmes d'un domaine est cruciale. L'émulateur PDC dans le domaine racine de forêt est le maître de temps pour la forêt entière, par défaut. L'émulateur PDC dans chaque domaine synchronise son temps avec l'émulateur PDC racine de la forêt. D'autres contrôleurs de domaine dans le domaine synchronisent leurs horloges par rapport à l'émulateur PDC de ce domaine. Tous autres membres du domaine synchronisent leur temps avec leur contrôleur de domaine par défaut.
- Agit en tant qu'explorateur principal de domaine. Quand vous ouvrez un réseau dans Windows, vous voyez une liste de groupes de travail et de domaines, et quand vous ouvrez un groupe de travail ou un domaine, vous voyez une liste d'ordinateurs. Le service Explorateur crée ces deux listes, appelées listes de parcours. Dans chaque segment réseau, un maître explorateur crée la liste de parcours : les listes de groupes de travail, de domaines et de serveurs dans ce segment. Le maître explorateur de domaine sert à fusionner les listes de chaque maître explorateur de sorte que les clients de parcours puissent récupérer une liste de parcours complète.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Instructions de placement des rôles de maîtres d'opérations

- Placez les rôles de niveau domaine sur un contrôleur de domaine hautes performances.
- Ne placez pas le rôle de niveau domaine de Maître d'infrastructure sur un serveur de catalogue global, excepté si votre forêt contient seulement un domaine ou si tous les contrôleurs de domaine dans votre forêt sont également des catalogues globaux.
- Laissez les deux rôles de niveau forêt sur un contrôleur de domaine du domaine racine de la forêt.
- Ajustez la charge de travail de l'émulateur PDC, s'il y a lieu, en déchargeant des rôles n'incluant pas les services AD DS sur d'autres serveurs.

Remarque : Vous pouvez afficher l'attribution des rôles de maître d'opérations en exécutant ce qui suit à partir d'une invite de commande :

```
Netdom query fsmo
```

Gestion des sauvegardes et des récupérations AD DS

Dans des versions précédentes de Windows, sauvegarder Active Directory impliquait la création d'une sauvegarde de SystemState, qui était une petite collection de fichiers qui comprenaient la base de données Active Directory et le registre.

- Restauration ne faisant pas autorité ou normale
  - Restaurer le contrôleur de domaine vers son état valide antérieur connu
  - Le contrôleur de domaine sera mis à jour à l'aide de la réplication standard des partenaires
- Restauration forcée
  - Restaurer le contrôleur de domaine vers son état valide antérieur connu
  - Marquer les objets que vous souhaitez voir faire autorité
  - Le contrôleur de domaine est mis à jour depuis ses partenaires à jour
  - Le contrôleur de domaine envoie des mises à jour faisant autorité à ses partenaires
- Restauration de serveur entier
  - En général effectuée dans l'environnement de récupération Windows
- Restauration d'un autre emplacement

Dans Windows Server 2012, le concept SystemState existe toujours, mais il est beaucoup plus grand. En raison des interdépendances entre les rôles de serveur, la configuration physique et Active Directory, le SystemState est maintenant un sous-ensemble d'une sauvegarde du serveur entier et, dans certaines configurations, peut être aussi grand. Pour sauvegarder un contrôleur de domaine, vous devez sauvegarder tous les volumes critiques entièrement.

Restauration des données AD DS

Quand un contrôleur de domaine ou son répertoire est corrompu, endommagé ou défaillant, vous avez plusieurs options avec lesquelles restaurer le système.

Restauration ne faisant pas autorité

La première option de ce genre est appelée restauration normale ou restauration ne faisant pas autorité. Dans une opération normale de restauration, vous restaurez une sauvegarde Active Directory à compter d'une date valide connue. En fait, vous faites remonter le contrôleur de domaine dans le temps. Quand AD DS redémarre sur le contrôleur de domaine, le contrôleur de domaine contacte ses partenaires de réplication et demande toutes les mises à jour suivantes. En fait, le contrôleur de domaine *rattrape* le reste du domaine à l'aide des mécanismes standard de réplication.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La restauration normale est utile quand le répertoire sur un contrôleur de domaine a été endommagé ou corrompu, mais que le problème ne s'est pas étendu à d'autres contrôleurs de domaine. Que diriez-vous d'une situation dans laquelle le dommage a été fait et le dommage a été répliqué ? Par exemple, si vous supprimez un ou plusieurs objets, et que cette suppression a été répliquée ?

Dans de telles situations, une restauration normale n'est pas suffisante. Si vous restaurez une bonne version d'Active Directory et redémarrez le contrôleur de domaine, la suppression (qui s'est produite à la suite de la sauvegarde) répliquera simplement vers le contrôleur de domaine.

Restauration forcée

Quand une bonne copie d'AD DS a été restaurée contenant des objets qui doivent remplacer des objets existants dans la base de données AD DS, une restauration forcée est nécessaire. Dans une restauration faisant autorité, vous restaurez la bonne version d'Active Directory tout comme vous le faites dans une restauration normale. Cependant, avant de redémarrer le contrôleur de domaine, vous marquez les objets supprimés par erreur ou précédemment endommagés que vous souhaitez conserver comme faisant autorité de sorte qu'ils répliquent à partir du contrôleur de domaine restauré vers ses partenaires de réplication. En réalité, quand vous marquez des objets comme faisant autorité, Windows incrémente le numéro de version de tous les attributs d'objet pour être si élevé que la version soit pratiquement sûre d'être supérieure au numéro de version de tous les autres contrôleurs de domaine.

Quand le contrôleur de domaine restauré est redémarré, il réplique à partir de ses partenaires de réplication toutes les modifications qui ont été apportées au répertoire. Il informe également ses partenaires qu'il comporte des modifications et les numéros de version des modifications garantissent que les partenaires prennent les modifications et les répliquent dans le service d'annuaire. Dans les forêts qui ont la Corbeille Active Directory activée, vous pouvez utiliser la corbeille Active Directory comme une alternative plus simple à une restauration faisant autorité.

Autres options de restauration

La troisième option pour restaurer le service d'annuaire est de restaurer le contrôleur de domaine entier. Ceci est fait en démarrant sur l'environnement de récupération Windows, puis en restaurant une sauvegarde de serveur complète du contrôleur de domaine. Par défaut, c'est une restauration normale. Si vous devez également marquer des objets comme faisant autorité, vous devez redémarrer le serveur en mode Restauration des services d'annuaire et définir ces objets comme faisant autorité avant de démarrer le contrôleur de domaine en mode de fonctionnement normal.

En conclusion, vous pouvez restaurer une sauvegarde du SystemState vers un autre emplacement. Cela vous permet d'examiner des fichiers et, potentiellement, de monter le fichier NTDS.dit. Vous ne devez pas copier les fichiers à partir d'un autre emplacement de restauration par dessus les versions de production de ces fichiers. Ne faites pas une restauration fragmentaire d'Active Directory. Vous pouvez également utiliser cette option si vous souhaitez utiliser l'option **Installation à partir du support** pour créer un nouveau contrôleur de domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 5
Gestion de la base de données AD DS

Au centre de l'environnement AD DS se trouve la base de données AD DS. La base de données AD DS contient toutes les informations critiques requises pour fournir la fonctionnalité AD DS. Maintenir correctement cette base de données est un aspect critique de la gestion AD DS et il y a plusieurs outils et recommandations que vous devez connaître de sorte à pouvoir gérer efficacement votre base de données AD DS. Cette leçon vous présentera la gestion de base de données AD DS et vous montre les outils et les méthodes pour la maintenir.

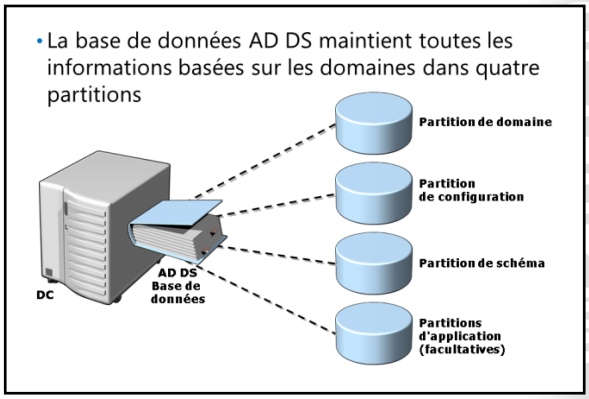
Objectifs de la leçon

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

- Expliquer l'architecture de la base de données AD DS.
- Décrire NTDSUtil.
- Expliquer les services AD DS redémarrables.
- Expliquer comment réaliser la gestion de base de données AD DS.
- Décrire comment créer des instantanés d'AD DS.
- Expliquer comment restaurer des objets supprimés.
- Décrire comment configurer la corbeille Active Directory.

Présentation de la base de données AD DS

Les informations AD DS sont enregistrées dans la base de données d'annuaire. Chaque partition d'annuaire, également appelée contexte de nommage, contient des objets ayant une étendue de réplication et une fin particulières. Il y a trois partitions AD DS sur chaque contrôleur de domaine, comme suit :



- Domaine. La partition de domaine contient tous les objets enregistrés dans un domaine, y compris des utilisateurs, des groupes, des ordinateurs et des conteneurs de stratégie de groupe (GPC).
- Configuration. La partition de configuration contient des objets qui représentent la structure logique de la forêt, y compris des informations sur des domaines, ainsi que la topologie physique, y compris des sites, des sous-réseaux et des services.
- Schéma : La partition de schéma définit les classes d'objets et leurs attributs pour l'annuaire entier.

Les contrôleurs de domaine peuvent également héberger des partitions d'application. Vous pouvez utiliser des partitions d'application pour limiter la réplication des données spécifiques à l'application à un sous-ensemble de contrôleurs de domaine. Le DNS intégré à Active Directory est un exemple classique d'une application qui tire profit des partitions d'application.

Chaque contrôleur de domaine maintient une copie, ou un réplica, de plusieurs partitions. La configuration est répliquée dans chaque contrôleur de domaine de la forêt, tout comme le schéma. La partition de domaine pour un domaine est répliquée à tous les contrôleurs de domaine dans un domaine, mais pas aux contrôleurs de domaine présents dans d'autres domaines, hormis pour les serveurs de catalogue global. Par conséquent, chaque contrôleur de domaine a au moins trois réplicas : la partition de domaine pour son domaine, sa configuration et son schéma.

Fichiers de la base de données AD DS

La base de données AD DS est enregistrée sous la forme d'un fichier nommé NTDS.dit. Quand vous installez et configurez AD DS, vous pouvez spécifier l'emplacement du fichier. L'emplacement par défaut est %systemroot%\NTDS. Dans NTDS.dit se trouvent toutes les partitions hébergées par le contrôleur de domaine : le schéma et la configuration de la forêt ; le contexte d'attribution de noms de domaine ; et, selon la configuration du serveur, le jeu d'attributs partiel et des partitions d'application.

Dans le dossier NTDS, il y a d'autres fichiers qui prennent en charge la base de données Active Directory. Les fichiers Edb*.log sont les journaux des transactions d'Active Directory. Quand il faut modifier l'annuaire, cela est d'abord écrit dans le fichier journal. La modification est soumise à l'annuaire en tant que transaction. Si la transaction échoue, elle peut être annulée.

Le tableau suivant décrit les différents composants de niveau fichier de la base de données AD DS.

Fichier	Description
NTDS.dit	• Principaux fichiers de la base de données AD DS • Contient tous les objets et partitions d'AD DS
EDB*.log	Journal(aux) des transactions
EDB.chk	Fichier de point de vérification de la base de données
Edbres00001.jrs Edbres00002.jrs	Fichier journal des transactions de réserve qui permet à l'annuaire de traiter des transactions si l'espace disque du serveur est insuffisant

Modifications et réplication de la base de données AD DS

En mode de fonctionnement normal, le journal des transactions enveloppe, avec de nouvelles transactions remplaçant les transactions anciennes qui avaient été déjà validées. Cependant, si un grand nombre de transactions sont effectuées au cours d'une courte période, AD DS crée des fichiers journaux de transaction supplémentaires, pour que vous puissiez voir plusieurs fichiers EDB*.log si vous regardez dans le dossier NTDS d'un contrôleur de domaine particulièrement occupé. Au fil du temps, ces fichiers sont supprimés automatiquement.

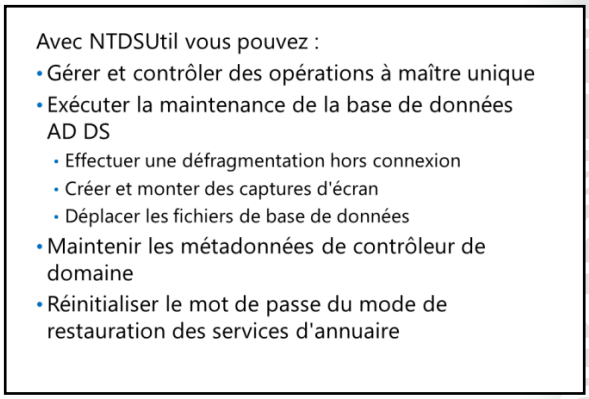
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le fichier EDB.chk agit comme un signet dans les fichier journaux, marquant l'emplacement avant lequel des transactions ont été soumises avec succès à la base de données et après lequel les transactions restent à valider.

Si un lecteur de disque manque d'espace, cela est très problématique pour le serveur. Cela est encore plus problématique si ce disque héberge la base de données AD DS car des transactions qui peuvent être en attente ne peuvent pas être écrites dans les journaux. Par conséquent, AD DS maintient deux fichiers journaux supplémentaires, edbres0001.jrs et edbres0002.jrs. Ce sont des fichiers vides de 10 mégaoctets (Mo) chacun. Quand un disque manque d'espace pour des journaux des transactions normaux, AD DS recrute l'espace utilisé par ces deux fichiers pour écrire les transactions qui sont actuellement dans une file d'attente. Après cela, il arrête sans risque les services AD DS et démonte la base de données. Naturellement, il sera important pour un administrateur de remédier au problème de faible espace disque aussi rapidement que possible. Le fichier fournit simplement une solution provisoire pour empêcher le service d'annuaire de refuser de nouvelles transactions.

Qu'est-ce que NTDSUtil ?

NTDSUtil est un fichier de ligne de commande exécutable que vous pouvez utiliser pour exécuter la maintenance de la base de données, y compris la création d'instantanés, la défragmentation hors connexion et le déplacement de fichiers de base de données.



Vous pouvez également utiliser **NTDSUtil** pour nettoyer des métadonnées de contrôleur de domaine. Si un contrôleur de domaine est supprimé du domaine quand il est hors connexion, il est impossible d'enlever les informations importantes du service d'annuaire. Vous pouvez alors utiliser NTDSUtil pour nettoyer les restes du contrôleur de domaine et il est très important que vous le fassiez.

NTDSUtil peut également réinitialiser le mot de passe utilisé pour ouvrir une session sur le mode Restauration des services d'annuaire. Ce mot de passe est configuré à l'origine pendant la configuration d'un contrôleur de domaine. Si vous oubliez le mot de passe, la commande **NTDSUtil set dsrm** peut le réinitialiser.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Présentation des services AD DS redémarrables

Dans la plupart des scénarios où la gestion d'AD DS est requise, vous devez redémarrer le contrôleur de domaine en mode Restauration des services d'annuaire.

Windows Server 2012 permet à des administrateurs d'arrêter et de démarrer AD DS comme n'importe quel autre service, et sans redémarrer un contrôleur de domaine, pour effectuer quelques tâches de gestion rapidement. Cette fonctionnalité est appelée Services de domaine Active Directory redémarrables.

- Les services AD DS peuvent être démarrés ou arrêtés à l'aide de la console Services
- Les services AD DS peuvent se trouver dans trois états :
  - AD DS démarrés
  - AD DS arrêtés
  - DSRM
- Il est impossible de restaurer l'état du système lorsque les services AD DS sont à l'état arrêté

Les services de domaine Active Directory redémarrables réduisent le temps nécessaire à l'exécution de certaines opérations. Vous pouvez arrêter AD DS de sorte à pouvoir appliquer des mises à jour à un contrôleur de domaine. De plus, les administrateurs peuvent arrêter les services de domaine Active Directory pour exécuter certaines tâches comme la défragmentation hors connexion de la base de données Active Directory, sans redémarrer le contrôleur de domaine. Les autres services qui s'exécutent sur le serveur et dont le fonctionnement ne dépend pas des services de domaine Active Directory, comme le protocole DHCP (Dynamic Host Configuration Protocol), demeurent disponibles pour satisfaire les requêtes client pendant que les services de domaine Active Directory sont arrêtés.

Les services AD DS redémarrables sont disponibles par défaut sur tous les contrôleurs de domaine qui exécutent Windows Server 2012. Il n'y a aucune configuration requise de niveau fonctionnel ou aucun autre préalable à l'utilisation de cette fonctionnalité.

Remarque : Vous ne pouvez pas effectuer une restauration d'état du système d'un contrôleur de domaine quand les services AD DS sont arrêtés. Pour terminer une restauration d'état du système d'un contrôleur de domaine, vous devez commencer en mode Restauration des services d'annuaire (DSRM). Vous pouvez cependant effectuer une restauration faisant autorité des objets Active Directory tandis qu'AD DS est arrêté à l'aide de Ntdsutil.exe.

Les services AD DS redémarrables ajoutent des modifications mineures aux composants logiciels enfichables existants de Microsoft Management Console (MMC). Un contrôleur de domaine exécutant Windows Server 2012 AD DS affiche le contrôleur de domaine dans le nœud Services (local) du composant logiciel enfichable Services de composants et du composant logiciel enfichable Gestion de l'ordinateur. Grâce au composant logiciel enfichable, un administrateur peut facilement arrêter et redémarrer AD DS de la même manière que n'importe quel autre service qui s'exécute localement sur le serveur.

Bien que l'arrêt des services de domaine Active Directory soit similaire à la connexion en mode de restauration des services d'annuaire, les services de domaine Active Directory redémarrables fournissent un état unique, connu sous le nom de services de domaine Active Directory arrêtés, pour un contrôleur de domaine exécutant Windows Server 2012.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

États du contrôleur de domaine

Les trois états possibles pour un contrôleur de domaine exécutant Windows Server 2012 sont les suivants :

- AD DS démarrés. Dans cet état, AD DS est démarré. Le contrôleur de domaine peut effectuer des tâches associées à AD DS normalement.
- AD DS arrêtés. Dans cet état, AD DS est arrêté. Bien que ce mode soit unique, le serveur possède certaines caractéristiques d'un contrôleur de domaine en mode DSRM et d'un serveur appartenant à un domaine.
- DSRM. Ce mode (ou état) permet des tâches d'administration standard d'AD DS.

Avec DSRM, la base de données Active Directory (Ntds.dit) sur le contrôleur de domaine local est hors connexion. Un autre contrôleur de domaine peut être contacté pour l'ouverture de session, s'il y en a un de disponible. Si aucun autre contrôleur de domaine ne peut être contacté, par défaut vous pouvez faire une des choses suivantes :

- Ouvrir une session au contrôleur de domaine localement en mode DSRM à l'aide du mot de passe de DSRM.
- Redémarrer le contrôleur de domaine pour ouvrir une session avec un compte de domaine.

Comme dans le cas d'un serveur membre, le serveur est joint au domaine. Cela signifie que la stratégie de groupe et d'autres paramètres sont encore appliqués à l'ordinateur. Cependant, un contrôleur de domaine ne doit pas rester dans l'état appelé « services de domaine Active Directory arrêtés » pendant une trop longue période de temps, parce qu'il ne peut alors traiter les requêtes d'ouverture de session ou répliquer avec les autres contrôleurs de domaine.

Démonstration : Exécution de la maintenance de la base de données AD DS

Il y a plusieurs tâches et outils relatifs que vous pouvez utiliser pour exécuter la maintenance de la base de données AD DS.

Cette démonstration montre comment :

- Arrêter AD DS.
- Exécuter une défragmentation hors connexion de la base de données AD DS.
- Vérifier l'intégrité de la base de données AD DS.
- Démarrer AD DS.

Procédure de démonstration

Arrêter AD DS

1. Sur LON-DC1, ouvrez la console Services.
2. Arrêtez le service **Services de domaine Active Directory**.

Exécuter une défragmentation hors connexion de la base de données AD DS

- Exécutez les commandes suivantes à partir d'une invite Windows PowerShell. Appuyez sur Entrée après chaque ligne :

```
ntdsutil
activate instance NTDS
files
compact to C:\
```

Vérifier l'intégrité de la base de données hors connexion

1. Exécutez les commandes suivantes à partir d'une invite Windows PowerShell. Appuyez sur Entrée après chaque ligne :

```
Integrity
quit
Quit
```

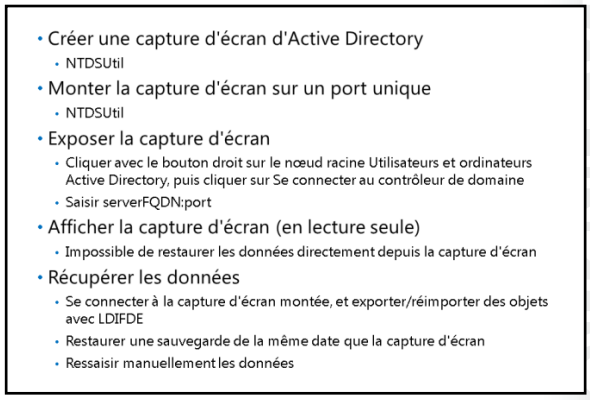
2. Fermez la fenêtre d'invite de commandes.

Démarrer AD DS

1. Ouvrez la console Services.
2. Démarrez le service **Services de domaine Active Directory**.

Création d'instantanés AD DS

NTDSUtil dans Windows Server 2012 peut créer et monter des instantanés d'AD DS. Un instantané est une forme de sauvegarde historique qui capture l'état exact du service d'annuaire au moment de l'instantané. Vous pouvez utiliser des outils pour explorer le contenu d'un instantané pour examiner l'état du service d'annuaire lorsque l'instantané a été fait, ou pour vous connecter à un instantané monté avec LDIFDE et exporter des objets d'une réimportation dans AD DS.



Création d'un instantané AD DS

Pour créer un instantané :

1. Ouvrez l'invite de commandes.
2. Saisissez **ntdsutil**, puis appuyez sur Entrée.
3. Saisissez **snapshot**, puis appuyez sur Entrée.
4. Saisissez **activate instance ntds**, puis appuyez sur Entrée.
5. Saisissez **create**, puis appuyez sur Entrée.
6. La commande renvoie un message qui indique que l'instantané configuré a été généré avec succès.
7. L'identificateur unique global (GUID) affiché est important pour des commandes de tâches ultérieures. Notez-le ou, sinon, copiez-le vers le **Presse-papiers**.
8. Saisissez **quit**, puis appuyez sur Entrée.

Planifiez des instantanés d'Active Directory régulièrement. Vous pouvez utiliser le Planificateur de tâches pour exécuter un fichier de commandes à l'aide des commandes NTDSUtil appropriées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Montage d'un instantané AD DS

Pour afficher le contenu d'un instantané, vous devez le monter comme nouvelle instance d'AD DS. Cela est également réalisé avec NTDSUtil.

Pour monter un instantané :

1. Ouvrez une invite de commandes avec élévation de privilèges.
2. Saisissez **ntdsutil**, puis appuyez sur Entrée.
3. Saisissez **activate instance ntds**, puis appuyez sur Entrée.
4. Saisissez **snapshot**, puis appuyez sur Entrée.
5. Saisissez **list all**, puis appuyez sur Entrée.
6. La commande renvoie une liste de tous les instantanés.
7. Saisissez mount **{GUID}**, où GUID représente l'identifiant unique global renvoyé par la commande de création d'instantané, puis appuyez sur Entrée.
8. Saisissez **quit**, puis appuyez sur Entrée.
9. Saisissez **quit**, puis appuyez sur Entrée.
10. Tapez **dsamain –dbpath c:\$snap_datetime_volumec$\windows\ntds\ntds.dit -ldapport 50000**, puis appuyez sur Entrée.
11. Le numéro de port, **50000**, peut être tout numéro de port TCP ouvert et unique.
12. Un message indique que le démarrage des Services de domaine Active Directory est terminé.
13. Ne fermez pas la fenêtre d'invite de commandes et ne laissez pas la commande que vous venez d'exécuter, Dsamain.exe, s'exécuter tandis que vous passez à l'étape suivante.

Affichage d'un instantané AD DS

Après que l'instantané a été monté, vous pouvez utiliser des outils pour vous connecter à et explorer l'instantané. Même les utilisateurs et ordinateurs Active Directory peuvent se connecter à l'instance.

Pour se connecter à un instantané avec des utilisateurs et des ordinateurs Active Directory :

1. Ouvrez Utilisateurs et ordinateurs Active Directory.
2. Cliquez avec le bouton droit sur le nœud racine, puis sur **Domain Controllers**.
3. La boîte de dialogue **Modifier le serveur d'annuaire** s'affiche.
4. Cliquez sur **<Tapez ici un nom de serveur d'annuaire:[port]>**.
5. Saisissez **LON-DC1:50000**, puis appuyez sur Entrée.
6. LON-DC1 est le nom du contrôleur de domaine sur lequel vous avez monté l'instantané, et 50000 est le numéro de port TCP que vous avez configuré pour l'instance. Vous êtes maintenant connecté à l'instantané.
7. Cliquez sur **OK**.

Notez que les instantanés sont en lecture seule. Vous ne pouvez pas modifier le contenu d'un instantané. D'ailleurs, il n'y a aucune méthode directe avec laquelle déplacer, copier ou restaurer des objets ou des attributs depuis l'instantané vers l'instance de production d'Active Directory.

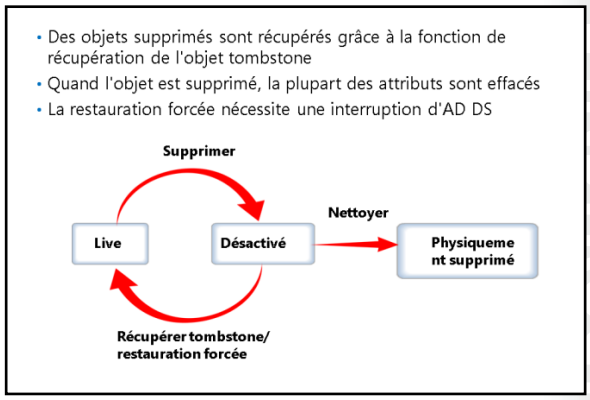
Démontage d'un instantané AD DS

Pour démonter l'instantané :

1. Basculez vers l'invite de commandes dans laquelle l'instantané est monté.
2. Appuyez sur **Ctrl+C** pour arrêter **DSAMain.exe**.
3. Saisissez **ntdsutil**, puis appuyez sur Entrée.
4. Saisissez **activate instance ntds**, puis appuyez sur Entrée.
5. Saisissez **snapshot**, puis appuyez sur Entrée.
6. Saisissez **unmount GUID**, où GUID représente l'identificateur unique global de l'instantané, puis appuyez sur Entrée.
7. Saisissez **quit**, puis appuyez sur Entrée.
8. Saisissez **quit**, puis appuyez sur Entrée.

Présentation de la restauration des objets supprimés

Quand un objet dans AD DS est supprimé, il est déplacé dans le conteneur d'objets supprimés et de nombreux attributs importants en sont retirés. Vous pouvez étendre la liste d'attributs qui restent quand un objet est supprimé, mais vous ne pouvez jamais retenir des valeurs d'attribut liées (telles que l'appartenance de groupe).



Tant que l'objet n'a pas été encore nettoyé par le processus de nettoyage de la mémoire après avoir atteint de la fin de sa durée de vie de la désactivation, vous pouvez restaurer ou récupérer l'objet supprimé.

Pour restaurer un objet supprimé :

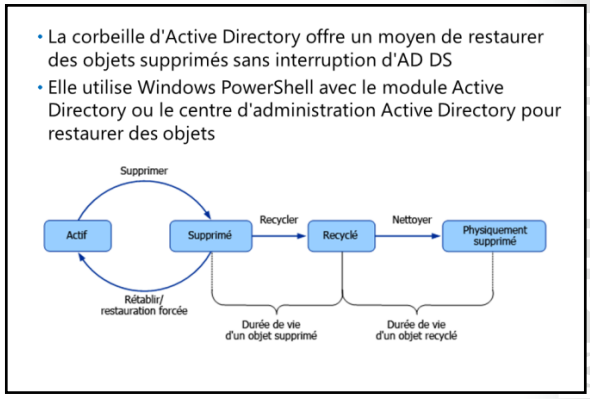
1. Cliquez sur Accueil, et dans la zone **Accueil la recherche**, saisissez **LDP.exe**, puis appuyez sur Ctrl+Maj+Entrée, qui exécute la commande en tant qu'administrateur.
2. La boîte de dialogue **Contrôle de compte d'utilisateur** apparaît.
3. Cliquez sur **Utiliser un autre compte**.
4. Dans la zone **Nom d'utilisateur**, saisissez le nom d'utilisateur d'un administrateur.
5. Dans la zone **Mot de passe**, saisissez le mot de passe pour le compte d'administrateur, puis appuyez sur Entrée.
6. LDP s'ouvre.
7. Cliquez sur le menu **Connexion**, sur **Se connecter**, puis cliquez sur **OK**.
8. Cliquez sur le menu **Connexion**, sur **Lier**, puis cliquez sur **OK**.
9. Cliquez sur le menu **Options**, puis sur **Contrôles**.
10. Dans la liste **Chargement prédéfini**, cliquez sur **Renvoyer des objets supprimés**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Cliquez sur le menu **Afficher**, sur **Arborescence**, puis cliquez sur **OK**.
12. Développez le domaine, puis double-cliquez sur **CN=Deleted Objects,DC=contoso,DC=com**.
13. Cliquez avec le bouton droit sur l'objet supprimé, puis cliquez sur **Modifier**.
14. Dans la zone **Attribut**, saisissez **isDeleted**.
15. Dans la section **Opération**, cliquez sur **Supprimer**.
16. Appuyez sur Entrée.
17. Dans la zone **Attribut**, saisissez **distinguishedName**.
18. Dans la zone **Valeurs**, saisissez le nom unique de l'objet dans le conteneur parent ou l'unité d'organisation dans lequel/laquelle vous souhaitez que la restauration de l'objet se produise. Par exemple, saisissez le nom unique de l'objet avant qu'il ait été supprimé.
19. Dans la section **Opération**, cliquez sur **Remplacer**.
20. Appuyez sur Entrée.
21. Activez la case à cocher **Étendu**.
22. Cliquez sur **Exécuter**, sur **Fermer**, puis fermez **LDP**.
23. Utilisez **Utilisateurs et ordinateurs Active Directory** pour remplir les attributs de l'objet, réinitialisez le mot de passe (pour un objet utilisateur), et activez l'objet (si désactivé).

Configuration de la Corbeille Active Directory



Dans Windows 2012, la corbeille Active Directory peut être activée pour fournir un processus simplifié de restauration des objets supprimés. Cette fonctionnalité surmonte des problèmes avec la restauration faisant autorité ou la récupération de l'objet tombstone. La corbeille Active Directory permet à des administrateurs de restaurer des objets supprimés avec leur fonctionnalité complète, sans devoir restaurer des données AD DS à partir de sauvegardes, puis de redémarrer AD DS ou des contrôleurs de domaine. La corbeille Active Directory repose sur l'infrastructure existante de récupération d'objet tombstone et améliore votre capacité à conserver et à récupérer des objets Active Directory supprimés par erreur.

Comment fonctionne la corbeille Active Directory

Quand vous activez la corbeille Active Directory, tous les attributs aux valeurs liées et non liées des objets Active Directory supprimés sont conservés et les objets sont restaurés dans leur intégralité vers le même état logique cohérent dans lequel ils étaient juste avant la suppression. Par exemple, les comptes d'utilisateur restaurés regagnent automatiquement toutes les appartenances de groupe et droits d'accès correspondants qu'ils avaient juste avant la suppression, dans les domaines. La corbeille Active Directory fonctionne pour des environnements AD DS et AD LDS (Active Directory Lightweight Directory Services).

Après avoir activé la corbeille Active Directory, quand un objet Active Directory est supprimé, le système conserve tous les attributs aux valeurs liées et non liées de l'objet et l'objet devient *logiquement supprimé*. Un objet supprimé est déplacé dans le conteneur Objets supprimés et son nom unique est méconnaissable. Un objet supprimé demeure dans le conteneur Objets supprimés dans un état logiquement supprimé pendant toute la durée de la durée de vie d'un objet supprimé. Pendant la durée de vie d'objet supprimé, vous pouvez récupérer un objet supprimé avec la corbeille Active Directory et en refaire un objet Active Directory vivant.

La durée de vie d'un objet supprimé est déterminée par la valeur de l'attribut **msDS-deletedObjectLifetime**. Pour un élément supprimé après que la corbeille Active Directory a été activé (objet recyclé), la durée de vie d'un objet recyclé est déterminée par la valeur de l'attribut existant **tombstoneLifetime**. Par défaut, **msDS-deletedObjectLifetime** est défini sur null. Quand **msDS-deletedObjectLifetime** est défini sur null, la durée de vie d'un objet supprimé est définie sur la valeur de la durée de vie d'un objet recyclé. Par défaut, la durée de vie d'un objet recyclé, qui est enregistrée dans l'attribut tombstoneLifetime, est également définie sur null. Quand l'attribut tombstoneLifetime est défini sur null, la durée de vie d'un objet recyclé se transfère par défaut sur 180 jours. Vous pouvez modifier les valeurs des attributs **msDS-deletedObjectLifetime** et **tombstoneLifetime** à tout moment. Quand **msDS-deletedObjectLife** est défini sur une certaine valeur autre que null, il n'assume plus la valeur de **tombstoneLifetime**.

Activation de la corbeille Active Directory

Vous pouvez activer la corbeille Active Directory seulement quand le niveau fonctionnel de la forêt est défini sur Windows Server 2008 R2 ou version supérieure.

Pour activer la corbeille Active Directory dans Windows 2012, vous pouvez effectuer l'une des opérations suivantes :

- À l'invite du module Active Directory pour Windows PowerShell, utilisez l'applet de commande **Enable-ADOptionalFeature**.
- À partir du centre d'administration Active Directory, sélectionnez le domaine, puis cliquez sur **Activer la corbeille Active Directory** dans le volet de tâches.

Seuls des éléments supprimés après l'activation de la corbeille Active Directory peuvent être restaurés à partir de la corbeille Active Directory.

Restauration d'éléments à partir de la corbeille d'Active Directory

Dans Windows Server 2012, le centre d'administration Active Directory fournit une interface graphique pour restaurer des objets AD DS qui sont supprimés. Quand la corbeille Active Directory a été activée, le conteneur Objets supprimés est visible dans le centre d'administration Active Directory. Les objets supprimés seront visibles dans ce conteneur jusqu'à ce que leur durée de vie d'objet supprimé ait expiré. Vous pouvez choisir de restaurer les objets à leur emplacement d'origine ou à un autre emplacement dans AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Gestion d'AD DS

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à Londres pour s'occuper du siège social et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

A. Datum fait plusieurs modifications d'organisation qui requièrent des modifications portant sur l'infrastructure AD DS. Un nouvel emplacement requiert une méthode sécurisée de fournir AD DS sur site et vous avez été invité à étendre les fonctions de la corbeille Active Directory à l'organisation entière.

Ordinateur(s) virtuel(s)	22411B-LON-DC1 22411B-LON-SVR1
Nom d'utilisateur	**Administrateur**
Mot de passe	**Pa$$w0rd**

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- Installer et configurer un RODC.
- Configurer et afficher des instantanés Active Directory.
- Configurer la corbeille Active Directory.

Configuration de l'atelier pratique

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22411B-LON-DC1**, et dans le volet **Actions**, cliquez sur **Accueil**.
3. Dans le volet **Actions**, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Ouvrez une session en utilisant les informations d'authentification suivantes :
    a. Nom d'utilisateur : **Administrateur**
    b. Mot de passe : **Pa$$w0rd**
    c. Domaine : **Adatum**
5. Répétez les étapes 2 à 4 pour **22411B-LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Installation et configuration d'un contrôleur de domaine en lecture seule (RODC)

Scénario

A. Datum ajoute une nouvelle filiale. Vous avez été invité à configurer un contrôleur de domaine en lecture seule pour entretenir des requêtes d'ouverture de session au niveau de la filiale. Vous devez également configurer les stratégies de mot de passe qui garantissent la mise en cache seulement des mots de passe pour les utilisateurs locaux de la filiale.

Les tâches principales de cet exercice sont les suivantes :

1. Vérifier la configuration requise pour installer un RODC
2. Installer un serveur RODC
3. Configurer une stratégie de réplication du mot de passe

▶ Tâche 1 : Vérifier la configuration requise pour installer un RODC

1. Sur LON-DC1, à partir du Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Dans les propriétés d'Adatum.com, vérifiez que le niveau fonctionnel de la forêt est au moins Windows Server® 2003.
3. Sur LON-SVR1, ouvrez **Gestionnaire de serveur** et vérifiez si l'ordinateur est un membre du domaine.
4. Utilisez **Propriétés système** pour placer LON-SVR1 dans un groupe de travail nommé **TEMPORAIRE**.
5. Redémarrez LON-SVR1.
6. Sur LON-DC1, ouvrez **Utilisateurs et ordinateurs Active Directory**.
7. Supprimez le compte d'ordinateur de **LON-SVR1** du conteneur **Computers**.
8. Dans l'unité d'organisation **Domain Controllers**, créez au préalable un compte de contrôleur de domaine en lecture seule à l'aide des paramètres par défaut, excepté ce qui suit :
   - Nom de l'ordinateur : **LON-SVR1**
   - Délégué à : **ADATUM\IT**
9. Fermez la fenêtre Utilisateurs et ordinateurs Active Directory.

▶ Tâche 2 : Installer un serveur RODC

1. Connectez-vous à LON-SVR1 en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-SVR1, ajoutez le rôle **Services AD DS**.
3. Terminez l'Assistant Installation des services de domaine Active Directory à l'aide des options par défaut excepté celles listées ci-dessous :
   - Domaine : **Adatum.com**
   - Informations d'identification réseau : **ADATUM\April (un membre du groupe informatique)**
   - Mot de passe pour April : **Pa$$w0rd**
   - Mot de passe du mode de restauration des services d'annuaire : **Pa$$w0rd**
   - Réplique à partir de : **LON-DC1.Adatum.com**
4. Une fois l'installation terminée, redémarrez LON-SVR1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer une stratégie de réplication du mot de passe

1. Sur LON-DC1, à partir du Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Dans le conteneur **Users**, affichez l'adhésion du **Groupe de réplication dont le mot de passe RODC est autorisé**, et vérifiez qu'il n'y a aucun membre actuel.
3. Dans l'**unité d'organisation Domain Controllers**, ouvrez les propriétés de **LON-SVR1**.
4. Sur l'onglet **Stratégie de réplication de mot de passe**, vérifiez que le **Groupe de réplication dont le mot de passe RODC est autorisé** et le **Groupe de réplication dont le mot de passe RODC est refusé** sont listés.
5. Sur LON-DC1, dans **Utilisateurs et ordinateurs Active Directory**, dans l'unité d'organisation **Research**, créez un nouveau groupe nommé **Utilisateurs de bureau distant**.
6. Ajoutez **Aziz**, **Colin**, **Lukas**, **Louise** et **LON-CL1** aux membres des **Utilisateurs de bureau distant**.
7. Sur LON-DC1, dans **Utilisateurs et ordinateurs Active Directory**, cliquez sur l'unité d'organisation **Domain Controllers**, puis ouvrez les propriétés de LON-SVR1.
8. Sur l'onglet **Stratégie de réplication de mot de passe**, autorisez le groupe **Utilisateurs de bureau distant** à répliquer des mots de passe sur LON-SVR1.
9. Sur LON-DC1, dans **Utilisateurs et ordinateurs Active Directory**, dans l'unité d'organisation **Domain Controllers**, ouvrez les propriétés de LON-SVR1.
10. Sur l'onglet **Stratégie de réplication de mot de passe**, ouvrez la configuration **Avancée**. Sur l'onglet **Stratégie résultante**, ajoutez **Aziz**, puis confirmez que le mot de passe d'Aziz peut être mis en cache.
11. Essayez d'ouvrir une session sur LON-SVR1 sous le nom d'**Aziz**. Cette ouverture de session échouera parce qu'Aziz n'a pas l'autorisation d'ouvrir une session sur le contrôleur de domaine en lecture seule, mais l'authentification est exécutée et les informations d'identification sont mises en cache.
12. Sur LON-DC1, dans **Utilisateurs et ordinateurs Active Directory**, dans l'unité d'organisation **Domain Controllers**, ouvrez les propriétés de LON-SVR1.
13. Sur l'onglet **Stratégie de réplication de mot de passe**, ouvrez la configuration **Avancée**.
14. Sur l'onglet **Utilisation de la stratégie**, sélectionnez l'option **Comptes authentifiés sur ce contrôleur de domaine en lecture seule**. Remarquez que le mot de passe d'Aziz a été mis en cache.
15. Sur LON-DC1, dans **Utilisateurs et ordinateurs Active Directory**, dans l'unité d'organisation **DomainControllers**, cliquez avec le bouton droit sur **LON-SVR1**, puis cliquez sur **Propriétés**.
16. Sur l'onglet **Stratégie de réplication** de mot de passe, ouvrez la configuration **Avancée**.
17. Sur l'onglet **Utilisation de stratégie**, préremplissez le mot de passe pour **Louise** et **LON-CL1**.
18. Lisez la liste de mots de passe mis en cache, puis confirmez que Louise et LON-CL1 ont été ajoutés.
19. Fermez toutes les fenêtres ouvertes sur LON-DC1.

Résultats : Après avoir terminé cet exercice, vous aurez installé et configuré un RODC.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Configuration des instantanés d'AD DS

Scénario

Dans le cadre du plan de récupération d'urgence global pour A. Datum, vous avez été chargé de tester le processus pour prendre des instantanés d'Active Directory et les afficher. Si le processus est réussi, vous les planifierez pour se produire régulièrement pour aider à la récupération des objets supprimés ou modifiés d'AD DS.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un instantané d'AD DS.
2. Modifier AD DS.
3. Monter un instantané d'Active Directory et créer une nouvelle instance.
4. Explorer un instantané avec des utilisateurs et des ordinateurs Active Directory.
5. Démonter un instantané d'Active Directory.

▶ Tâche 1 : Créer un instantané d'AD DS

1. Sur LON-DC1, ouvrez une fenêtre d'invite de commandes, puis saisissez les commandes ci-dessous, chacune étant suivie d'Entrée :

```
ntdsutil
snapshot
activate instance ntds
create
quit
Quit
```

2. La commande renvoie un message qui indique que l'instantané configuré a été généré avec succès. L'identificateur unique global (GUID) affiché est important pour des commandes de tâches ultérieures. Notez-le ou copiez-le vers le **Presse-papiers**.

▶ Tâche 2 : Modifier AD DS

1. Sur LON-DC1, ouvrez le Gestionnaire de serveur.
2. À partir du Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory**.
3. Supprimez le compte d'Adam Barr de l'unité d'organisation **Marketing**.

▶ Tâche 3 : Monter un instantané d'Active Directory et créer une nouvelle instance

1. Ouvrez une invite de commandes d'administration, puis saisissez les commandes ci-dessous, chacune étant suivie d'Entrée :

```
ntdsutil
snapshot
activate instance ntds
list all
```

   La commande renvoie une liste de tous les instantanés.

2. Saisissez les commandes suivantes, chacune suivie d'une pression sur la touche Entrée :

```
mount guid
quit
Quit
```

   Où *guid* représente l'identificateur unique global de l'instantané que vous avez créé.

3. Utilisez l'instantané pour commencer une instance d'Active Directory en tapant la commande suivante, toute sur une ligne, puis appuyez sur Entrée :

```
dsamain /dbpath c:\$snap_datetime_volumec$\windows\ntds\ntds.dit /ldapport 50000
```

Notez que *datetime* sera une valeur unique. Il ne doit y avoir qu'un dossier sur votre lecteur C:/ avec un nom qui commence par $snap.

Un message indique que le démarrage d'AD DS est terminé. Laissez Dsamain.exe fonctionner et ne fermez pas l'invite de commandes.

▶ Tâche 4 : Explorer un instantané avec des utilisateurs et des ordinateurs Active Directory

1. Basculez vers **Utilisateurs et ordinateurs Active Directory**. Cliquez avec le bouton droit sur le composant logiciel enfichable, puis sur **Changer de controlêur de domaine...**. Saisissez le nom de serveur d'annuaire et le port **LON-DC1:50000**, puis appuyez sur Entrée. Cliquez sur **OK**.
2. Localisez l'objet du compte d'utilisateur **Adam Barr** dans l'unité d'organisation **Marketing**. Notez que l'objet d'Adam Barr est affiché parce que l'instantané a été pris avant de le supprimer.

▶ Tâche 5 : Démonter un instantané d'Active Directory

1. Dans l'invite de commandes, appuyez sur Ctrl+C. pour arrêter DSAMain.exe.
2. Saisissez les commandes suivantes :

```
ntdsutil
snapshot
activate instance ntds
list all
unmount guid
list all
quit
Quit
```

Où *guid* représente l'identificateur unique global de l'instantané.

Résultats : Après avoir terminé cet exercice, vous aurez configuré des instantanés d'AD DS.

Exercice 3 : Configuration de la Corbeille Active Directory

Scénario

Dans le cadre de la planification de récupération d'urgence pour AD DS, vous devez configurer et tester la corbeille Active Directory pour autoriser la récupération de niveau d'objet et de conteneur.

Les tâches principales de cet exercice sont les suivantes :

1. Activer la corbeille Active Directory.
2. Créer et supprimer des utilisateurs test.
3. Restaurer les utilisateurs supprimés.
4. Pour préparer le module suivant

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Activer la corbeille Active Directory

1. Sur LON-DC1, à partir du Gestionnaire de serveur, ouvrez le **Centre d'administration Active Directory**.
2. Activer la Corbeille.
3. Appuyez sur F5 pour actualiser le **Centre d'administration Active Directory**.

▶ Tâche 2 : Créer et supprimer des utilisateurs test

1. Dans **Centre d'administration Active Directory,** créez les utilisateurs suivants dans l'unité d'organisation **Research**. Donnez à chacun un mot de passe **Pa$$w0rd** :
   - **Test1**
   - **Test2**
2. Supprimez les comptes **Test1** et **Test2**.

▶ Tâche 3 : Restaurer les utilisateurs supprimés

1. Dans **Centre d'administration Active Directory**, naviguez jusqu'au dossier **Deleted Objects** pour le domaine **Adatum**.
2. Restaurez **Test1** vers son emplacement d'origine.
3. Restaurez **Test2** vers l'unité d'organisation relative au service informatique IT.
4. Confirmez que Test1 est maintenant situé dans l'unité d'organisation Research et que Test2 est dans l'unité d'organisation IT.

▶ Pour préparer le module suivant

- Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels.

Résultats : À la fin de cet exercice, vous devez avoir configuré la corbeille Active Directory.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Recommandations pour administrer AD DS

- Ne virtualisez pas tous les contrôleurs de domaine virtuels sur le même hôte hyperviseur ou serveur.
- Les instantanés d'ordinateur virtuel fournissent un excellent point de référence ou une méthode de récupération rapide, mais vous ne devez pas les utiliser comme remplacement pour des sauvegardes régulières. En outre, ils ne vous permettront pas de récupérer des objets par le rétablissement d'un instantané plus ancien.
- Utilisez des contrôleurs de domaine en lecture seule quand la sécurité physique rend un contrôleur de domaine accessible en écriture irréalisable.
- Utilisez le meilleur outil pour le travail. La console Utilisateurs et ordinateurs Active Directory est l'outil le plus utilisé généralement pour gérer AD DS, mais ce n'est pas toujours le meilleur. Vous pouvez utiliser le centre d'administration Active Directory pour effectuer des tâches à grande échelle ou ces tâches qui impliquent plusieurs objets. Vous pouvez également utiliser le module Active Directory pour que Windows PowerShell crée des scripts réutilisables pour des tâches d'administration fréquemment répétées.
- Activez la corbeille Active Directory si votre niveau fonctionnel de la forêt prend en charge la fonctionnalité. Cela peut être inestimable pour gagner du temps lors de la récupération d'objets supprimés accidentellement dans AD DS.

Outils

Outil	Utilisé pour	Emplacement
Gestionnaire Hyper-V	Gestion des hôtes virtualisés sur Windows Server 2012	Gestionnaire de serveur - Outils
Module Active Directory pour Windows PowerShell	Gestion AD DS au moyen de scripts et à partir de la ligne de commande	Gestionnaire de serveur - Outils
Utilisateurs et ordinateurs Active Directory	Gestion des objets dans AD DS	Gestionnaire de serveur – Outils
Centre d'administration Active Directory	Gestion d'objets dans AD DS, activation et gestion de la corbeille Active Directory	Gestionnaire de serveur - Outils
Ntdsutil.exe	Gestion des instantanés AD DS	Invite de commandes
Dsamain.exe	Montage des instantanés d'AD DS pour l'exploration	Invite de commandes

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4

Gestion des comptes d’utilisateurs et de service

Table des matières :

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

Leçon 1 : Automatisation de la gestion des comptes d’utilisateurs **4-2**

Leçon 2 : Configuration des paramètres de stratégie de mot de passe et de verrouillage de compte d’utilisateur **4-8**

Leçon 3 : Configuration des comptes de service gérés **4-15**

Atelier pratique : Gestion des comptes d’utilisateurs et de service **4-22**

Contrôle des acquis et éléments à retenir **4-26**

Vue d’ensemble du module

La gestion des comptes d’utilisateurs dans un environnement d’entreprise peut être une tâche ardue. Assurez-vous de configurer correctement les comptes d’utilisateurs dans votre environnement et de les protéger contre l’utilisation non autorisée et contre les utilisateurs qui abusent de leurs privilèges de compte. Si vous utilisez des comptes de service dédiés pour les services système et les processus d’arrière plan, et que vous définissez des stratégies de comptes appropriées, vous pouvez vous assurer que votre environnement Windows Server® 2012 donne aux utilisateurs et aux applications l’accès dont ils ont besoin pour fonctionner correctement.

Ce module indique comment gérer d’importants groupes de comptes d’utilisateurs, explique les différentes options disponibles pour fournir la sécurité par mot de passe adaptée aux comptes dans votre environnement, et présente comment configurer des comptes pour assurer l’authentification des services système et des processus en arrière plan.

Objectifs

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

- automatiser la création de compte d’utilisateur ;
- configurer les paramètres de stratégie de mot de passe et de verrouillage de compte ;
- configurer des comptes de service gérés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Automatisation de la gestion des comptes d'utilisateurs

Les utilisateurs et les ordinateurs Active Directory®, ainsi que le centre d'administration Active Directory fournissent des interfaces utilisateur graphiques pour la création d'un ou plusieurs comptes d'utilisateurs. Même s'il est facile de naviguer dans l'interface fournie par ces outils, la création de plusieurs utilisateurs ou la réalisation de modifications pour plusieurs utilisateurs peut être compliquée. Windows Server 2012 vous offre un certain nombre d'outils qui vous permettent de gérer des comptes d'utilisateurs de façon plus efficace dans votre domaine de services de domaine Active Directory (AD DS). Cette leçon présente les outils qui vous permettent d'effectuer des tâches telles que la modification d'attributs d'utilisateur pour de nombreux d'utilisateurs, la recherche d' utilisateurs, ainsi que l'importation et l'exportation d'utilisateurs à partir et vers des sources de données ou répertoires externes.

Objectifs de la leçon

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

- expliquer comment exporter des utilisateurs à l'aide de l'outil Échange de données de valeurs séparées par des virgules ;
- expliquer comment importer des utilisateurs à l'aide de l'outil Échange de données de valeurs séparées par des virgules ;
- décrire comment importer des comptes d'utilisateurs à l'aide du standard Internet LDIFDE (LDAP Data Interchange Format) ;
- expliquer comment importer des comptes d'utilisateurs à l'aide de Windows PowerShell®.

Démonstration : Exportation de comptes d'utilisateurs à l'aide de l'outil Échange de données de valeurs séparées par des virgules

L'outil Échange de données de valeurs séparées par des virgules est un outil de ligne de commande qui exporte ou importe des objets AD DS à partir ou vers un fichier texte délimité par des virgules, également appelé fichier de valeurs séparées par des virgules ou fichier .csv. Vous pouvez créer, modifier et ouvrir des fichiers .csv à l'aide d'outils courants tels que Bloc-notes ou Microsoft Office Excel®. En outre, vous pouvez utiliser ces fichiers pour exporter les informations d'AD DS en vue de les utiliser dans d'autres zones de votre organisation ou pour importer les informations d'autres sources pour la création ou la modification des objets AD DS de votre domaine.

Voici la syntaxe de base de la commande de l'outil Échange de données de valeurs séparées par des virgules pour l'exportation :

```
csvde -f filename
```

Cependant, cette commande exporte tous les objets de votre domaine Active Directory. Vous pouvez limiter l'étendue de l'exportation à l'aide des quatre paramètres suivants :

- -d RootDN. Spécifie le nom unique du conteneur à partir duquel l'exportation commence. La valeur par défaut est le domaine lui-même.
- -p SearchScope. Spécifie l'étendue de recherche relative au conteneur spécifié par -d. SearchScope peut prendre la valeur base (cet objet uniquement), onelevel (objets de ce conteneur) ou subtree (ce conteneur et tous les sous-conteneurs). La valeur par défaut est subtree.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- -r Filter. Filtre les objets retournés dans l'étendue configurée par -d et -p. Le filtre est spécifié dans la syntaxe de requête du protocole LDAP (Lightweight Directory Access Protocol). Vous allez utiliser un filtre dans l'atelier pratique de cette leçon. La syntaxe de la requête LDAP n'est pas traitée dans ce cours. Pour plus d'informations, consultez la page http://go.microsoft.com/fwlink/?LinkId=168752 (Certains de ces sites adressées dans ce cours sont en anglais.).
- -l ListOfAttributes. Spécifie les attributs à exporter. Utilisez le nom LDAP pour chaque attribut, séparé par une virgule, comme dans

```
-l DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName
```

Après l'exportation via l'outil Échange de données de valeurs séparées par des virgules, les noms de l'attribut LDAP s'affichent sur la première ligne. Chaque objet s'affiche par la suite (à raison d'un objet par ligne) et doit contenir exactement les attributs listés sur la première ligne, comme illustré dans les exemples suivants :

```
 DN,objectClass,sn,givenName,sAMAccountName,userPrincipalName
"CN=David Jones,OU=Employees,OU=User
Accounts,DC=contoso,DC=com",user,Jones,David,david.jones,david.jones@contoso.com
"CN=Lisa Andrews,OU=Employees,OU=User
Accounts,DC=contoso,DC=com",user,Andrews,Lisa,lisa.andrews,lisa.andrews@contoso.com
```

Dans cette démonstration, vous allez apprendre à :

- exporter des comptes d'utilisateurs avec l'outil Échange de données de valeurs séparées par des virgules.

Procédure de démonstration

1. Sur l'ordinateur LON-DC1, ouvrez une invite de commandes.
2. Dans la fenêtre d'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
csvde -f E:\Labfiles\Mod04\UsersNamedRex.csv -r "(name=Rex*)" -l
DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName
```

3. Ouvrez E:\Labfiles\Mod04\UsersNamedRex.csv avec Bloc-notes.
4. Examinez le fichier, puis fermez Bloc-notes.
5. Fermez toutes les fenêtres ouvertes sur LON-DC1.

Démonstration : Importation de comptes d'utilisateurs à l'aide de l'outil Échange de données de valeurs séparées par des virgules

Vous pouvez également utiliser l'outil Échange de données de valeurs séparées par des virgules pour créer des comptes d'utilisateurs en important un fichier .csv. Si les informations utilisateurs figurent dans des bases de données existantes Excel ou Microsoft Office Access®, l'outil Échange de données de valeurs séparées par des virgules constitue une excellente façon de tirer profit de ces informations afin d'automatiser la création de comptes d'utilisateurs.

Voici la syntaxe de base de la commande de l'outil Échange de données de valeurs séparées par des virgules pour l'importation :

```
csvde -i -f filename -k
```

Le paramètre -i spécifie le mode d'importation. Sans ce paramètre, le mode par défaut de l'outil Échange de données de valeurs séparées par des virgules est l'exportation. Le paramètre -f identifie le nom de fichier d'importation ou d'exportation. Le paramètre -k est utile lors des opérations d'importation, car il indique à l'outil Échange de données de valeurs séparées par des virgules d'ignorer les erreurs, y compris « L'objet existe déjà »

Le fichier d'importation lui-même est un fichier texte délimité par des virgules (.csv ou .txt) où la première ligne définit les attributs importés par leurs noms d'attribut LDAP. Chaque objet s'affiche par la suite (à raison d'un objet par ligne) et doit contenir exactement les attributs listés sur la première ligne ; un exemple de fichier se présente comme suit :

```
DN,objectClass,sn,givenName,sAMAccountName,userPrincipalName
"CN=David Jones,OU=Employees,OU=User
Accounts,DC=contoso,DC=com",user,Jones,David,david.jones,david.jones@contoso.com
"CN=Lisa Andrews,OU=Employees,OU=User
Accounts,DC=contoso,DC=com",user,Andrews,Lisa,lisa.andrews,lisa.andrews@contoso.com
```

Ce fichier, une fois importé par la commande de l'outil Échange de données de valeurs séparées par des virgules, crée un objet utilisateur pour Lisa Andrews dans l'unité d'organisation des employés. Le fichier configure les noms d'ouverture de session, le nom et le prénom de l'utilisateur. Vous ne pouvez pas utiliser l'outil Échange de données de valeurs séparées par des virgules pour importer des mots de passe. Sans mot de passe, le compte d'utilisateur sera désactivé au départ. Vous pouvez activer l'objet dans AD DS après avoir réinitialisé le mot de passe.

Dans cette démonstration, vous allez apprendre à :

- importer des comptes d'utilisateurs avec l'outil Échange de données de valeurs séparées par des virgules.

Procédure de démonstration

1. Sur LON-DC1, ouvrez **E:\Labfiles\Mod04\NewUsers.csv** avec Bloc-notes. Examinez les informations relatives aux utilisateurs listés dans le fichier.
2. Ouvrez une invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

   ```
   csvde -i -f E:\Labfiles\Mod04\NewUsers.csv -k
   ```

3. Dans le Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory** et confirmez que les utilisateurs ont été créés avec succès.
4. Examinez les comptes pour confirmer que le prénom, le nom, le nom d'utilisateur principal et le nom de connexion avant l'installation de Windows® 2000 sont indiqués conformément aux instructions du fichier NewUsers.csv.
5. Redéfinissez les mots de passe des deux comptes sur **Pa$$w0rd**.
6. Activez les deux comptes.
7. Fermez toutes les fenêtres ouvertes sur LON-DC1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Importation de comptes d'utilisateurs avec LDIFDE

Vous pouvez également utiliser LDIFDE.exe pour importer ou exporter des objets Active Directory, notamment des utilisateurs. Le format LDIF est un format de fichier standard que vous pouvez utiliser pour stocker des informations et effectuer des opérations en lots dans les répertoires conformes aux normes LDAP. LDIF prend en charge les opérations d'importation et d'exportation, ainsi que les opérations en lots qui modifient des objets dans le répertoire. La commande LDIFDE implémente ces opérations en lots à l'aide des fichiers LDIF.

Le format de fichier LDIF se compose d'un bloc de lignes qui, ensemble, constituent une opération unique. Plusieurs opérations d'un fichier unique sont séparées par une ligne vierge. Chaque ligne, comportant une opération, se compose d'un nom d'attribut suivi de deux-points et de la valeur de l'attribut. Par exemple, supposons que vous souhaitiez importer des objets utilisateurs pour deux commerciaux nommés Bonnie Kearney et Bobby Moore. Le contenu du fichier LDIF ressemble à l'exemple suivant :

```
dn: CN=Bonnie Kearney,OU=Employees,OU=User Accounts,DC=contoso,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Bonnie Kearney
sn: Kearney
title: Opérations
description: Operations (London)
givenName: Bonnie
displayName: Kearney, Bonnie
company: Contoso, Ltd.
sAMAccountName: bonnie.kearney
userPrincipalName: bonnie.kearney@contoso.com
mail: bonnie.kearney@contoso.com
dn: CN=Bobby Moore,OU=Employees,OU=User Accounts,DC=contoso,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Bobby Moore
sn: Moore
title: Legal
description: Legal (New York)
givenName: Bobby
displayName: Moore, Bobby
company: Contoso, Ltd.
sAMAccountName: bobby.moore
userPrincipalName: bobby.moore@contoso.com
mail: bobby.moore@contoso.com
```

Chaque opération commence avec l'attribut du nom de domaine (DN) de l'objet qui est la cible de l'opération. La ligne suivante, changeType, spécifie le type d'opération : ajouter, modifier ou supprimer.

Comme vous pouvez le voir, le format de fichier LDIF n'est pas aussi intuitif ni familier que le format texte séparé par des virgules. Cependant, étant donné que le format LDIF est aussi un standard, de nombreux services d'annuaire et bases de données peuvent exporter les fichiers LDIF.

Après la création ou l'obtention d'un fichier LDIF, vous pouvez exécuter les opérations indiquées par le fichier à l'aide de la commande LDIFDE. Dans une invite de commandes, saisissez ldifde /? pour les informations d'utilisation. Voici les deux commutateurs les plus importants pour la commande LDIFDE :

- -i. Active le mode d'importation. Sans ce paramètre, LDIFDE exporte les informations.
- -f Nom de fichier. Le fichier à partir duquel effectuer l'importation et vers lequel réaliser l'exportation.

Dans cette démonstration, vous allez apprendre à :

- importer des comptes d'utilisateurs avec LDIFDE.

Procédure de démonstration

1. Ouvrez **E:\Labfiles\Mod04\NewUsers.ldf** avec Bloc-notes. Examinez les informations relatives aux utilisateurs listés dans le fichier.
2. Ouvrez une invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
ldifde -i -f E:\Labfiles\Mod04\NewUsers.ldf -k
```

3. Ouvrez Utilisateurs et ordinateurs Active Directory, puis confirmez que les utilisateurs ont été créés avec succès.
4. Examinez les comptes afin de confirmer que les propriétés de l'utilisateur sont indiquées conformément aux instructions de NewUsers.ldf.
5. Redéfinissez les mots de passe des deux comptes sur **Pa$$w0rd**.
6. Activez les deux comptes.
7. Fermez toutes les fenêtres ouvertes sur LON-DC1.

   Question : Quels avantages offre LDIFDE par rapport à l'outil Échange de données de valeurs séparées par des virgules lors de la gestion des comptes d'utilisateurs dans un environnement AD DS ?

Démonstration : Importation de comptes d'utilisateurs avec Windows PowerShell

Le module Active Directory pour Windows PowerShell peut également utiliser le contenu d'un fichier .csv pour importer des objets dans AD DS.

Deux applets de commande sont utilisées pour effectuer cette tâche :

- **Import-CSV**. Cette applet de commande crée des objets à partir des fichiers .csv. Ces derniers peuvent être dirigés vers d'autres applets de commande Windows PowerShell.
- **New-ADUser**. Cette applet de commande est utilisée pour créer les objets importés depuis l'applet de commande Import-CSV.

Dans cette démonstration, vous allez apprendre à :

- importer des comptes d'utilisateurs avec Windows PowerShell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

1. Sur LON-DC1, dans Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory** et sous **Adatum.com**, créez une nouvelle unité d'organisation nommée **ImportUsers**.
2. Ouvrez **E:\Labfiles\Mod04\ImportUsers.ps1** avec Bloc-notes. Examinez le contenu du fichier.
3. À côté de **$impfile**, modifiez le champ **path and filename to csv** en **E:\Labfiles\Mod04\ImportUsers.csv**, puis enregistrez le fichier.
4. Ouvrez le **module Active Directory pour Windows PowerShell**.
5. Saisissez les commandes suivantes, puis appuyez sur Entrée après chaque commande. Lorsque vous êtes invité à modifier la stratégie d'exécution, appuyez sur Entrée pour accepter l'option par défaut **O** :

```
Set-ExecutionPolicy remotesigned
E:\Labfiles\Mod04\importusers.ps1
```

6. Dans la boîte de dialogue de demande de mot de passe, saisissez **Pa$$w0rd**.
7. Ouvrez **Utilisateurs et ordinateurs Active Directory** et vérifiez que les comptes d'utilisateurs ont été importés dans l'unité d'organisation **ImportUsers**.
8. Fermez toutes les fenêtres ouvertes sur LON-DC1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2

Configuration des paramètres de stratégie de mot de passe et de verrouillage de compte d'utilisateur

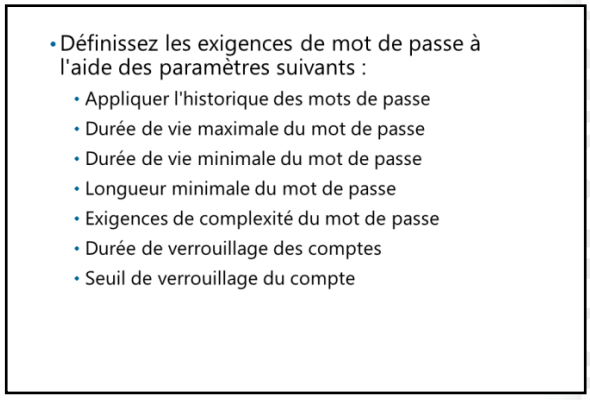
En tant qu'administrateur, vous devez vérifier que les comptes utilisateurs de votre environnement sont conformes aux paramètres de sécurité établis par votre organisation. Windows Server 2012 utilise des stratégies de comptes pour configurer les paramètres relatifs à la sécurité pour les comptes d'utilisateurs. Ce module vous aide à identifier les paramètres disponibles pour configurer la sécurité de compte, ainsi que les méthodes disponibles pour configurer ces paramètres.

Objectifs de la leçon

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

- expliquer les stratégies des comptes d'utilisateurs ;
- expliquer comment configurer des stratégies de comptes d'utilisateurs ;
- décrire les objets PSO (Password Settings Objects) ;
- expliquer comment configurer des objets PSO.

Comprendre les stratégies des comptes d'utilisateurs



Dans AD DS, les stratégies de comptes définissent les paramètres par défaut des attributs de sécurité attribués aux objets utilisateurs. Dans AD DS, les stratégies de comptes se trouvent dans deux groupes différents de paramètres : stratégie de mot de passe et verrouillage de compte. Vous pouvez configurer les deux groupes de paramètres dans les paramètres de stratégie locale pour un serveur individuel Windows Server 2012 ou pour le domaine entier à l'aide de la console de gestion des stratégies de groupe (GPMC) dans AD DS. Si les paramètres de stratégie locale et les paramètres de stratégie de groupe ne concordent pas, ces derniers remplacent les premiers

Dans Gestion des stratégies de groupe au sein de AD DS, la plupart des paramètres de stratégie peuvent être appliqués à différents niveaux de la structure AD DS : domaine, site ou unité d'organisation. Cependant, les stratégies de comptes ne peuvent être appliquées qu'à un seul niveau dans AD DS : au domaine entier. Par conséquent, seul un ensemble de paramètres de stratégie de compte peut être appliqué à un domaine AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Stratégie de mot de passe

Définissez la stratégie de mot de passe à l'aide des paramètres suivants :

- Appliquer l'historique des mots de passe. Il s'agit du nombre de nouveaux mots de passe uniques devant être associés à un compte d'utilisateur avant de pouvoir réutiliser un ancien mot de passe. Par défaut, ce paramètre est défini à 24 anciens mots de passe. Lorsque vous utilisez ce paramètre avec le paramètre de durée de vie minimale du mot de passe, le paramètre d'application de l'historique de mot de passe empêche la réutilisation constante du même mot de passe.
- Durée de vie maximale du mot de passe. Il s'agit du nombre de jours pendant lesquels l'utilisateur peut utiliser un mot de passe avant de devoir le modifier. Le changement régulier des mots de passe facilite la prévention de la corruption des mots de passe. Cependant, vous devez équilibrer ce critère de sécurité par rapport aux considérations logistiques, en raison du fait que les utilisateurs sont amenés à modifier leurs mots de passe trop souvent. Le paramètre par défaut de 42 jours est probablement adapté à la plupart des organisations.
- Durée de vie minimale du mot de passe. Il s'agit du nombre de jours pendant lesquels l'utilisateur doit utiliser un mot de passe avant de pouvoir le modifier. La valeur par défaut est d'un jour, ce qui est convenable si vous appliquez également l'historique de mot de passe. Vous pouvez restreindre l'utilisation constante du même mot de passe si vous utilisez ce paramètre en même temps qu'un paramètre court pour appliquer l'historique de mot de passe.
- Longueur minimale du mot de passe. Il s'agit du nombre minimal de caractères que le mot de passe d'un utilisateur doit contenir. La valeur par défaut est de sept. Il s'agit de la valeur minimale par défaut fréquemment utilisée. Cependant, vous devez envisager d'augmenter la longueur du mot de passe à au moins 10 caractères pour améliorer la sécurité.
- Exigences de complexité. Windows Server comprend un filtre de mot de passe par défaut qui est activé par défaut et vous ne devez pas le désactiver. Le filtre requiert qu'un mot de passe présente les caractéristiques suivantes :
  - Il ne doit contenir ni votre nom de famille, ni votre nom d'utilisateur.
  - Il doit comporter au moins six caractères.
  - Il doit contenir des caractères tirés de trois des quatre groupes ci-dessous :
    - lettres majuscules [A…Z] ;
    - lettres minuscules [a…z] ;
    - chiffres [0…9] ;
    - caractères spéciaux non alphanumériques, tels que !@#)(*&^%.

Stratégie de verrouillage du compte

Vous pouvez définir des seuils de verrouillage de compte, la durée du verrouillage et un mode de déverrouillage des comptes. Les seuils de verrouillage de compte exigent que les comptes deviennent inutilisables après un certain nombre d'échecs d'ouverture de session au cours d'une période définie. Les stratégies de verrouillage de compte permettent de détecter et d'éviter les attaques en force sur les mots de passe des comptes. Les paramètres disponibles sont les suivants :

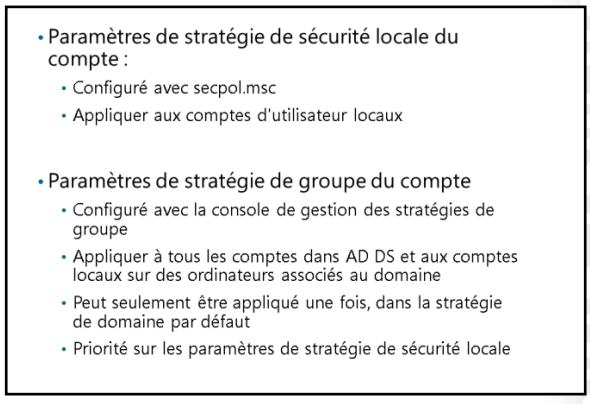
- Durée de verrouillage des comptes. Définit le nombre de minutes pendant lesquelles un compte verrouillé reste verrouillé. Une fois que ce délai indiqué est écoulé, le compte est déverrouillé automatiquement. Pour indiquer qu'un administrateur doit déverrouiller le compte, définissez la valeur à 0. Pensez à utiliser des stratégies de mot de passe précises pour forcer les administrateurs à déverrouiller les comptes présentant un niveau de sécurité élevé. Configurez ensuite ce paramètre à 30 minutes pour les utilisateurs normaux.
- Seuil de verrouillage du compte. Détermine le nombre d'échecs d'ouverture de session autorisés avant qu'un compte d'utilisateur ne soit verrouillé. Une valeur nulle indique que le compte ne sera jamais verrouillé. Vous devez indiquer une valeur assez élevée pour tenir compte des utilisateurs n'ayant pas saisi correctement leurs mots de passe, mais assez basse pour faire échouer les tentatives d'attaques en force des mots de passe. En général, les valeurs de ce paramètre vont de trois à cinq.
- Réinitialiser le compteur de verrouillages du compte après. Détermine le nombre de minutes qui doivent s'écouler après un échec d'ouverture de session, avant que le compteur d'ouvertures de sessions infructueuses ne soit réinitialisé à 0. Ce paramètre s'applique lorsqu'un utilisateur a saisi un mot de passe incorrect, sans pour autant dépasser le seuil de verrouillage de compte. Pensez à définir cette valeur sur 30 minutes.

Stratégie Kerberos

Les options de configuration de la stratégie Kerberos contiennent les paramètres du ticket TGT (Ticket-Granting Ticket) de protocole Kerberos version 5, ainsi que les paramètres de durées de vie et d'horodatage des tickets de session. Les paramètres par défaut sont adaptés à la plupart des organisations.

Configuration de stratégies de compte d'utilisateur

Il existe plusieurs options permettant de configurer les stratégies de comptes d'utilisateurs lors de l'administration d'un environnement AD DS.



Paramètres de stratégie locale avec Secpol.msc

Chaque ordinateur Windows Server 2012 possède son propre ensemble de stratégies de comptes, qui s'appliquent aux comptes créés et gérés sur l'ordinateur local. Pour configurer ces paramètres de stratégie, ouvrez la console Stratégie de sécurité locale en exécutant **secpol.msc** dans l'invite de commandes. Les paramètres de stratégie de mot de passe et de stratégie de compte peuvent se trouver dans la console Stratégie de sécurité locale. Il vous suffit de développer **Paramètres de sécurité**, puis **Stratégies de comptes**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Stratégie de groupe avec la gestion des stratégies de groupe

Dans l'environnement de domaine AD DS, les paramètres de stratégie de compte à l'échelle du domaine sont configurés dans la console de gestion des stratégies de groupe. Les paramètres peuvent être trouvés dans **Configuration ordinateur**, en développant le nœud **Stratégies**, en développant sous le nœud **Paramètres Windows**, en développant le nœud **Paramètres de sécurité**, puis en développant le nœud **Stratégies de comptes**.

Les paramètres trouvés dans le nœud **Stratégies de comptes** sont les mêmes paramètres trouvés dans la stratégie de sécurité locale, en plus des paramètres de stratégie Kerberos qui s'appliquent à l'authentification de domaine.

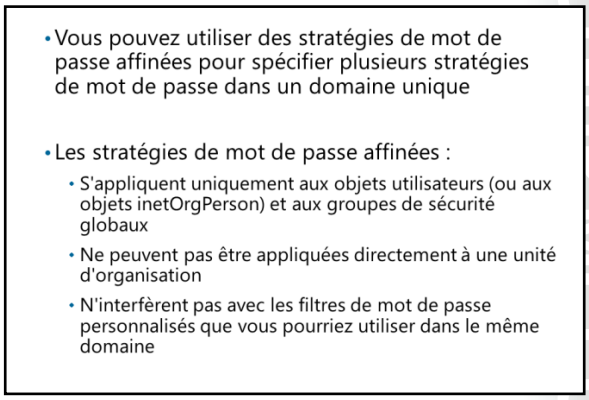
Les paramètres de stratégie de compte de stratégie de groupe existent dans le modèle de chaque objet Stratégie de groupe (GPO) créé dans la console GPMC. Cependant, vous pouvez appliquer une stratégie de compte seulement une fois dans un domaine et seulement dans un objet Stratégie de groupe. C'est la stratégie de domaine par défaut, et elle lie à la racine du domaine AD DS. En tant que tels, les paramètres de stratégie de compte dans la stratégie de domaine par défaut s'appliquent à chaque ordinateur qui est joint au domaine.

Remarque : En cas de conflit entre les paramètres de stratégie de compte dans la stratégie de sécurité locale et les paramètres de stratégie de compte dans l'objet Stratégie de groupe de la stratégie de domaine par défaut, les paramètres de stratégie de domaine par défaut ont la priorité.

Question : Pourquoi utiliseriez-vous secpol.msc pour configurer les paramètres de stratégie de compte locale pour un ordinateur Windows Server 2012 au lieu d'utiliser les paramètres de stratégie de compte de stratégie de groupe basés sur le domaine ?

Qu'est-ce que les objets PSO ?

En commençant par Windows Server® 2008, les administrateurs peuvent définir plus d'une stratégie de mot de passe dans un domaine unique en implémentant des stratégies de mot de passe affinées. Celles-ci vous permettent d'avoir un contrôle plus granulaire sur les exigences de mot de passe utilisateur, et vous pouvez avoir différentes exigences de mot de passe pour différents utilisateurs ou groupes.



Pour prendre en charge la fonctionnalité de stratégie de mot de passe affinée, AD DS sous Windows Server 2008 et versions plus récentes comprend deux types d'objet :

- Conteneur de paramètre de mot de passe. Windows Server crée ce conteneur par défaut, et vous pouvez l'afficher dans le conteneur System du domaine. Le conteneur enregistre les objets PSO que vous créez et liez aux groupes de sécurité globale ou aux utilisateurs.
- Objets de paramètres de mot de passe. Les membres du groupe d'administrateurs du domaine créent des objets PSO, puis définissent les paramètres spécifiques de mot de passe et de verrouillage de compte à lier à un groupe de sécurité ou utilisateur spécifique.

Les stratégies de mot de passe affinée s'appliquent seulement aux objets utilisateurs (ou aux objets inetOrgPerson, si vous les utilisez au lieu des objets utilisateurs) et aux groupes de sécurité globale. En liant des Objets de paramètres de mot de passe à un utilisateur ou à un groupe, vous modifiez un attribut appelé **msDS-PSOApplied**, qui est vide par défaut. Cette approche traite maintenant des paramètres de mot de passe et de verrouillage de compte pas en tant qu'exigences à l'l'échelle du domaine, mais en tant qu'attributs à un utilisateur ou à un groupe.

Par exemple, pour configurer une stratégie stricte de mot de passe pour les comptes d'administrateur, créez un groupe de sécurité globale, ajoutez les comptes d'utilisateur administrateur comme membres et liez un objet PSO au groupe. L'application des stratégies de mot de passe affinée à un groupe de cette manière est plus gérable que l'application des stratégies à chaque compte d'utilisateur individuel. Si vous créez un nouveau compte de service, vous l'ajoutez simplement au groupe et le compte est alors géré par l'objet PSO.

Par défaut, seuls les membres du groupe Administrateurs du domaine peuvent définir des stratégies de mot de passe affinée. Cependant, vous pouvez également déléguer la capacité de définir ces stratégies à d'autres utilisateurs.

Application des stratégies de mot de passe affinées

Vous ne pouvez pas appliquer une stratégie de mot de passe affinée à une unité d'organisation directement. Pour appliquer une stratégie de mot de passe affinée aux utilisateurs d'une unité d'organisation, vous pouvez utiliser un groupe des clichés instantanés. Un groupe des clichés instantanés est un groupe de sécurité globale qui mappe logiquement à une unité d'organisation, et applique une stratégie de mot de passe affinée. Vous pouvez ajouter les utilisateurs d'une unité d'organisation comme membres du groupe des clichés instantanés nouvellement crée, puis vous appliquez la stratégie de mot de passe affinée à ce groupe des clichés instantanés. Si vous déplacez un utilisateur d'une unité d'organisation à une autre, vous devez mettre à jour l'appartenance des groupes des clichés instantanés correspondants.

Les paramètres gérés par une stratégie de mot de passe affinée sont identiques à ceux des nœuds de stratégie de mot de passe et de stratégie de comptes d'un objet Stratégie de groupe. Cependant, les stratégies de mot de passe affinée ne sont ni implémentées dans le cadre de la stratégie de groupe, ni appliquées dans le cadre d'un objet Stratégie de groupe. Il y a plutôt une classe distincte d'objet dans Active Directory qui gère les paramètres pour la stratégie de mot de passe affinée : PSO.

Vous pouvez créer un ou plusieurs objets PSO dans votre domaine. Chacun contient un ensemble complet de paramètres de mot de passe et de stratégie de verrouillage. Les paramètres d'un objet PSO est appliqué en liant l'objet des paramètres de mot de passe à un ou plusieurs groupes de sécurité globale ou utilisateurs.

Pour utiliser une stratégie de mot de passe affinée, votre niveau fonctionnel du domaine doit être au moins Windows Server 2008, ce qui signifie que tous vos contrôleurs de domaine dans le domaine exécutent au moins Windows Server 2008, et le niveau fonctionnel du domaine a été élevé au moins à Windows Server 2008.

Pour confirmer et modifier le niveau fonctionnel du domaine :

1. Ouvrez la fenêtre Domaines et approbations Active Directory.
2. Dans l'arborescence de la console, développez **Domaines et approbations Active Directory**, puis développez l'arborescence jusqu'à ce que vous puissiez voir le domaine.
3. Cliquez avec le bouton droit sur le domaine, puis cliquez sur **Augmenter le niveau fonctionnel du domaine**.

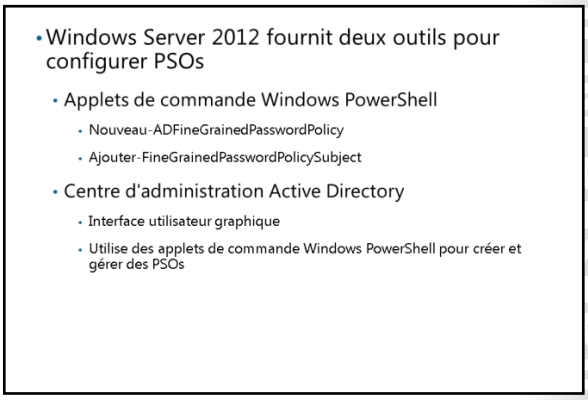
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des objets PSO

Vous pouvez créer et appliquer des objets PSO dans l'environnement Windows Server 2012 à l'aide de l'un des outils suivants :

- Centre d'administration Active Directory
- Windows PowerShell



Configuration des objets PSO à l'aide de Windows PowerShell

Dans Windows Server 2012, les nouveaux applets de commande Windows PowerShell dans le module Active Directory pour Windows PowerShell peuvent être utilisés pour créer et gérer des objets PSO dans votre domaine.

- New-ADFineGrainedPasswordPolicy

  Cet applet de commande est utilisé pour créer un nouvel objet PSO et définir les paramètres de l'objet de paramètres de mot de passe. Par exemple, la commande suivante crée un nouvel objet PSO nommé TestPwd, puis spécifie ses paramètres :

```
New-ADFineGrainedPasswordPolicy TestPswd -ComplexityEnabled:$true -
LockoutDuration:"00:30:00" -LockoutObservationWindow:"00:30:00" -LockoutThreshold:"0"
-MaxPasswordAge:"42.00:00:00" -MinPasswordAge:"1.00:00:00" -MinPasswordLength:"7" -
PasswordHistoryCount:"24" -Precedence:"1" -ReversibleEncryptionEnabled:$false -
ProtectedFromAccidentalDeletion:$true
```

- Add-FineGrainedPasswordPolicySubject

  Cet applet de commande vous permet de lier un utilisateur ou un groupe à un objet PSO existant. Par exemple, la commande suivante lie l'objet PSO TestPwd au groupe AD DS nommé group1 :

```
Add-ADFineGrainedPasswordPolicySubject TestPswd -Subjects Marketing
```

Configuration des objets PSO à l'aide de centre d'administration Active Directory

Le centre d'administration Active Directory fournit une interface graphique pour créer et gérer des objets PSO. Pour gérer des objets PSO dans le centre d'administration Active Directory, suivez cette procédure :

1. Ouvrez **Centre d'administration Active Directory.**
2. Cliquez sur **Gérer**, cliquez sur **Ajouter des nœuds de navigation**, sélectionnez le domaine cible approprié dans la boîte de dialogue **Ajouter des nœuds de navigation**, puis cliquez sur **OK**.
3. Dans le volet de navigation Centre d'administration Active Directory, ouvrez le conteneur **System**, puis cliquez sur **classe d'objets PSC (Password Settings Container)**.
4. Dans le volet **Tâches**, cliquez sur **Nouveau**, puis cliquez sur **Paramètres de mot de passe**.
5. Complétez ou modifiez les champs à l'intérieur de la page de propriété pour créer un nouvel **Objet de paramètres de mot de passe**.

6. Sous **S'applique directement à**, cliquez sur **Ajouter**, saisissez **Marketing**, puis cliquez sur **OK**.
7. Cela associe l'objet **Stratégie de mot de passe** aux membres du groupe global que vous avez créé pour l'environnement de test.
8. Cliquez sur **OK** pour envoyer la création de l'objet PSO.

Remarque : L'interface de centre d'administration Active Directory pour la gestion d'objet de paramètres de mot de passe utilise les applets de commande Windows PowerShell indiqués précédemment pour la création et la gestion des objets PSO.

Considérations pour configurer les Objets de paramètres de mot de passe

Il est possible de lier plusieurs objets PSO à un utilisateur ou à un groupe de sécurité. Vous pouvez faire cela si un utilisateur est membre de plusieurs groupes de sécurité (associés ou non à un objet PSO) ou que vous attribuez plusieurs objets PSO directement à un objet utilisateur. Dans ces cas, il est important de comprendre que vous ne pouvez appliquer qu'un seul objet PSO comme stratégie de mot de passe efficace.

Si vous attribuez plusieurs objets PSO à un utilisateur ou à un groupe, l'attribut **msDS-PasswordSettingsPrecedence** aide à déterminer l'objet PSO en résultant. Un objet PSO ayant une valeur inférieure a la priorité sur un objet des paramètres PSO ayant une valeur supérieure.

Le processus suivant décrit comment Active Directory DS détermine l'objet PSO résultant si vous liez plusieurs objets PSO à un utilisateur ou à un groupe :

1. Tout objet PSO que vous liez directement à un objet utilisateur est l'objet PSO résultant. Si vous liez plusieurs objets PSO directement à l'objet utilisateur, l'objet PSO ayant la valeur **demsDS-PasswordSettingsPrecedence** la plus basse est l'objet PSO résultant. Si deux objets PSO ont la même priorité, celui des deux qui a l'attribut **objectGUID** le plus petit mathématiquement est l'objet **PSO** résultant.
2. Si vous ne liez aucun objet PSO directement à l'objet utilisateur, AD DS compare les objets PSO pour tous les groupes de sécurité globale qui contiennent l'objet utilisateur. L'objet PSO ayant la valeur **msDS-PasswordSettings** la plus basse

   La valeur **Priorité** est l'objet PSO résultant. Si vous appliquez plusieurs objets PSO au même utilisateur et qu'ils ont la même valeur **msDS-PasswordSettingsPrecedence**, AD DS applique l'objet PSO ayant l'identificateur unique global (GUID) le plus petit mathématiquement.
3. Si vous ne liez aucun objet PSO à l'objet utilisateur, directement ou indirectement (par l'appartenance de groupe), AD DS applique la stratégie de domaine par défaut.

Tous les objets utilisateurs contiennent un nouvel attribut appelé **msDS-ResultantPSO**. Vous pouvez utiliser cet attribut pour aider à déterminer le nom unique de l'objet PSO que AD DS applique à l'objet utilisateur. Si vous ne liez pas d'objet PSO à l'objet utilisateur, cet attribut ne contient aucune valeur et l'objet Stratégie de groupe de stratégie de domaine par défaut contient la stratégie de mot de passe efficace.

Pour afficher l'effet d'une stratégie qu'AD DS applique à un utilisateur, ouvrez Utilisateurs et ordinateurs Active Directory, puis, sur le menu **Affichage**, vérifiez que l'option **Fonctionnalités avancées** est activée. Ouvrez ensuite les propriétés d'un compte d'utilisateur. Vous pouvez afficher l'attribut **msDS-ResultantPSO** sur l'onglet **Éditeur d'attributs**, si l'option **Afficher les attributs construits** a été configurée dans les options **Filtre**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Configuration des comptes de service gérés

La création des comptes d'utilisateurs pour fournir l'authentification aux applications, aux services système et aux processus en arrière plan est une pratique courante dans l'environnement Windows. Historiquement, les comptes ont été créés et souvent nommés pour l'utilisation par un service spécifique. Windows Server 2012 prend en charge les objets comme un compte AD DS appelés comptes de service gérés, qui facilitent la gestion des comptes du service et présentent moins de risque de sécurité pour votre environnement.

Cette leçon vous présentera les comptes de service gérés et la nouvelle fonctionnalité relative à ces comptes sous Windows Server 2012.

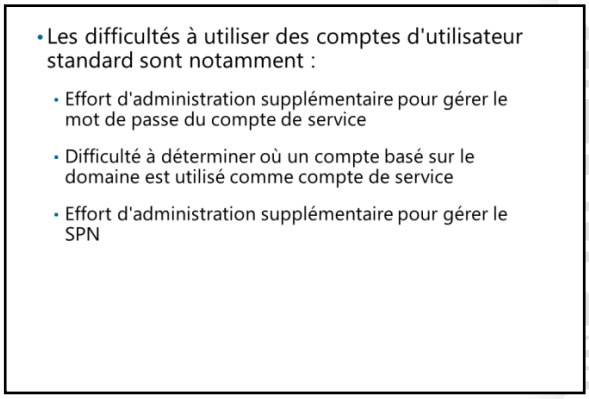
Objectifs de la leçon

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

- identifier les difficultés d'utiliser des comptes d'utilisateur standard pour les services ;
- décrire les comptes de service gérés ;
- expliquer comment configurer des comptes de service gérés ;
- décrire les comptes de service gérés du groupe.

Quelles sont les difficultés à utiliser des comptes d'utilisateur standard pour les services ?

Beaucoup d'applications telles que Microsoft SQL Server® ou Internet Information Services (IIS) contiennent les services qui sont installés sur le serveur qui héberge l'application. Ces services s'exécutent en général au démarrage du serveur ou sont déclenchés par d'autres événements. Les services s'exécutent souvent en arrière-plan et n'ont besoin d'aucune intervention de l'utilisateur.



Pour qu'un service démarre et authentifie, un compte du service est utilisé. Un compte du service peut être un compte qui est local à l'ordinateur, tel que les comptes de service local intégré, de service réseau ou de système local. Vous pouvez également configurer un compte du service pour utiliser un compte basé sur domaine, situé dans AD DS.

Pour aider à centraliser l'administration et à répondre aux impératifs de l'application, beaucoup d'organisations choisissent d'utiliser un compte basé sur le domaine pour exécuter les services d'application. Cela offre un certain avantage par rapport à l'utilisation d'un compte local. Cependant, il y a un certain nombre de difficultés associées, telles que :

- Un effort d'administration supplémentaire peut être nécessaire pour gérer le mot de passe de compte du service de manière sécurisée. Cela comprend des tâches telles que la modification du mot de passe et la résolution des situations qui provoquent un verrouillage de compte. Les comptes du service sont en général configurés également pour avoir des mots de passe qui n'expirent pas, ce qui peut aller à l'encontre les stratégies de sécurité de votre organisation.
- Il peut s'avérer difficile de déterminer où un compte basé sur le domaine est utilisé comme compte de service. Un compte d'utilisateur standard peut être utilisé pour plusieurs services sur divers serveurs dans tout l'environnement. Une tâche simple, telle que la modification du mot de passe, peut provoquer des problèmes d'authentification pour certaines applications. Il est important de savoir où et comment un compte d'utilisateur standard est utilisé quand il est associé avec un service d'application.
- Un effort d'administration supplémentaire peut être nécessaire pour gérer le nom principal de service. L'utilisation d'un compte d'utilisateur standard peut requérir l'administration manuelle du nom principal de service. Si le compte d'ouverture de session du service change, le nom de l'ordinateur est modifié. Ou, si une propriété de nom d'hôte du système DNS est modifiée, les inscriptions du nom principal de service peuvent devoir être manuellement modifiées pour refléter la modification. Un nom principal de service mal configuré pose des problèmes d'authentification avec le service d'application.

Windows Server 2012 prend en charge un objet AD DS utilisé pour faciliter la gestion de compte du service, appelé compte de service géré. Les rubriques suivantes fournissent des informations sur les exigences et l'utilisation des comptes de service gérés sous Windows Server 2012.

Qu'est ce qu'un compte de service géré ?



Un compte de service géré est une classe d'objets AD DS qui active le mot de passe simplifié et la gestion du nom du principal du serveur pour les comptes de service.

Beaucoup d'applications réseau utilisent un compte pour exécuter des services ou pour fournir l'authentification. Par exemple, une application sur un ordinateur local pourrait utiliser les comptes de service local, de service réseau ou du système local. Ces comptes du service peuvent fonctionner très bien. Cependant, ils sont en général partagés entre plusieurs applications et services, ce qui est difficile à gérer pour une application spécifique. En outre, vous ne pouvez pas gérer ces comptes de service local au niveau du domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Alternativement, il est tout à fait courant qu'une application puisse utiliser un compte de domaine standard qui est configuré spécifiquement pour l'application. Cependant, l'inconvénient majeur est que vous devez gérer des mots de passe manuellement, ce qui augmente l'effort d'administration.

Un compte de service géré peut fournir à une application son propre unique compte, tout en éliminant le besoin d'administrer les informations d'identification du compte manuellement par un administrateur.

Comment fonctionne un compte de service géré ?

Les comptes de service gérés sont enregistrés dans AD DS comme des objets **msDS-ManagedServiceAccount**. Cette classe hérite des aspects structurels de la classe Ordinateur (qui hérite de la classe Utilisateur). Cela permet à un compte de service géré d'accomplir des fonctions comme un utilisateur, telles que la fourniture de l'authentification et du contexte de sécurité pour un service en cours d'exécution. Cela permet également à un compte de service géré d'utiliser le même mécanisme de mise à jour de mot de passe utilisé par les objets Ordinateur dans AD DS, un processus qui ne requiert aucune intervention de l'utilisateur.

Les comptes de service gérés offrent les avantages suivants pour simplifier l'administration :

- Gestion automatique des mots de passe. Un compte de service géré gère automatiquement son propre mot de passe, y compris les modifications de mot de passe.
- Gestion simplifiée du nom du principal du serveur. La gestion du nom du principal du serveur peut être effectuée automatiquement si votre domaine est configuré au niveau fonctionnel du domaine de Windows Server 2008 R2 ou versions plus récentes.

Les comptes de service géréss sont enregistrés dans le conteneur **CN=Managed Service Accounts, DC=<domain>, DC=<com**>. Vous pouvez voir cela en activant l'option Fonctionnalité avancée dans le menu Affichage dans Utilisateurs et ordinateurs Active Directory. Ce conteneur est visible par défaut dans le centre d'administration Active Directory.

Configurations requises pour l'usage des comptes de service gérés

Pour utiliser un compte de service géré, le serveur qui exécute le service ou l'application doit exécuter Windows Server 2008 R2 ou Windows Server 2012. Vous devez également vérifier que .NET Framework 3.5.x et le module Active Directory pour Windows PowerShell sont tous les deux installés sur le serveur.

 **Remarque :** Un compte de service géré standard ne peut être ni partagé entre plusieurs ordinateurs, ni utilisé dans les clusters de serveurs où le service est répliqué entre les nœuds.

Pour simplifier et fournir la gestion complètement automatique de mot de passe et de nom principal du serveur, nous recommandons vivement que le domaine AD DS soit au niveau fonctionnel de Windows Server 2008 R2 ou version plus récente. Cependant, si vous avez un contrôleur de domaine exécutant Windows Server 2008 ou Windows Server 2003®, vous pouvez mettre à jour le schéma Active Directory vers Windows Server 2008 R2 pour prendre en charge cette fonctionnalité. Le seul inconvénient est que l'administrateur de domaine doit configurer les données du nom principal du serveur manuellement pour les comptes de service gérés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour mettre à jour le schéma dans Windows Server 2008, Windows Server 2003 ou des environnements de mode mixte, vous devez effectuer les tâches suivantes :

1. Exécutez **adprep/forestprep** au niveau de la forêt et exécutez adprep/domainprep au niveau du domaine.
2. Déployez un contrôleur de domaine exécutant Windows Server 2008 R2, Windows Server 2008 avec le Service passerelle de gestion Active Directory ou Windows Server 2003 avec le Service passerelle de gestion Active Directory.

Remarque : Le Service passerelle de gestion Active Directory permet aux administrateurs avec des contrôleurs de domaine exécutant Windows Server 2003 ou Windows Server 2008 d'utiliser des applets de commande Windows PowerShell pour gérer des comptes de service gérés.

Considérations pour les comptes de service gérés sur des contrôleurs de domaine de Windows Server 2012

Sur Windows 2012, les comptes de service gérés sont créés comme le nouveau type d'objet de compte de groupe de service géré par défaut. Cependant, pour adapter cela, vous devez remplir l'une des conditions pour les comptes de service gérés de groupe avant que vous puissiez créer n'importe quel compte de service géré sur un contrôleur de domaine de Windows 2012.

Sur un contrôleur de domaine de Windows 2012, une clé racine de services de distribution de clé doit être créée pour le domaine avant qu'aucun compte de service géré puisse être créé. Pour créer la clé racine, exécutez l'applet de commande suivant à partir du module Active Directory PowerShell pour Windows PowerShell :

```
Add-KDSRootKey –EffectiveTime ((Get-Date).AddHours(-10))
```

Vous trouverez des informations supplémentaires sur les Comptes de service gérés de groupe (notamment des explications supplémentaires sur l'applet de commande ci-dessus) et la création de clé racine de Services de distribution de clés plus loin dans cette leçon.

Démonstration : Configuration des comptes de service gérés à l'aide de Windows PowerShell

La création et la configuration d'un compte de service géré requièrent l'utilisation de quatre applets de commande du module Active Directory pour Windows PowerShell :

- Add-KDSRootkey crée la clé racine des services de distribution de clés pour prendre en charge les comptes de service gérés de groupe, une configuration requise sur les contrôleurs de domaine de Windows Server 2012 :

  ```
  Add-KDSRootKey –EffectiveTime ((Get-Date).AddHours(-10))
  ```

- New-ADServiceAccount crée le compte de service géré dans AD DS :

  ```
  New-ADServiceAccount –Name <MSA Name> -DNSHostname <DC DNS Name>
  ```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Add-ADComputerServiceAccount associe le compte de service géré avec un compte ordinateur dans le domaine AD DS :

```
Add-ADComputerServiceAccount –identity <Host Computer Name> -ServiceAccount <MSA
Name>
```

- Install-ADServiceAccount installe le compte de service géré sur un ordinateur hôte dans le domaine, et met le compte de service géré à disposition des services sur l'ordinateur hôte :

```
Install-ADServiceAccount –Identity <MSA Name>
```

Dans cette démonstration, vous allez apprendre à :

- créer la clé racine des services de distribution de clés pour le domaine ;

créer et associer un compte de service géré.

Procédure de démonstration

Créer la clé racine des services de distribution de clés pour le domaine.

1. Sur LON-DC1, à partir du Gestionnaire de serveur, ouvrez la console **Module Active Directory pour Windows PowerShell**.
2. Utilisez l'applet de commande Add-KDSRootKey pour créer la clé racine des services de distribution de clés du domaine.

Créer et associer un compte de service géré

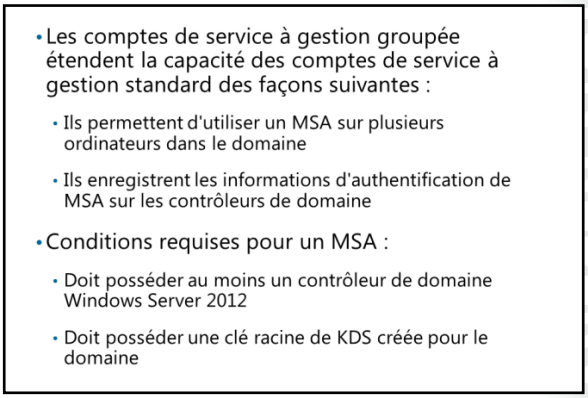
1. Sur LON-DC1, ouvrez la console **Module Active Directory pour Windows PowerShell**.
2. Utilisez l'applet commande **New-ADServiceAccount** pour créer un compte de service géré.
3. Utilisez l'applet de commande **Add-ADComputerServiceAccount** pour associer le compte de service géré avec LON-SVR1.
4. Utilisez l'applet de commande **Get- ADServiceAccount** pour afficher le compte de service géré nouvellement créé et confirmez la bonne configuration.

Installer un compte de service géré

1. Sur LON-SVR1, ouvrez la console **Module Active Directory pour Windows PowerShell**.
2. Utilisez l'applet de commande **Install-ADServiceAccount** pour installer le Compte de service géré sur LON-SVR1.
3. Ouvrez **Gestionnaire de serveur**, et démarrez **Console de services**.
4. Ouvrez les pages **Propriétés** pour le service **Identité de l'application**, puis sélectionnez l'onglet **Connexion**.
5. Configurez le service **Identité de l'application** pour utiliser **ADATUM\SampleApp_SVR1$**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les comptes de service gérés du groupe ?



Les comptes de service géré de groupe vous permettent d'étendre les fonctions des comptes de service géré standards à plus d'un seul serveur dans votre domaine. Dans les scénarios de batterie de serveurs tels que des groupes ou des Serveurs IIS de (NLB) d'équilibrage de la charge réseau, il y a souvent un besoin de diriger des services de système ou d'application sous le même compte du service. Les comptes de service géré standards ne peuvent pas fournir la fonctionnalité de compte de service géré aux services qui s'exécutent sur plus d'un serveur. À l'aide des comptes de service géré de groupe, vous pouvez configurer plusieurs serveurs pour utiliser le même compte de service géré, tout en gardant les avantages des comptes de service géré, comme la maintenance automatique de mot de passe et la gestion simplifiée du nom principal de service.

Configurations requises pour les comptes de service géré de groupe

Pour prendre en charge la fonctionnalité Compte de service géré de groupe, votre environnement doit répondre aux exigences suivantes :

- Au moins un contrôleur de domaine doit exécuter Windows Server 2012 pour stocker les informations de mot de passe géré.
- Une clé racine de services KDS doit être créée sur un contrôleur de domaine dans le domaine.

  Pour créer la clé racine de services KDS, exécutez la commande suivante à partir du module Active Directory pour Windows PowerShell sur un contrôleur de domaine de Windows Server 2012 :

```
Add-KdsRootKey –EffectiveImmediately
```

Remarque : Le commutateur **– EffectiveImmediately** utilise le temps actuel pour établir l'horodatage qui marque la clé comme valide. Cependant, en utilisant **– EffectiveImmediately**, le temps effectif réel est défini à 10 heures plus tard que le temps actuel. Cette différence de 10 heures permet à la réplication des services de domaine Active Directory de répliquer les modifications à d'autres contrôleurs de domaine dans le domaine. À des fins de test, il est possible d'ignorer cette fonctionnalité en définissant le paramètre **– EffectiveTime** à 10 heures avant l'heure actuelle :

Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comprendre la fonctionnalité de compte de service géré de groupe

Les comptes de service géré de groupe activent la fonctionnalité de compte de service géré à travers plusieurs serveurs en déléguant la gestion des informations de mot de passe du compte de service géré aux contrôleurs de domaine de Windows Server 2012. Ce faisant, la gestion des mots de passe ne dépend plus des relations entre un serveur unique et AD DS, mais elle est plutôt contrôlée entièrement par AD DS.

L'objet compte de groupe de service géré contient une liste d'entités de sécurité (des ordinateurs ou des groupes AD DS) qui sont autorisés à récupérer les informations de mot de passe du compte de groupe de service géré depuis AD DS, puis utilisent le compte de service géré de groupe pour l'authentification des services.

Les comptes de service géré de groupe sont créés à l'aide des mêmes applets de commande du module Active Directory pour Windows PowerShell. En fait, les applets de commande utilisés pour la gestion des comptes de service géré créeront des comptes de service géré de groupe, par défaut.

Sur un contrôleur de domaine de Windows Server 2012, créez un nouveau compte de service géré à l'aide de l'applet de commande **New-ADServiceAccount** avec le paramètre **–PrinicipalsAllowedToRetrieveManagedPassword**. Ce paramètre accepte un ou plusieurs comptes d'ordinateur séparés par des virgules ou des groupes AD DS qui sont autorisés à obtenir les informations de mot de passe pour le compte de service géré de groupe qui est enregistré dans AD DS sur des contrôleurs de domaine de Windows Server 2012.

Par exemple, l'applet de commande suivant créera un nouveau compte de service géré de groupe appelé SQLFarm, et permet aux hôtes LON-SQL1, LON-SQL2, et LON-SQL3 d'utiliser le compte de service géré de groupe :

```
New_ADServiceAccount –Name LondonSQLFarm –PrincipalsAllowedToRetrieveManagedPassword
LON-SQL1, LON-SQL2, LON-SQL3
```

Une fois qu'un ordinateur a été ajouté en utilisant **-PrincipalsAllowedToRetrieveManagedPassword**, le compte du service Compte de service géré de groupe est disponible pour être attribué aux services à l'aide du même processus d'attribution en tant que Comptes de service géré standard.

Utilisation des groupes AD DS pour gérer des batteries de serveurs de compte de service géré de groupe

Les groupes de sécurité AD DS peuvent être utilisés pour identifier des comptes de service géré de groupe. Quand vous utilisez un groupe AD DS pour le paramètre **PrincipalsAllowedToRetriveManagedPassword**, tous les ordinateurs qui sont membres de ce groupe seront autorisés à récupérer le mot de passe et à utiliser la fonctionnalité de groupe de compte de service géré. Lors de l'utilisation d'un groupe AD DS comme principal autorisé à récupérer un mot de passe géré, tous les comptes qui sont membres du groupe auront également la même fonction.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Gestion des comptes d'utilisateurs et de service

Scénario

A. Datum est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à London pour assister le bureau de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client de Windows Server 2012, et doit implémenter des modifications de la façon dont les comptes d'utilisateurs sont gérés dans l'environnement.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- configurer les paramètres de stratégie de mot de passe et de verrouillage de compte ;
- créer et associer un compte de service géré.

Configuration de l'atelier pratique

Durée approximative : Durée approximative : 45 minutes

Ordinateur virtuel	20411B-LON-DC1
Nom d'utilisateur	**Administrator**
Mot de passe	**Pa$$w0rd**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet **Actions**, cliquez sur **Accueil**.
3. Dans le volet **Actions**, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Ouvrez une session en utilisant les informations d'authentification suivantes :
    a. Nom d'utilisateur : **ADATUM\Administrateur**
    b. Mot de passe : **Pa$$w0rd**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configuration des paramètres de stratégie de mot de passe et de verrouillage de compte

Scénario

A. Datum a récemment complété un examen de la sécurité des stratégies mots de passe et de verrouillage de compte. Vous devez implémenter les recommandations contenues dans le rapport pour contrôler la complexité et la longueur des mots de passe. Vous devez également configurer les paramètres appropriés de verrouillage de compte. Une partie de votre configuration de stratégie de mot de passe comprendra une stratégie de mot de passe spécifique à attribuer au groupe de sécurité des gestionnaires. Ce groupe a besoin d'une stratégie de mot de passe différente de celle qui a été appliquée au niveau du domaine.

Le rapport a recommandé que les paramètres suivants de mot de passe devraient être appliqués à tous les comptes dans le domaine :

- Historique des mots de passe : **20 mots de passe**
- Durée de vie maximale du mot de passe : **45 jours**
- Durée de vie minimale du mot de passe : **1 jour**
- Longueur du mot de passe : **10 caractères**
- Complexité activée : **Oui**
- Durée de verrouillage des comptes : **30 minutes**
- Seuil de verrouillage du compte : **5 tentatives**
- Réinitialiser le compteur de verrouillages du compte après : **15 minutes**

Le rapport a également recommandé qu'une stratégie distincte soit appliquée aux utilisateurs du groupe de gestionnaires, en raison des privilèges élevés attribués à ces comptes d'utilisateurs. La stratégie appliquée aux groupes de gestionnaires devrait contenir les paramètres suivants :

- Historique des mots de passe : **20 mots de passe**
- Durée de vie maximale du mot de passe **: 20 jours**
- Durée de vie minimale du mot de passe : **1 jour**
- Longueur du mot de passe : **15 caractères**
- Complexité activée : Oui
- Durée de verrouillage des comptes : 0 minute (un administrateur devra déverrouiller le compte)
- Seuil de verrouillage du compte : **3 tentatives**
- Réinitialiser le compteur de verrouillages du compte après **: 30 minutes**

Les tâches principales de cet exercice sont les suivantes :

1. Configurez une stratégie de mot de passe basée sur le domaine
2. Configurez une stratégie de verrouillage du compte
3. Configurez et appliquez une stratégie de mot de passe affinée

▶ Tâche 1 : Configurez une stratégie de mot de passe basée sur le domaine

1. Sur LON-DC1, ouvrez la console **Gestion des stratégies de groupe**.
2. Modifiez la stratégie de domaine par défaut et configurez les paramètres suivants de stratégie de mot de passe du compte :
   - Historique des mots de passe : **20 mots de passe**
   - Durée de vie maximale du mot de passe : **45 jours**
   - Durée de vie minimale du mot de passe : **1 jour**
   - Longueur du mot de passe : **10 caractères**
   - Complexité activée : Oui

▶ Tâche 2 : Configurez une stratégie de verrouillage du compte

1. Dans l'éditeur de gestion des stratégies de groupe, configurez les paramètres suivants de stratégie de verrouillage de compte pour la stratégie de domaine par défaut :
   - Durée de verrouillage des comptes : **30 minutes**
   - Seuil de verrouillage du compte : **5 tentatives**
   - Réinitialiser le compteur de verrouillages du compte après : **15 minutes**
2. Fermez l'Éditeur de gestion des stratégies de groupe.
3. Fermez Gestion de stratégies de groupe.

▶ Tâche 3 : Configurez et appliquez une stratégie de mot de passe affinée

1. Sur LON-DC1, ouvrez la console **Centre d'administration Active Directory**.
2. Modifiez l'étendue de groupe pour le groupe **Managers** à **Global**.

 **Remarque :** Vérifiez que vous ouvrez la page Propriétés du groupe Managers et non l'unité d'organisation Managers.

3. Dans le centre d'administration Active Directory, configurez une stratégie de mot de passe affinée pour le groupe **ADATUM\Managers** avec les paramètres suivants :
   - Nom : **ManagersPSO**
   - Ordre de priorité : **10**
   - Longueur du mot de passe : **15 caractères**
   - Historique des mots de passe : **20 mots de passe**
   - Complexité activée : Oui
   - Durée de vie minimale du mot de passe : **1 jour**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Durée de vie maximale du mot de passe : **30 jours**
- Nombre de tentatives de connexion infructueuses autorisées : **3 tentatives**
- Réinitialiser le compteur de tentatives de connexion échouées après : **30 minutes**
- Jusqu'à ce qu'un administrateur déverrouille manuellement le compte : activée

4. Fermez le Centre d'administration Active Directory.

Résultats : Après avoir complété cet exercice, vous aurez configuré des paramètres de stratégie de mot de passe et de verrouillage de compte.

Exercice 2 : Création et association d'un compte de service géré

Scénario

Vous devez configurer un compte de service géré pour prendre en charge une nouvelle application Web qui est déployée au service Web DefaultAppPool sur LON-DC1. L'utilisation d'un compte de service géré aidera à gérer les exigences de sécurité du mot de passe pour le compte.

Les principales tâches de cet exercice sont les suivantes :

1. Créer et associer un compte de service géré.
2. installer un compte de service géré sur LON-DC1.
3. Pour préparer le module suivant

▶ Tâche 1 : Créer et associer un compte de service géré

1. Sur LON-DC1, ouvrez la console **Module Active Directory pour Windows PowerShell**.
2. Créez la clé racine des services de distribution de clés en utilisant l'applet de commande **Add-KdsRootKey** . Configurez l'heure effective à moins 10 heures, ainsi la clé sera valide immédiatement.
3. Créez le nouveau compte de service nommé Webservice pour l'hôte LON-DC1.
4. Associez le compte géré Webservice avec LON-DC1.
5. Vérifiez que le compte de service géré de groupe a été créé à l'aide de l'applet de commande **Get-ADServiceAccount**.

▶ Tâche 2 : Installer un compte de service géré sur LON-DC1 .

1. Sur LON-DC1, installez le compte du service Webservice.
2. Depuis le menu Outils du Gestionnaire de serveur, ouvrez le Gestionnaire des services Internet (IIS).
3. Configurez DefaultAppPool pour utiliser le compte Webservice$ comme identité.
4. Arrêtez et démarrez le pool d'applications.

▶ Pour préparer le module suivant

- Une fois l'atelier terminé, rétablissez l'état initial des ordinateurs virtuels.

Résultats : Après avoir complété cet exercice, vous aurez créé et associé un compte de service géré.

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
Les comptes d'utilisateurs contenus dans un fichier .csv ne s'importent pas en utilisant l'outil Échange de données de valeurs séparées par des virgules.	
Les paramètres de mot de passe de l'utilisateur ne s'appliquent pas comme prévu.	
L'applet de commande **New-ADServiceAccount** échoue avec les messages relatifs aux clés.	

Outils

Outil	À quoi sert-il ?	Emplacement
Outil d'échange de données de valeurs séparées par des virgules	Importation et exportation des utilisateurs à l'aide des fichiers .csv	Invite de commandes : csvde.exe
LDIFDE	Importation, exportation et modification des utilisateurs à l'aide des fichiers .ldf	Invite de commandes : ldifde.exe
Stratégie de sécurité locale	Configuration des paramètres de stratégie de sécurité locale	Secpol.msc
Console de gestion des stratégies de groupe	Configuration des paramètres de stratégie de compte de stratégie de groupe de domaine	Gestionnaire de serveur – Outils
Centre d'administration Active Directory	Création et gestion des objets PSO	Gestionnaire de serveur – Outils
Module Active Directory pour Windows PowerShell	Création et gestion des Comptes de service géréss	Gestionnaire de serveur - Outils

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 5

Implémentation d'une infrastructure de stratégie de groupe

Table des matières :

Vue d'ensemble du module **5-1**

Leçon 1 : Présentation de la stratégie de groupe **5-2**

Leçon 2 : Implémentation et administration des objets de stratégie de groupe **5-12**

Leçon 3 : Étendue de la stratégie de groupe et traitement de la stratégie de groupe **5-20**

Leçon 4 : Dépanner l'application des objets de stratégie de groupe **5-39**

Atelier pratique : Implémentation d'une infrastructure de stratégie de groupe **5-46**

Contrôle des acquis et éléments à retenir **5-53**

Vue d'ensemble du module

La stratégie de groupe fournit une infrastructure dans laquelle vous pouvez définir des paramètres de manière centralisée et les déployer aux utilisateurs et aux ordinateurs de votre entreprise. Dans un environnement géré par une infrastructure bien implémentée de stratégie de groupe, il y a très peu de configuration par un administrateur touchant directement l'ordinateur d'un utilisateur. Vous pouvez définir, appliquer et mettre à jour toute la configuration à l'aide des paramètres des objets de stratégie de groupe (GPO) ou du filtrage d'objets de stratégie de groupe. À l'aide des paramètres de l'objet de stratégie de groupe, vous pouvez affecter un site ou un domaine entier au sein d'une entreprise ou focaliser sur une seule unité d'organisation (OU). Ce module détaillera ce qu'est la stratégie de groupe, comment elle fonctionne et comment l'implémenter mieux dans votre organisation.

Objectifs

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

- Décrire les composants et les technologies qui comportent la structure de stratégie de groupe.
- Configurer et comprendre divers types de paramètre de stratégie.
- Limiter en étendue les objets de stratégie de groupe à l'aide des liens, des groupes de sécurité, des filtres WMI (Windows® Management Instrumentation), du traitement par boucle de rappel et du ciblage de préférence.
- Décrire comment les objets de stratégie de groupe sont traités.
- Localiser les journaux des événements qui contiennent des événements liés à la stratégie de groupe et dépanner l'application de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Présentation de la stratégie de groupe

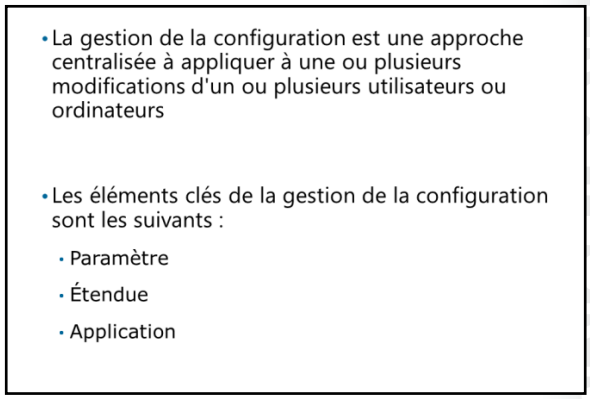
Une infrastructure de stratégie de groupe comporte des composants d'interaction, et vous devez comprendre ce que chaque composant fait, comment ces composants fonctionnent ensemble et comment vous pouvez les assembler dans différentes configurations. Cette leçon dresse un panorama complet des composants, des procédures et des fonctions de stratégie de groupe.

Objectifs de la leçon

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

- Identifier les besoins de l'entreprise auxquels peut répondre la gestion de la configuration.
- Décrire les composants principaux et la terminologie de la stratégie de groupe.
- Expliquer les avantages d'implémenter des objets de stratégie de groupe.
- Décrire les objets de stratégie de groupe.
- Expliquer la fonction et le comportement des composants d'objet de stratégie de groupe côté client.
- Expliquer l'actualisation des objets de stratégie de groupe.
- Créer et configurer des objets de stratégie de groupe.

Qu'est-ce que la gestion de la configuration ?



Si vous avez uniquement un ordinateur dans votre environnement, à domicile, par exemple, et que vous devez modifier l'arrière-plan du bureau, vous pouvez le faire de plusieurs façons différentes. La plupart des personnes ouvriraient probablement **Apparence et personnalisation** à partir de **Panneau de configuration**, et font la modification à l'aide de l'interface Windows. Bien que cela fonctionne bien pour un seul ordinateur, cela peut être pénible si vous souhaitez faire cette modification sur plusieurs ordinateurs. L'implémentation de n'importe quelle modification et le maintien d'un environnement cohérent est plus difficile avec plusieurs ordinateurs.

La gestion de la configuration est une approche centralisée à appliquer à une ou plusieurs modifications d'un ou plusieurs utilisateurs ou ordinateurs. Les éléments clés de la gestion de la configuration sont les suivants :

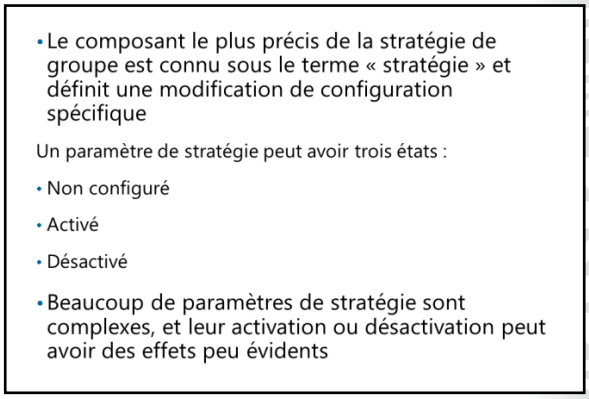
- Paramètre. Un paramètre est également appelé une définition centralisée d'une modification. Le paramètre amène un utilisateur ou un ordinateur à un état désiré de configuration.
- Étendue. L'étendue la modification est la capacité de modifier les ordinateurs des utilisateurs.
- Application. L'application est un mécanisme ou processus qui assure que le paramètre est appliqué aux utilisateurs et aux ordinateurs au sein de l'étendue.

La stratégie de groupe est une structure au sein de Windows, avec des composants qui résident dans les services de domaine Active Directory® (AD DS), sur des contrôleurs de domaine, et sur chaque serveur et client Windows, qui vous permet de gérer la configuration dans un domaine AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble des stratégies de groupe

Le composant le plus granulaire de la stratégie de groupe est un paramètre de stratégie individuel, également appelé une stratégie qui définit une modification de configuration spécifique à appliquer, comme un paramètre de stratégie qui empêche un utilisateur d'accéder aux outils de modification de registre. Si vous définissez ce paramètre de stratégie, puis vous l'appliquez à l'utilisateur, ce dernier ne pourra pas exécuter des outils tels que Regedit.exe.



Il est important de savoir que certains paramètres affectent un utilisateur et sont appelés paramètres de configuration utilisateur (ou stratégies d'utilisateur), et d'autres affectent l'ordinateur et sont appelés paramètres de configuration de l'ordinateur (ou stratégies d'ordinateur).

La stratégie de groupe gère divers paramètres de stratégie, et la structure de la stratégie de groupe est extensible. En fin de compte, vous pouvez gérer n'importe quel paramètre configurable avec la stratégie de groupe.

Dans l'éditeur de gestion des stratégies de groupe, vous pouvez définir un paramètre de stratégie en double-cliquant dessus. La boîte de dialogue **Propriétés** du paramètre de stratégie s'affiche. Un paramètre de stratégie peut avoir trois états : **Non configuré**, **Activé** et **Désactivé**.

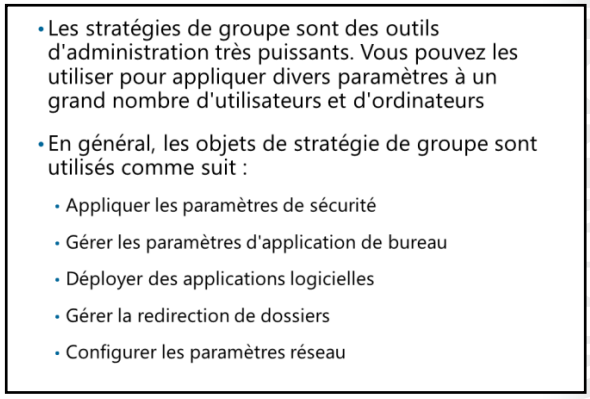
Dans un nouvel objet de stratégie de groupe, chaque paramètre de stratégie est par défaut **Non configuré**. Cela signifie que l'objet de stratégie de groupe ne peut pas modifier la configuration existante de ce paramètre particulier pour un utilisateur ou un ordinateur. Si vous activez ou désactivez un paramètre de stratégie, cela modifie la configuration des utilisateurs et des ordinateurs auxquels l'objet de stratégie de groupe est appliqué. Quand vous remettez un paramètre à son état **Non configuré**, vous le remettez à sa valeur par défaut.

L'effet de la modification dépend du paramètre de stratégie. Par exemple, si vous activez le paramètre de stratégie **Empêche l'accès aux outils de modifications du Registre**, les utilisateurs ne peuvent pas lancer l'éditeur du registre Regedit.exe. Si vous désactivez le paramètre de stratégie, vérifiez que les utilisateurs peuvent lancer l'éditeur du registre. Remarquez le double négatif dans ce paramètre de stratégie : vous désactivez une stratégie qui empêche une action, vous permettez ainsi cette action.

Certains paramètres de stratégie regroupent plusieurs configurations en une seule stratégie et celles-ci pourraient requérir des paramètres supplémentaires.

Remarque : Beaucoup de paramètres de stratégie sont complexes, et leur activation ou désactivation peut avoir des effets peu évidents. En outre, certains paramètres de stratégie affectent uniquement certaines versions du système d'exploitation Windows. Veillez à examiner le texte explicatif d'un paramètre de stratégie dans le volet d'informations de l'éditeur de gestion des stratégies de groupe ou sur l'onglet **Expliquer** dans la boîte de dialogue **Propriétés** du paramètre de stratégie. En outre, testez toujours les effets d'un paramètre de stratégie et ses interactions avec d'autres paramètres de stratégie avant de déployer une modification de votre environnement de production.

Avantages de l'utilisation de la stratégie de groupe



Les stratégies de groupe sont des outils d'administration très puissants. Vous pouvez les utiliser pour appliquer divers paramètres à un grand nombre d'utilisateurs et d'ordinateurs. Puisque vous pouvez les appliquer à divers niveaux, allant du local au domaine, vous pouvez également concentrer ces paramètres de façon très précise.

Essentiellement, vous pouvez utiliser les stratégies de groupe pour configurer des paramètres que vous ne souhaitez pas que les utilisateurs configurent. En outre, vous pouvez utiliser des stratégies de groupe pour standardiser des environnements de bureau sur tous les ordinateurs dans une unité d'organisation ou dans une entreprise entière, afin de fournir une sécurité supplémentaire et certains paramètres système avancés, et à d'autres fins présentées en détails dans les sections suivantes.

Appliquer les paramètres de sécurité

Dans le système d'exploitation Windows Server® 2012, les objets de stratégie de groupe comprennent un grand nombre de paramètres relatifs à la sécurité que vous pouvez appliquer aux utilisateurs et aux ordinateurs. Par exemple, vous pouvez appliquer des paramètres au pare-feu Windows et configurer les paramètres d'audit et autres paramètres de sécurité. Vous pouvez également configurer des ensembles complets des attributions des droits d'utilisateurs.

Gérer les paramètres de bureau et des applications

Vous pouvez utiliser une stratégie de groupe pour fournir un environnement cohérent de bureau et des applications à tous les utilisateurs au sein de votre organisation. À l'aide des objets de stratégie de groupe, vous pouvez configurer chaque paramètre qui affecte l'apparence et la convivialité de l'environnement utilisateur et configurer également les paramètres de certaines applications qui prennent en charge les objets de stratégie de groupe.

Déployer les logiciels

Les stratégies de groupe vous permettent de déployer les logiciels aux utilisateurs et aux ordinateurs. Vous pouvez utiliser la stratégie de groupe pour déployer tous les logiciels qui sont au format .msi. En outre, vous pouvez appliquer l'installation de logiciels automatique ou laisser vos utilisateurs décider s'ils souhaitent que les logiciels soient déployés à leurs machines.

Remarque : Le déploiement de grands packages avec des objets de stratégie de groupe peut ne pas être le moyen le plus efficace pour distribuer une application aux ordinateurs de votre organisation. Dans de nombreuses circonstances, il peut être plus efficace de distribuer les applications dans le cadre de l'image d'ordinateur de bureau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gérer la redirection de dossiers

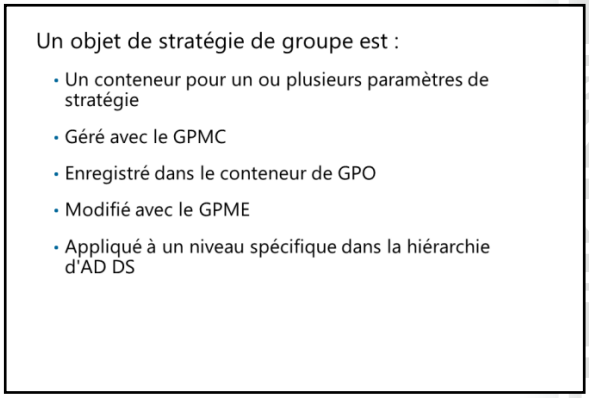
Avec la redirection de dossier, vous pouvez gérer et sauvegarder des données de manière rapide et facile. En redirigeant des dossiers, vous assurez également que les utilisateurs aient accès à leurs données indépendamment de l'ordinateur sur lequel ils se connectent. En outre, vous pouvez centraliser toutes les données d'utilisateurs en un seul endroit sur le serveur réseau, tout en offrant une expérience utilisateur semblable à l'enregistrement de ces dossiers sur leurs ordinateurs. Par exemple, vous pouvez configurer la redirection de dossier pour rediriger les dossiers Documents des utilisateurs vers un dossier partagé sur un serveur réseau.

Configurer les paramètres réseau

L'utilisation de la stratégie de groupe vous permet de configurer divers paramètres réseau sur des ordinateurs client. Par exemple, vous pouvez appliquer des paramètres aux réseaux sans fil pour permettre aux utilisateurs de se connecter uniquement aux identifiants SSID spécifiques, et avec des paramètres prédéfinis d'authentification et de chiffrement. Vous pouvez également déployer les stratégies qui s'appliquent aux paramètres de réseau câblé et configurer également le côté client des services, tels que la protection d'accès réseau (NAP).

Objets de stratégie de groupe

Les paramètres de stratégie sont définis et existent au sein d'un objet de stratégie de groupe. Un objet de stratégie de groupe est un objet qui contient un ou plusieurs paramètres de stratégie qui s'appliquent à un ou plusieurs paramètres de configuration pour un utilisateur ou un ordinateur.



Remarque : Les objets de stratégie de groupe peuvent être gérés dans AD DS à l'aide de la console Gestion des stratégies de groupe (GPMC).

Les objets de stratégie de groupe sont affichés dans un conteneur nommé « Objets de stratégie de groupe ».

Pour créer un nouvel objet de stratégie de groupe, cliquez avec le bouton droit sur le conteneur **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.

Pour modifier les paramètres de configuration dans un objet de stratégie de groupe, cliquez avec le bouton droit sur l'objet de stratégie de groupe, puis cliquez sur **Modifier**. Le composant logiciel enfichable Éditeur de gestion des stratégies de groupe s'ouvre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

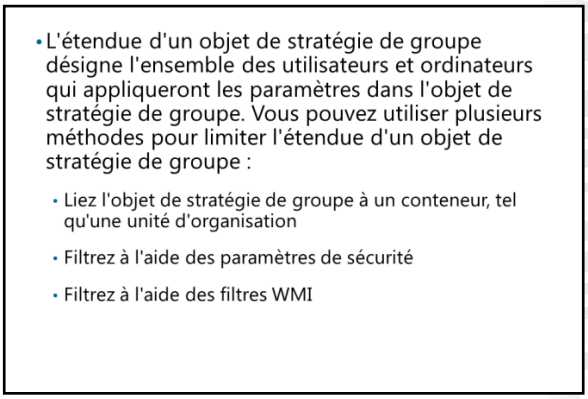
L'éditeur de gestion des stratégies de groupe affiche les milliers de paramètres de stratégie disponibles dans un objet de stratégie de groupe selon une hiérarchie organisée qui commence par la division entre les paramètres de l'ordinateur et les paramètres utilisateurs : le nœud **Configuration ordinateur** et le nœud **Configuration utilisateur**.

Les deux niveaux suivants de la hiérarchie sont des nœuds appelés **Stratégies** et **Préférences**. Vous apprendrez la différence entre ces deux nœuds plus tard dans ce module. En descendant le long de la hiérarchie, vous pouvez voir que l'éditeur de gestion des stratégies de groupe affiche les dossiers, qui sont également appelés des nœuds ou des groupes de paramètre de stratégie. Dans les dossiers, il y a les paramètres de stratégie eux-mêmes.

Remarque : L'objet de stratégie de groupe doit être appliqué à un domaine, à un site, ou à une unité d'organisation dans la hiérarchie AD DS pour les paramètres au sein de l'objet pour entrer en vigueur.

Étendue des objets de stratégie de groupe

La configuration est définie par les paramètres de stratégie dans les objets de stratégie de groupe. Cependant, les modifications de configuration dans un objet de stratégie de groupe n'affectent pas les ordinateurs ou les utilisateurs dans votre organisation jusqu'à ce que vous spécifiiez les ordinateurs ou les utilisateurs auxquels l'objet de stratégie de groupe s'applique. Ce phénomène est appelé étendue de l'objet de stratégie de groupe. L'étendue d'un objet de stratégie de groupe désigne l'ensemble des utilisateurs et ordinateurs qui appliqueront les paramètres dans l'objet de stratégie de groupe.



Vous pouvez utiliser plusieurs méthodes pour gérer l'étendue des objets de stratégie de groupe. La première est la liaison de l'objet de stratégie de groupe. Vous pouvez lier des objets de stratégie de groupe aux sites, aux domaines et aux unités d'organisation dans AD DS. Le site, le domaine ou l'unité d'organisation devient alors l'étendue maximale de l'objet de stratégie de groupe. Tous les ordinateurs et utilisateurs au sein du site, du domaine ou de l'unité d'organisation, y compris ceux au sein des unités d'organisation enfants, seront affectés par les configurations que les paramètres de stratégie dans l'objet de stratégie de groupe spécifient.

Remarque : Vous pouvez lier un objet de stratégie de groupe à plusieurs domaines, unités d'organisation ou sites. La liaison des objets de stratégie de groupe à plusieurs sites peut présenter des problèmes de performances quand la stratégie est appliquée, et vous devez éviter de lier un objet de stratégie de groupe à plusieurs sites. C'est parce que dans un réseau multisite, les objets de stratégie de groupe sont enregistrés dans les contrôleurs de domaine du domaine racine de forêt. La conséquence de cela est que les ordinateurs dans d'autres domaines peuvent devoir parcourir une liaison lente de réseau étendu (WAN) pour obtenir les objets de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez rétrécir davantage l'étendue de l'objet de stratégie de groupe avec l'un des deux types de filtres. Les filtres de sécurité spécifient les groupes de sécurité qui tombent au sein de l'étendue de l'objet de stratégie de groupe, mais auxquels l'objet de stratégie de groupe devrait ou ne devrait pas s'appliquer explicitement. Les filtres WMI spécifient une étendue à l'aide des caractéristiques d'un système, telles que la version du système d'exploitation ou l'espace disque disponible. Utilisez les filtres de sécurité et les filtres WMI pour rétrécir ou spécifier l'étendue dans l'étendue initiale que la liaison de l'objet de stratégie de groupe a créée.

Remarque : Windows Server 2008 comprend un nouveau composant de stratégie de groupe : Les préférences de stratégie de groupe. Les paramètres qui sont configurés par des préférences de stratégie de groupe dans un objet de stratégie de groupe peuvent être filtrés ou ciblés selon plusieurs critères. Les préférences ciblées vous permettent de raffiner davantage l'étendue des préférences dans un objet de stratégie de groupe unique.

Client de stratégie de groupe et extensions côté client

Application de la stratégie de groupe

Il est important de comprendre comment les stratégies de groupe s'appliquent aux ordinateurs client. Le plan ci-dessous détaille le processus :

1. Le client de stratégie de groupe récupère des GPO
2. Le client télécharge et met les GPO en cache
3. Les CSE traitent les paramètres

- Des paramètres de stratégie dans le nœud de configuration de l'ordinateur sont appliqués au démarrage du système puis toutes les 90 à 120 minutes
- Des paramètres de stratégie de configuration utilisateur sont appliqués à l'ouverture de session puis toutes les 90 à 120 minutes

1. Quand l'actualisation de la stratégie de groupe commence, un service qui s'exécute sur tous les ordinateurs Windows, appelé le client de stratégie de groupe dans Windows Vista®, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, et Windows Server 2012, détermine les GPO qui s'appliquent à l'ordinateur ou à l'utilisateur.
2. Ce service télécharge tous les objets de stratégie de groupe qui ne sont pas déjà mis en cache.
3. Les extensions côté client (CSE) interprètent les paramètres dans un objet de stratégie de groupe et effectuent les modifications appropriées à l'ordinateur local ou à l'utilisateur qui a actuellement ouvert une session. Il y a des extensions CSE pour chaque catégorie majeure de paramètre de stratégie. Par exemple, il y a une extension CSE de sécurité qui applique des modifications de sécurité, une extension CSE qui exécute les scripts de démarrage et d'ouverture de session, une extension CSE qui installe les logiciels, et une extension CSE qui effectue des modifications aux clés et aux valeurs de Registre. Chaque version de Windows a ajouté des extensions CSE pour étendre l'étendue fonctionnelle de la stratégie de groupe, et il y a plusieurs dizaines d'extensions CSE dans Windows.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'un des concepts les plus importants dont il faut se souvenir au sujet de la stratégie de groupe est qu'elle est très pilotée par le client. Le client de stratégie de groupe extrait les objets de stratégie de groupe du domaine, déclenchant ainsi les extensions CSE qui doivent s'appliquer les paramètres localement. La stratégie de groupe n'est pas une technologie Push.

En fait, vous pouvez configurer le comportement des extensions CSE à l'aide de la stratégie de groupe. La plupart des extensions CSE appliqueront des paramètres dans un objet de stratégie de groupe uniquement si cet objet de stratégie de groupe a changé. Ce comportement améliore le traitement de la stratégie globale, en éliminant les applications redondantes des mêmes paramètres. La plupart des stratégies sont appliquées de telle manière que les utilisateurs standards ne puissent pas modifier le paramètre sur leur ordinateur ; ils seront toujours sujets à la configuration appliquée par la stratégie de groupe. Cependant, les utilisateurs standard peuvent modifier certains paramètres, et beaucoup d'eux peuvent être modifiés si un utilisateur est un administrateur sur ce système. Si les utilisateurs dans votre environnement sont des administrateurs sur leurs ordinateurs, vous devez envisager de configurer les extensions CSE pour réappliquer les paramètres de stratégie, même si l'objet de stratégie de groupe n'a pas changé. De cette façon, si un utilisateur administrateur modifie une configuration de sorte qu'elle ne soit plus conforme avec la stratégie, cette configuration sera réinitialisée à son état conforme à la prochaine actualisation de la stratégie de groupe.

Remarque : Vous pouvez configurer des extensions CSE pour réappliquer des paramètres de stratégie lors de l'actualisation en tâche de fond suivante, même si l'objet de stratégie de groupe n'a pas changé. Vous pouvez faire cette opération en configurant un objet de stratégie de groupe dont l'étendue est appliquée aux ordinateurs, puis en définissant les paramètres dans le nœud Configuration de l'ordinateur\Stratégies\Modèles d'administration\Système**Stratégie de groupe.** Pour chaque extension CSE que vous souhaitez configurer, ouvrez son paramètre de stratégie du traitement de la stratégie, tel que le traitement de la stratégie du Registre pour l'extension CSE du Registre. Cliquez sur **Activé**, et activez la case à cocher **Traiter même si les objets de stratégie de groupe n'ont pas changé**.

L'extension de sécurité CSE gère une exception importante aux paramètres de traitement de la stratégie par défaut. Les paramètres de sécurité sont réappliqués toutes les 16 heures, même si un objet de stratégie de groupe n'a pas changé.

Remarque : Activez le paramètre de stratégie **Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session** pour tous les clients Windows. Sans ce paramètre, les clients Windows XP, Windows Vista, Windows 7 et Windows 8 exécutent, par défaut, uniquement des actualisations en tâche de fond. Cela signifie qu'un client peut démarrer, et un utilisateur pourrait ensuite se connecter sans recevoir les dernières stratégies du domaine. Le paramètre est situé dans Configuration de l'ordinateur\Stratégies\Modèles d'administration\Système\Ouverture de session. Veillez à lire le texte explicatif du paramètre de stratégie.

Actualisation de la stratégie de groupe

Les paramètres de stratégie dans le nœud **Configuration de l'ordinateur** sont appliqués au démarrage du système, puis toutes les 90 à 120 minutes. Les paramètres de stratégie de configuration utilisateur sont appliqués à l'ouverture de session, puis toutes les 90 à 120 minutes. L'application des stratégies est appelée « actualisation de la stratégie de groupe ».

Remarque : Vous pouvez également forcer l'actualisation d'une stratégie à l'aide de la commande **GPUpdate**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Procédure de création d'un objet de stratégie de groupe et configurer ses paramètres

Les paramètres de stratégie de groupe, également appelés « stratégies », sont contenus dans un objet de stratégie de groupe, et vous pouvez les afficher et les modifier à l'aide de l'éditeur de gestion des stratégies de groupe. Cette démonstration traite plus en détail les catégories de paramètres disponibles dans un objet de stratégie de groupe.

Configuration ordinateur et configuration utilisateur

Il y a deux grandes subdivisions des paramètres de la stratégie : les paramètre de l'ordinateur, qui sont contenus dans le nœud **Configuration ordinateur,** et les paramètres utilisateurs, qui sont contenus dans le nœud **Configuration utilisateur** :

- le nœud **Configuration ordinateur** contient les paramètres qui sont appliqués aux ordinateurs, indépendamment de celui qui y ouvre une session. Les paramètres de l'ordinateur sont appliqués lorsque le système d'exploitation démarre, pendant les actualisations en tâche de fond, et ensuite toutes les 90 à 120 minutes.
- Le nœud **Configuration utilisateur** contient les paramètres qui sont appliqués quand un utilisateur ouvre une session dans l'ordinateur, pendant les actualisations en tâche de fond, et ensuite toutes les 90 à 120 minutes.

Dans les nœuds **Configuration ordinateur** et **Configuration utilisateur**, il y a les nœuds **Stratégies** et **Préférences**. Les stratégies sont des paramètres qui sont configurés et se comportent de manière similaire aux paramètres de stratégie dans les systèmes d'exploitation Windows plus anciens. Les préférences ont été présentées dans Windows Server 2008.

Dans les nœuds **Stratégies** de la configuration ordinateur et de la configuration utilisateur, il y a une hiérarchie des dossiers qui contiennent des paramètres de stratégie. Puisqu'il y a des milliers de paramètres, leur examen individuel dépasse le cadre de ce cours. Cependant, il est intéressant de définir les grandes catégories des paramètres dans les dossiers.

Nœud des paramètres du logiciel

Le nœud **Paramètres du logiciel** est le premier nœud. Il contient uniquement l'extension d'installation du logiciel, qui vous aide à spécifier comment les applications sont installées et gérées au sein de votre organisation.

Nœud des paramètres de Windows

Dans chacun des deux nœuds **Configuration ordinateur** et **Configuration utilisateur**, le nœud **Stratégies** contient un nœud **Paramètres Windows**, qui comprend les nœuds **Scripts**, **Paramètres de sécurité**, et **QoS basée sur la stratégie**.

 **Remarque :** Il contient également le dossier de stratégie de résolution de noms, qui contient des paramètres pour configurer Windows 8 DirectAccess, lequel est présenté dans un module ultérieur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Nœud de scripts

L'extension de scripts vous permet de spécifier deux types de scripts : démarrage/arrêt (dans le nœud **Configuration ordinateur**) et ouverture/fermeture de session (dans le nœud **Configuration utilisateur**). Les scripts démarrage/arrêt fonctionnent au démarrage ou à l'arrêt de l'ordinateur. Les scripts ouverture/fermeture de session fonctionnent quand un utilisateur ouvre ou ferme une session. Quand vous attribuez plusieurs scripts ouverture/fermeture de session ou démarrage/arrêt à un utilisateur ou à un ordinateur, l'extension CSE de scripts exécute les scripts de haut en bas. Vous pouvez déterminer l'ordre d'exécution de plusieurs scripts dans la boîte de dialogue **Propriétés**. Lorsqu'un ordinateur est arrêté, l'extension CSE traite d'abord les scripts de fermeture de session, ensuite les scripts d'arrêt. Par défaut, le délai de traitement des scripts est de 10 minutes. Si les scripts de fermeture de session et d'arrêt ont besoin de plus de 10 minutes pour être traités, vous devez régler la valeur du délai avec un paramètre de stratégie. Vous pouvez vous servir de n'importe quel langage de script ActiveX® pour écrire les scripts. Microsoft® Visual Basic® Scripting Edition (VBScript), Microsoft JScript®, Perl et les fichiers de commandes par lot Microsoft MS-DOS® (.bat et .cmd) sont certaines des possibilités. Les scripts d'ouverture de session sur un répertoire réseau partagé dans une autre forêt sont pris en charge pour l'ouverture de session réseau dans les forêts. Windows 7 et Windows 8 prennent également tous deux en charge les scripts Windows PowerShell®.

Nœud des paramètres de sécurité

Le nœud **Paramètres de sécurité** permet à un administrateur de sécurité de configurer la sécurité à l'aide des objets de stratégie de groupe. Cela peut être fait par la suite, ou plutôt, à l'aide d'un modèle de sécurité pour définir la sécurité des systèmes.

Nœud de qualité de service (QoS) basée sur la stratégie

Ce nœud de qualité de service (QoS), appelé nœud **Qualité de service (QoS) basée sur la stratégie**, définit les stratégies qui gèrent le trafic réseau. Par exemple, vous pouvez souhaiter vérifier que les utilisateurs du service financier ont la priorité pour exécuter une application réseau critique au cours de la période de déclaration financière de fin d'année. Le nœud **Qualité de service (QoS) basée sur la stratégie** vous permet de le faire.

Dans le nœud **Configuration utilisateur** uniquement, le dossier des paramètres Windows contient les nœuds supplémentaires **Services d'installation à distance**, **Redirection de dossiers** et **Maintenance Internet Explorer**. Les stratégies de services d'installation à distance (RIS) contrôlent le comportement d'une installation du système d'exploitation distante. La redirection de dossiers vous permet de rediriger les données d'utilisateur et les dossiers de paramètres tels que AppData, Bureau, Documents, Images, Musique, et Favoris de leur emplacement de profil utilisateur par défaut à un autre emplacement sur le réseau, où ils peuvent être gérés de manière centralisée. La maintenance Internet Explorer vous permet d'administrer et de personnaliser Windows Internet Explorer®.

Nœud de modèles d'administration

Dans les nœuds **Configuration ordinateur** et **Configuration utilisateur**, le nœud **Modèles d'administration** contient les paramètres de stratégie de groupe basés sur le registre. Il y a des milliers de tels paramètres disponibles pour configurer l'environnement utilisateur et ordinateur. En tant qu'administrateur, vous pouvez passer énormément de temps à manipuler ces paramètres. Pour vous aider, une description de chaque paramètre de stratégie est disponible dans deux emplacements :

- Dans l'onglet **Expliquer** dans la boîte de dialogue **Propriétés** du paramètre. En outre, l'onglet **Paramètres** de la boîte de dialogue **Propriétés** de chaque paramètre répertorie également le système d'exploitation ou le logiciel requis pour le paramètre.
- Dans l'onglet **Étendu** de l'Éditeur de gestion des stratégies de groupe. L'onglet **Étendu** apparaît sur la partie droite inférieure du volet d'informations, et donne une description de chaque paramètre sélectionné dans une colonne entre l'arborescence de la console et le volet de paramètres. Le système d'exploitation ou le logiciel requis pour chaque paramètre est également répertorié.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Demonstration

Cette démonstration montre comment :

1. ouvrir la console Gestion des stratégies de groupe ;
2. créer un objet de stratégie de groupe appelé « Bureau » dans le conteneur « Stratégie de groupe » ;
3. dans la configuration ordinateur, empêcher le dernier nom de connexion de s'afficher, puis empêcher Windows Installer de s'exécuter ;
4. dans la configuration utilisateur, supprimer le lien Rechercher du menu Accueil, puis masquer l'onglet de paramètres d'affichage.

Procédure de démonstration

Utiliser la console GPMC pour créer un nouvel objet de stratégie de groupe

1. Connectez-vous à LON-DC1 en tant qu'administrateur.
2. Ouvrez la console Gestion des stratégies de groupe.
3. Créez un nouvel objet de stratégie de groupe appelé « Bureau ».

Configurer les paramètres de stratégie de groupe

1. Ouvrez la nouvelle stratégie Bureau pour sa modification.
2. Dans la configuration ordinateur, empêchez le dernier nom de connexion de s'afficher, puis empêchez Windows Installer de s'exécuter.
3. Dans la configuration utilisateur, supprimez le lien Rechercher du menu **Accueil**, puis masquez l'onglet de paramètres d'affichage.
4. Fermez toutes les fenêtres.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Implémentation et administration des objets de stratégie de groupe

Dans cette leçon, vous examinerez des objets de stratégie de groupe plus en détails, et apprendrez comment créer, lier, modifier, gérer et administrer de tels objets et leurs paramètres.

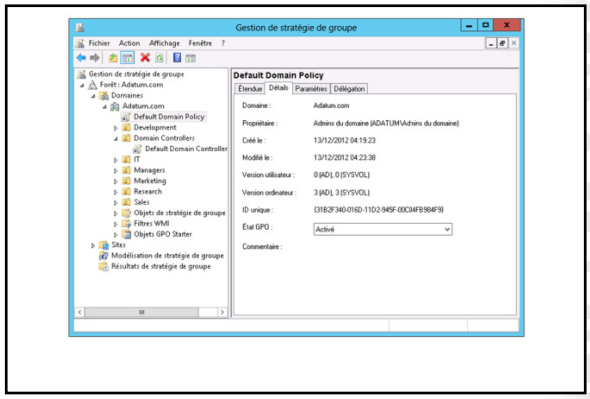
Objectifs de la leçon

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

- Décrire les objets de stratégie de groupe basés sur un domaine.
- Expliquer comment créer, lier, et modifier des objets de stratégie de groupe.
- Expliquer le stockage d'objet de stratégie de groupe.
- décrire les objets de stratégie de groupe Starter.
- Exécuter des tâches courantes de gestion des objets de stratégie de groupe.
- Expliquer comment déléguer l'administration des objets de stratégie de groupe.
- Décrire comment utiliser Windows PowerShell pour gérer des objets de stratégie de groupe.

Objets de stratégie de groupe basés sur un domaine.

Les objets de stratégie de groupe basés sur un domaine sont créés dans AD DS et enregistrés sur des contrôleurs de domaine. Vous pouvez les utiliser pour gérer la configuration de manière centralisée pour les utilisateurs et les ordinateurs du domaine. Le reste de ce cours se rapporte aux objets de stratégie de groupe basés sur un domaine plutôt qu'aux objets de stratégie de groupe locaux, sauf indication contraire.



Quand vous installez AD DS, deux objets de stratégie de groupe par défaut sont créés : Stratégie de contrôleurs de domaine par défaut et stratégie de domaine par défaut.

Stratégie de domaine par défaut

Cet objet de stratégie de groupe est lié au domaine et n'a ni groupe de sécurité, ni filtre WMI. Par conséquent, il affecte tous les utilisateurs et ordinateurs du domaine, y compris les ordinateurs qui sont des contrôleurs de domaine. Cet objet de stratégie de groupe contient des paramètres de stratégie qui spécifient les stratégies de mot de passe, de verrouillage de compte et de protocole Kerberos version 5. Vous ne devez pas ajouter de paramètres de stratégie indépendants à cet objet de stratégie de groupe. Si vous devez configurer d'autres paramètres à appliquer largement à votre domaine, créez des objets de stratégie de groupe supplémentaires qui sont liés au domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Stratégie des contrôleurs de domaine par défaut

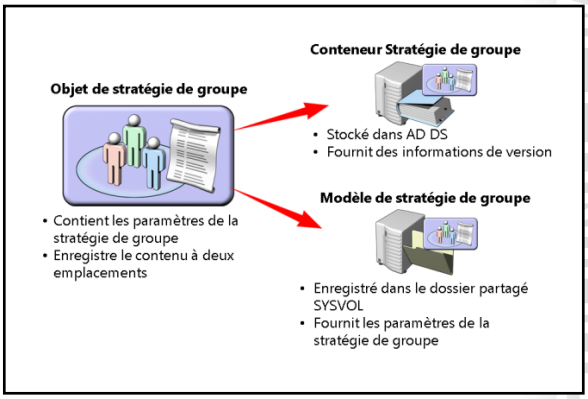
Cet objet de stratégie de groupe est lié à l'unité d'organisation des contrôleurs de domaine. Puisque les comptes d'ordinateur des contrôleurs de domaine sont maintenus exclusivement dans l'unité d'organisation des contrôleurs de domaine, et que d'autres comptes d'ordinateur doivent être maintenus dans d'autres unités d'organisation, cet objet de stratégie de groupe affecte uniquement les contrôleurs de domaine. Vous devez modifier l'objet de stratégie de groupe des contrôleurs de domaine par défaut pour implémenter vos stratégies d'audit et pour attribuer les droits d'utilisateur requis sur les contrôleurs de domaine.

Remarque : Les ordinateurs Windows ont également des objets de stratégie de groupe locaux, qui sont utilisés quand les ordinateurs ne sont pas connectés aux environnements de domaine. Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, et Windows Server 2012 prennent en charge la notion de plusieurs objets de stratégie de groupe locaux. L'objet de stratégie de groupe d'ordinateur local est identique à celui des versions Windows précédentes. Dans le nœud **Configuration ordinateur**, vous pouvez configurer tous les paramètres relatifs à l'ordinateur. Dans le nœud **Configuration utilisateur**, vous pouvez configurer les paramètres que vous souhaitez appliquer à tous les utilisateurs sur l'ordinateur. Les paramètres utilisateur dans l'objet de stratégie de groupe de l'ordinateur local peuvent être modifiés par les paramètres utilisateurs dans deux nouveaux objets de stratégie de groupe locaux : administrateurs et non-administrateurs. Ces deux objets de stratégie de groupe appliquent des paramètres utilisateurs aux utilisateurs connectés selon qu'ils sont membres du groupe d'administrateurs locaux, auquel cas ils utilisent l'objet de stratégie de groupe administrateurs, ou pas membres du groupe d'administrateurs et utilisent, dans ce cas, l'objet de stratégie de groupe non administrateurs. Vous pouvez affiner davantage les paramètres utilisateur avec un objet de stratégie de groupe local qui s'applique à un compte utilisateur spécifique. Les objets de stratégie de groupe locaux spécifiques à l'utilisateur sont associés aux comptes d'utilisateurs locaux et non ceux du domaine.

Il est important de comprendre que le paramètre de l'objet de stratégie de groupe basé sur un domaine est combiné avec ceux appliqués en utilisant les objets de stratégie de groupe locaux, mais comme les objets de stratégie de groupe basés sur un domaine s'appliquent en dernier, ils ont la priorité sur les paramètres de l'objet de stratégie de groupe local.

Stockage de l'objet de stratégie de groupe

Les paramètres de stratégie de groupe sont présentés sous forme d'objets de stratégie de groupe dans les outils d'interface utilisateur AD DS, mais un objet de stratégie de groupe représente en réalité deux composants : un conteneur de stratégie de groupe et un modèle de stratégie de groupe.



Le conteneur de stratégie de groupe est un objet AD DS enregistré dans le conteneur d'objets de stratégie de groupe au sein du contexte d'attribution de noms de domaine du répertoire. Comme tous les objets AD DS, chaque conteneur de stratégie de groupe comprend un attribut d'identificateur global universel (GUID) qui identifie de façon distincte l'objet dans AD DS. Le conteneur de stratégie de groupe définit des attributs de base de l'objet de stratégie de groupe, mais il ne contient aucun de ces paramètres. Les paramètres sont contenus dans le modèle de stratégie de groupe, une collection de fichiers enregistrés dans le volume système (SYSVOL) de chaque contrôleur de domaine dans le chemin d'accès **%SystemRoot%\SYSVOL\Domaine\Stratégies\GPOGUID**, où GPOGUID est l'identificateur GUID du conteneur de stratégie de groupe. Quand vous apportez des modifications aux paramètres d'un objet de stratégie de groupe, celles-ci sont enregistrées dans le modèle de stratégie de groupe du serveur où l'objet de stratégie de groupe a été ouvert.

Par défaut, lors de l'actualisation de la stratégie de groupe, les extensions CSE appliquent des paramètres dans un objet de stratégie de groupe uniquement si celui-ci a été mis à jour.

Le client de stratégie de groupe peut identifier un objet de stratégie de groupe mis à jour par son numéro de version. Chaque objet de stratégie de groupe a un numéro de version qui est incrémenté chaque fois qu'une modification est faite. Le numéro de version est enregistré comme attribut de conteneur de stratégie de groupe et dans un fichier texte, Group Policy template.ini, dans le dossier Modèle de stratégie de groupe. Le client de stratégie de groupe connaît le numéro de version de chaque objet de stratégie de groupe qu'il a précédemment appliqué. Si, pendant l'actualisation de la stratégie de groupe, le client de stratégie de groupe découvre que le numéro de version du conteneur de la stratégie de groupe a été modifié, les extensions CSE seront informées que l'objet de la stratégie de groupe est mis à jour.

Réplication GPO

Le conteneur de la stratégie de groupe et le modèle de la stratégie de groupe sont tous les deux répliqués entre tous les contrôleurs de domaine dans AD DS. Cependant, différents mécanismes de réplication sont utilisés pour ces deux éléments.

Le conteneur de la stratégie de groupe dans AD DS est répliqué par l'agent de duplication d'annuaire (DRA). L'agent de récupération de données utilise une topologie générée par le vérificateur de cohérence des connaissances (KCC), que vous pouvez définir ou raffiner manuellement. Le résultat est que le conteneur de la stratégie de groupe est répliqué en quelconques secondes à tous les contrôleurs de domaine dans un site et est répliqué entre les sites selon votre configuration de réplication intersite.

Le modèle de la stratégie de groupe dans le volume SYSVOL est répliqué à l'aide de l'une des deux technologies suivantes : Le service de réplication de fichiers (FRS) est utilisé pour répliquer le volume SYSVOL dans les domaines exécutant Windows Server 2008, Windows Server 2008 R2, Windows Server 2003, et Windows 2000. Si tous les contrôleurs de domaine exécutent Windows Server 2008 ou une version ultérieure, vous pouvez configurer la réplication du volume SYSVOL à l'aide de la réplication DFS, qui est un mécanisme beaucoup plus efficace et plus fiable.

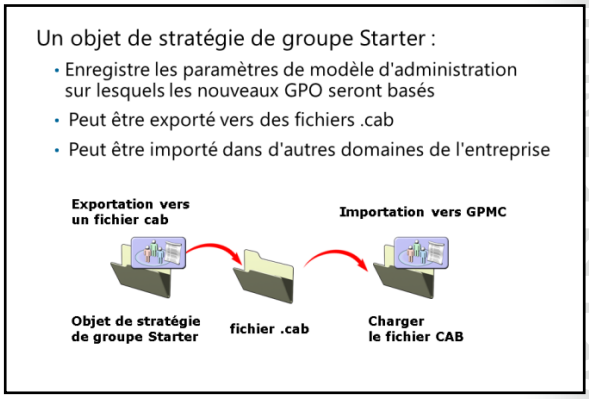
Puisque le conteneur de la stratégie de groupe et le modèle de la stratégie de groupe sont répliqués séparément, il est possible qu'ils deviennent hors de synchronisation pendant une courte période.

En général, quand cela se produit, le conteneur de la stratégie de groupe répliquera d'abord sur un contrôleur de domaine. Les systèmes qui ont obtenu leur liste triée d'objets de stratégie de groupe à partir de ce contrôleur de domaine identifieront le nouveau conteneur de stratégie de groupe, tenteront de télécharger le modèle de stratégie de groupe et remarqueront que les numéros de version ne sont pas identiques. Une erreur de traitement de stratégie sera enregistrée dans les journaux des événements. Si l'inverse se produit, et l'objet de stratégie de groupe réplique sur un contrôleur de domaine avant le conteneur de stratégie de groupe, les clients obtenant leur liste triée d'objets de stratégie de groupe de ce contrôleur de domaine ne seront pas avisés du nouvel objet de stratégie de groupe jusqu'à ce que le conteneur de stratégie de groupe ait été répliqué.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Objets de stratégie de groupe Starter

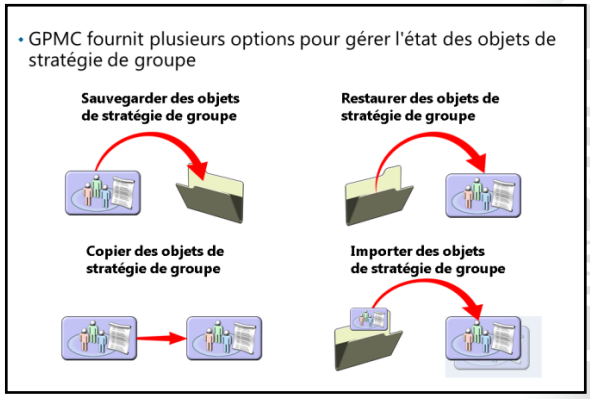


Un objet de stratégie de groupe Starter est utilisé comme modèle, à partir duquel d'autres objets de stratégie de groupe sont créés dans la console GPMC. Les objets de stratégie de groupe Starter ne peuvent contenir que des paramètres de modèle d'administration. Vous pouvez utiliser un objet de stratégie de groupe Starter pour fournir un point de départ pour de nouveaux objets de stratégie de groupe créés dans votre domaine. L'objet de stratégie de groupe Starter peut déjà contenir des paramètres spécifiques qui sont des bonnes pratiques recommandées pour votre environnement. Les objets de stratégie de groupe Starter peuvent être exportés vers et importés depuis des fichiers .cab pour rendre la distribution vers d'autres environnements simple et efficace.

La console GPMC enregistre les objets de stratégie de groupe Starter dans un dossier nommé « StarterGPOs » situé dans le volume SYSVOL.

Les objets de stratégie de groupe Starter préconfigurés de Microsoft sont disponibles pour des systèmes d'exploitation client Windows. Ces objets de stratégie de groupe Starter contiennent les paramètres du modèle d'administration, qui reflètent les bonnes pratiques Microsoft recommandées pour la configuration de l'environnement client.

Tâches courantes de gestion des objets de stratégie de groupe



Comme les données critiques et les ressources AD DS connexes, vous devez sauvegarder les objets de stratégie de groupe pour protéger l'intégrité d'AD DS et des objets de stratégie de groupe. La console GPMC offre non seulement les options de base de sauvegarde et de restauration, mais également le contrôle supplémentaire des objets de stratégie de groupe à des fins administratives. Les options de gestion des objets de stratégie de groupe comprennent les suivantes :

Sauvegarde des objets de stratégie de groupe

Vous pouvez sauvegarder des objets de stratégie de groupe individuellement ou collectivement avec la console GPMC. Vous devez indiquer uniquement un emplacement de sauvegarde, qui peut être n'importe quel dossier local ou partagé valide. Vous devez avoir l'autorisation de lecture de l'objet de stratégie de groupe pour le sauvegarder. Chaque fois que vous effectuez une sauvegarde, une nouvelle version de sauvegarde de l'objet de stratégie de groupe est créée, ce qui fournit un enregistrement historique.

Restauration des objets de stratégie de groupe sauvegardés

Vous pouvez restaurer n'importe quelle version d'un objet de stratégie de groupe. Si l'une devient corrompue ou si vous la supprimez, vous pouvez alors restaurer l'une des versions historiques de cet objet de stratégie de groupe. L'interface de restauration vous offre la capacité d'afficher les paramètres enregistrés dans la version sauvegardée avant de la restaurer.

Importation de paramètres des objets de stratégie de groupe à partir d'un objet de stratégie de groupe sauvegardé

Vous pouvez importer les paramètres de stratégie d'un objet de stratégie de groupe dans un autre. L'importation d'un objet de stratégie de groupe vous permet de transférer des paramètres à partir d'un objet de stratégie de groupe sauvegardé vers un objet de stratégie de groupe existant. L'importation d'un objet de stratégie de groupe transfère uniquement les paramètres de l'objet de stratégie de groupe. Le processus d'importation n'importe pas les liaisons de l'objet de stratégie de groupe. Les entités de sécurité définies dans la source peuvent devoir être migrées à la cible.

 **Remarque :** Il n'est pas possible de fusionner les paramètres importés avec les paramètres actuels de l'objet de stratégie de groupe cible. Les paramètres importés remplaceront tous les paramètres existants.

Copie des objets de stratégie de groupe

Vous pouvez copier les objets de stratégie de groupe à l'aide de la console GPMC, dans le même domaine et entre les domaines. Une opération de copie copie un objet de stratégie de groupe dynamique existant dans le domaine de destination souhaité. Un nouvel objet de stratégie de groupe est toujours créé pendant ce processus. Le nouvel objet de stratégie de groupe est nommé « copie d'OldGPOName ». Par exemple, si vous avez copié un objet de stratégie de groupe nommé « Bureau », la nouvelle version sera appelée « Copie de Bureau ». Une fois le fichier copié et collé dans le conteneur des objets de stratégie de groupe, vous pouvez renommer la stratégie. Le domaine de destination peut être n'importe quel domaine approuvé où vous avez les droits de créer de nouveaux objets de stratégie de groupe. Lors de la copie entre domaines, les entités de sécurité définies dans la source peuvent devoir être migrées à la cible.

 **Remarque :** Il n'est pas possible de copier les paramètres à partir de plusieurs objets de stratégie de groupe dans un seul objet de stratégie de groupe.

Tables de migration

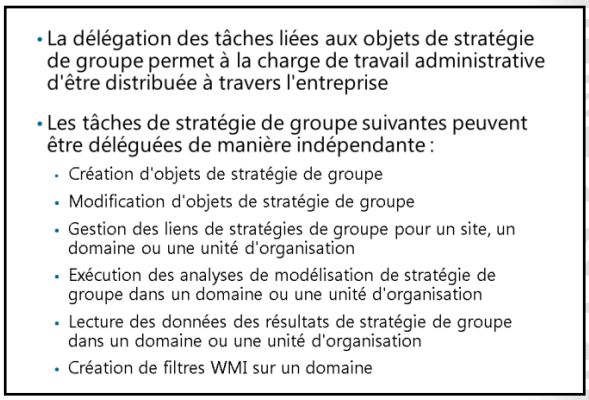
Lors de l'important des objets de stratégie de groupe ou leur copie entre les domaines, vous pouvez utiliser des tables de migration pour modifier les références dans l'objet de stratégie de groupe qui doivent être réglées pour le nouvel emplacement. Par exemple, vous pouvez devoir remplacer le chemin d'accès de la convention d'affectation des noms (UNC) pour la redirection des dossiers par un chemin UNC adapté au nouveau groupe d'utilisateurs auquel l'objet de stratégie de groupe sera appliqué. Vous pouvez créer des tables de migration avant ce processus ou les créer pendant l'opération d'importation ou de copie entre domaines.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Délégation de l'administration des stratégies de groupe

La délégation des tâches liées aux objets de stratégie de groupe vous permet de distribuer la charge de travail administrative à travers l'entreprise. Vous pouvez charger un groupe en créant et en modifiant des objets de stratégie de groupe, alors qu'un autre groupe assure les fonctions de rapport et d'analyse. Un troisième groupe pourrait être chargé de la création des filtres WMI.



Vous pouvez déléguer les tâches de stratégie de groupe suivantes indépendamment :

- Création d'objets de stratégie de groupe
- Modification d'objets de stratégie de groupe
- Gestion des liaisons de stratégies de groupe pour un site, un domaine ou une unité d'organisation
- Exécution des analyses de modélisation de stratégie de groupe dans un domaine ou une unité d'organisation donné
- Lecture des données des résultats de stratégie de groupe pour des objets dans un domaine ou une unité d'organisation donné
- Création de filtres WMI dans un domaine

Le groupe Propriétaires créateurs de la stratégie de groupe laisse ses membres créer de nouveaux objets de stratégie de groupe, et modifie ou supprime les objets de stratégie de groupe qu'ils ont créés.

Autorisations de stratégie de groupe par défaut

Par défaut, l'utilisateur et les groupes suivants ont le contrôle total de la gestion d'objet de stratégie de groupe :

- Admins du domaine
- Administrateurs de l'entreprise
- Propriétaire créateur
- Système local

Le groupe Utilisateur authentifié dispose des autorisations Appliquer la stratégie de groupe et Lire.

Création d'objets de stratégie de groupe

Par défaut, seuls les administrateurs du domaine, les administrateurs de l'entreprise et les propriétaires créateurs de la stratégie de groupe peuvent créer de nouveaux objets de stratégie de groupe. Vous pouvez utiliser deux méthodes pour accorder ce droit à un groupe ou à un utilisateur :

- Ajouter l'utilisateur ou le groupe au groupe de propriétaires créateurs de la stratégie de groupe.
- Accorder explicitement au groupe ou à l'utilisateur l'autorisation de créer des objets de stratégie de groupe à l'aide de la console GPMC.

Modification d'objets de stratégie de groupe

Pour modifier un objet de stratégie de groupe, l'utilisateur doit y avoir l'accès aussi bien en lecture qu'en écriture. Vous pouvez accorder cette autorisation à l'aide de la console GPMC.

Gestion des liaisons des objets de stratégie de groupe

La capacité de lier des objets de stratégie de groupe à un conteneur est une autorisation qui est spécifique à ce conteneur. Dans la console GPMC, vous pouvez gérer cette autorisation à l'aide de l'onglet Délégation du conteneur. Vous pouvez également la déléguer via l'Assistant Délégation de contrôle dans les utilisateurs et les ordinateurs Active Directory.

Modélisation et résultats de stratégie de groupe

Vous pouvez déléguer la capacité d'utiliser les outils de création de rapports de la même façon via la console GPMC ou l'Assistant Délégation de contrôle dans les utilisateurs et les ordinateurs Active Directory.

Création des filtres WMI

Vous pouvez déléguer la capacité de créer et de gérer les filtres WMI de la même façon via la console GPMC ou l'Assistant Délégation de contrôle dans les utilisateurs et les ordinateurs Active Directory.

Gestion d'objets de stratégie de groupe avec Windows PowerShell

En plus d'utiliser la console Gestion des stratégies de groupe et l'éditeur de gestion des stratégies de groupe, vous pouvez également exécuter des tâches d'administration courantes des objets de stratégie de groupe à l'aide de Windows PowerShell.

Le tableau suivant présente certaines des tâches d'administration les plus courantes, qui sont possibles avec Windows PowerShell.

En plus d'utiliser la console de gestion des stratégies de groupe et l'éditeur de gestion des stratégies de groupe, vous pouvez également exécuter des tâches d'administration communes avec des objets de stratégie de groupe à l'aide de Windows PowerShell

- Par exemple, la commande suivante crée un nouvel objet de stratégie de groupe intitulé « Ventes » :
  - New-GPO -Name Sales -commentaire « Voici l'objet de stratégie de groupe Ventes »
- La commande suivante importe les paramètres des objets de stratégie de groupe Ventes enregistrés dans le dossier C:\Sauvegardes dans le nouvel objet de stratégie de groupe Ventes :
  - import-gpo -BackupGpoName Sales -TargetName NewSales -chemin c:\sauvegardes

Nom de l'applet de commande	Description
New-GPO	Crée un nouvel objet de stratégie de groupe
New-GPLink	Crée un nouvelle liaison de l'objet de stratégie de groupe pour l'objet de stratégie de groupe spécifié
Backup-GPO	Sauvegarde les objets de stratégie de groupe spécifiés
Restore-GPO	Restaure les objets de stratégie de groupe spécifiés
Copy-GPO	Copie un objet de stratégie de groupe

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Nom de l'applet de commande	Description
Get-GPO	Obtient les objets de stratégie de groupe spécifiés
Import-GPO	Importe les paramètres sauvegardés dans un objet de stratégie de groupe spécifié
Set-GPInheritance	Accorde les autorisations spécifiées à un utilisateur ou à un groupe de sécurité pour les objets de stratégie de groupe spécifiés

Par exemple, la commande suivante crée un nouvel objet de stratégie de groupe intitulé « Ventes » :

```
New-GPO -Name Sales -comment "Voici l'objet de stratégie de groupe Ventes"
```

Le code suivant importe les paramètres des objets Stratégie de groupe Ventes enregistrés dans le dossier C:\Sauvegardes dans l'objet de stratégie de groupe NewSales :

```
import-gpo -BackupGpoName Sales -TargetName NewSales -chemin c:\sauvegardes
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Étendue de la stratégie de groupe et traitement de la stratégie de groupe

Un objet de stratégie de groupe est, par lui-même, une collection d'instructions de configuration qui seront traitées par les extensions CSE des ordinateurs. Jusqu'à ce que l'objet de stratégie de groupe soit défini en étendue, il n'applique à aucun utilisateur, ni ordinateur. L'étendue de l'objet de stratégie de groupe détermine les extensions CSE dont les ordinateurs recevront et traiteront l'objet de stratégie de groupe, et seuls les ordinateurs ou les utilisateurs au sein de l'étendue d'un objet de la stratégie de groupe appliqueront les paramètres dans cet objet de stratégie de groupe. Dans cette leçon, vous apprendrez à gérer l'étendue d'un objet de stratégie de groupe. Les mécanismes suivants sont utilisés pour définir l'étendue d'un objet de stratégie de groupe :

- La liaison de l'objet de stratégie de groupe à un site, à un domaine ou à une unité d'organisation, et si cette liaison est activée ou non
- L'option Appliquer d'un objet de stratégie de groupe
- L'option Bloquer l'héritage sur une unité d'organisation
- Filtrage du groupe de sécurité
- Filtrage WMI
- Activation ou désactivation du nœud de stratégie
- Ciblage des préférences
- Traitement de stratégie par boucle de rappel

Vous devez pouvoir définir les utilisateurs ou les ordinateurs auxquels vous envisagez de déployer ces configurations. En conséquence, vous devez maîtriser l'art de définir en étendue les objets de stratégie de groupe. Dans cette leçon, vous apprendrez chacun des mécanismes avec lesquels vous pouvez définir l'étendue d'un objet de stratégie de groupe et, dans ce processus, vous maîtriserez les concepts de l'application, de l'héritage et de la priorité de la stratégie de groupe.

Objectifs de la leçon

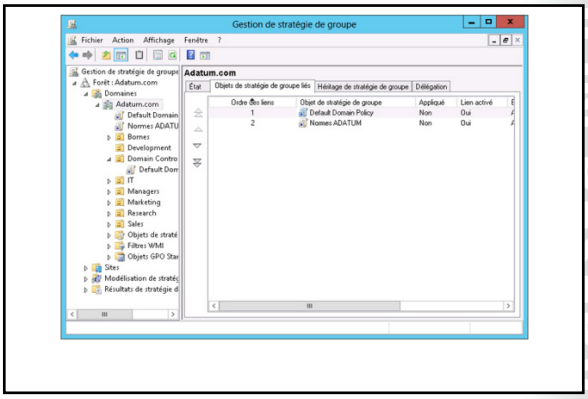
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les liaisons de l'objet de stratégie de groupe.
- Expliquer le traitement d'objet de stratégie de groupe.
- Décrire l'héritage et la priorité de l'objet de stratégie de groupe.
- Utiliser les filtres de sécurité pour filtrer l'étendue de l'objet de stratégie de groupe.
- Expliquer comment utiliser les filtres WMI pour filtrer l'étendue de l'objet de stratégie de groupe.
- Décrire comment activer et désactiver des objets de stratégie de groupe.
- Expliquer comment et quand utiliser le traitement par boucle de rappel.
- Expliquer les considérations pour les ordinateurs qui sont déconnectés ou qui sont connectés par des liaisons lentes.
- Expliquer quand les paramètres de stratégie de groupe entrent en vigueur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Liaisons des objets de stratégie de groupe



Vous pouvez lier un objet de stratégie de groupe à un ou plusieurs sites, domaines ou unités d'organisation AD DS. Une fois que vous avez lié un objet de stratégie de groupe, les utilisateurs ou les ordinateurs dans ce conteneur sont dans l'étendue de l'objet de stratégie de groupe, y compris les ordinateurs et les utilisateurs dans les unités d'organisation enfants.

Liez un objet de stratégie de groupe

Pour lier un objet de stratégie de groupe, soit :

- Cliquez avec le bouton droit sur le domaine ou l'unité d'organisation dans l'arborescence de la console GPMC, puis cliquez sur **Lier en tant qu'objet de stratégie de groupe existant**.
- Si vous n'avez pas encore créé un objet de stratégie de groupe, cliquez sur **Créer un objet de stratégie de groupe dans ce {domaine | unité d'organisation | site} et le lier ici**.

Vous pouvez choisir les mêmes commandes pour lier un objet de stratégie de groupe à un site, mais par défaut, vos sites AD DS ne sont pas visibles dans la console GPMC. Pour montrer des sites dans la console GPMC, cliquez avec le bouton droit sur **Sites** dans l'arborescence de la console GPMC, puis cliquez sur **Montrer les sites**.

Remarque : Un objet de stratégie de groupe lié à un site affecte tous les ordinateurs dans ce site, abstraction faite du domaine auquel les ordinateurs appartiennent, tant que tous ces ordinateurs appartiennent à la même forêt Active Directory. Par conséquent, quand vous liez un objet de stratégie de groupe à un site, cet objet de stratégie de groupe peut être appliqué à plusieurs domaines dans une forêt. Les objets de stratégie de groupe liés aux sites sont enregistrés sur des contrôleurs de domaine dans le domaine où vous créez l'objet de stratégie de groupe. Par conséquent, les contrôleurs de domaine pour ce domaine doivent être accessibles pour que les objets de stratégie de groupe liés aux sites soient appliqués correctement. Si vous implémentez des stratégies liées aux sites, vous devez examiner l'application de la stratégie au moment de la planification de votre infrastructure réseau. Vous pouvez soit placer un contrôleur de domaine du domaine de l'objet de stratégie de groupe dans le site auquel la stratégie est liée, soit vérifier qu'une connectivité WAN fournit l'accessibilité à un contrôleur de domaine dans le domaine de l'objet de stratégie de groupe.

Quand vous liez un objet de stratégie de groupe à un conteneur, vous définissez l'étendue initiale de l'objet de stratégie de groupe. Sélectionnez un objet de stratégie de groupe, puis cliquez sur l'onglet **Étendue** pour identifier les conteneurs auxquels l'objet de stratégie de groupe est lié. Dans le volet d'informations de la console GPMC, les liaisons de l'objet de stratégie de groupe sont affichés dans la première section de l'onglet **Étendue**.

L'incidence des liaisons de l'objet de stratégie de groupe est que le client de stratégie de groupe télécharge l'objet de stratégie de groupe si les objets de l'ordinateur ou de l'utilisateur tombent dans l'étendue de la liaison. L'objet de stratégie de groupe ne sera téléchargé que s'il est nouveau ou mis à jour. Le client de la stratégie de groupe met l'objet de stratégie de groupe en cache pour rendre l'actualisation de la stratégie plus efficace.

Lier un objet de stratégie de groupe à plusieurs unités d'organisation

Vous pouvez lier un objet de stratégie de groupe à plus d'un site ou d'une unité d'organisation. Il est courant, par exemple, d'appliquer la configuration aux ordinateurs dans plusieurs unités d'organisation. Vous pouvez définir la configuration dans un objet de stratégie de groupe unique, puis lier cet objet de stratégie de groupe à chaque unité d'organisation. Si vous modifiez par la suite les paramètres dans l'objet de stratégie de groupe, vos modifications s'appliqueront à toutes les unités d'organisation auxquelles l'objet de stratégie de groupe est lié.

Supprimer ou désactiver une liaison de l'objet de stratégie de groupe

Une fois que vous avez lié un objet de stratégie de groupe, la liaison de l'objet de stratégie de groupe apparaît dans la console GPMC sous le site, le domaine ou l'unité d'organisation. L'icône de la liaison de l'objet de stratégie de groupe comporte une petite flèche de raccourci. Quand vous cliquez avec le bouton droit sur la liaison de l'objet de stratégie de groupe, un menu contextuel apparaît :

- Pour supprimer une liaison de l'objet de stratégie de groupe, cliquez avec le bouton droit sur la liaison de l'objet de stratégie de groupe dans l'arborescence de la console GPMC, puis cliquez sur **Supprimer**.

La suppression d'une liaison de l'objet de stratégie de groupe ne supprime pas l'objet de stratégie de groupe lui-même, qui reste dans son conteneur. Cependant, la suppression de la liaison modifie l'étendue de l'objet de stratégie de groupe, de sorte qu'il ne s'applique plus aux ordinateurs et aux utilisateurs au sein de l'objet du conteneur lié précédemment.

Vous pouvez également modifier une liaison de l'objet de stratégie de groupe en la désactivant :

- Pour désactiver une liaison de l'objet de stratégie de groupe, cliquez avec le bouton droit sur la liaison de l'objet de stratégie de groupe dans l'arborescence de la console GPMC, puis désactivez l'option **Liaison activée**.

La désactivation de la liaison modifie également l'étendue de l'objet de stratégie de groupe de sorte qu'elle ne s'applique plus aux ordinateurs et aux utilisateurs au sein de ce conteneur. Cependant, la liaison demeure de sorte que vous puissiez l'activer à nouveau plus facilement.

Démonstration : Procédure de liaison des objets de stratégie de groupe

Cette démonstration montre comment :

- Ouvrez la console Gestion des stratégies de groupe.
- créer deux objets de stratégie de groupe ;
- lier le premier objet de stratégie de groupe au domaine ;
- lier le deuxième objet de stratégie de groupe à l'unité d'organisation informatique ;
- désactiver la liaison du premier objet de stratégie de groupe ;
- supprimer le deuxième objet de stratégie de groupe ;
- activer de nouveau la liaison du premier objet de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

Créer et modifier deux objets de stratégie de groupe

1. ouvrir la console Gestion des stratégies de groupe ;
2. Créez deux nouveaux objets de stratégie de groupe appelés Supprimer la commande Exécuter et Ne pas supprimer la commande Exécuter.
3. Modifiez les paramètres des deux objets de stratégie de groupe.

Liez les objets de stratégie de groupe à différents emplacements

1. Liez l'objet de stratégie de groupe Supprimer la commande Exécuter au domaine. L'objet de stratégie de groupe Supprimer la commande Exécuter est maintenant joint au domaine Adatum.com.
2. Liez l'objet de stratégie de groupe Ne pas supprimer la commande Exécuter à l'unité d'organisation informatique. L'objet de stratégie de groupe Ne pas supprimer la commande Exécuter est maintenant joint à l'unité d'organisation informatique.
3. Affichez l'héritage de l'objet de stratégie de groupe sur l'unité d'organisation informatique. L'onglet Héritage de la stratégie de groupe montre l'ordre de priorité des objets de stratégie de groupe.

Désactiver une liaison d'objet de stratégie de groupe

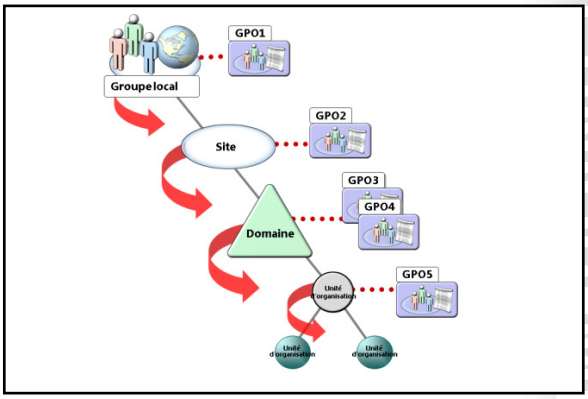
1. Désactivez l'objet de stratégie de groupe Supprimer la commande Exécuter sur le domaine Adatum.com.
2. Actualisez le volet Héritage de stratégie de groupe pour l'unité d'organisation informatique, puis notez les résultats dans le volet droit. L'objet de stratégie de groupe Supprimer la commande Exécuter n'est plus listé.

Supprimer une liaison d'objet de stratégie de groupe

1. Sélectionnez l'unité d'organisation relative Informatique, puis supprimez la liaison de l'objet de stratégie de groupe Ne pas supprimer la commande Exécuter. Vérifiez la suppression de l'objet de stratégie de groupe Ne pas supprimer la commande Exécuter et l'absence de l'objet de stratégie de groupe Supprimer la commande Exécuter.
2. Activez l'objet de stratégie de groupe Supprimer la commande Exécuter sur le domaine Adatum.com. Actualisez la fenêtre Héritage de stratégie de groupe pour l'unité d'organisation Informatique, puis notez les résultats dans le volet droit.

Ordre de traitement de la stratégie de groupe

Tous les objets de stratégie de groupe qui s'appliquent à un utilisateur, à un ordinateur ou à tous les deux ne s'appliquent pas immédiatement. Les objets de stratégie de groupe sont appliqués dans un ordre particulier. Cet ordre signifie que les paramètres traités en premier peuvent être remplacés par les paramètres conflictuels traités plus tard.



La stratégie de groupe suit l'ordre de traitement hiérarchique suivant :

1. Stratégies de groupe locales. Chaque ordinateur exécutant Windows 2000 ou version ultérieure a au moins une stratégie de groupe locale. Les stratégies locales sont appliquées en premier lieu.
2. Stratégies de groupe de site. Les stratégies liées aux sites sont traitées en second lieu. S'il y a plusieurs stratégies de site, elles sont traitées de façon synchrone dans l'ordre de préférence répertorié.
3. Stratégies de groupe du domaine. Les stratégies liées aux domaines sont traitées en troisième lieu. S'il y a plusieurs stratégies de domaine, elles sont traitées de façon synchrone dans l'ordre de préférence répertorié.
4. Stratégies de groupe de l'unité d'organisation. Les stratégies liées aux unités d'organisation de haut niveau sont traitées en quatrième lieu. S'il y a plusieurs stratégies d'unités d'organisation de haut niveau, elles sont traitées de façon synchrone dans l'ordre de préférence répertorié.
5. Stratégies de groupe d'unité d'organisation enfant. Les stratégies liées aux unités d'organisation enfants de haut niveau sont traitées en cinquième lieu. S'il y a plusieurs stratégies d'unité d'organisation enfant, elles sont traitées de façon synchrone dans l'ordre de préférence répertorié. Quand il y a plusieurs niveaux d'unités d'organisation enfants, les stratégies des unités d'organisation de niveau supérieur sont appliquées en premier lieu et les stratégies des unités d'organisation de niveau inférieur sont appliquées ensuite.

Dans l'application Stratégie de groupe, la règle générale est que la dernière stratégie appliquée prévaut. Par exemple, une stratégie qui restreint l'accès au panneau de configuration appliqué au niveau du domaine pourrait être inversée par une stratégie appliquée au niveau de l'unité d'organisation pour les objets contenus dans cette unité d'organisation particulière.

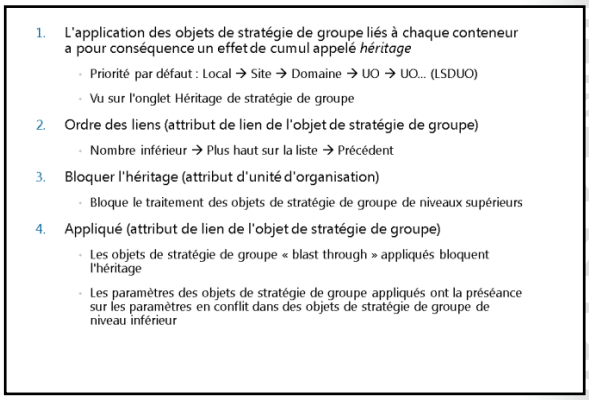
Si vous liez plusieurs objets de stratégie de groupe à une unité d'organisation, leur traitement a lieu dans l'ordre que l'administrateur spécifie sur l'onglet Objets de stratégie de groupe liés de l'unité d'organisation dans la console GPMC.

Par défaut, le traitement est activé pour toutes les liaisons de l'objet de stratégie de groupe. Vous pouvez désactiver la liaison de l'objet de stratégie de groupe d'un conteneur pour bloquer complètement l'application d'un objet de stratégie de groupe pour un site, un domaine ou une unité d'organisation donné. Notez que si l'objet de stratégie de groupe est lié à d'autres conteneurs, ils continueront à le traiter si leurs liaisons sont activées.

Vous pouvez également désactiver la configuration utilisateur ou ordinateur d'un objet de stratégie de groupe particulier indépendant de l'utilisateur ou de l'ordinateur. Si une section d'une stratégie est connue comme étant vide, la désactivation de l'autre côté accélère le traitement de la stratégie. Par exemple, si vous avez une stratégie qui fournit uniquement la configuration du bureau utilisateur, vous pourriez désactiver le côté ordinateur de la stratégie.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de l'héritage et de la priorité de l'objet de stratégie de groupe



Vous pouvez configurer un paramètre de stratégie dans plus d'un objet de stratégie de groupe, ce qui engendre des conflits des objets de stratégie de groupe les uns avec les autres. Par exemple, vous pouvez activer un paramètre de stratégie dans un objet de stratégie de groupe, le désactiver dans un autre objet de stratégie de groupe et ne pas le configurer dans un troisième objet de stratégie de groupe. Dans ce cas, la priorité des objets de stratégie de groupe détermine le paramètre de stratégie que le client applique. Un objet de stratégie de groupe de priorité supérieure l'emporte sur un objet de stratégie de groupe de priorité inférieure. La priorité est indiquée sous forme de nombre dans la console GPMC. Plus le nombre est petit, c'est-à-dire plus il est proche de 1, plus la priorité est élevée. Par conséquent, un objet de stratégie de groupe ayant une priorité de 1 l'emportera sur les autres objets de stratégie de groupe. Sélectionnez le conteneur AD DS approprié, puis cliquez sur l'onglet **Héritage de stratégie de groupe** pour afficher la priorité de chaque objet de stratégie de groupe.

Quand un paramètre de stratégie est activé ou désactivé dans un objet de stratégie de groupe ayant une priorité plus élevée, le paramètre configuré entre en vigueur. Cependant, souvenez-vous que les paramètres de stratégie sont définis à l'état « Non configuré », par défaut. Si un paramètre de stratégie n'est pas configuré dans un objet de stratégie de groupe ayant une priorité plus élevée, le paramètre de stratégie (activé ou désactivé) dans un objet de stratégie de groupe ayant une priorité inférieure entrera en vigueur.

Vous pouvez lier plus d'un objet de stratégie de groupe à un objet de conteneur AD DS. L'ordre des liaisons des objets de stratégie de groupe détermine la priorité des objets de stratégie de groupe dans un tel scénario. Les objets de stratégie de groupe ayant un ordre de liaison supérieur ont la priorité sur les objets de stratégie de groupe ayant un ordre de liaison inférieur. Quand vous sélectionnez une unité d'organisation dans la console GPMC, l'onglet Objets de stratégie de groupe liés montre l'ordre des liaisons des objets de stratégie de groupe liés à cette unité d'organisation.

Le comportement par défaut de la stratégie de groupe est que les objets de stratégie de groupe liés dans un conteneur de niveau supérieur sont hérités par les conteneurs de niveau inférieur. Quand un ordinateur démarre ou un utilisateur ouvre une session, le client de la stratégie de groupe examine l'emplacement de l'objet de l'ordinateur ou de l'utilisateur dans AD DS, et évalue les objets de stratégie de groupe ayant l'étendue qui comprend l'ordinateur ou l'utilisateur. Puis, les extensions CSE appliquent les paramètres de stratégie de ces objets de stratégie de groupe. Les stratégies sont appliquées séquentiellement, en commençant par celles qui sont liées au site, suivie de celles liées au domaine, puis celles liées aux unités d'organisation, en partant de l'unité d'organisation de niveau supérieur jusqu'à celle où existe l'objet utilisateur ou ordinateur. C'est une application superposée des paramètres ; ainsi un objet de stratégie de groupe appliqué plus tard dans le processus, parce qu'il a une priorité supérieure, l'emporte sur les paramètres appliqués plus tôt dans le processus.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'application séquentielle des objets de stratégie de groupe crée un effet appelé *héritage de stratégie*. Les stratégies sont héritées, de sorte que l'ensemble résultant des stratégies de groupe pour un utilisateur ou un ordinateur soit l'effet cumulatif des stratégies de site, de domaine et de l'unité d'organisation.

Par défaut, les objets de stratégie de groupe hérités ont une priorité inférieure à celle des objets de stratégie de groupe liés directement au conteneur. Par exemple, vous pourriez configurer un paramètre de stratégie pour désactiver l'utilisation des outils de modification du registre pour tous les utilisateurs dans le domaine, en configurant le paramètre de stratégie dans un objet de stratégie de groupe lié au domaine. Cet objet de stratégie de groupe et son paramètre de stratégie sont hérités par tous les utilisateurs dans le domaine. Cependant, si vous souhaitez que les administrateurs puissent utiliser des outils de modification du registre, vous liez un objet de stratégie de groupe à l'unité d'organisation qui contient les comptes des administrateurs, puis vous configurez le paramètre de stratégie pour permettre l'utilisation des outils de modification du registre. Puisque l'objet de stratégie de groupe lié à l'unité d'organisation des administrateurs a une priorité supérieure à celle de l'objet de stratégie de groupe hérité, les administrateurs pourront utiliser les outils de modification du registre.

Priorité de plusieurs objets de stratégie de groupe liés

Si plusieurs objets de stratégie de groupe sont liés à un objet de conteneur AD DS, l'ordre des liaisons des objets détermine leur priorité.

Pour modifier la priorité d'une liaison de l'objet de stratégie de groupe :

1. Sélectionnez l'objet de conteneur AD DS dans l'arborescence de la console GPMC.
2. Cliquez sur l'onglet **Objets de stratégie de groupe liés** dans le volet d'informations.
3. Sélectionnez l'objet de stratégie de groupe.
4. Utilisez les flèches **Haut**, **Bas**, **Aller au début**, et **Aller à la fin** pour modifier l'ordre des liaisons de l'objet de stratégie de groupe sélectionné.

Bloquer l'héritage

Vous pouvez configurer un domaine ou une unité d'organisation pour empêcher l'héritage des paramètres de stratégie. Cette opération est appelée « blocage de l'héritage ». Pour sélectionner le blocage de l'héritage, cliquez avec le bouton droit sur le domaine ou l'unité d'organisation dans l'arborescence de la console GPMC, puis sélectionnez **Bloquer l'héritage**.

L'option Bloquer l'héritage est une propriété d'un domaine ou d'une unité d'organisation ; ainsi, elle bloque tous les paramètres de la stratégie de groupe des objets de stratégie de groupe liés aux parents dans la hiérarchie de stratégie de groupe. Par exemple, quand vous bloquez l'héritage sur une unité d'organisation, l'application de l'objet de stratégie de groupe commence avec tous les objets de stratégie de groupe liés directement à cette unité d'organisation. Par conséquent, les objets de stratégie de groupe liés aux unités d'organisation, domaines ou sites de niveau supérieur ne s'appliqueront pas.

Vous devez utiliser l'option Bloquer l'héritage avec modération parce que le blocage de l'héritage rend plus difficile l'évaluation de la priorité et de l'héritage de la stratégie de groupe. Avec le filtrage du groupe de sécurité, vous pouvez soigneusement limiter en étendue un objet de stratégie de groupe de sorte qu'il ne s'applique qu'aux bons utilisateurs et ordinateurs en premier lieu, rendant inutile l'utilisation de l'option Bloquer l'héritage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Appliquer une liaison d'objet de stratégie de groupe

En outre, vous pouvez définir une liaison d'objet de stratégie de groupe à l'état **Appliqué**. Pour appliquer une liaison d'objet de stratégie de groupe, cliquez avec le bouton droit sur celle-ci dans l'arborescence de la console, puis sélectionnez **Appliqué** dans le menu contextuel.

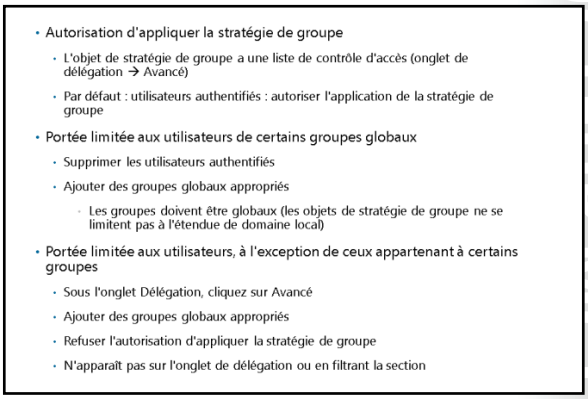
Quand vous définissez une liaison de l'objet de stratégie de groupe à l'état Appliqué, l'objet de stratégie de groupe prend le niveau de priorité le plus élevé ; les paramètres de stratégie dans cet objet de stratégie de groupe prévaudront sur tous les paramètres de stratégie conflictuels dans d'autres objets de stratégie de groupe. En outre, une liaison appliquée s'appliquera aux conteneurs enfants même lorsque ces conteneurs sont définis sur Bloquer l'héritage. L'option Appliqué entraîne l'application de la stratégie à tous les objets dans son étendue. L'option Appliqué amène les stratégies à remplacer toutes les stratégies conflictuelles et s'appliqueront indépendamment du fait qu'une option Bloquer l'héritage soit définie.

L'application est utile quand vous devez configurer un objet de stratégie de groupe qui définit une configuration exigée par vos stratégies d'entreprise en matière de sécurité informatique et d'utilisation. Par conséquent, vous souhaitez vérifier que d'autres objets de stratégie de groupe ne remplacent pas ces paramètres. Vous pouvez le faire en appliquant la liaison de l'objet de stratégie de groupe.

Évaluation de la priorité

Pour faciliter l'évaluation de la priorité de l'objet de stratégie de groupe, vous pouvez simplement sélectionner une unité d'organisation (ou un domaine), puis cliquez sur l'onglet **Héritage de stratégie de groupe**. Cet onglet affichera la priorité résultante des objets de stratégie de groupe, compte tenu de la liaison de l'objet de stratégie de groupe, de l'ordre des liaisons, du blocage de l'héritage et de l'application de la liaison. Cet onglet ne tient compte ni des stratégies liées à un site, ni de la sécurité de l'objet de stratégie de groupe, ni du filtrage WMI.

Utilisation du filtrage de sécurité pour modifier l'étendue de groupe



Bien que vous puissiez utiliser les options Application et Bloquer l'héritage pour contrôler l'application des objets de stratégie de groupe aux objets du conteneur, vous pourriez devoir appliquer des objets de stratégie de groupe uniquement à certains groupes d'utilisateurs ou d'ordinateurs plutôt qu'à tous les utilisateurs ou les ordinateurs dans l'étendue de l'objet de stratégie de groupe. Bien que vous ne puissiez pas directement lier un objet de stratégie de groupe à un groupe de sécurité, il y a une façon d'appliquer des objets de stratégie de groupe à des groupes de sécurité spécifiques. Les stratégies dans un objet de stratégie de groupe s'appliquent uniquement aux utilisateurs qui ont les autorisations Autoriser lecture et Autoriser application de la stratégie de groupe à l'objet de stratégie de groupe.

Chaque objet de stratégie de groupe a une liste de contrôle d'accès qui définit les autorisations de l'objet de stratégie de groupe. Deux autorisations, Autoriser lecture et Autoriser application de la stratégie de groupe, sont requises pour qu'un objet de stratégie de groupe s'applique à un utilisateur ou à un ordinateur. Par exemple, si un objet de stratégie de groupe est limité en étendue à un ordinateur par sa liaison de l'unité d'organisation de l'ordinateur, mais que l'ordinateur n'a pas les autorisations Lire et Appliquer la stratégie de groupe, il ne téléchargera pas et n'appliquera pas l'objet de stratégie de groupe. Par conséquent, en définissant les autorisations appropriées pour les groupes de sécurité, vous pouvez filtrer un objet de stratégie de groupe pour qu'il s'applique uniquement aux ordinateurs et utilisateurs spécifiés.

Par défaut, les utilisateurs authentifiés ont l'autorisation Appliquer la stratégie de groupe - Autoriser sur chaque nouvel objet de stratégie de groupe. Cela signifie que par défaut, tous les utilisateurs et ordinateurs sont affectés par les objets de stratégie de groupe définis pour leur domaine, site, ou unité d'organisation, indépendamment des autres groupes dont ils pourraient être membres. Par conséquent, il y a deux façons de filtrer l'étendue de l'objet de stratégie de groupe :

- Supprimez l'autorisation Appliquer la stratégie de groupe (définie actuellement sur Autoriser) pour le groupe d'utilisateurs authentifiés, mais ne définissez pas cette autorisation sur Refuser. Puis, déterminez les groupes auxquels l'objet de stratégie de groupe devrait être appliqué et définissez les autorisations Lire et Appliquer la stratégie de groupe pour ces groupes sur Autoriser.
- Déterminez les groupes auxquels l'objet de stratégie de groupe ne devrait être appliqué et définissez l'autorisation Appliquer la stratégie de groupe pour ces groupes sur Refuser. Si vous refusez l'autorisation Appliquer stratégie de groupe à un objet de stratégie de groupe, l'utilisateur ou l'ordinateur n'appliquera pas les paramètres dans l'objet de stratégie de groupe, même si l'utilisateur ou l'ordinateur est membre d'un autre groupe auquel l'autorisation Appliquer la stratégie de groupe est accordée.

Filtrage d'un objet de stratégie de groupe à appliquer à des groupes spécifiques

Pour appliquer un objet de stratégie de groupe à un groupe de sécurité spécifique :

1. Sélectionnez l'objet de stratégie de groupe dans le conteneur d'objets de stratégie de groupe dans l'arborescence de la console.
2. Dans la section Filtrage de sécurité, sélectionnez le groupe **Utilisateurs authentifiés**, puis cliquez sur **Supprimer**.

 **Remarque :** Vous ne pouvez pas filtrer des objets de stratégie de groupe avec des groupes de sécurité locaux du domaine.

3. Cliquez sur **OK** pour confirmer la modification.
4. Cliquez sur **Ajouter**.
5. Sélectionnez le groupe auquel vous souhaitez appliquer la stratégie, puis cliquez sur **OK**.

Filtrage d'un objet de stratégie de groupe à exclure des groupes spécifiques

L'onglet **Étendue** d'un objet de stratégie de groupe ne vous permet pas d'exclure des groupes spécifiques. Pour exclure un groupe, c'est-à-dire que vous lui refuser l'autorisation Appliquer la stratégie de groupe, vous devez utiliser l'onglet **Délégation**.

Pour refuser à un groupe l'autorisation Appliquer la stratégie de groupe :

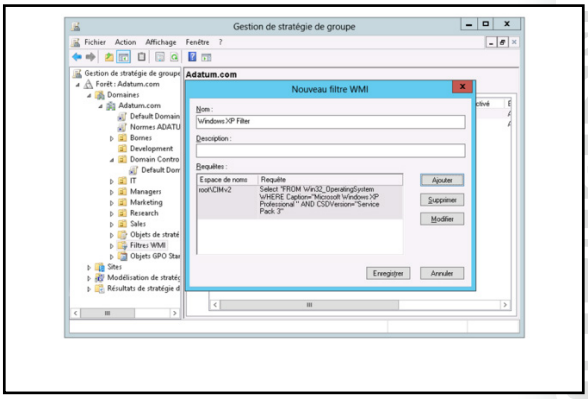
1. Sélectionnez l'objet de stratégie de groupe dans le conteneur d'objets de stratégie de groupe dans l'arborescence de la console.
2. Cliquez sur l'onglet **Délégation**.
3. Cliquez sur le bouton **Avancé**. La boîte de dialogue **Paramètres de sécurité** s'affiche.
4. Cliquez sur le bouton **Ajouter**.
5. Sélectionnez le groupe que vous souhaitez exclure de l'objet de stratégie de groupe. Souvenez-vous ce groupe doit être un groupe global. L'étendue de l'objet de stratégie de groupe ne peut pas être filtrée par des groupes locaux de domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Cliquez sur **OK**. Le groupe que vous avez sélectionné dispose de l'autorisation Autoriser la lecture par défaut.
7. Désactivez la case à cocher de l'autorisation **Autoriser la lecture**.
8. Activez la case à cocher **Refuser Appliquer la stratégie de groupe**.
9. Cliquez sur **OK**. Vous êtes prévenu que les autorisations Refuser remplacent les autres autorisations. Puisque les autorisations Refuser remplacent les autorisations Autoriser, nous recommandons que vous les utilisez avec modération. Microsoft Windows vous rappelle cette bonne pratique par un message d'avertissement. Le processus d'exclusion des groupes avec l'autorisation Refuser Appliquer la stratégie de groupe est bien plus laborieux que le processus d'inclusion des groupes dans la section Filtrage de sécurité de l'onglet **Étendue**.
10. Confirmez que vous souhaitez continuer.

Remarque : Les refus ne sont pas exposés sur l'onglet **Étendue**. Malheureusement, quand vous excluez un groupe, l'exclusion n'est pas montrée dans la section Filtrage de sécurité de l'onglet **Étendue**. C'est pourtant une raison de plus d'utiliser les refus avec modération.

Définition des filtres WMI



WMI est une technologie d'infrastructure de gestion qui permet aux administrateurs de surveiller et de contrôler des objets gérés dans le réseau. Une requête WMI est capable de filtrer des systèmes selon des caractéristiques, y compris la mémoire vive (RAM), la vitesse du processeur, la capacité de disque, l'adresse IP, la version du système d'exploitation et le niveau de service pack, les applications installées et les propriétés d'imprimante. Puisque WMI expose presque chaque propriété de chaque objet dans un ordinateur, la liste d'attributs que vous pouvez utiliser dans une requête WMI est pratiquement illimitée. Les requêtes WMI sont écrites à l'aide du langage de requête WMI (WQL).

Vous pouvez utiliser une requête WMI pour créer un filtre WMI, avec lequel vous pouvez filtrer un objet de stratégie de groupe. Vous pouvez utiliser la stratégie de groupe pour déployer les applications logicielles et les services packs. Vous pouvez créer un objet de stratégie de groupe pour déployer une application, puis utiliser un filtre WMI pour spécifier que la stratégie doit s'appliquer uniquement aux ordinateurs ayant certains systèmes d'exploitation et service packs, par exemple Windows XP Service Pack 3 (SP3). La requête WMI permettant d'identifier de tels systèmes est la suivante :

```
Select * FROM Win32_OperatingSystem WHERE Caption="Microsoft Windows XP Professional"
AND CSDVersion="Service Pack 3"
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Quand le client de la stratégie de groupe évalue des objets de stratégie de groupe qu'il a téléchargés pour déterminer lesquels doivent être remis aux extensions CSE pour traitement, il effectue la requête par rapport au système local. Si le système répond aux critères de la requête, le résultat de requête est un Vrai logique et les extensions CSE traitent l'objet de stratégie de groupe.

WMI expose les espaces de noms, où résident les classes qui peuvent être interrogées. Beaucoup de classes utiles, notamment Win32_Operating System, se trouvent dans une classe appelée racine\CIMv2.

Pour créer un filtre WMI :

1. Cliquez avec le bouton droit sur le nœud **Filtres WMI** dans l'arborescence de la console GPMC, puis cliquez sur **Nouveau**. Saisissez un nom et une description du filtre, puis cliquez sur le bouton **Ajouter**.
2. Dans la zone **Espace de noms**, saisissez l'espace de noms de votre requête.
3. Dans la zone **Requête**, saisissez la requête.
4. Cliquez sur **OK**.

Pour filtrer un objet de stratégie de groupe avec un filtre WMI :

1. Sélectionnez l'objet de stratégie de groupe ou la liaison de l'objet de stratégie de groupe dans l'arborescence de la console.
2. Cliquez sur l'onglet **Étendue**.
3. Cliquez sur la liste déroulante **WMI**, puis sélectionnez **Filtre WMI**.

Vous pouvez filtrer un objet de stratégie de groupe avec un seul filtre WM, mais vous pouvez créer un filtre WMI avec une requête complexe qui utilise plusieurs critères. Vous pouvez lier un filtre WMI unique à un ou plusieurs objets de stratégie de groupe. L'onglet Général d'un filtre WMI affiche les objets de stratégie de groupe qui utilisent le filtre WMI :

Il y a trois avertissements importants concernant les filtres WMI :

- D'abord, la syntaxe WQL des requêtes WMI peut être délicate à maîtriser. Vous pouvez souvent trouver des exemples sur Internet quand vous effectuez une recherche à l'aide des mots clés filtre WMI et requête WMI, ainsi qu'avec une description de la requête que vous souhaitez créer.
- En second lieu, les filtres WMI sont chers en termes de performance de traitement de stratégie de groupe. Puisque le client de stratégie de groupe doit effectuer la requête WMI à chaque intervalle de traitement de stratégie, il y a une légère incidence sur les performances système toutes les 90 à 120 minutes. Avec les performances des ordinateurs d'aujourd'hui, cette incidence peut être imperceptible. Cependant, vous devez tester les effets d'un filtre WMI avant de le déployer à grande échelle dans votre environnement de production.

 **Remarque :** Notez que la requête WMI est traitée uniquement une fois, même si vous l'utilisez pour filtrer l'étendue de plusieurs objets de stratégie de groupe.

- Troisièmement, les filtres WMI ne sont pas traités par les ordinateurs exécutant le système d'exploitation Microsoft Windows 2000 Server. Si un objet de stratégie de groupe est filtré avec un filtre WMI, un système Windows 2000 Server ignore le filtre, puis traite l'objet de stratégie de groupe comme si les résultats du filtre étaient vrais.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Procédure de filtrage des stratégies

Cette démonstration montre comment :

- créer un objet de stratégie de groupe qui supprime le lien menu Aide du menu Accueil, puis liez-le à l'unité d'organisation Informatique ;
- utiliser le filtrage de sécurité pour exempter un utilisateur de l'objet de stratégie de groupe ;
- tester l'application de la stratégie de groupe.

Procédure de démonstration

Créez un nouvel objet de stratégie de groupe et liez-le à une unité d'organisation Informatique.

1. Ouvrez la console Gestion des stratégies de groupe sur LON-DC1.
2. Créez un nouvel objet de stratégie de groupe appelé **Supprimer le menu Aide,** puis liez-le à l'unité d'organisation **IT**.
3. Modifiez les paramètres de l'objet de stratégie de groupe pour supprimer le menu Aide du menu **Accueil**.

Filtrer l'application de la stratégie de groupe en utilisant le filtrage des groupes de sécurité

1. Supprimez l'entrée **Utilisateurs authentifiés** de la liste **Filtrage de sécurité** pour l'objet de stratégie de groupe **Supprimer le menu Aide** dans l'unité d'organisation Informatique.
2. Ajoutez l'utilisateur **Ed Meadows** à la liste **Filtrage de sécurité**. Maintenant, seul Ed Meadows a l'autorisation d'appliquer la stratégie.

Filtrer l'application de la stratégie de groupe en utilisant le filtrage WMI

1. Créez un filtre WMI appelé filtre XP.
2. Ajoutez la requête suivante au filtre :

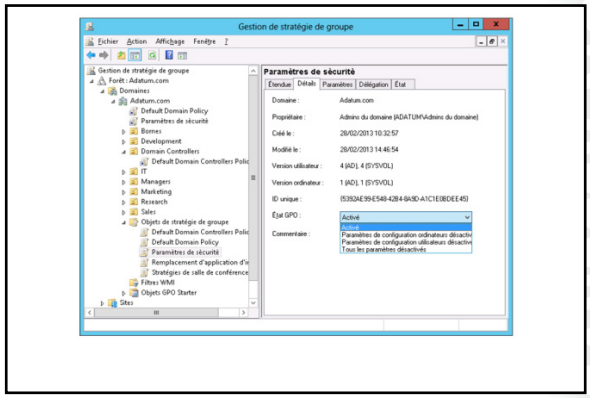
```
Select * from Win32_OperatingSystem where Caption = "Microsoft Windows XP
Professional"
```

3. Enregistrez la requête sous le nom **Filtre XP**.
4. Créez un nouvel objet de stratégie de groupe appelé **Mises à jour logicielles pour XP**, et liez-le ensuite à l'unité d'organisation Informatique.
5. Modifiez les propriétés de la stratégie pour utiliser le filtre XP.
6. Fermez la console Gestion des stratégies de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Activer ou désactiver les objets de stratégie de groupe et les nœuds d'objet de stratégie de groupe

Vous pouvez empêcher le traitement des paramètres dans les nœuds **Configuration ordinateur** ou **Configuration utilisateur** pendant l'actualisation de la stratégie en modifiant l'état de l'objet de stratégie de groupe.



Pour activer ou désactiver les nœuds d'un objet de stratégie de groupe, sélectionnez l'objet de stratégie de groupe ou la liaison de l'objet de stratégie de groupe dans l'arborescence de la console, cliquez sur l'onglet **Détails** illustré, puis sélectionnez l'un des éléments suivants de la liste déroulante État GPO :

- Activé. Les paramètres de configuration ordinateur et les paramètres de configuration utilisateur seront traités par les extensions CSE pendant l'actualisation de la stratégie.
- Tous les paramètres désactivés. Les extensions CSE ne traiteront pas l'objet de stratégie de groupe pendant l'actualisation de la stratégie.
- Paramètres de configuration ordinateur désactivés. Pendant l'actualisation de la stratégie d'ordinateur, les paramètres de configuration de l'ordinateur dans l'objet de stratégie de groupe ne seront pas appliqués.
- Paramètres de configuration utilisateurs désactivés. Pendant l'actualisation de la stratégie utilisateur, les paramètres de configuration utilisateur de l'objet de stratégie de groupe ne seront pas appliqués.

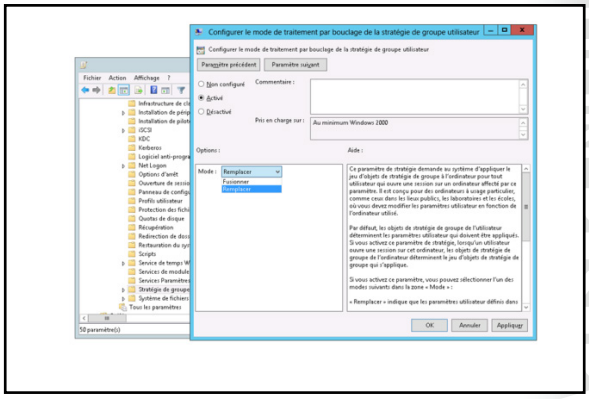
Vous pouvez configurer l'état de l'objet de stratégie de groupe pour optimiser le traitement de stratégie. Par exemple, si un objet de stratégie de groupe contient uniquement des paramètres utilisateurs, alors la définition de l'option État GPO sur désactiver les paramètres de l'ordinateur empêche le client de stratégie de groupe de tenter de traiter l'objet de stratégie de groupe pendant l'actualisation de la stratégie d'ordinateur. Puisque l'objet de stratégie de groupe ne contient aucun paramètre de l'ordinateur, il n'est pas nécessaire de traiter l'objet de stratégie de groupe, et vous pouvez économiser ainsi quelques cycles de processeur.

Remarque : Vous pouvez définir une configuration qui doit entrer en vigueur en cas d'urgence, d'incident de sécurité ou d'autres incidents dans un objet de stratégie de groupe, puis lier l'objet de stratégie de groupe de sorte qu'il soit limité en étendue aux utilisateurs et ordinateurs appropriés. Puis, désactivez l'objet de stratégie de groupe. Si vous avez besoin de la configuration soit déployée, activez l'objet de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Traitement de stratégie par boucle de rappel



Par défaut, les paramètres d'un utilisateur proviennent des objets de stratégie de groupe limités en étendue à l'objet utilisateur dans AD DS. Indépendamment de l'ordinateur où l'utilisateur ouvre une session, l'ensemble résultant des stratégies qui déterminent l'environnement d'utilisateur est identique. Il y a cependant des situations où vous pouvez souhaiter configurer un utilisateur différemment, selon l'ordinateur utilisé. Par exemple, vous pouvez souhaiter verrouiller et standardiser des bureaux d'utilisateur quand les utilisateurs se connectent aux ordinateurs dans des environnements attentivement gérés, tels que les salles de conférence, les zones d'accueil, les laboratoires, les classes, et les bornes. Cela est également important pour les scénarios d'infrastructure de bureau virtuel (VDI), y compris les ordinateurs virtuels distants et les services de bureau à distance (RDS).

Imaginez un scénario où vous souhaitez appliquer une apparence d'entreprise standard au bureau Windows sur tous les ordinateurs des salles de conférence et autres zones publiques de votre site. Comment envisagez-vous de gérer de manière centralisée cette configuration à l'aide de la stratégie de groupe ? Les paramètres de stratégie qui configurent l'apparence de bureau sont situés dans le nœud **Configuration** utilisateur d'un objet de stratégie de groupe. Par conséquent, les paramètres s'appliquent par défaut aux utilisateurs, indépendamment de l'ordinateur où ils se connectent. Le traitement de stratégie par défaut ne vous permet pas de limiter en étendue les paramètres utilisateurs à appliquer aux ordinateurs, indépendamment de ceux où l'utilisateur ouvre une session. C'est alors que le traitement de stratégie par boucle peut être utile.

Le traitement de stratégie par boucle de rappel modifie l'algorithme par défaut que le client de stratégie de groupe utilise pour obtenir la liste triée des objets de stratégie de groupe à appliquer à une configuration utilisateur. Au lieu que la configuration utilisateur soit déterminée par le nœud **Configuration** utilisateur des objets de stratégie de groupe limités en étendue à l'objet utilisateur, la configuration utilisateur peut être déterminée par les stratégies du nœud Configuration utilisateur des objets de stratégie de groupe limités en étendue à l'objet ordinateur.

Le paramètre de stratégie **Configurer le mode de traitement par boucle de la stratégie de groupe utilisateur**, situé dans le dossier **Configuration ordinateur\Stratégies\Modèles d'administration\Système\Stratégie de groupe** dans l'Éditeur de gestion des stratégies de groupe, peut être, comme tous les paramètres de stratégie, défini sur **Non configuré**, **Activé** ou **Désactivé**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

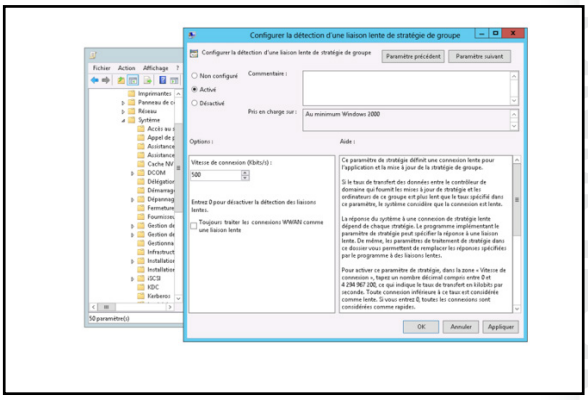
Lorsqu'elle est activée, la stratégie peut spécifier le mode **Remplacer** ou **Fusionner**:

- Remplacer. Dans ce cas, la liste d'objet de stratégie de groupe pour l'utilisateur est remplacée entièrement par la liste d'objet de stratégie de groupe déjà obtenue pour l'ordinateur au démarrage de l'ordinateur. Les paramètres contenus dans les stratégies de configuration utilisateur des objets de stratégie de groupe de l'ordinateur sont appliqués à l'utilisateur. Le mode **Remplacer** est utile dans une situation de classe où les utilisateurs doivent recevoir une configuration standard plutôt que la configuration appliquée à ces utilisateurs dans un environnement moins géré.
- Fusionner. Dans ce cas, la liste d'objet de stratégie de groupe pour l'ordinateur obtenue au démarrage de l'ordinateur est ajoutée à la liste des objets de stratégie de groupe obtenue pour l'utilisateur au moment de la connexion. Puisque la liste d'objet de stratégie de groupe obtenue pour l'ordinateur est appliquée ultérieurement, les paramètres dans les objets de stratégie de groupe sur la liste de l'ordinateur ont la priorité en cas de conflit avec des paramètres de la liste utilisateur. Ce mode est utile pour appliquer les paramètres supplémentaires aux configurations typiques des utilisateurs. Par exemple, vous pouvez permettre à un utilisateur de recevoir la configuration classique de l'utilisateur lors de l'ouverture de session sur un ordinateur situé dans une salle de conférence ou une zone d'accueil, mais vous remplacez le papier peint par une image bitmap standard et désactivez l'utilisation de certains périphériques ou applications.

Remarque : Notez que, lorsque vous combinez le traitement par boucle de rappel au filtrage de groupe de sécurité, l'application des paramètres utilisateur pendant l'actualisation de la stratégie utilise les informations d'identification de l'ordinateur pour déterminer les objets de stratégie de groupe à appliquer dans le cadre du traitement par boucle de rappel. Cependant, l'utilisateur connecté doit également posséder l'autorisation Appliquer la stratégie de groupe pour que l'objet de stratégie de groupe soit appliqué avec succès. Notez également que l'indicateur de traitement par boucle de rappel est configuré par session plutôt que par objet de stratégie de groupe.

Considérations pour les liaisons lentes et les systèmes déconnectés

Certains paramètres que vous pouvez configurer avec la stratégie de groupe peuvent être affectés par la vitesse de la liaison entre l'ordinateur de l'utilisateur et votre réseau de domaine. Par exemple, le déploiement du logiciel à l'aide des objets de stratégie de groupe n'est pas adapté aux liaisons plus lentes. En outre, il est important de prendre en compte l'effet des stratégies de groupe sur les ordinateurs déconnectés du réseau de domaine.



Liaisons lentes

Le client de stratégie de groupe traite la question des liaisons lentes en détectant la vitesse de connexion au domaine et en déterminant si la connexion doit être considérée comme une liaison lente. Cette détermination est alors utilisée par chaque extension CSE afin de décider d'appliquer ou non les paramètres. L'extension logicielle, par exemple, est configurée pour ignorer le traitement de stratégie, de sorte que le logiciel n'est pas installé si une liaison lente est détectée.

Remarque : Par défaut, une liaison est considérée lente s'elle a un débit inférieur à 500 kilobits par seconde (Kbits/s). Cependant, vous pouvez configurer ce seuil à un débit différent.

Si la stratégie de groupe détecte une liaison lente, elle paramètre un indicateur pour signaler la liaison aux extensions CSE. Ces dernières peuvent alors déterminer s'il est nécessaire de traiter les paramètres de stratégie de groupe applicables. Le tableau suivant décrit le comportement par défaut des extensions côté client.

Extension côté client	Traitement des liaisons lentes	Modification possible ?
Traitement de la stratégie du Registre	Actif	Non
Maintenance Internet Explorer	Inactif	Oui
Stratégie d'installation de logiciels	Inactif	Oui
Stratégie de redirection de dossiers	Inactif	Oui
Stratégie de scripts	Inactif	Oui
Stratégie de sécurité	Actif	Non
Stratégie IPsec (Internet Protocol Security)	Inactif	Oui
Stratégie sans fil	Inactif	Oui
Stratégie de récupération du système de fichiers EFS	Actif	Oui
Stratégie de quota de disque	Inactif	Oui

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Ordinateurs déconnectés

Si un utilisateur travaille sans être connecté au réseau, les paramètres précédemment appliqués par la stratégie de groupe demeurent en vigueur. De cette manière, l'expérience d'un utilisateur est identique, indépendamment de sa connexion au réseau. Il existe des exceptions à la règle, dont notamment le fait que les scripts de démarrage, d'ouverture de session, de fermeture de session et d'arrêt ne s'exécutent pas si l'utilisateur est déconnecté.

Si un utilisateur distant se connecte au réseau, le client de stratégie de groupe sort de veille et détermine si une fenêtre d'actualisation de stratégie de groupe a été manquée. Si tel est le cas, il exécute une actualisation de stratégie de groupe pour obtenir les derniers objets de stratégie de groupe du domaine. Encore une fois, les extensions CSE déterminent, selon leurs paramètres de traitement de stratégie, si les paramètres de ces objets de stratégie de groupe sont appliqués.

Remarque : Ce processus ne s'applique pas aux systèmes Windows XP ou Windows Server 2003. Il s'applique uniquement à Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows 7, Windows 8 et Windows Server 2012.

Identification du moment où les paramètres entrent en vigueur

Plusieurs processus doivent être effectués avant que les paramètres de stratégie de groupe ne soient réellement appliqués à un utilisateur ou à un ordinateur. Cette rubrique présente ces processus.

- La réplication de l'objet de stratégie de groupe doit avoir lieu
- Les modifications apportées au groupe doivent être répliquées
- La stratégie de groupe doit être actualisée
- L'utilisateur doit fermer ou ouvrir une session, ou l'ordinateur doit être redémarré
- Actualisation manuelle
- La plupart de CSE ne réappliquent pas les paramètres de l'objet de stratégie de groupe inchangés

La réplication de l'objet de stratégie de groupe doit avoir lieu

Avant qu'un objet de stratégie de groupe ne puisse entrer en vigueur, le conteneur Stratégie de groupe dans Active Directory doit être répliqué sur le contrôleur de domaine à partir duquel le client de stratégie de groupe obtient sa liste triée d'objets de stratégie de groupe. En outre, le modèle de stratégie de groupe du volume SYSVOL doit répliquer sur le même contrôleur de domaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les modifications apportées au groupe doivent être incorporées

Enfin, si vous avez ajouté un nouveau groupe ou avez modifié l'appartenance d'un groupe utilisé pour filtrer l'objet de stratégie de groupe, cette modification doit également être répliquée. En outre, la modification doit être dans le jeton de sécurité de l'ordinateur et de l'utilisateur, ce qui nécessite un redémarrage (pour que l'ordinateur mette à jour son appartenance de groupe) ou une fermeture de session, puis une ouverture de session (pour que l'utilisateur mette à jour son appartenance de groupe).

L'actualisation de la stratégie de groupe de l'utilisateur ou de l'ordinateur doit avoir lieu

L'actualisation a lieu au démarrage (pour les paramètres de l'ordinateur), à l'ouverture de session (pour les paramètres de l'utilisateur) et toutes les 90 à 120 minutes ensuite, par défaut.

Remarque : Gardez à l'esprit que l'incidence pratique de l'intervalle d'actualisation de la stratégie de groupe est la suivante : lorsque vous apportez une modification à votre environnement, l'entrée en vigueur de la modification prend, en moyenne, deux fois moins de temps, soit 45 à 60 minutes.

Par défaut, les clients Windows XP, Windows Vista, Windows 7, et Windows 8 exécutent uniquement des actualisations en tâche de fond au démarrage et à l'ouverture de session, ce qui signifie qu'un client peut démarrer et qu'un utilisateur peut se connecter sans recevoir les dernières stratégies du domaine. Nous vous recommandons fortement de modifier ce comportement par défaut de sorte que les modifications de stratégie soient implémentées de façon gérée et prévisible. Activez le paramètre de stratégie **Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session pour tous les clients Windows**. Le paramètre est situé dans **Configuration de l'ordinateur\Stratégies\Modèles d'administration\Système\Ouverture de session**. Veillez à lire le texte explicatif du paramètre de stratégie. Notez que cette modification n'affecte pas la durée de démarrage ou d'ouverture de session pour les ordinateurs qui ne sont pas connectés à un réseau. Si l'ordinateur détecte qu'il est déconnecté, il « n'attend pas » un réseau.

Ouverture de session ou redémarrage

Bien que la plupart des paramètres soient appliqués pendant une actualisation de stratégie en arrière-plan, certaines extensions CSE n'appliquent pas le paramètre jusqu'à l'événement suivant de démarrage ou d'ouverture de session. Par exemple, les stratégies de script de démarrage et d'ouverture de session nouvellement ajoutées ne fonctionnent pas tant que l'ordinateur n'a pas été redémarré ou qu'une nouvelle session n'a pas été ouverte. L'installation logicielle a lieu au démarrage suivant si le logiciel est attribué dans les paramètres de l'ordinateur. Les modifications des stratégies de redirection de dossiers entrent pas en vigueur à l'ouverture de session suivante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Actualiser manuellement la stratégie de groupe

Lorsque vous expérimentez avec le traitement de stratégie de groupe dépannage de la stratégie de groupe, vous pouvez avoir besoin d'initialiser une actualisation de stratégie de groupe manuelle de sorte à ne pas avoir à attendre l'actualisation en tâche de fond suivante. Vous pouvez utiliser la commande **GPUpdate** pour initier une actualisation de la stratégie de groupe. Utilisée seule, cette commande déclenche un traitement identique à une actualisation de stratégie de groupe en tâche de fond. La stratégie d'ordinateur et la stratégie d'utilisateur sont toutes deux actualisées. Utilisez le paramètre **/target:computer** ou **/target:user** pour limiter l'actualisation aux paramètres de l'ordinateur ou de l'utilisateur, respectivement. Pendant l'actualisation en tâche de fond, par défaut, des paramètres sont appliqués uniquement si l'objet de stratégie de groupe a été mis à jour. Le commutateur **/force** fait en sorte que le système réapplique tous les paramètres de l'ensemble des objets de stratégie de groupe limités en étendue à l'utilisateur ou à l'ordinateur. Certains paramètres de stratégie requièrent une fermeture de session ou un redémarrage avant d'entrer réellement en vigueur. Les commutateurs **/logoff** et **/boot** de **GPUpdate** causent une fermeture de session ou un redémarrage, respectivement. Vous pouvez utiliser ces commutateurs lorsque vous appliquez des paramètres qui nécessitent une fermeture de session ou un redémarrage.

Par exemple, la commande qui provoque une actualisation totale de l'application, et, s'il y a lieu, le redémarrage et l'ouverture de session pour appliquer des paramètres de stratégie mis à jour est :

```
gpupdate /force /logoff /boot
```

La plupart des extensions CSE ne réappliquent pas les paramètres si l'objet de stratégie de groupe n'a pas changé

Gardez à l'esprit que la plupart des extensions CSE appliquent les paramètres d'un objet de stratégie de groupe uniquement si celui-ci a changé. Cela signifie que, si un utilisateur peut modifier un paramètre spécifié initialement par la stratégie de groupe, le paramètre ne sera pas ramené en conformité aux paramètres spécifiés par l'objet de stratégie de groupe tant que l'objet de stratégie de groupe n'a pas changé. Heureusement, la plupart des paramètres de stratégie ne peuvent pas être modifiés par un utilisateur sans privilèges. Cependant, si un utilisateur est un administrateur de son ordinateur, ou si le paramètre de stratégie affecte une partie du registre ou du système que l'utilisateur l'autorisation de modifier, cela peut devenir un réel problème.

Vous pouvez demander à chaque extension CSE de réappliquer les paramètres des objets de stratégie de groupe, même si ceux-ci n'ont pas été modifiés. Le comportement de traitement de chaque extension CSE peut être configuré dans les paramètres de stratégie figurant sous Configuration de l'ordinateur\Modèles d'administration\Système\Stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Dépanner l'application des objets de stratégie de groupe

Avec l'interaction de nombreux paramètres dans plusieurs objets de stratégie de groupe limités en étendue à l'aide d'un large choix de méthodes, l'application de stratégie de groupe peut être complexe à analyser et à comprendre. Par conséquent, vous devez être équipé pour évaluer et dépanner efficacement votre implémentation de stratégie de groupe, identifier les problèmes potentiels avant qu'ils surgissent et résoudre les difficultés imprévues. Windows Server fournit des outils indispensables à la prise en charge de la stratégie de groupe. Dans cette leçon, vous explorerez l'utilisation de ces outils dans des scénarios de dépannage et de support technique proactifs et réactifs.

Objectifs de la leçon

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

- Décrire comment actualiser les objets de stratégie de groupe sur un ordinateur client.
- Analyser l'ensemble des objets de stratégie de groupe et des paramètres de stratégie appliqués à un utilisateur ou à un ordinateur.
- Générer des rapports de jeu de stratégie résultant (RSoP) pour contribuer à l'analyse des paramètres de l'objet de stratégie de groupe.
- Modéliser proactivement l'incidence des modifications de la stratégie de groupe ou Active Directory sur le RSOP.
- Localiser les journaux des événements contenant les événements relatifs à la stratégie de groupe.

Actualisation des objets de stratégie de groupe

Les paramètres de configuration de l'ordinateur sont appliqués au démarrage, puis actualisés à intervalles réguliers. Tous les scripts de démarrage sont exécutés au démarrage de l'ordinateur. L'intervalle par défaut est de 90 minutes, mais il est configurable. L'exception à l'intervalle défini concerne les contrôleurs de domaine, dont les paramètres sont actualisés toutes les cinq minutes.

- Quand vous appliquez des objets de stratégie de groupe, souvenez-vous de ce qui suit :
  - Les paramètres de l'ordinateur s'appliquent au démarrage
  - Les paramètres utilisateur s'appliquent à la connexion
  - Les stratégies sont actualisées à intervalles réguliers et configurables
  - Les paramètres de sécurité sont actualisés au moins toutes les 16 heures
  - Les stratégies sont actualisées manuellement en utilisant :
    - La commande **Gpupdate**
    - L'applet de commande Windows PowerShell **Invoke-Gpupdate**
  - Avec la nouvelle fonctionnalité d'actualisation des stratégies à distance dans Windows Server 2012, vous pouvez actualiser les stratégies à distance

Les paramètres utilisateur sont appliqués à l'ouverture de session et actualisés à intervalles réguliers er configurables ; la valeur par défaut est également de 90 minutes. Tous les scripts d'ouverture de session sont exécutés à l'ouverture de la session.

Remarque : Divers paramètres utilisateur requièrent deux ouvertures de session avant que l'utilisateur perçoive l'effet de l'objet de stratégie de groupe. Cela est dû au fait que les utilisateurs ouvrant une session sur le même ordinateur utilisent des informations d'identification mises en cache pour accélérer les ouvertures de session. Cela signifie que, bien que les paramètres de stratégie soient fournis à l'ordinateur, l'utilisateur est déjà connecté et les paramètres n'entreront donc pas en vigueur avant l'ouverture de session suivante. Le paramètre de redirection de dossier en est un exemple.

Vous pouvez modifier l'intervalle d'actualisation en configurant un paramètre de stratégie de groupe. Pour les paramètres de l'ordinateur, le paramètre d'intervalle d'actualisation se trouve dans le nœud **Configuration de l'ordinateur\Stratégies\Modèles d'administration\Système\Stratégie de groupe**. Pour les paramètres utilisateurs, l'intervalle d'actualisation se trouve dans les paramètres correspondants sous la Configuration utilisateur. Les paramètres de sécurité constituent une exception à l'intervalle d'actualisation. La section paramètres de sécurité de la stratégie de groupe est actualisée au moins toutes les 16 heures, indépendamment de l'intervalle défini pour l'intervalle d'actualisation.

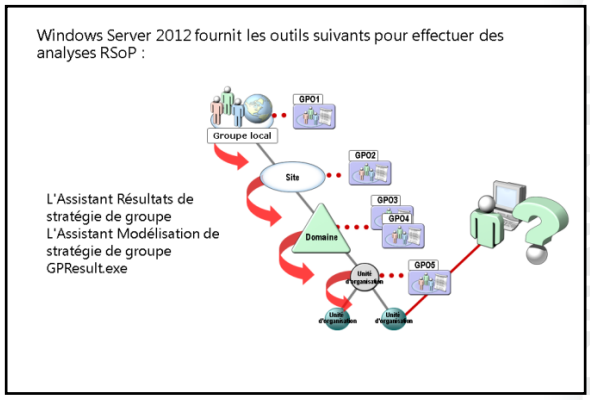
Vous pouvez également actualiser la stratégie de groupe manuellement. L'utilitaire de ligne de commande **Gpupdate** actualise et fournit toutes les nouvelles configurations de stratégie de groupe. La commande **Gpupdate /force** actualise tous les paramètres de stratégie de groupe. Il existe également un nouvel applet de commande Windows PowerShell **Invoke-Gpupdate**, qui remplit la même fonction.

L'Actualisation des stratégies à distance est une nouvelle fonctionnalité de Windows Server 2012. Cette fonctionnalité permet aux administrateurs d'utiliser la console GPMC pour cibler une unité d'organisation et forcer l'actualisation de la stratégie de groupe sur tous ses ordinateurs et utilisateurs actuellement connectés. Pour ce faire, cliquez avec le bouton droit sur n'importe quelle unité d'organisation, puis cliquez sur **Mise à jour de la stratégie de groupe**. La mise à jour se produit dans un délai de 10 minutes.

Remarque : Parfois, l'échec de l'application d'un objet de stratégie de groupe résulte des problèmes au niveau de la technologie sous-jacente responsable de la réplication d'AD DS et du volume SYSVOL. Dans Windows Server 2012, vous pouvez afficher l'état de réplication à l'aide de **Gestion des stratégies de groupe**, en sélectionnant le nœud **Domaine**, en cliquant sur l'onglet **État**, puis en cliquant sur **Détecter**.

Jeu de stratégie résultant

L'héritage des stratégies de groupe, les filtres et les exceptions sont complexes, et il est souvent difficile de déterminer les paramètres de stratégie à appliquer.



RSoP est l'effet net des objets de stratégie de groupe appliqués à un utilisateur ou à un ordinateur, compte tenu des liaisons de l'objet de stratégie de groupe, des exceptions, telles que Appliqué et Bloquer l'héritage, et l'application de la sécurité et des filtres WMI.

RSoP constitue également une collection d'outils qui vous permettent d'évaluer, de modéliser et de dépanner l'application des paramètres de stratégie de groupe. RSoP peut interroger un ordinateur local ou distant, puis générer un rapport sur les paramètres précis appliqués à l'ordinateur et aux utilisateurs connectés à l'ordinateur. RSoP peut également modéliser les paramètres de stratégie prévus pour être appliqués à un utilisateur ou à un ordinateur dans divers scénarios, notamment le déplacement de l'objet entre des unités d'organisation ou des sites, ou la modification de l'appartenance de groupe de l'objet. Avec ces fonctions, RSoP peut vous aider à gérer et à dépanner les stratégies conflictuelles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

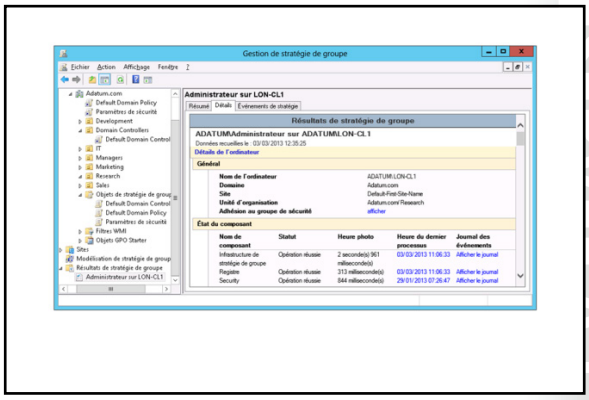
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Windows Server 2012 fournit les outils suivants pour effectuer des analyses RSoP :

- L'Assistant Résultats de stratégie de groupe
- L'Assistant Modélisation de stratégie de groupe
- GPResult.exe

Générer des rapports RSoP

Pour vous aider à analyser l'effet cumulatif des objets de stratégie de groupe et des paramètres de stratégie sur un utilisateur ou un ordinateur dans votre organisation, la console GPMC comprend l'Assistant Résultats de stratégie de groupe. Si vous souhaitez comprendre exactement quels paramètres de stratégie sont appliqué à un utilisateur ou à un ordinateur, et pour quelles raisons, l'Assistant Résultats de stratégie de groupe est l'outil à utiliser.



Générer des rapports RSoP avec l'Assistant Résultats de stratégie de groupe

L'Assistant Résultats de stratégie de groupe peut atteindre le fournisseur WMI sur un ordinateur local ou distant qui exécute Windows Vista ou une version plus récente. Le fournisseur WMI peut signaler tout ce qu'il y à savoir sur la manière dont la stratégie de groupe a été appliquée au système. Il sait à quel moment le traitement a eu lieu, quels objets de stratégie de groupe ont été appliqués, quels objets de stratégie de groupe n'ont pas été appliqués et pourquoi, les erreurs rencontrées, et les paramètres de stratégie précis qui ont pris la priorité ainsi que leur objet de stratégie de groupe source.

Il existe plusieurs exigences pour l'exécution de l'Assistant Résultats de stratégie de groupe, notamment :

- L'ordinateur cible doit être en ligne.
- Vous devez posséder des informations d'identification de l'administrateur sur l'ordinateur cible.
- L'ordinateur cible doit exécuter Windows XP ou une version plus récente. L'Assistant Résultats de stratégie de groupe ne peut pas accéder aux systèmes Windows 2000.
- Vous devez pouvoir accéder à WMI sur l'ordinateur cible. Cela signifie que l'ordinateur doit être en ligne, connecté au réseau et accessible par les ports 135 et 445.

Remarque : L'exécution de l'analyse de RSoP à l'aide de l'Assistant Résultats de stratégie de groupe n'est qu'un exemple d'administration à distance. Pour exécuter l'administration à distance, vous devez configurer des règles de trafic entrant pour le pare-feu utilisé par vos clients et serveurs.

- Le service WMI doit être démarré sur l'ordinateur cible.
- Si vous souhaitez analyser RSoP pour un utilisateur, cet utilisateur doit s'être connecté au moins une fois à l'ordinateur. Il n'est cependant pas nécessaire que l'utilisateur soit actuellement connecté.

Une fois que vous avez vérifié que les exigences sont satisfaites, vous êtes prêt à exécuter une analyse de RSoP.

Pour exécuter un rapport RSoP, cliquez avec le bouton droit sur **Résultats de stratégie de groupe** dans l'arborescence de la console GPMC, puis cliquez sur **Assistant Résultats de stratégie de groupe.**

L'Assistant vous invite à sélectionner un ordinateur. Il se connecte alors au fournisseur WMI sur cet ordinateur, et fournit une liste des utilisateurs qui y sont connectés. Vous pouvez alors sélectionner l'un des utilisateurs, ou vous pouvez ignorer l'analyse RSoP pour les stratégies de configuration utilisateur.

L'Assistant génère un rapport RSoP détaillé au format DHTML. Si la configuration de sécurité renforcée d'Internet Explorer est définie, vous êtes invité à autoriser la console à afficher le contenu dynamique. Vous pouvez développer ou réduire chaque section du rapport en cliquant sur le lien Afficher ou Masquer, ou en double-cliquant sur le titre de la section.

Le rapport est affiché sur trois onglets :

- Résumé. L'onglet **Résumé** affiche l'état de traitement de la stratégie de groupe lors de la dernière actualisation. Vous pouvez identifier les informations recueillies sur le système, les objets de stratégie de groupe appliqués et refusés, l'appartenance au groupe de sécurité qui pourrait avoir affecté des objets de stratégie de groupe filtrés avec les groupes de sécurité, les filtres WMI analysés, et l'état des extensions CSE.
- Paramètres. L'onglet **Paramètres** affiche les paramètres de jeu de stratégie résultant appliqués à l'ordinateur ou à l'utilisateur. Cet onglet vous montre exactement ce qui est arrivé à l'utilisateur suite aux effets de votre implémentation de stratégie de groupe. Vous pouvez apprendre énormément d'informations grâce à l'onglet **Paramètres**, même si certaines données ne sont pas prises en compte, notamment les paramètres IPsec, sans fil et de stratégie de quota de disque.
- Événements de stratégie. L'onglet **Événements de stratégie** affiche des événements de stratégie de groupe à partir des journaux d'événements de l'ordinateur cible.

Après avoir généré un rapport RSoP à l'aide de l'Assistant Résultats de stratégie de groupe, vous pouvez cliquer avec le bouton droit sur ce rapport pour exécuter de nouveau la requête, imprimer le rapport ou enregistrer le rapport comme fichier XML ou fichier HTML qui conserve le développement et la réduction dynamiques des sections. Vous pouvez ouvrir les deux types de fichier avec Internet Explorer ; le rapport RSoP est donc portable hors de la console GPMC.

Si vous cliquez avec le bouton droit le nœud du rapport lui-même, dans le dossier Résultats de stratégie de groupe dans l'arborescence de la console, vous pouvez alors basculer vers **Affichage avancé**. Dans Affichage avancé, RSoP est affiché à l'aide du composant logiciel enfichable RSoP qui indique tous les paramètres appliqués, notamment les stratégies IPsec, sans fil et de quota de disque.

Générer les rapports RSoP avec GPResult.exe

La commande **GPResult.exe** est la version ligne de commande de l'Assistant Résultats de stratégie de groupe. GPResult puise dans le même fournisseur WMI que l'Assistant, génère les mêmes informations et vous permet, au demeurant, de créer les mêmes rapports graphiques. GPResult fonctionne uniquement sur Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008 et Windows Server 2012.

 **Remarque :** Windows 2000 comprend une commande **GPResult.exe**, qui génère un rapport limité du traitement de la stratégie de groupe. Cependant, elle n'est pas aussi sophistiquée que la commande incluse dans les versions Windows récentes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous exécutez la commande GPResult, vous êtes susceptible d'utiliser les options suivantes :

```
/scomputername
```

Cette option spécifie le nom ou l'adresse IP d'un système distant. Si vous utilisez un point (.) comme nom d'ordinateur ou n'incluez pas l'option /s, l'analyse RSoP est exécutée sur l'ordinateur local :

```
/scope [user | computer]
```

Cette commande affiche l'analyse RSoP des paramètres utilisateur ou ordinateur. Si vous omettez l'option /scope, l'analyse RSoP comprend les paramètres utilisateur et ordinateur :

```
/userusername
```

Cette commande spécifie le nom de l'utilisateur dont vous souhaitez afficher les données RSoP.

```
/r
```

Cette option affiche un résumé des données RSoP :

```
/v
```

Cette option affiche les données RSoP détaillées, qui présentent les informations les plus significatives :

```
/z
```

Cela affiche les données très détaillées, notamment les détails de tous les paramètres de stratégie appliqués au système. Vous n'avez généralement pas besoin de toutes ces informations pour le dépannage typique de la stratégie de groupe :

```
/udomain\user/ppassword
```

Cette commande fournit les informations d'identification qui se trouvent dans le groupe Administrateurs d'un système distant. Sans ces informations d'identification, **GPResult** s'exécute à l'aide des informations d'identification avec lesquelles vous êtes connecté :

```
[/x | /h] filename
```

Cette option enregistre les rapports sous format XML ou HTML. Ces options sont disponibles dans le Service Pack 1 de Windows Vista (SP1) et versions plus récentes, Windows Server 2008 et versions plus récentes, Windows 7, et Windows 8.

Dépannage de la stratégie de groupe avec l'Assistant Résultats de stratégie de groupe ou GPResult.exe

En tant qu'administrateur, vous êtes susceptible de rencontrer des scénarios qui requièrent le dépannage des stratégies de groupe. Vous pouvoir avoir à diagnostiquer et résoudre des problèmes, notamment :

- Les objets de stratégie de groupe ne sont pas appliqués du tout.
- Le jeu de stratégies résultant pour un ordinateur ou un utilisateur n'est pas ce qui a été prévu.

L'Assistant Résultats de stratégie de groupe et **GPResult.exe** offrent souvent l'analyse la plus précieuse des problèmes de traitement et d'application des stratégies de groupe. Souvenez-vous que ces outils examinent le fournisseur WMI RSoP pour fournir un rapport exact des événements d'un système. L'examen du rapport RSoP vous indique souvent les objets de stratégie de groupe limités en étendue de manière incorrecte ou les erreurs de traitement de la stratégie qui ont empêché l'application des paramètres de l'objet de stratégie de groupe.

Démonstration : Procédure d'exécution de l'analyse de scénarios avec l'Assistant Modélisation de stratégie de groupe

Si vous déplacez un ordinateur ou un utilisateur entre les sites, les domaines ou les unités d'organisation, ou si modifiez son appartenance de groupe de sécurité, les objets de stratégie de groupe limités en étendue à cet utilisateur ou ordinateur seront modifiés. Par conséquent, le RSoP pour l'ordinateur ou l'utilisateur sera différent. Le RSoP changera également si la liaison est lente ou si le traitement par boucle de rappel a lieu, ou s'il y a une modification d'une caractéristique système ciblée par un filtre WMI.

Avant d'apporter l'une de ces modifications, vous devez évaluer l'impact potentiel d'un utilisateur ou un ordinateur sur le RSoP. L'Assistant Résultats de stratégie de groupe peut exécuter l'analyse RSoP uniquement sur ce qui s'est produit réellement. Pour prédire l'avenir et effectuer les analyses de scénarios, vous pouvez utiliser l'Assistant Modélisation de stratégie de groupe.

Pour effectuer une modélisation de stratégie de groupe, cliquez avec le bouton droit sur le nœud **Modélisation de stratégie de groupe** dans l'arborescence de la console GPMC, cliquez sur l'Assistant Modélisation de stratégie de groupe, puis suivez les étapes indiquées dans l'Assistant.

La modélisation est effectuée à l'aide d'une simulation sur un contrôleur de domaine ; vous êtes ainsi d'abord invité à sélectionner un contrôleur de domaine. Vous n'avez pas besoin d'être connecté localement au contrôleur de domaine, mais la requête de modélisation sera effectuée sur le contrôleur de domaine. Vous êtes alors invité à spécifier les paramètres de la simulation, notamment à :

- Sélectionner un objet utilisateur ou ordinateur à évaluer, ou à spécifier l'unité d'organisation, le site ou le domaine à évaluer.
- Indiquer si le traitement de liaison lente doit être simulé.
- Spécifier si vous souhaitez simuler le traitement par boucle de rappel et, si oui, à sélectionner le mode **Remplacer ou Fusionner**.
- Sélectionner un site à simuler.
- Sélectionner les groupes de sécurité pour l'utilisateur et pour l'ordinateur.
- Sélectionner les filtres WMI à appliquer dans la simulation du traitement de stratégie utilisateur et ordinateur.

Une fois que vous avez spécifié les paramètres de la simulation, un rapport très similaire à celui des résultats de stratégie de groupe présenté précédemment est généré. L'onglet **Résumé** montre une vue d'ensemble des objets de stratégie de groupe qui seront traités, et l'onglet **Paramètres** détaille les paramètres de stratégie qui seront appliqués à l'utilisateur ou à l'ordinateur. Ce rapport peut lui aussi être enregistré en cliquant dessus avec le bouton droit, puis en sélectionnant **Enregistrer le rapport**.

Demonstration

Cette démonstration montre comment :

- exécuter **GPResult.exe** à partir de l'invite de commandes ;
- exécuter **GPResult.exe** à partir de l'invite de commandes, puis exporter les résultats vers un fichier HTML ;
- ouvrir la console GPMC ;
- exécuter l'Assistant Création de rapport de stratégie de groupe, puis afficher les résultats ;
- exécuter l'Assistant Modélisation de stratégie de groupe, puis afficher les résultats.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

Utiliser GPResult.exe pour créer un rapport

1. Sur l'ordinateur LON-DC1, ouvrez une invite de commandes.
2. Exécutez les commandes suivantes :

```
Gpresult /t
Gpresult /h results.html
```

3. Ouvrez le rapport results.html dans Internet Explorer, puis examinez le rapport.

Créer un rapport à l'aide de l'Assistant Création de rapport de stratégie de groupe

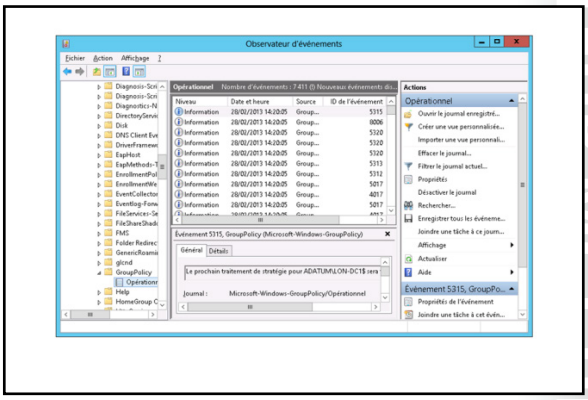
1. Fermez l'invite de commandes, puis ouvrez la console Gestion des stratégies de groupe.
2. Dans le nœud **Résultats de stratégie de groupe**, lancez l'Assistant Résultats de stratégie de groupe.
3. Remplissez l'Assistant à l'aide des valeurs par défaut.
4. Examinez le rapport, puis enregistrez-le au bureau.

Créer un rapport à l'aide de l'Assistant Modélisation de stratégie de groupe

1. À partir du nœud **Modélisation de stratégie de groupe**, lancez l'Assistant **Modélisation de stratégie de groupe**.
2. Spécifiez l'utilisateur du rapport comme Ed Meadows et le conteneur d'ordinateur comme l'unité d'organisation informatique.
3. Renseignez l'Assistant en utilisant les valeurs par défaut, puis examinez le rapport.
4. Fermez la console Gestion des stratégies de groupe.

Examiner les journaux des événements de stratégie

Windows Vista, Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012 améliorent votre capacité à dépanner la stratégie de groupe, non seulement grâce aux outils RSoP, mais également grâce à la journalisation améliorée des événements de stratégie de groupe, notamment :



- Le journal système, où vous trouverez des informations de haut niveau sur la stratégie de groupe, y compris les erreurs créées par le client de stratégie de groupe lorsqu'il ne peut pas se connecter à un contrôleur de domaine ou localiser des objets de stratégie de groupe.
- Le journal des applications, qui capture des événements enregistrés par les extensions CSE.
- Le journal des opérations de stratégie de groupe, qui fournit des informations détaillées sur le traitement de stratégie de groupe.

Pour rechercher des journaux de stratégie de groupe, ouvrez le composant logiciel enfichable Observateur d'événements ou la console. Les journaux système et d'applications se trouvent dans le nœud **Journaux Windows**. Le journal des opérations de stratégie de groupe se trouve dans

Journaux des applications et services\Microsoft \Windows\GroupPolicy\Opérations.

Atelier pratique : Implémentation d'une infrastructure de stratégie de groupe

Scénario

A. Datum est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à Londres pour assister le bureau de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

Vous avez été invité à utiliser la stratégie de groupe pour implémenter des paramètres de sécurité standardisés afin de verrouiller des écrans d'ordinateur lorsque les utilisateurs laissent des ordinateurs sans surveillance pendant 10 minutes ou plus. Vous devez également configurer un paramètre de stratégie qui empêche l'accès à certains programmes sur les stations de travail locales.

Après un certain temps, il vous a été signalé qu'une application critique échoue au démarrage de l'économiseur d'écran, et un ingénieur vous a demandé d'empêcher que le paramètre ne s'applique à l'équipe d'ingénieurs de recherche qui utilise l'application quotidiennement. Vous avez été invité également à configurer des ordinateurs de la salle de conférence de sorte qu'ils utilisent un délai d'expiration de 45 minutes.

Après la création des stratégies, vous devez évaluer le jeu de stratégies résultant pour les utilisateurs dans votre environnement afin de vérifier que l'infrastructure de stratégie de groupe est optimisée et que toutes les stratégies sont appliquées comme prévu.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- Créer et configurer un objet de stratégie de groupe.
- gérer l'étendue de la stratégie de groupe ;
- Résoudre les problèmes liés à l'application de la stratégie de groupe.
- Gérer les objets de stratégie de groupe.

Configuration de l'atelier pratique

Durée approximative : 90 minutes

Ordinateur(s) virtuel(s)	22411B-LON-DC1 22411B-LON-CL1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.

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 : **Administrateur**
   b. Mot de passe : **Pa$$w0rd**
   c. Domaine : **Adatum**
5. Répétez les étapes 2 et 3 pour **22411B-LON-CL1**. Ne vous connectez pas à LON-CL1 tant qu'il ne vous a pas été demandé de le faire.

Exercice 1 : Création et configuration d'objets de stratégie de groupe

Scénario

Vous avez été invité à utiliser la stratégie de groupe pour implémenter des paramètres de sécurité standardisés afin de verrouiller des écrans d'ordinateur lorsque les utilisateurs laissent des ordinateurs sans surveillance pendant 10 minutes ou plus. Vous devez également configurer un paramètre de stratégie qui empêche les utilisateurs d'exécuter l'application Bloc-notes sur les postes de travail locaux.

Les tâches principales de cet exercice sont les suivantes :

1. Créer et modifier un objet de stratégie de groupe.
2. Lier l'objet de stratégie de groupe ;
3. Afficher les effets des paramètres de l'objet de stratégie de groupe.

▶ Tâche 1 : Créer et modifier un objet de stratégie de groupe

1. Sur LON-DC1, dans le Gestionnaire de serveur, ouvrez la console de gestion des stratégies de groupe.
2. Créez un objet de stratégie de groupe appelé **Normes ADATUM** dans le conteneur **Objets de stratégie de groupe**.
3. Modifiez la stratégie **Normes ADATUM**, puis naviguez vers **Configuration utilisateur**, **Stratégies**, **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordenateur local**, **Système**.
4. Empêchez les utilisateurs d'exécuter **notepad.exe** en configurant le paramètre de stratégie de **Ne pas exécuter les applications Windows spécifiées**.
5. Naviguez jusqu'au dossier **Configuration utilisateur, Stratégies**, **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordenateur local**, **Panneau de configuration**, **Personnalisation**, puis configurez la stratégie **Dépassement du délai d'expiration de l'écran de veille** sur **600 secondes**.
6. Activez le paramètre de stratégie **Un mot de passe protège l'écran de veille**, puis fermez la fenêtre Éditeur de gestion des stratégies de groupe.

▶ Tâche 2 : Lier l'objet de stratégie de groupe

- Liez l'objet de stratégie de groupe **Normes ADATUM** au domaine **Adatum.com**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Afficher les effets des paramètres de l'objet de stratégie de groupe

1. Ouvrez une session sur LON-CL1 en tant que **ADATUM\Pat** avec le mot de passe **Pa$$w0rd**.
2. Tentez de modifier les paramètres de temps d'attente et de reprise de l'écran de veille. La stratégie de groupe vous en empêche.
3. Tentez d'exécuter le **Bloc-notes**. La stratégie de groupe vous en empêche.

Résultats : À la fin de cet exercice, vous devez avoir correctement créé, modifié et lié les objets de stratégie de groupe requis.

Exercice 2 : Gestion de l'étendue des objets de stratégie de groupe

Scénario

Après un certain temps, vous êtes informé qu'une application critique utilisée par l'équipe technique de recherche échoue au démarrage de l'écran de veille. Vous avez été invité à empêcher le paramètre de l'objet de stratégie de groupe de s'appliquer aux membres du groupe de sécurité Ingénierie. Vous avez été également invité à configurer des ordinateurs de salle de conférence de sorte que la stratégie d'entreprise ne s'y applique pas. Cependant, un délai d'activation de l'écran de veille de 45 minutes doit toujours s'y appliquer.

Les tâches principales de cet exercice sont les suivantes :

1. Créer et lier les objets de stratégie de groupe requis.
2. Vérifier l'ordre de priorité.
3. Configurer l'étendue d'un objet de stratégie de groupe avec le filtrage de sécurité.
4. Configurez le traitement par boucle de rappel.

▶ Tâche 1 : Créer et lier les objets de stratégie de groupe requis.

1. Sur LON-DC1, ouvrez **Utilisateurs et ordinateurs Active Directory** et dans l'unité d'organisation **Research**, créez une sous-unité d'organisation appelée **Ingénieurs**, puis fermez les utilisateurs et les ordinateurs Active Directory.
2. Dans la console Gestion des stratégies de groupe, créez un nouvel objet de stratégie de groupe lié à l'unité d'organisation **Ingénieurs** appelé **Remplacement de l'application d'ingénierie**.
3. Configurez le paramètre de stratégie **Dépassement du délai d'expiration de l'écran de veille** sur **Désactivé**, puis fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 2 : Vérifier l'ordre de priorité

- Dans l'arborescence de la console Gestion des stratégies de groupe, sélectionnez l'unité d'organisation **Ingénieurs**, puis cliquez sur l'onglet **Héritage de stratégie de groupe**. Vous constatez que l'objet de stratégie de groupe Remplacement d'application d'ingénierie a la priorité sur l'objet de stratégie de groupe Normes ADATUM. Le paramètre de stratégie de délai d'expiration de l'écran de veille que vous venez de configurer dans l'objet de stratégie de groupe Remplacement d'application d'ingénierie sera appliqué après le paramètre dans l'objet de stratégie de groupe Normes ADATUM. Par conséquent, le nouveau paramètre remplacera le paramètre de normes et *l'emportera*. Le délai d'expiration de l'écran de veille sera désactivé pour les utilisateurs couverts par l'étendue de l'objet de stratégie de groupe Remplacement d'application d'ingénierie.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer l'étendue d'un objet de stratégie de groupe avec le filtrage de sécurité

1. Sur LON-DC1, ouvrez **Utilisateurs et ordinateurs Active Directory**. Dans l'unité d'organisation **Research\Ingénieurs**, créez un groupe de sécurité global appelé **Application GPO_Engineering Override_Apply**.
2. Dans la console **Gestion des stratégies de groupe**, sélectionnez l'objet de stratégie de groupe **Remplacement d'application d'ingénierie**. Vous constatez que dans la section de filtrage de sécurité, l'objet de stratégie de groupe s'applique par défaut à tous les utilisateurs authentifiés. Configurez l'objet de stratégie de groupe de sorte qu'il s'applique uniquement au groupe **Application GPO_Engineering Override_Apply**.
3. Dans le dossier **Users**, créez un groupe de sécurité global appelé **GPO_ADATUM Standards_Exempt**.
4. Dans la console Gestion de stratégie de groupe, sélectionnez l'objet de stratégie de groupe **Normes ADATUM**. Vous constatez que dans la section de filtrage de sécurité, l'objet de stratégie de groupe s'applique par défaut à tous les utilisateurs authentifiés.
5. Configurez la délégation de l'objet de stratégie de groupe afin de refuser l'application de la stratégie de groupe au groupe **GPO_ADATUM Standards_Exempt**.

▶ Tâche 4 : Configurer le traitement par boucle de rappel

1. Sur LON-DC1, basculez vers **Utilisateurs et ordinateurs Active Directory**.
2. Créez une nouvelle unité d'organisation appelée **Bornes**.
3. Sous Bornes, créez une sous-unité d'organisation appelée **Salles de conférence**.
4. Basculez vers la console Gestion de stratégie de groupe.
5. Créez un nouvel objet de stratégie de groupe appelé **Stratégies de salle de conférence** et liez-le à l'unité d'organisation **Bornes\Salles de conférence**.
6. Confirmez que l'objet de stratégie de groupe **Stratégies de salle de conférence** est limité en étendue à **Utilisateurs authentifiés**.
7. Modifiez l'objet de stratégie de groupe **Stratégies de salle de conférence** et modifiez la stratégie **Dépassement du délai d'expiration de l'écran de veille** de sorte à activer l'écran de veille après **45 minutes**.
8. Modifiez le paramètre de stratégie **Configurer le mode de traitement par boucle de la stratégie de groupe utilisateur** de sorte qu'il utilise le mode **Fusionner**.

Résultats : À la fin de cet exercice, vous devez avoir correctement configuré l'étendue requise des objets de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Vérification de l'application des objets de stratégie de groupe

Scénario

Après la création des stratégies, vous devez évaluer le jeu de stratégies résultant pour les utilisateurs dans votre environnement afin de garantir que l'infrastructure de stratégie de groupe est intègre et que toutes les stratégies sont appliquées comme prévu.

Les tâches principales de cet exercice sont les suivantes :

1. Exécuter l'analyse du jeu de stratégie résultant (RSoP).
2. Analyser RSoP avec GPResults.
3. Évaluer les résultats de l'objet de stratégie de groupe à l'aide de l'Assistant Modélisation de stratégie de groupe.
4. Examiner les événements de stratégie et déterminer l'état d'infrastructure de l'objet de stratégie de groupe.

▶ Tâche 1 : Exécuter l'analyse du jeu de stratégie résultant (RSoP)

1. Sur LON-CL1, vérifiez que vous êtes toujours connecté en tant que ADATUM\Pat. S'il y a lieu, indiquez le mot de passe **Pa$$w0rd**.
2. Exécutez **l'invite de commandes** en tant qu'administrateur, avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
3. Exécutez la commande **gpupdate /force**. Une fois la commande exécutée, notez l'heure système actuelle que vous devrez connaître pour une tâche ultérieure dans cet atelier pratique :

   Heure : _____
4. Redémarrez LON-CL1, puis attendez qu'il redémarre avant de passer à la tâche suivante.
5. Sur LON-DC1, basculez vers la console **Gestion de stratégie de groupe**.
6. Utilisez **Assistant Résultats de stratégie de groupe** pour exécuter un rapport RSoP pour **Pat** sur **LON-CL1**.
7. Examinez les résultats Résumé de la stratégie de groupe. Pour la configuration utilisateur et ordinateur, identifiez l'heure de la dernière actualisation de stratégie et la liste des objets Stratégie de groupe autorisés et refusés. Identifiez les composants qui ont été utilisés pour traiter les paramètres de stratégie.
8. Cliquez sur l'onglet **Détails**. Examinez les paramètres appliqués pendant l'application de la stratégie utilisateur et ordinateur, puis identifiez l'objet de stratégie de groupe à partir duquel les paramètres ont été obtenus.
9. Cliquez sur l'onglet **Événements de stratégie**, puis localisez l'événement qui journalise l'actualisation de stratégie que vous avez déclenchée à l'aide de la commande GPUpdate dans la tâche 1.
10. Cliquez sur l'onglet **Résumé**, cliquez avec le bouton droit sur la page, puis sélectionnez **Enregistrer le rapport**. Enregistrez le rapport en tant que fichier HTML sur votre bureau. Ouvrez ensuite le rapport RSoP à partir du bureau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Analysez RSoP avec GPResults

1. Ouvrez une session sur LON-CL1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez une invite de commandes et exécutez la commande **gpresult /r**. Les résultats récapitulatifs de RSoP sont affichés. Les informations sont très similaires à celles contenues dans l'onglet **Résumé** du rapport RSoP généré par l'Assistant Résultats de stratégie de groupe.
3. Saisissez **gpresult /v**, puis appuyez sur Entrée. Un rapport RSoP plus détaillé est généré. Vous constatez que beaucoup des paramètres de stratégie de groupe appliqués par le client sont répertoriés dans ce rapport.
4. Saisissez **gpresult /z** et appuyez sur Entrée. Le rapport RSoP le plus détaillé est généré.
5. Saisissez **gpresult /h:"%userprofile%\Desktop\RSOP.html"**, puis appuyez sur Entrée. Un rapport RSoP est enregistré comme fichier HTML sur votre bureau.
6. Ouvrez le rapport RSoP enregistré à partir de votre bureau. Comparez le rapport, ses informations, et sa mise en forme avec le rapport RSoP que vous avez enregistré dans la tâche précédente.

▶ Tâche 3 : Évaluez les résultats de l'objet de stratégie de groupe à l'aide de l'Assistant Modélisation de stratégie de groupe

1. Basculez vers LON-DC1.
2. Démarrez l'**Assistant Modélisation de stratégie de groupe**.
3. Sélectionnez **ADATUM\Mike** en tant qu'utilisateur, et **LON-CL1** comme ordinateur pour la modélisation.
4. Lorsque vous y êtes invité, activez la case à cocher **Traitement en boucle**, puis cliquez sur **Fusionner**. Bien que l'objet de stratégie de groupe Salle de conférence spécifie le traitement par boucle de rappel, vous devez indiquer à l'Assistant Modélisation de stratégie de groupe qu'il doit prendre en compte le traitement par boucle de rappel dans sa simulation.
5. Sur la page **Autres chemins d'accès Active Directory**, sélectionnez l'emplacement **Bornes\Salles de conférence** lorsque vous y êtes invité. Vous simulez l'effet de LON-CL1 comme ordinateur de salle de conférence.
6. Acceptez toutes les autres options comme valeurs par défaut.
7. Dans l'onglet **Résumé**, faites défiler et développez s'il y a lieu, **Détails de l'utilisateur**, **Objets de stratégie de groupe**, et **Objets GPO appliqués**.
8. Vérifiez si l'objet de stratégie de groupe Stratégies de salle de conférence s'applique à Mike comme stratégie utilisateur quand il ouvre une session sur LON-CL1, si LON-CL1 se trouve dans l'unité d'organisation Salles de conférence.
9. Faites défiler et développez s'il y a lieu, **Détails de l'utilisateur**, **Stratégies**, **Modèles d'administration** et **Panneau de configuration/Personnalisation**.
10. Confirmez que le délai d'activation de l'écran de veille est de 2 700 secondes (45 minutes), le paramètre configuré par l'objet de stratégie de groupe Stratégies de salle de conférence qui remplace la valeur par défaut de 10 minute configurée par l'objet de stratégie de groupe Normes ADATUM.

▶ Tâche 4 : Examinez les événements de stratégie et déterminez l'état d'infrastructure de l'objet de stratégie de groupe

1. Sur LON-CL1, assurez-vous que vous avez ouvert une session en tant **ADATUM\Administrateur**.
2. Ouvrez **Panneau de configuration**, puis accédez à **Observateur d'événements**.
3. Recherchez et passez en revue les événements de stratégie de groupe **Journal** système.
4. Recherchez et examinez les événements de stratégie de groupe dans le journal d'**applications**. Examinez les événements et identifiez les événements de stratégie de groupe qui ont été écrits dans ce journal. Quels sont les événements liés à l'application de stratégie de groupe et ceux liés aux activités effectuées pour gérer la stratégie de groupe ? Notez que, selon la durée d'exécution de l'ordinateur virtuel, il peut n'y avoir aucun événement de stratégie de groupe dans le journal des applications.
5. Accédez au journal **d'opérations de la stratégie de groupe** et localisez le premier événement associé à l'actualisation de la stratégie de groupe que vous avez initialisée dans l'exercice 1, à l'aide de la commande GPUpdate. Examinez cet événement et les événements qui l'ont suivi.

Résultats : À la fin de cet exercice, vous devez avoir utilisé avec succès les outils RSoP pour vérifier l'application correcte de vos objets de stratégie de groupe.

Exercice 4 : Gestion des objets de stratégie de groupe

Scénario

Vous devez sauvegarder tous les objets de stratégie de groupe critiques. Utilisez la fonctionnalité de sauvegarde de gestion des stratégies de groupe pour sauvegarder l'objet de stratégie de groupe Norme ADATUM.

Les tâches principales de cet exercice sont les suivantes :

1. Exécutez une sauvegarde des objets de stratégie de groupe.
2. Exécutez une restauration des objets de stratégie de groupe.
3. Pour préparer le module suivant

▶ Tâche 1 : Exécuter une sauvegarde des objets de stratégie de groupe.

1. Basculez vers LON-DC1 et, dans la console Gestion des stratégies de groupe, dans le volet de navigation, cliquez sur le dossier **Objets de stratégie de groupe**.
2. Sauvegardez l'objet de stratégie de groupe **Normes ADATUM** dans **C:**.

▶ Tâche 2 : Exécuter une restauration d'objets de stratégie de groupe.

- Dans la console Gestion des stratégies de groupe, restaurez la sauvegarde précédente de **Normes ADATUM**.

▶ Pour préparer le module suivant

- Une fois l'atelier terminé, rétablissez tous les ordinateurs virtuels à leurs états initiaux.

Résultats : À la fin de cet exercice, vous devez avoir effectué avec succès des tâches de gestion courantes sur vos objets de stratégie de groupe.

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
Les paramètres de stratégie de groupe ne sont pas appliqués à tous les utilisateurs ou ordinateurs de l'unité d'organisation à laquelle l'objet de stratégie de groupe est appliqué	
Les paramètres de stratégie de groupe ont besoin de deux redémarrages pour entrer en vigueur	

Outils

Outil	Utilisation	Emplacement
Rapport de stratégie de groupe RSoP	Informations de génération de rapport sur les stratégies actuellement fournies aux clients.	Console de gestion des stratégies de groupe
GPResult	Utilitaire de ligne de commandes qui affiche des informations RSoP.	Utilitaire de ligne de commandes
GPUpdate	Actualisation des paramètres de stratégie de groupe locaux et basés sur les services de domaine Active Directory (AD DS).	Utilitaire de ligne de commandes
Dcgpofix	Restauration des objets de stratégie de groupe par défaut à leur état d'origine après l'installation initiale.	Utilitaire de ligne de commandes
GPOLogView	Exportation d'événements associés à la stratégie de groupe à partir des journaux système et d'opérations sous forme de fichiers texte, HTML ou XML. Pour utilisation avec Windows Vista®, Windows 7, et les versions plus récentes.	Utilitaire de ligne de commandes
Scripts de gestion des stratégies de groupe	Exemples de script qui effectuent diverses tâches de dépannage et de maintenance.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 6

Gestion des bureaux des utilisateurs avec la stratégie de groupe

Table des matières :

Vue d'ensemble du module **6-1**

Leçon 1 : Implémentation des modèles d'administration **6-2**

Leçon 2 : Configuration de la redirection de dossiers et des scripts **6-12**

Leçon 3 : Configuration des préférences de stratégies de groupe **6-20**

Leçon 4 : Gestion des logiciels à l'aide de la stratégie de groupe **6-39**

Atelier pratique : Gestion des bureaux des utilisateurs avec la stratégie de groupe **6-46**

Contrôle des acquis et éléments à retenir **6-53**

Vue d'ensemble du module

À l'aide des objets de stratégie de groupe, vous pouvez mettre en place des environnements de bureau au sein de votre organisation en utilisant les modèles d'administration, la redirection des dossiers, les préférences de stratégie de groupe et, le cas échéant, utiliser le déploiement de logiciel afin d'installer et de mettre à jour des programmes d'application. Il est important de savoir utiliser ces diverses fonctionnalités d'objet de stratégie de groupe de sorte que vous puissiez configurer les paramètres des ordinateurs de vos utilisateurs correctement.

Objectifs

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

- Décrire et implémenter des modèles d'administration.
- Configurer la redirection de dossiers et les scripts à l'aide des objets de stratégie de groupe.
- Configurer les préférences des objets de stratégie de groupe.
- Déployer le logiciel à l'aide des objets de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Implémentation des modèles d'administration

Les fichiers de modèle d'administration fournissent la majorité des paramètres d'objet de stratégie de groupe disponibles, qui modifient les clés de Registre spécifiques. L'utilisation des modèles d'administration est parfois désigné sous le nom de stratégie basée sur le Registre. Pour de nombreuses applications, l'utilisation de la stratégie basée sur le Registre que les fichiers de modèle d'administration fournissent est la voie la plus simple et la plus efficace de prendre en charge la gestion centralisée des paramètres de stratégie. Dans cette leçon, vous allez apprendre à configurer des modèles d'administration.

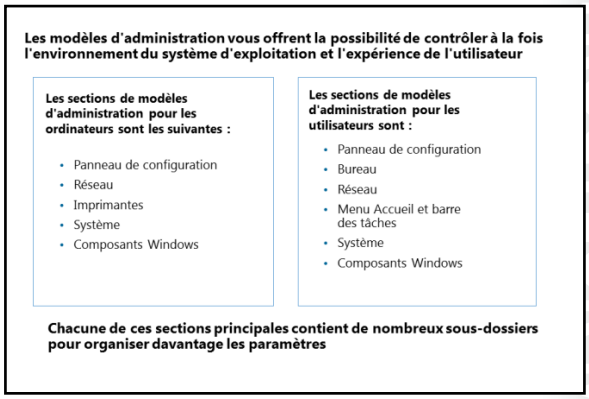
Objectifs de la leçon

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

- Décrire des modèles d'administration de stratégie de groupe.
- Décrire les fichiers ADM et ADMX, ou les modèles d'administration.
- Décrire le magasin central.
- Décrire les scénarios d'exemple d'utilisation des modèles d'administration.
- Expliquer comment configurer les paramètres des modèles d'administration.

Que sont les modèles d'administration ?

Les modèles d'administration vous offrent la possibilité de contrôler à la fois l'environnement du système d'exploitation et l'expérience de l'utilisateur. Il existe deux ensembles de modèles d'administration : l'un pour les utilisateurs et l'un pour les ordinateurs.



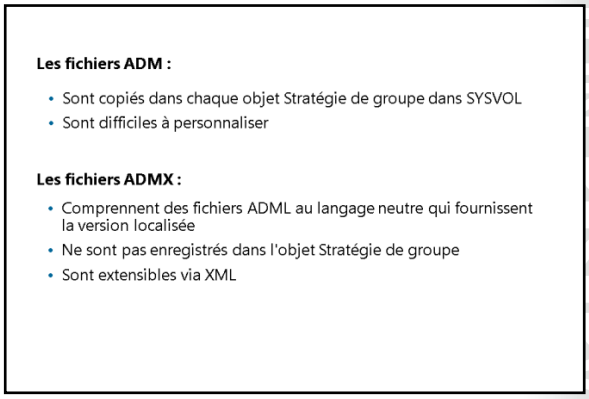
Grâce aux sections dédiées aux modèles d'administration de l'objet de stratégie de groupe, vous pouvez déployer des centaines de modifications au Registre. Les modèles d'administration possèdent les caractéristiques suivantes :

- Ils sont organisés en sous-dossiers qui traitent des zones spécifiques de l'environnement, telles que le réseau, le système et les composants Windows®.
- Les paramètres de la section informatique modifient la ruche HKEY_LOCAL_MACHINE dans le Registre et les paramètres de la section utilisateur modifient la ruche HKEY_CURRENT_USER dans le Registre.
- Quelques paramètres existent à la fois pour l'utilisateur et l'ordinateur. Par exemple, il existe un paramètre empêchant l'exécution de Windows Messenger à la fois dans le modèle Utilisateur et dans le modèle Ordinateur. En cas de paramètres contradictoires, le paramètre de l'ordinateur est prioritaire.
- Quelques paramètres sont disponibles seulement pour certaines versions du système d'exploitation Windows. Par exemple, un certain nombre de nouveaux paramètres peuvent seulement être appliqués à Windows 7 et aux versions plus récentes du système d'exploitation Windows. Double-cliquer sur un paramètre permet d'afficher les versions prises en charge pour ce paramètre.

Que sont les fichiers ADM et ADMX ?

Fichiers ADM

En général, les fichiers ADM sont utilisés pour définir les paramètres qu'un administrateur peut configurer grâce à la stratégie de groupe. Chaque système d'exploitation Windows et Service Pack successif comprend une version plus récente de ces fichiers. Les fichiers ADM utilisent leur propre langage de balisage. Par conséquent, il est difficile de personnaliser les fichiers ADM. Les modèles ADM sont situés dans le dossier %SystemRoot%\Inf.



L'un des inconvénients majeurs des fichiers ADM est qu'ils sont copiés dans chaque objet de stratégie de groupe créé et consomment environ 3 mégaoctets de (Mo) d'espace. Ceci peut augmenter énormément la taille du dossier du volume système (SYSVOL) et accroître le trafic de réplication.

Fichiers ADMX

Windows Vista® et Windows Server® 2008 ont présenté un nouveau format d'affichage des paramètres de stratégie basés sur le Registre. Ces paramètres sont définis à l'aide d'un format de fichier XML basé sur des normes appelé fichier ADMX. Ces nouveaux fichiers remplacent les fichiers ADM.

Les outils de stratégie de groupe sur Windows Vista et les systèmes d'exploitation les plus récents, ainsi que sur Windows Server 2008, continuent à identifier les fichiers ADM personnalisés qui se trouvent dans votre environnement existant, mais ignorent n'importe quel fichier ADM remplacé par un fichier ADMX. À la différence des fichiers ADM, les fichiers ADMX ne sont pas enregistrés dans un objet de stratégie de groupe. L'éditeur d'objet de stratégie de groupe lit et affiche automatiquement les paramètres du magasin local de fichiers ADMX. Par défaut, les fichiers ADMX sont enregistrés dans le dossier Windows\PolicyDefinitions, mais ils peuvent être enregistrés dans un emplacement central.

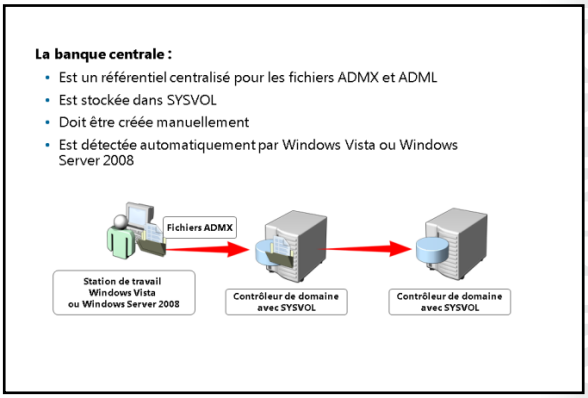
Les fichiers ADMX sont indépendants de la langue. Les descriptions en langage simple des paramètres ne font pas partie des fichiers ADMX. Elles sont enregistrées dans des fichiers ADML spécifiques à chaque langue. Ceci signifie que les administrateurs qui parlent diverses langues, tels que l'anglais et l'espagnol, peuvent examiner le même objet de stratégie de groupe et voir les descriptions de stratégie dans leur propre langue, en utilisant leurs propres fichiers ADML correspondant à chaque langue. Les fichiers ADML sont stockés dans un sous-dossier du dossier PolicyDefinitions. Par défaut, seuls les fichiers de langue ADML pour la langue du système d'exploitation installé sont ajoutés.

Migrer les modèles d'administration classiques vers ADMX

L'outil de migration ADMX est un composant logiciel enfichable pour Microsoft® Management Console (MMC) qui simplifie le processus de conversion de vos modèles ADM existants de stratégie de groupe vers le nouveau format ADMX et qui fournit une interface utilisateur graphique pour créer et modifier des modèles d'administration. Vous pouvez télécharger l'outil de migration ADMX à partir du site Web de Microsoft, à la page http://go.microsoft.com/fwlink/?linkID=270013

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le magasin central



Pour des entreprises basées sur un domaine, vous pouvez créer un emplacement de magasin central pour les fichiers ADMX, accessible à tout personne possédant l'autorisation de créer ou de modifier l'objet de stratégie de groupe. L'éditeur d'objet de stratégie de groupe sur Windows Vista et Windows Server 2008 (ou les versions plus récentes) lit et affiche automatiquement des paramètres de stratégie de modèle d'administration à partir des fichiers ADMX que le magasin central met en cache, et ignore alors ceux enregistrés localement. Si le contrôleur de domaine est indisponible, le magasin local est utilisé.

Vous devez créer le magasin central, puis le mettre à jour manuellement sur un contrôleur de domaine. L'utilisation des fichiers ADMX dépend du système d'exploitation de l'ordinateur sur lequel vous créez ou modifier l'objet de stratégie de groupe. Par conséquent, le contrôleur de domaine peut être un serveur doté de Windows 2000 ou une version plus récente. Le service de réplication de fichiers (FRS) ne répliquera pas le contrôleur de domaine vers d'autres contrôleurs de ce domaine. Selon votre système d'exploitation serveur et votre configuration, vous pouvez utiliser le service FRS ou la réplication de système de fichiers (DFS-R) pour répliquer les données.

Pour créer un magasin central pour des fichiers .admx et .adml, créez un dossier nommé PolicyDefinitions à l'emplacement suivant : \\FQDN\SYSVOL\NDC\stratégies

Par exemple, pour créer un magasin central pour le domaine Test.Microsoft.com, créez un dossier PolicyDefinitions à l'emplacement suivant : \\Test.Microsoft.Com\SYSVOL\Test.Microsoft.Com\Stratégies

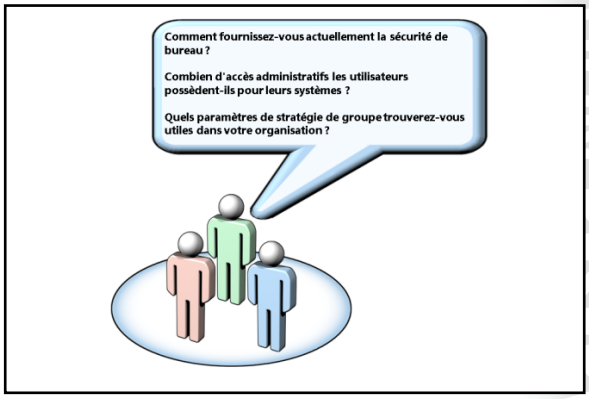
Un utilisateur doit copier tous les fichiers et sous-dossiers du dossier PolicyDefinitions. Le dossier PolicyDefinitions d'un ordinateur basé sur Windows 7 se trouve dans le dossier Windows. Le dossier PolicyDefinitions enregistre tous les fichiers .admx et fichiers .adml pour toutes les langues autorisées sur l'ordinateur client.

Remarque : Vous devez mettre le dossier PolicyDefinitions à jour pour chaque Service Pack et pour tout autre logiciel supplémentaire, tel que les fichiers ADMX de Microsoft Office 2010.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Discussion : Utilisations pratiques des modèles d'administration



Passez quelques minutes à examiner les modèles d'administration et envisagez les différentes utilisations de certains d'entre eux dans votre organisation.

Soyez préparé à partager des informations sur l'utilisation actuelle des objets de stratégie de groupe et des scripts d'ouverture de session faite par votre organisation, telles que :

- Comment fournissez-vous actuellement la sécurité de bureau ?
- Combien d'accès administratifs les utilisateurs possèdent-ils pour leurs systèmes ?
- Quels paramètres de stratégie de groupe trouverez-vous utiles dans votre organisation ?

Démonstration : Configuration des paramètres à l'aide de modèles d'administration

Les outils de modification de stratégie de groupe dans Windows Server 2012 fournissent plusieurs fonctionnalités qui facilitent la configuration et la gestion des objets de stratégie de groupe. Dans cette démonstration, vous allez passer en revue ces options.

Filtrer les paramètres de stratégie pour les modèles d'administration

Un inconvénient présent dans les outils de modification de stratégie de groupe des versions précédentes de Windows est l'impossibilité de rechercher un paramètre de stratégie spécifique. Avec des milliers de stratégies possibles, il peut être difficile de localiser exactement le paramètre que vous souhaitez configurer. L'éditeur de gestion des stratégies de groupe dans Windows Server 2012 résout ce problème pour les paramètres de modèle d'administration. Vous pouvez désormais créer des filtres pour localiser les paramètres de stratégie spécifiques.

Pour créer un filtre :

1. Cliquez avec le bouton droit sur **Modèles d'administration**, puis cliquez sur **Options de filtre**.
2. Pour localiser une stratégie spécifique, activez la case à cocher **Activer les filtres par mots clés**, saisissez les mots clés, puis sélectionnez les champs dans lesquels effectuer la recherche.

Vous pouvez également filtrer les paramètres de stratégie de groupe qui s'appliquent à des versions de Windows spécifiques, Windows Internet Explorer® et d'autres composants Windows.

Malheureusement, le filtre s'applique uniquement aux paramètres des nœuds des modèles d'administration.

Critères de filtrage basés sur des commentaires

Vous pouvez également rechercher et filtrer en fonction des commentaires sur le paramètre de stratégie. Windows Server 2012 vous permet d'ajouter des commentaires aux paramètres de stratégie dans le nœud des modèles d'administration. Pour cela, double-cliquez sur un paramètre de stratégie, puis cliquez sur l'onglet **Commentaire**.

Ajouter des commentaires à des paramètres de stratégie configurés est considéré comme une pratique d'excellence. Vous devez documenter la justification pour un paramètre et son effet désiré. Vous devez également ajouter les commentaires à l'objet de stratégie de groupe lui-même. Windows Server 2012 vous permet de joindre des commentaires à un objet de stratégie de groupe. Dans l'éditeur de gestion des stratégies de groupe, dans l'arborescence de la console, cliquez avec le bouton droit sur le nœud racine, cliquez sur **Propriétés**, puis cliquez sur l'onglet **Commentaire**.

Procédure de copie des paramètres d'objet de stratégie de groupe

Les objets de stratégie de groupe Starter ne peuvent contenir que des paramètres de stratégie de modèles d'administration. Cependant, en plus d'utiliser des objets de stratégie de groupe Starter, il existe deux autres moyens de copier des paramètres d'un objet de stratégie de groupe dans un nouvel objet :

- Vous pouvez copier et coller des objets de stratégie de groupe entiers dans le conteneur d'objets de stratégie de groupe du GPMC, afin d'avoir un nouvel objet de stratégie de groupe possédant tous les paramètres de l'objet de stratégie de groupe source.
- Pour transférer des paramètres entre les objets de stratégie de groupe dans différents domaines ou forêts, cliquez avec le bouton droit sur un objet de stratégie de groupe, puis cliquez sur **Sauvegarde**. Dans le domaine cible, créez un nouvel objet de stratégie de groupe, cliquez avec le bouton droit sur l'objet de stratégie de groupe, puis cliquez sur **Importer des paramètres**. Vous pourrez importer les paramètres de l'objet de stratégie de groupe sauvegardé.



Documentation supplémentaire : Recherche de stratégie de groupe
http://go.microsoft.com/fwlink/?linkID=270014

Cette démonstration montre comment :

- Filtrer les paramètres de stratégie du modèle d'administration.
- Appliquer des commentaires aux paramètres de stratégie des modèles d'administration.
- Ajouter des commentaires aux paramètres de stratégie des modèles d'administration.
- Créer un nouvel objet de stratégie de groupe en copiant un objet de stratégie de groupe existant.
- Créer un nouvel objet de stratégie de groupe en important les paramètres auparavant exportés depuis un autre objet de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

Filtrer les paramètres de stratégie du modèle d'administration

1. Sur LON-DC1, ouvrez la console de gestion des stratégies de groupe .
2. Créez un nouvel objet de stratégie de groupe (GPO) appelé **GPO1**.
3. Ouvrez **GPO1** pour modification.
4. Localisez le nœud **Configuration utilisateur**, **Stratégies**, **Modèles d'administration**.
5. Filtrez les paramètres pour afficher uniquement ceux qui contiennent les mots clés *écran de veille*.
6. Filtrez les paramètres pour afficher uniquement des valeurs configurées.

Ajouter des commentaires à un paramètre de stratégie

1. Localisez la valeur de **Personnalisation** dans **Configuration utilisateur\Stratégies\ Modèles d'administration\Panneau de configuration**.
2. Ajoutez un commentaire aux deux paramètres **Le mot de passe protège l'écran de veille** et **Activer l'écran de veille**.

Ajouter des commentaires à un objet de stratégie de groupe (GPO)

- Ouvrez le nœud racine de la stratégie GPO1, puis ajoutez un commentaire à l'onglet **Commentaire**.

Créer un nouvel objet de stratégie de groupe en copiant un objet de stratégie de groupe existant

- Copiez GPO1, et collez-le dans le dossier d'objets de stratégie de groupe.

Créer un nouvel objet de stratégie de groupe en important les paramètres auparavant exportés depuis un autre objet

1. Sauvegardez **GPO1.**
2. Créez un nouvel objet de stratégie de groupe appelé **ADATUM Import**.
3. Importez les paramètres de la sauvegarde de **GPO1** dans l'objet de stratégie de groupe **ADATUM Import**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration de la redirection de dossiers et des scripts

Dans Windows Server 2012, les objets de stratégie de groupe vous permettent de déployer des scripts sur des utilisateurs et des ordinateurs. Vous pouvez également rediriger les dossiers qui sont compris dans le profil d'utilisateur vers un serveur central. Ces fonctionnalités vous permettent de configurer les paramètres de bureau des utilisateurs plus facilement et de créer un environnement de bureau standardisé qui répond à vos besoins d'organisation où vous le souhaitez.

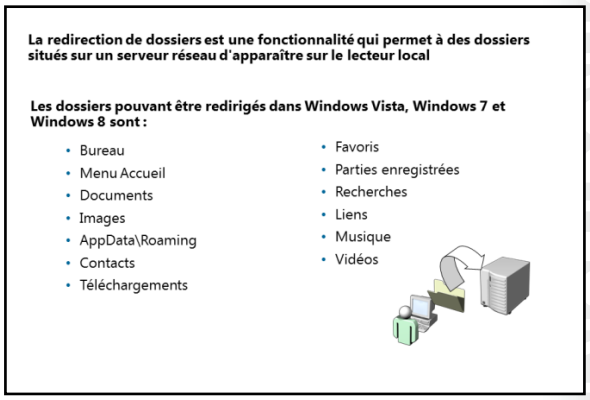
Objectifs de la leçon

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

- Décrire la redirection de dossiers.
- Expliquer les paramètres disponibles pour configurer la redirection de dossiers :
- Décrire les paramètres de sécurité pour les dossiers redirigés.
- Expliquer comment configurer la redirection de dossiers.
- Décrire les paramètres de stratégie de groupe pour appliquer des scripts.
- Expliquer comment configurer les scripts à l'aide des stratégies de groupe.

Qu'est-ce que la redirection de dossiers ?

Vous pouvez utiliser la fonctionnalité de redirection de dossiers pour gérer les données de façon efficace et, éventuellement, sauvegarder des données. En redirigeant des dossiers, vous pouvez garantir un accès utilisateur aux données, indépendamment des ordinateurs auxquels les utilisateurs se connectent. La redirection de dossiers possède les caractéristiques suivantes :



- Lorsque vous redirigez des dossiers, vous modifiez l'emplacement de stockage des dossiers, depuis le disque dur local de l'ordinateur de l'utilisateur vers un dossier partagé sur un serveur de fichiers réseau.
- Une fois redirigé vers un serveur de fichiers, un dossier apparaît encore à l'utilisateur comme s'il était stocké sur le disque dur local.
- Vous pouvez utiliser la technologie des fichiers hors connexion en même temps que la redirection pour synchroniser des données dans le dossier redirigé vers le disque dur local de l'utilisateur. Ceci garantit aux utilisateurs un accès à leurs données si une panne de réseau se produit ou si l'utilisateur travaille hors connexion.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

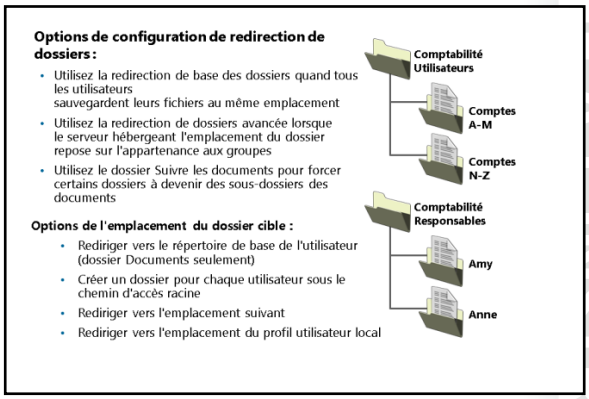
Avantages de la redirection de dossiers

Il y a beaucoup d'avantages à la redirection de dossier, notamment :

- Les utilisateurs qui se connectent à plusieurs ordinateurs peuvent accéder à leurs données tant qu'ils peuvent accéder au partage réseau.
- Les dossiers en mode hors connexion permettent aux utilisateurs d'accéder à leurs données même s'ils se déconnectent du réseau local (LAN).
- Les données qui sont enregistrées sur des serveurs en partages réseau sont sauvegardées.
- La taille de profil itinérant peut être réduite considérablement grâce à la redirection des données du profil.

Paramètres de configuration de la redirection de dossiers

Dans un objet de stratégie de groupe, les paramètres suivants sont disponibles pour configurer la redirection de dossiers :



- *Aucun*. Aucun constitue la valeur par défaut. La redirection de dossiers n'est pas activée.
- *De base*. La redirection de base est utilisée pour :
  - Les utilisateurs qui doivent rediriger leurs dossiers vers un espace commun.
  - Les utilisateurs qui ont besoin de conserver leurs données privées.
- *Avancée*. La redirection avancée vous permet de spécifier des emplacements réseau différents pour différents groupes de sécurité Active Directory®.
- *Suivre le dossier Documents*. L'option Suivre la redirection du dossier Documents est disponible uniquement pour les dossiers Images, Musique et Vidéos. Ce paramètre transforme le dossier concerné en sous-dossier du dossier Documents.

Emplacements du dossier cible pour les paramètres De base et Avancé

Si vous choisissez De base ou Avancé, vous pouvez choisir les emplacements de dossier cible suivants :

- *Créer un dossier pour chaque utilisateur sous le chemin d'accès racine*. Cette option crée un dossier sous la forme \\serveur\partage\nom de compte d'utilisateur\nom du dossier. Par exemple, si vous souhaitez enregistrer les paramètres de bureau de vos utilisateurs dans un dossier partagé appelé Documents sur un serveur appelé LON-DC1, vous pouvez définir le chemin d'accès de racine \\lon-dc1\Documents.

  Chaque utilisateur possède un chemin d'accès unique pour que le dossier redirigé vérifie que les données demeurent privées. Par défaut, cet utilisateur possède les droits d'accès exclusifs à ce dossier. Dans le cas du dossier Documents, le contenu du dossier actuel est déplacé vers le nouvel emplacement.
- *Rediriger vers l'emplacement suivant*. Cette option utilise un chemin d'accès précis pour l'emplacement de redirection. Avec cette option, plusieurs utilisateurs partagent le même chemin d'accès pour le dossier redirigé. Par défaut, cet utilisateur possède les droits d'accès exclusifs à ce dossier. Dans le cas du dossier Documents, le contenu du dossier actuel est déplacé vers le nouvel emplacement.

- *Rediriger vers l'emplacement du profil utilisateur local*. Cette option déplace l'emplacement du dossier vers le profil d'utilisateur local sous le dossier Utilisateurs.
- *Rediriger vers le répertoire d'accueil de l'utilisateur*. Cette option est disponible uniquement dans le dossier Documents.

Remarque : Après la création et l'application initiales d'un objet de stratégie de groupe qui fournit des paramètres de redirection de dossier, les utilisateurs doivent ouvrir deux sessions avant que la redirection n'entre en vigueur. Les utilisateurs doivent suivre cette procédure car ils se connecteront avec des informations d'identification mises en cache.

Question : Les utilisateurs du même service se connectent souvent à différents ordinateurs. Ils ont besoin d'un accès à leur dossier Documents. Ils ont également besoin de conserver des données privées. Quel paramètre de redirection de dossiers choisiriez-vous ?

Paramètres de sécurité pour les dossiers redirigés

Vous devez créer et configurer les autorisations manuellement sur un dossier réseau partagé afin de stocker les dossiers redirigés. Cependant, la redirection de dossiers peut également créer les dossiers redirigés de l'utilisateur.

Autorisations NTFS pour le dossier racine

Créateur/Propriétaire	Contrôle total – sous-dossiers et fichiers seulement
Administrateur	Aucun
Groupe de sécurité d'utilisateurs qui sauvegardent des données sur le partage	Liste du dossier/Lecture des données, Création de dossiers/Ajout de données-Ce dossier uniquement
Système local	Contrôle total

Autorisations de partage pour le dossier racine

Créateur/Propriétaire	Contrôle total – sous-dossiers et fichiers seulement
Groupe de sécurité d'utilisateurs qui sauvegardent des données sur le partage	Contrôle total

Autorisations NTFS pour le dossier redirigé de chaque utilisateur

Créateur/Propriétaire	Contrôle total – sous-dossiers et fichiers seulement
%Username%	Contrôle total, propriétaire du dossier
Administrateurs	Aucun
Système local	Contrôle total

Les autorisations d'accès au dossier sont traitées comme suit :

- Lorsque vous utilisez cette option, les autorisations d'accès au sous-dossier appropriées sont automatiquement définies.
- Si vous créez des dossiers manuellement, vous devrez connaître les autorisations appropriées. Cette diapositive illustre ces autorisations.

Démonstration : Configuration de la redirection de dossiers

Cette démonstration montre comment :

- Créer un dossier partagé.
- Créer un objet de stratégie de groupe pour rediriger le dossier Documents.
- Tester la redirection de dossiers.

Procédure de démonstration

Créer un dossier partagé

1. Sur LON-DC1, créez un dossier nommé **C:\Redirect**.
2. Partagez le dossier avec **Tout le monde** avec l'autorisation de lecture/écriture.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Créer un objet de stratégie de groupe pour rediriger le dossier Documents

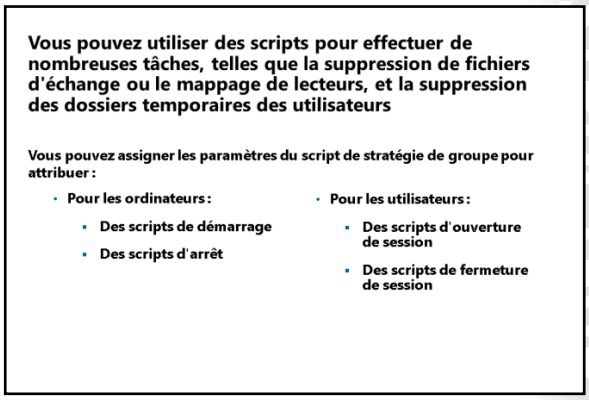
1. Ouvrez la console Gestion des stratégies de groupe. Créez un objet de stratégie de groupe nommé **Redirection des dossiers**, puis liez-le au domaine Adatum.
2. Modifiez l'objet de stratégie de groupe **Redirection des dossiers** .
3. Configurez les propriétés du dossier **Documents** afin qu'il utilise le paramètre Dossier **de redirection De base de tout le monde vers le même emplacement**.
4. Vérifiez que l'emplacement du **dossier cible** est défini sur **Créer un dossier pour chaque utilisateur sous le chemin d'accès racine**.
5. Précisez le chemin d'accès de la racine : **\\LON-DC1\Redirect.**
6. Fermez toutes les fenêtres ouvertes sur LON-DC1.

Tester la redirection de dossiers

1. Ouvrez une session sur LON-CL1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Vérifiez les propriétés du dossier **Documents**. Le chemin d'accès sera **\\LON-DC1\Redirect**.
3. Déconnectez-vous de LON-CL1.

Paramètres de stratégie de groupe pour appliquer des scripts

Vous pouvez utiliser des scripts de stratégie de groupe pour effectuer un certain nombre de tâches. Vous pouvez avoir besoin d'effectuer certaines actions chaque fois qu'un ordinateur démarre ou s'arrête, ou bien quand les utilisateurs se connectent ou se déconnectent. Par exemple, vous pouvez utiliser les scripts pour :



- Nettoyer les bureaux lorsque les utilisateurs ferment leurs sessions et arrêtent leurs ordinateurs.
- Supprimer le contenu des répertoires temporaires.
- Mapper les lecteurs ou les imprimantes.
- Définir des variables d'environnement.

Les scripts qui sont attribués à l'ordinateur s'exécutent dans le contexte de sécurité du compte Système local. Les scripts qui sont attribués à l'utilisateur qui ouvre une session s'exécutent dans le contexte de sécurité de cet utilisateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

D'autres paramètres de stratégie de groupe contrôlent certains aspects du fonctionnement des scripts. Par exemple, si plusieurs scripts sont attribués, vous pouvez contrôler s'ils s'exécutent de manière synchrone ou asynchrone.

Vous pouvez écrire des scripts en n'importe quelle langue de script que le client Windows peut interpréter, telle que VBScript et Jscript, ou bien via une commande ou un lot de fichiers.

Remarque : Dans Windows Server 2008 R2 et Windows Server 2012, l'interface utilisateur (UI) dans l'éditeur de stratégie de groupe pour les scripts d'ouverture de session, de fermeture de session, de démarrage et d'arrêt fournit un onglet supplémentaire pour les scripts Windows PowerShell®. Vous pouvez déployer votre script Windows PowerShell en l'ajoutant à cet onglet. Windows Server 2008 R2, Windows Server 2012, Windows 7 ou Windows 8 peuvent exécuter des scripts Windows PowerShell via la stratégie de groupe.

Les scripts sont stockés dans les dossiers partagés sur le réseau. Vous devez vérifier que le client a accès à cet emplacement réseau. Si les clients ne peuvent pas accéder à l'emplacement réseau, les scripts ne fonctionnent pas. Bien que n'importe quel emplacement réseau enregistre des scripts, prenez l'habitude d'utiliser le partage Netlogon parce que tous les utilisateurs et ordinateurs qui sont authentifiés pour les services AD DS ont accès à cet emplacement.

Pour la plupart de ces paramètres, utiliser les préférences de stratégie de groupe est une meilleure alternative que la configuration dans les images système Windows ou l'utilisation des scripts d'ouverture de session. Les préférences de stratégie de groupe seront évoquées plus en détail plus tard dans ce module.

Démonstration : Configuration des scripts avec des objets de stratégie de groupe

Cette démonstration montre comment :

- Créez un script d'ouverture de session pour mapper un lecteur réseau.
- Créer et lier un objet de stratégie de groupe pour utiliser le script et enregistrer le script dans le partage Netlogon.
- Vous connecter au client pour tester les résultats.

Procédure de démonstration

Créer un script d'ouverture de session pour mapper un lecteur réseau

1. Sur LON-DC1, lancez le **Bloc-notes**, puis saisissez la commande suivante :

```
Net use t: \\LON-dc1\Redirect
```

2. Enregistrez le fichier comme **Map.bat**.
3. Copiez le fichier dans le bloc-notes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Créer et lier un objet de stratégie de groupe pour utiliser le script et enregistrer le script dans le partage Netlogon

1. Utilisez la console de gestion des stratégies de groupe pour créer un nouvel objet de stratégie de groupe nommé **Drivemap**, puis liez-le au domaine **Adatum.com**.
2. Modifiez l'objet de stratégie de groupe pour configurer un script d'ouverture de session utilisateur.
3. Collez le script **Map.bat** dans le partage **Netlogon**.
4. Ajoutez le script **Map.bat** aux scripts d'ouverture de session.

Vous connecter au client pour tester les résultats

1. Sur la machine LON-CL1, connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$word**.
2. Vérifiez que le lecteur est mappé.
3. Déconnectez-vous de LON-CL1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Configuration des préférences de stratégies de groupe

Dans les versions précédentes de Windows Server, vous ne pouviez pas utiliser les stratégies de groupe pour contrôler les paramètres courants qui affectent l'utilisateur et l'environnement informatique, tels que des lecteurs mappés. En général, ces paramètres étaient livrés par des scripts d'ouverture de session ou des solutions de création d'images.

Cependant, Windows Server 2012 comprend les préférences de stratégie de groupe intégrées à la console GPMC, qui activent des paramètres tels que des lecteurs mappés à livrer via la stratégie de groupe. En outre, vous pouvez configurer des préférences en installant les outils d'administration de serveur distant (RSAT) sur un ordinateur qui exécute Windows 7 ou Windows 8. Cela vous permet de fournir de nombreux paramètres courants grâce à la stratégie de groupe.

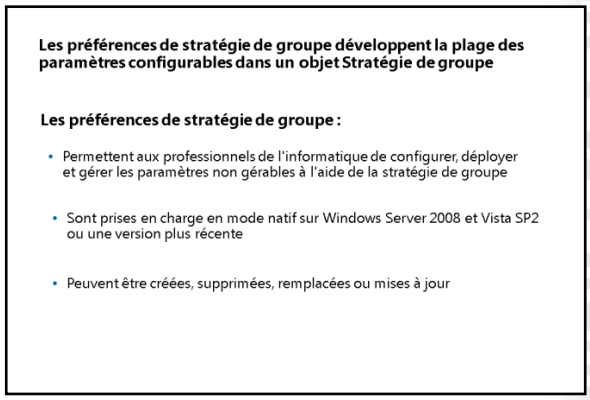
Objectifs de la leçon

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

- Décrire les préférences de stratégie de groupe.
- Identifier les différences entre les paramètres de stratégie de groupe et les préférences.
- Décrire les fonctionnalités des préférences de stratégie de groupe.
- Expliquer comment configurer les paramètres à l'aide des préférences.

Que sont les préférences de stratégie de groupe ?

Les extensions de préférence de stratégie de groupe comprennent plus de 20 extensions de stratégie de groupe qui développent la plage des paramètres configurables dans un objet de stratégie de groupe. Vous pouvez maintenant utiliser les préférences pour appliquer un certain nombre de paramètres qui devaient par le passé être appliqués par des scripts, tels que des mappages lecteur.



Les préférences de stratégie de groupe sont prises en charge en mode natif sur Windows Server 2008 et les versions plus récentes, ainsi que sur le Service Pack 2 de Windows Vista (SP2) et les versions plus récentes. Vous pouvez télécharger et installer des extensions côté client (CSE) des préférences de stratégie de groupe pour Windows Server 2003, Windows XP Service Pack 3 (SP3) et le Service Pack 1 de Windows Vista (SP1), afin de fournir la prise en charge des préférences sur ces systèmes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les exemples des nouvelles extensions des préférences de stratégie de groupe comprennent :

- Les options des dossiers
- Le mappage de lecteurs
- Imprimantes
- La planification des tâches
- Services
- Menu Accueil

La configuration des préférences de stratégie de groupe ne requiert aucun outil spécial ou installation de logiciel. Elles font partie, en mode natif, de la GPMC dans Windows Server 2008 (et les versions plus récentes) et sont appliqués de la même manière que des paramètres de stratégie de groupe, par défaut. Les préférences possèdent deux sections distinctes : les paramètres Windows et les paramètres du panneau de configuration.

Quand vous configurez une nouvelle préférence, vous pouvez exécuter les quatre actions de base suivantes :

- *Créer*. Créer un nouveau paramètre de préférence pour l'utilisateur ou l'ordinateur.
- *Supprimer*. Supprimer un paramètre de préférence existant pour l'utilisateur ou l'ordinateur.
- *Remplacer*. Supprimer et recréer un paramètre de préférence pour l'utilisateur ou l'ordinateur. Les préférences de stratégie de groupe remplacent alors tous les paramètres et fichiers existants associés à l'élément de préférence.
- *Mettre à jour*. Modifier un paramètre de préférence existant pour l'utilisateur ou l'ordinateur.

Comparaison des préférences de stratégie de groupe et des paramètres d'objet de stratégie de groupe

Les préférences sont semblables aux stratégies car elles appliquent des configurations à l'utilisateur ou à l'ordinateur. Cependant, il existe plusieurs différences dans la manière dont vous pouvez les configurer et les appliquer. L'une de ces différences réside dans le fait que les préférences ne sont pas appliquées. Cependant, vous pouvez configurer des préférences à réappliquer automatiquement.

Paramètres de stratégie de groupe	Les préférences de stratégie de groupe
Appliquent strictement les paramètres de stratégie en écrivant les paramètres dans les zones du registre que les utilisateurs standard ne peuvent pas modifier	Sont écrits sur les emplacements normaux dans le registre que l'application ou la fonctionnalité du système d'exploitation utilise pour enregistrer le paramètre
Désactivent généralement l'interface utilisateur pour les paramètres que la stratégie de groupe gère	N'entraîne pas l'application ou la fonctionnalité du système d'exploitation à désactiver l'interface utilisateur pour les paramètres qu'elle configure
Actualisent les paramètres de stratégie à un intervalle régulier	Actualisent les préférences au même intervalle que les paramètres de stratégie de groupe par défaut

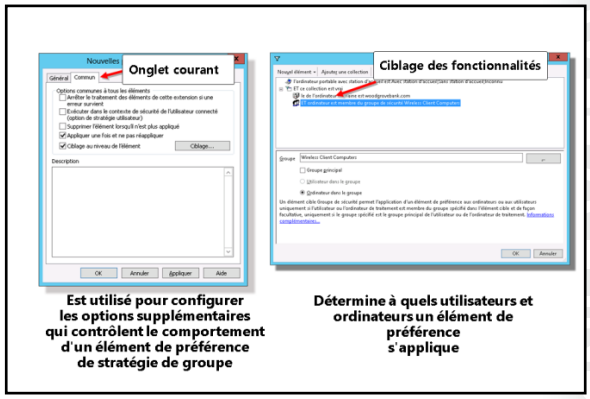
Voici une liste d'autres différences entre les paramètres de stratégie de groupe et les préférences :

- Les paramètres de préférence ne sont pas appliqués.
- Les paramètres de stratégie de groupe désactivent l'interface utilisateur pour les paramètres que la stratégie gère. Les préférences n'agissent pas ainsi.

- Les paramètres de stratégie de groupe sont appliqués à intervalles réguliers. Vous pouvez appliquer des préférences une fois seulement ou à intervalles réguliers.
- L'utilisateur final peut modifier n'importe quel paramètre de préférence qui est appliqué par la stratégie de groupe, mais les paramètres de stratégie empêchent les utilisateurs de les modifier.
- Dans certains cas, vous pouvez configurer les mêmes paramètres via un paramètre de stratégie aussi bien qu'un élément de préférence. Si des paramètres de stratégie de groupe et de préférence contradictoires sont configurés et appliqués au même objet, la valeur du paramètre de stratégie s'applique toujours.

Fonctionnalités des préférences de stratégie de groupe

Après avoir créé une préférence de stratégie de groupe, vous devez configurer ses propriétés. Différentes préférences nécessiteront différentes informations d'entrée. Par exemple, les préférences de raccourci nécessitent des chemins d'accès cibles, tandis que les variables d'environnement nécessitent des types et des valeurs variables. Les préférences fournissent également un certain nombre de fonctionnalités dans les propriétés communes afin d'aider le déploiement.



Onglet Propriétés générales

L'onglet Propriétés générales est l'endroit où des données de base sont fournies. La première étape est de préciser l'action associée à la préférence : créer, supprimer, remplacer ou mettre à jour. Différents paramètres seront disponibles, selon l'action initiale sélectionnée. Par exemple, si vous créez un mappage de lecteur, vous devez fournir un chemin d'accès UNC et une option pour la lettre de lecteur, que vous souhaitez attribuer.

Onglet Propriétés communes

Les propriétés communes sont cohérentes pour toutes les préférences. Vous pouvez utiliser l'onglet Propriétés communes pour contrôler le comportement de la préférence comme suit :

- *Arrêter de traiter des éléments dans cette extension si une erreur se produit.* Si une erreur se produit pendant le traitement d'une préférence, aucune autre préférence dans cet objet de stratégie de groupe ne sera traitée.
- *Exécuter dans le contexte de sécurité de l'utilisateur connecté.* Les préférences peuvent s'exécuter en tant que le système reconnaît l'utilisateur connecté. Ce paramètre force le contexte de sécurité de l'utilisateur connecté.
- *Supprimer l'élément lorsqu'il n'est plus appliqué.* À la différence des paramètres de stratégie, les préférences ne sont pas supprimées lorsque l'objet de stratégie de groupe qui les a livrées est supprimé. Ce paramètre modifiera ce comportement.
- *Appliquer une fois et ne pas réappliquer.* Normalement, les préférences sont actualisées au même intervalle que les paramètres de stratégie de groupe. Ce paramètre modifie ce comportement pour appliquer le paramètre une seule fois à l'ouverture de session ou au démarrage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Utiliser le ciblage au niveau de l'élément.* L'une des fonctionnalités les plus puissantes des préférences est le ciblage au niveau de l'élément. Vous pouvez utiliser cette fonctionnalité pour spécifier des critères facilement, afin de pouvoir déterminer exactement quels utilisateurs ou ordinateurs recevront une préférence. Les critères comprennent, sans s'y limiter :
  - Nom de l'ordinateur
  - Plage d'adresses IP
  - Système d'exploitation
  - Groupe de sécurité
  - Utilisateur
  - Requêtes WMI (Windows Management Instrumentation)

Démonstration : Configuration des préférences de stratégies de groupe

Cette démonstration montre comment :

- Configurer un raccourci bureau avec des préférences de stratégie de groupe.
- Cibler la préférence.
- Configurer un nouveau dossier avec des préférences de stratégie de groupe.
- Cibler la préférence.
- Tester la préférence.

Procédure de démonstration

Configurer un raccourci sur le bureau avec des préférences de stratégie de groupe

1. Sur la machine LON-DC1, ouvrez la console de gestion de stratégie de groupe puis **Default Domain Policy** pour modification.
2. Accédez à **Configuration ordinateur\Préférences\Paramètres Windows\Raccourcis**.
3. Créez un nouveau raccourci vers le programme Notepad.exe.

Cibler la préférence

- Visez la préférence pour l'ordinateur LON-CL1.

Configurer un nouveau dossier avec des préférences de stratégie de groupe

1. Accédez à **Configuration utilisateur\Préférences\Paramètres Windows\Dossiers**.
2. Créez un dossier pour le dossier **C:\Rapports**.

Cibler la préférence

- Visez cette préférence pour les ordinateurs qui exécutent le système d'exploitation Windows 8.

Tester les préférences

1. Basculez vers la machine LON-CL1 et actualisez les stratégies de groupe en utilisant la commande suivante à l'invite de commandes :

```
gpupdate /force
```

2. Connectez-vous et vérifiez la présence du dossier C:\Rapports et du raccourci vers le Bloc-notes sur le Bureau.

Leçon 4
Gestion des logiciels à l'aide de la stratégie de groupe

Windows Server 2012 comporte une fonctionnalité appelée Installation et maintenance du logiciel qui utilise les services AD DS, la stratégie de groupe et le service Windows Installer pour installer, gérer et supprimer des logiciels sur les ordinateurs de votre organisation. Dans cette leçon, vous allez apprendre à gérer des logiciels avec des stratégies de groupe.

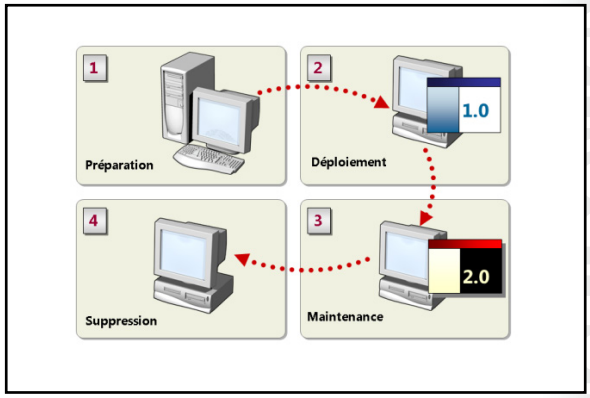
Objectifs de la leçon

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

- Décrire la façon dont la distribution de logiciels grâce à la stratégie de groupe répond au cycle de vie de logiciel.
- Décrire la façon dont Windows Installer améliore la distribution de logiciels.
- Décrire la différence entre attribution et publication de logiciels.
- Expliquer la façon de gérer les mises à jour de logiciel à l'aide des stratégies de groupe.

De quelle façon la distribution de logiciels au moyen de la stratégie de groupe répond au cycle de vie de logiciel

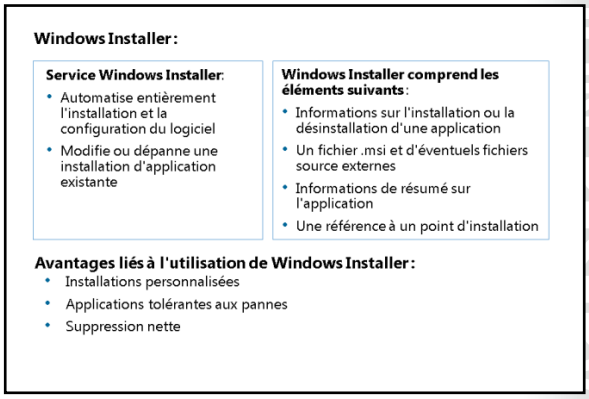
Le cycle de vie des logiciels est composé de quatre phases : préparation, déploiement, maintenance et suppression. Vous pouvez utiliser la stratégie de groupe pour gérer toutes les phases, excepté la préparation. Vous pouvez appliquer des paramètres de stratégie de groupe à des utilisateurs ou des ordinateurs sur un site, un domaine ou une unité d'organisation pour automatiser l'installation, la mise à niveau ou la suppression de logiciels.



L'application de paramètres de stratégie de groupe à des logiciels vous permet de gérer les diverses phases du déploiement de logiciels sans déployer ceux-ci individuellement sur chaque ordinateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comment Windows Installer améliore la distribution de logiciels



Windows Server 2012 utilise le service Windows Installer pour permettre à la stratégie de groupe de déployer et de gérer des logiciels. Ce composant automatise l'installation et la suppression d'applications en appliquant durant le processus d'installation un jeu de règles de configuration définies de façon centralisée. Le service Windows Installer installe les fichiers de package Microsoft Installer (MSI). Les fichiers MSI contiennent une base de données qui enregistre toutes les instructions requises pour installer l'application. De petits applications peuvent être entièrement enregistrées en tant que fichiers MSI, tandis que des applications plus importantes possèderont beaucoup de fichiers sources associés référencés par MSI. Beaucoup de fournisseurs de logiciels fournissent des fichiers MSI pour leurs applications.

Le service Windows Installer possède les caractéristiques suivantes :

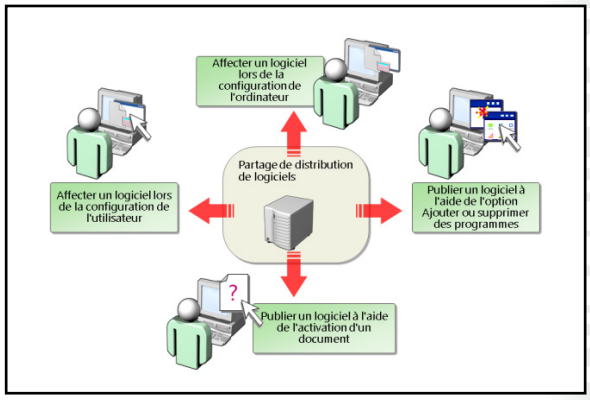
- Ce service fonctionne avec des privilèges élevés, de sorte que le logiciel puisse être installé par le service Windows Installer, peu importe l'utilisateur connecté au système. Les utilisateurs ont uniquement besoin de l'accès au point de distribution de logiciels.
- Les applications sont tolérantes aux pannes. Si une application est corrompue, le service Installer détectera et réinstallera ou réparera l'application.
- Windows Installer ne peut pas installer des fichiers .exe. Pour distribuer un package logiciel qui s'installe avec un fichier .exe, le fichier .exe doit être converti en fichier .msi à l'aide d'un utilitaire tiers.

Question : Les utilisateurs ont-ils besoin de droits d'administration pour installer manuellement les applications qui possèdent des fichiers MSI ?

Question : Pouvez-vous nous citer quelques inconvénients du déploiement de logiciels par la stratégie de groupe ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Publication et attribution de logiciels



Il existe deux types de déploiement disponibles pour livrer le logiciel aux clients. Les administrateurs peuvent soit installer le logiciel pour des utilisateurs ou des ordinateurs à l'avance en attribuant le logiciel, soit donner aux utilisateurs l'option d'installer le logiciel quand ils en ont besoin en publiant le logiciel dans AD DS. Les sections de configuration utilisateur et ordinateur d'un objet de stratégie de groupe possèdent une section de paramètres de logiciel. Vous pouvez ajouter un logiciel à un objet de stratégie de groupe en ajoutant un nouveau package au nœud d'installation de logiciel, puis en précisant s'il faut l'attribuer ou le publier.

Vous pouvez également choisir le déploiement avancé d'un package. Utilisez cette option pour appliquer un fichier de personnalisation à un package pour un déploiement personnalisé. Par exemple, dans le cas où vous utilisez l'outil de personnalisation Office pour créer un fichier de personnalisation de configuration pour déployer Microsoft Office 2010.

Attribution de logiciel

L'attribution de logiciel possède les caractéristiques suivantes :

- Lorsque vous attribuez un logiciel à un utilisateur, le menu Accueil de l'utilisateur publie le logiciel lorsqu'il se connecte. L'installation ne commence pas tant que l'utilisateur n'a pas double-cliqué sur l'icône de l'application ou sur un fichier qui lui est associé.
- Les utilisateurs ne partagent pas des applications déployées. Lorsque vous attribuez le logiciel à un utilisateur, une application que vous installez pour un utilisateur au moyen de la stratégie de groupe ne sera pas disponibles à d'autres utilisateurs.
- En général, lorsque vous attribuez une application à un ordinateur, elle s'installera la prochaine fois que l'ordinateur démarrera. L'application sera à la disposition de tous les utilisateurs de l'ordinateur.

Publication du logiciel

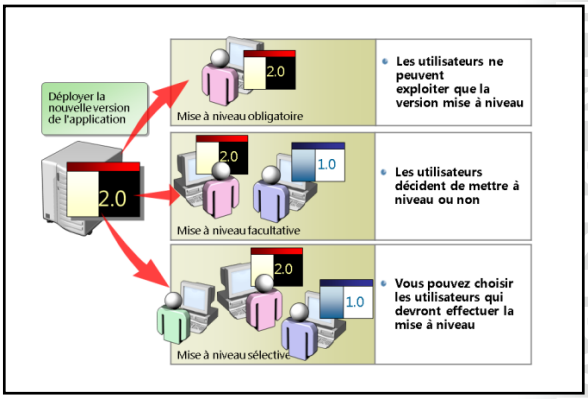
La publication de logiciel possède les caractéristiques suivantes :

- Le raccourci de Programmes dans le panneau de configuration affiche un programme publié à l'utilisateur. Les utilisateurs peuvent installer l'application à l'aide de l'applet de programmes, ou vous pouvez la configurer de sorte que l'activation du document installe l'application.
- Les applications que les utilisateurs n'ont pas l'autorisation d'installer ne sont pas publiées pour eux.
- Les applications ne peuvent pas être publiées pour des ordinateurs.

Remarque : Lorsque vous configurez la stratégie de groupe pour déployer des applications, elles doivent être mappées à des chemins d'accès UNC. Si vous utilisez des chemins locaux, le déploiement échouera.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Administration des mises à niveau de logiciels à l'aide de la stratégie de groupe



Les fournisseurs de logiciels publient des mises à jour de logiciels de temps en temps. Celles-ci abordent habituellement des problèmes mineurs, tels qu'une mise à jour ou des améliorations de fonctionnalité, qui ne justifient pas une réinstallation complète. Microsoft publie des correctifs logiciels comme des fichiers .MSP.

Les mises à jour majeures qui fournissent de nouvelles fonctionnalités requièrent la mise à niveau d'un package logiciel vers une version plus récente. Vous pouvez utiliser l'onglet Mises à niveau pour mettre un package à niveau à l'aide de l'objet de stratégie de groupe. Quand vous effectuerez des mises à niveau à l'aide de la stratégie de groupe, vous remarquerez les caractéristiques suivantes :

- Vous pouvez redéployer un package si le fichier Windows Installer d'origine a été modifié.
- Les mises à niveau supprimeront souvent l'ancienne version d'une application et installeront une version plus récente, conservant habituellement les paramètres d'application.
- Vous pouvez supprimer des packages logiciels s'ils ont été livrés à l'origine à l'aide de la stratégie de groupe. C'est utile si une application sectorielle (LOB) est remplacée par une application différente. La suppression peut être obligatoire ou facultative.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Gestion des bureaux des utilisateurs avec la stratégie de groupe

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à London pour assister le siège social et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

A. Datum vient juste d'ouvrir une nouvelle filiale. Les utilisateurs dans ce bureau ont besoin d'une méthode automatisée pour mapper des lecteurs aux ressources du serveur partagées et vous décidez d'utiliser les préférences de stratégie de groupe. En outre, vous avez été invité à créer un raccourci à l'application Bloc-notes pour tous les utilisateurs qui appartiennent au groupe de sécurité informatique. Pour aider à réduire des tailles de profil, vous avez été invité à configurer la redirection de dossiers pour rediriger plusieurs dossiers de profil vers le lecteur de base de chaque utilisateur.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- Implémenter des paramètres à l'aide des préférences de stratégie de groupe.
- Configurer la redirection de dossiers.

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-CL1
Nom d'utilisateur	**ADATUM\Administrateur**
Mot de passe	**Pa$$w0rd**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
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 la machine 22411B-LON-CL1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Implémentation des paramètres à l'aide des préférences de stratégie de groupe

Scénario

A. Datum utilise des scripts d'ouverture de session pour fournir aux utilisateurs des mappages de lecteur aux partages de fichiers. La maintenance de ces scripts est un problème actuel parce qu'ils sont importants et complexes. Votre gestionnaire vous a demandé d'implémenter les mappages de lecteur à l'aide des préférences de stratégie de groupe de sorte que des scripts d'ouverture de session puissent être supprimés. Vous avez aussi été invité à placer un raccourci à l'application Bloc-notes pour tous les utilisateurs qui appartiennent au groupe de sécurité informatique.

Les tâches principales de cet exercice sont les suivantes :

1. Créer le script d'ouverture de session requis
2. Créer un nouvel objet de stratégie de groupe et le lier à l'unité d'organisation Filiale 1
3. Modifier la stratégie de domaine par défaut avec les préférences de stratégie de groupe requises
4. Tester les préférences

▶ Tâche 1 : Créer le script d'ouverture de session requis

1. Ouvrez une session sur LON-DC1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez l'explorateur de fichiers et créez un dossier, puis partagez-le avec **Des personnes spécifiques** en utilisant les propriétés suivantes :
   - Chemin d'accès : **C:\Branch1**
   - Nom de partage : **Branch1**
   - Autorisations : **Tout le monde, Lecture/écriture**.
3. Lancez le **Bloc-notes**, puis saisissez la commande suivante :

```
Net use S: \\LON-dc1\Branch1
```

4. Sauvegardez le fichier sur le bureau sous le nom **BranchScript.bat**.
5. Sur le bureau, copiez le fichier dans le presse-papiers. Vous collerez le fichier dans le dossier approprié plus tard dans l'atelier pratique.

▶ Tâche 2 : Créer un nouvel objet de stratégie de groupe et le lier à l'unité d'organisation Filiale 1

1. Sur la machine LON-DC1, ouvrez **Utilisateurs et ordinateurs Active Directory**, puis créez une unité d'organisation dans le domaine **Adatum.com** appelée **Filiale 1**.
2. Déplacez l'utilisateur **Holly Dickson** de l'unité d'organisation **IT** à l'unité d'organisation **Filiale 1**.
3. Déplacer l'ordinateur **LON-CL1** vers l'unité d'organisation **Filiale 1**.
4. Ouvrez la console Gestion des stratégies de groupe.
5. Créer un nouvel objet de stratégie de groupe appelé **Branch1** et le lier à l'unité d'organisation **Filiale 1**.

6. Ouvrez l'objet de stratégie de groupe **Branch1** pour édition.
7. Modifiez l'objet de stratégie de groupe pour configurer un script d'ouverture de session utilisateur.
8. Collez le script **BranchScript.bat** dans le partage **Netlogon**.
9. Ajoutez le script **BranchScript.bat** au paramètre d'objet de stratégie de groupe des scripts d'ouverture de session.

▶ Tâche 3 : Modifier la stratégie de domaine par défaut avec les préférences de stratégie de groupe requises

1. Sur la machine LON-DC1, ouvrez **Default Domain Policy** pour modification.
2. Accédez à **Configuration utilisateur\Préférences\Paramètres Windows\Raccourcis**.
3. Créez un nouveau raccourci vers le programme **Notepad.exe** :
   - Nom : **Bloc-notes**
   - Action : **Créer**
   - Emplacement : **Bureau**
   - Chemin d'accès cible : **C:\Windows\notepad.exe**
4. Ciblez la préférence pour des membres du groupe de sécurité **informatique**.
5. Fermez toutes les fenêtres.

▶ Tâche 4 : Tester les préférences

1. Basculez vers la machine LON-CL1 et redémarrez l'ordinateur.
2. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Ouvrez une fenêtre d'invite de commandes et exécutez la commande **gpupdate /force** pour actualiser les paramètres de stratégie de groupe.
4. Déconnectez-vous de LON-CL1.
5. Connectez-vous en tant que **ADATUM\Holly** avec le mot de passe **Pa$$w0rd**.
6. Vérifiez qu'un lecteur est mappé à \\LON-DC1\Branch1.
7. Vérifier que le raccourci vers le Bloc-notes a été ajouté sur le Bureau de Holly.
8. Si le raccourci n'apparaît pas, répétez les étapes 2 à 5.
9. Déconnectez-vous de LON-CL1.

Résultats : À la fin de cet exercice, vous devriez avoir créé les scripts et les paramètres de préférence requis avec succès, et les avoir alors attribués à l'aide des objets de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Configuration de la redirection de dossiers

Scénario

Pour aider à réduire des tailles de profil, vous avez été invité à configurer la redirection de dossiers pour les utilisateurs de la filiale afin de rediriger plusieurs dossiers de profil vers le lecteur de base de chaque utilisateur.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un répertoire partagé pour stocker les dossiers redirigés
2. Créer un nouvel objet de stratégie de groupe et le lier à l'unité d'organisation de la filiale
3. Modifier les paramètres de redirection de dossiers dans la stratégie
4. Tester le paramètre de redirection de dossiers
5. Pour préparer le module suivant

▶ Tâche 1 : Créer un répertoire partagé pour stocker les dossiers redirigés

- Sur LON-DC1, ouvrez l'explorateur de fichiers et créez un dossier, puis partagez-le avec **Des personnes spécifiques** en utilisant les propriétés suivantes :
  - Chemin d'accès : **C:\Branch1\Redirect**
  - Nom de partage : **Branch1Redirect**
  - Autorisations : **Tout le monde**, **Lecture/écriture**.

▶ Tâche 2 : Créer un nouvel objet de stratégie de groupe et le lier à l'unité d'organisation de la filiale

- Sur LON-DC1, ouvrez la console de gestion des stratégies de groupe, puis créez et liez un objet de stratégie de groupe nommé **Redirection de dossiers** à l'unité d'organisation **Filiale 1**.

▶ Tâche 3 : Modifier les paramètres de redirection de dossiers dans la stratégie

1. Ouvrez l'objet de stratégie de groupe **Redirection de dossier** pour le modifier.
2. Sous Configuration utilisateur, accédez à la redirection de dossiers puis configurez les propriétés du dossier **Documents** pour utiliser le paramètre **De base - Rediriger les dossiers de tout le monde vers le même emplacement**.
3. Vérifiez que l'emplacement du **dossier cible** est défini sur Créer un dossier pour chaque utilisateur sous le chemin d'accès racine.
4. Précisez le chemin d'accès de la racine : **\\LON-DC1\Branch1Redirect**.
5. Fermez toutes les fenêtres ouvertes sur LON-DC1.

▶ Tâche 4 : Tester le paramètre de redirection de dossiers

1. Basculez vers LON-CL1.
2. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

3. Ouvrez une fenêtre d'invite de commandes et exécutez la commande **gpupdate /force** pour actualiser la stratégie de groupe.
4. Déconnectez-vous, puis reconnectez-vous en tant que **ADATUM\Holly** avec le mot de passe **Pa$$word**.
5. Accédez au bureau.,
6. Cliquez avec le bouton droit sur le Bureau et utilisez le menu de personnalisation pour activer **Les fichiers d'utilisateur** sur le bureau.
7. À partir du bureau, ouvrez le dossier **Holly Dickson**.
8. Cliquez avec le bouton droit sur **Mes documents**, puis cliquez sur **Propriétés**.
9. Dans la boîte de dialogue **Propriétés de : Mes documents**, remarquez que l'emplacement du dossier est désormais le partage réseau dans un sous-dossier nommé comme l'utilisateur.
10. Si la redirection de dossiers n'est pas claire, déconnectez-vous, et connectez-vous en tant que **ADATUM\Holly** avec le mot de passe **Pa$$word**. Répétez les étapes 7 à 9.
11. Déconnectez-vous de LON-CL1.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, 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 **22411B-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 **22411B-LON-CL1**.

Résultats : À la fin de cet exercice, vous devriez avoir configuré avec succès la redirection de dossiers vers un dossier partagé sur le serveur LON-DC1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthodes conseillées concernant la gestion de stratégie de groupe

- Intégrer des commentaires sur les paramètres de l'objet de stratégie de groupe
- Utiliser un magasin central pour des modèles d'administration avec des clients sous Windows Vista, Windows 7 et Windows 8
- Utiliser les préférences de stratégie de groupe pour configurer les paramètres qui ne sont pas disponibles dans l'ensemble de paramètres de la stratégie de groupe
- Utiliser l'installation de logiciel de stratégie de groupe pour déployer des packages au format .msi pour un grand nombre d'utilisateurs ou d'ordinateurs

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Vous avez configuré la redirection de dossiers pour une unité d'organisation mais aucun des dossiers de l'utilisateur n'est redirigé sur l'emplacement réseau. Lorsque vous regardez dans le dossier racine, vous observez qu'un sous-répertoire nommé pour chaque utilisateur a été créé, mais il est vide.	
Vous avez attribué une application à une unité d'organisation. Après plusieurs ouvertures de session, les utilisateurs soulignent que personne n'a installé l'application.	
Vous possédez un mélange d'ordinateurs sous Windows XP et Windows 8. Après avoir configuré plusieurs paramètres dans les modèles d'administration d'un objet de stratégie de groupe, les utilisateurs du système d'exploitation Windows XP remarquent que certains paramètres sont appliqués et que d'autres ne le sont pas.	
Certaines préférences de stratégie de groupe ne sont pas appliquées.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Questions de contrôle des acquis

Question : Pourquoi certains paramètres de stratégie de groupe nécessitent-ils deux ouvertures de session avant d'être actifs ?

Question : Comment pouvez-vous prendre en charge des préférences de stratégie de groupe sur Windows XP ?

Question : Quel est l'avantage de posséder un magasin central ?

Question : Quelle est la principale différence entre les paramètres de stratégie de groupe et les préférences de stratégie de groupe ?

Question : Quelle est la différence entre publier et attribuer un logiciel au moyen de la stratégie de groupe ?

Question : Pouvez-vous utiliser des scripts Windows PowerShell comme scripts de démarrage ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 7

Configuration et résolution des problèmes d'accès à distance

Table des matières :

Vue d'ensemble du module **7-1**

Leçon 1 : Configuration de l'accès réseau **7-2**

Leçon 2 : Configuration de l'accès VPN **7-11**

Leçon 3 : Vue d'ensemble des stratégies réseau **7-22**

Leçon 4 : Résolution des problèmes du service de routage et d'accès à distance **7-29**

Atelier pratique A : Configuration de l'accès à distance **7-36**

Leçon 5 : Configuration de DirectAccess **7-41**

Atelier pratique B : Configuration de DirectAccess **7-56**

Contrôle des acquis et éléments à retenir **7-66**

Vue d'ensemble du module

La plupart des organisations ont des utilisateurs qui travaillent à distance, peut-être depuis leur domicile ou sur des sites client. Pour faciliter ces connexions à distance, vous devez mettre en œuvre des technologies d'accès à distance pour prendre en charge cette main-d'œuvre distribuée. Vous devez vous familiariser avec les technologies qui permettent aux utilisateurs distants de se connecter à l'infrastructure réseau de votre organisation. Ces technologies comprennent les réseaux privés virtuels (VPN) et DirectAccess, une fonctionnalité des systèmes d'exploitation Windows® 7 et Windows 8. Il est important que vous compreniez comment configurer et sécuriser vos clients d'accès à distance à l'aide des stratégies réseau. Ce module décrit ces technologies d'accès à distance.

Objectifs

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

- configurer l'accès réseau ;
- créer et configurer une solution VPN ;
- décrire le rôle des stratégies réseau ;
- dépanner le service de routage et d'accès à distance ;
- configurer DirectAccess.

Leçon 1
Configuration de l'accès réseau

L'accès réseau au sein du système d'exploitation Windows Server® 2012 fournit les services requis permettant aux utilisateurs distants de se connecter à votre réseau. Pour prendre en charge les besoins de votre organisation et de vos utilisateurs distants, il est important que vous puissiez installer et configurer ces composants d'accès réseau Windows Server 2012 avec succès.

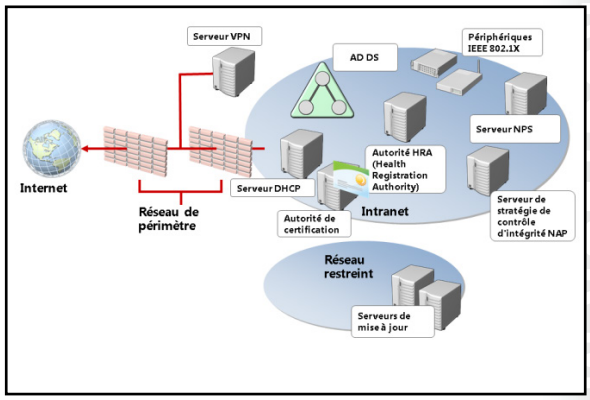
Objectifs de la leçon

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

- décrire les composants d'une infrastructure de services d'accès réseau ;
- décrire le rôle Services de stratégie et d'accès réseau ;
- décrire le service Routage et accès distant ;
- expliquer ce que sont l'autorisation et l'authentification de l'accès réseau ;
- expliquer les méthodes d'authentification utilisées dans le cadre d'un accès réseau ;
- décrire une infrastructure à clé publique (PKI) ;
- expliquer le mode d'utilisation des serveurs DHCP (Dynamic Host Configuration Protocol) avec le service Routage et accès distant.

Composants d'une infrastructure de services d'accès réseau

L'infrastructure sous-jacente d'une infrastructure de services d'accès réseau complète dans Windows Server 2012 inclut généralement les composants suivants :



- *Serveur de réseau privé virtuel (VPN)*. Fournit la connectivité d'accès à distance en fonction de différents protocoles de tunneling VPN sur un réseau public, comme Internet.
- Services de domaine Active Directory® (AD DS). Répondent aux demandes d'authentification lors des tentatives de connexion des clients d'accès à distance.
- Services de certificats Active Directory (AD CS). Vous pouvez utiliser des certificats numériques pour fournir l'authentification dans des scénarios d'accès à distance. En déployant AD CS, vous pouvez créer une infrastructure à clé publique dans votre organisation afin de prendre en charge la délivrance, la gestion et la révocation des certificats.
- Serveur DHCP. Fournit une configuration IP aux connexions d'accès à distance entrantes acceptées pour la connectivité réseau au réseau local de l'entreprise.

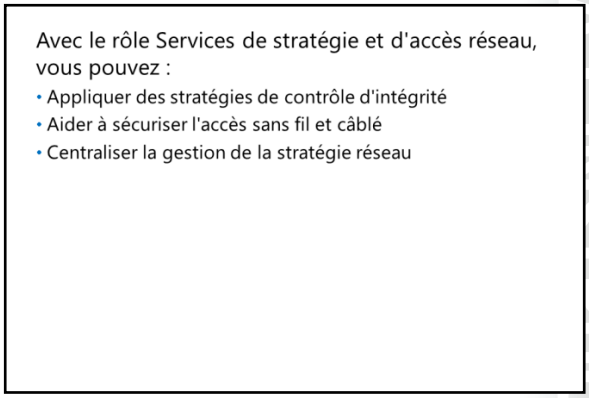
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Network Policy Server (NPS). Fournit des services d'authentification pour d'autres composants d'accès réseau.
- Composants de protection d'accès réseau (NAP) :
  - Serveur de stratégie de contrôle d'intégrité NAP. Évalue l'intégrité du système par rapport aux stratégies de contrôle d'intégrité configurées qui décrivent des spécifications d'intégrité et des comportements de mise en œuvre ; par exemple, les clients qui se connectent doivent être en conformité pour accéder au réseau.
  - Autorité HRA (Health Registration Authority). Obtient des certificats d'intégrité pour les clients qui passent avec succès la vérification de la stratégie de contrôle d'intégrité.
  - Serveurs de mise à jour. Proposent des services de mise à jour aux clients qui ne répondent pas aux conditions d'intégrité du réseau d'entreprise. Les serveurs de mise à jour sont des serveurs spéciaux sur un réseau limité.

Qu'est-ce que le rôle Services de stratégie et d'accès réseau ?

Le rôle Services de stratégie et d'accès réseau dans Windows Server 2012 fournit les solutions de connectivité réseau suivantes :

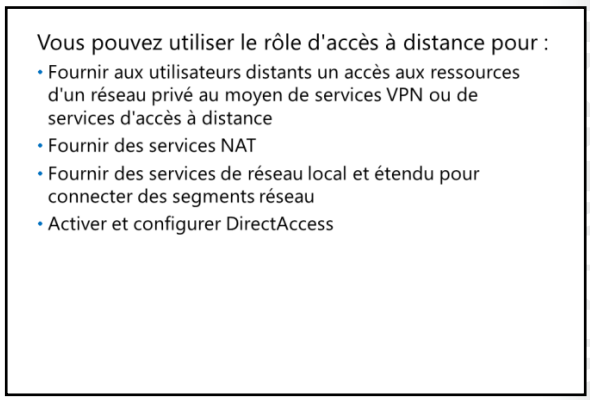


- Applique les stratégies de contrôle d'intégrité. Établit et applique automatiquement les stratégies de contrôle d'intégrité. Ces stratégies définissent les configurations requises en matière de logiciels, de matériel et de mise à jour de sécurité.
- Fournit un accès sans fil et câblé sécurisé. Lorsque vous déployez des points d'accès sans fil 802.1X, l'accès sans fil sécurisé offre aux utilisateurs sans fil une méthode d'authentification facile à déployer reposant sur un certificat ou un mot de passe sécurisé. Lorsque vous déployez des commutateurs d'authentification 802.1X, ces derniers vous permettent de sécuriser votre réseau câblé en veillant à ce que les utilisateurs de l'intranet soient authentifiés avant qu'ils ne puissent se connecter au réseau ou obtenir une adresse IP à l'aide du protocole DHCP.
- Centralise la gestion de la stratégie réseau avec un serveur et un proxy RADIUS (Remote Authentication Dial-in User Service). Plutôt que configurer la stratégie d'accès réseau au niveau de chaque serveur d'accès réseau (tel que les points d'accès sans fil, les commutateurs d'authentification 802.1X, les serveurs VPN et les serveurs d'accès à distance), vous pouvez créer à un seul et même emplacement des stratégies qui spécifient tous les aspects des demandes de connexion réseau. Ces stratégies peuvent inclure qui est autorisé à se connecter, à quel moment et quel niveau de sécurité doit être utilisé pour la connexion à votre réseau.

Remarque : Les composants d'accès à distance constituent un rôle serveur distinct dans Windows Server 2012.

Qu'est-ce que le rôle Accès à distance ?

Le rôle Accès à distance permet de fournir aux utilisateurs l'accès à distance au réseau de votre organisation à l'aide de l'une des technologies suivantes :



- Accès VPN. Un VPN fournit une connexion point à point entre les composants d'un réseau privé via un réseau public, comme Internet, par exemple. Les protocoles de tunneling permettent à un client VPN d'établir et de gérer une connexion au port virtuel d'écoute d'un serveur VPN. Vous pouvez également connecter des succursales à votre réseau à l'aide de solutions VPN, déployer des routeurs logiciels complets sur votre réseau et partager des connexions Internet sur l'intranet.
- DirectAccess. DirectAccess active l'accès à distance transparent aux ressources intranet sans établir de connexion VPN au préalable. DirectAccess fournit une connectivité transparente à l'infrastructure d'applications pour les utilisateurs internes et distants.

Vous pouvez déployer les technologies suivantes au cours de l'installation du rôle Accès à distance :

- Service d'accès à distance (RAS) DirectAccess et VPN. Le service d'accès à distance DirectAccess et VPN permet d'activer et de configurer :
  - des solutions DirectAccess pour votre organisation ;
  - des connexions VPN pour fournir aux utilisateurs finaux l'accès à distance au réseau de votre organisation.
- Service de routage. Il fournit un routeur logiciel complet ainsi qu'une plateforme ouverte pour le routage et l'interconnexion. Il offre des services de routage aux entreprises dans le réseau local et les environnements de réseau étendu.

  Lorsque vous choisissez le routage, la traduction d'adresses réseau (NAT) est également installée. Lorsque vous déployez la traduction NAT, le serveur qui exécute l'accès à distance est configuré pour partager une connexion Internet avec les ordinateurs d'un réseau privé et pour traduire le trafic entre son adresse publique et le réseau privé. Avec la traduction NAT, les ordinateurs du réseau privé profitent d'une certaine protection dans la mesure où le routeur sur lequel vous configurez la traduction NAT ne transfère pas le trafic Internet dans le réseau privé, à moins qu'un client du réseau privé ne le demande ou que le trafic soit explicitement autorisé.

  Lorsque vous déployez une connexion VPN et la traduction NAT, vous configurez le serveur qui exécute l'accès à distance pour fournir la traduction NAT au réseau privé et accepter les connexions VPN. Les ordinateurs sur Internet ne pourront pas déterminer les adresses IP des ordinateurs sur le réseau privé. Toutefois, les clients VPN pourront se connecter aux ordinateurs sur le réseau privé comme s'ils étaient connectés au même réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Authentification réseau et autorisation

Il est essentiel de bien saisir la différence entre l'authentification et l'autorisation pour comprendre pourquoi les tentatives de connexion sont acceptées ou refusées.

- Authentification :
  - Vérifie les informations d'identification d'une tentative de connexion
  - Utilise un protocole d'authentification pour envoyer les informations d'identification du client d'accès à distance au serveur d'accès à distance sous la forme de texte en clair ou sous forme chiffrée
- L'autorisation :
  - Vérifie que la tentative de connexion est autorisée
  - Se produit une fois que l'authentification a réussi

- L'authentification est la vérification des informations d'identification lors de la tentative de connexion. Ce processus consiste à envoyer les informations d'identification du client d'accès à distance au serveur d'accès à distance sous forme de texte en clair ou sous forme chiffrée à l'aide d'un protocole d'authentification.
- L'autorisation est la procédure par laquelle le serveur vérifie que la tentative de connexion est autorisée. La phase d'autorisation ne se déroule qu'en cas de réussite de la phase d'authentification.

Pour qu'une tentative de connexion soit acceptée, elle doit être authentifiée et autorisée. Il est possible qu'elle soit authentifiée en utilisant des informations d'identification valides, mais qu'elle ne soit pas autorisée ; dans ce cas, la tentative de connexion est refusée.

Si vous configurez un serveur d'accès à distance pour l'authentification Windows, les fonctionnalités de sécurité de Windows Server 2012 vérifient les informations d'authentification, tandis que les propriétés de numérotation du compte d'utilisateur et les stratégies d'accès à distance stockées localement autorisent la connexion. Si la tentative de connexion est à la fois authentifiée et autorisée, elle est alors acceptée.

Si vous configurez le serveur d'accès à distance pour l'authentification RADIUS, les informations d'identification de la tentative de connexion sont transmises au serveur RADIUS à des fins d'authentification et d'autorisation. Si la tentative de connexion est à la fois authentifiée et autorisée, le serveur RADIUS renvoie un message d'acceptation au serveur d'accès à distance et la tentative de connexion est acceptée. Si la tentative de connexion n'est pas authentifiée ou n'est pas autorisée, le serveur RADIUS renvoie un message de refus au serveur d'accès à distance et la tentative de connexion est refusée.

Méthodes d'authentification

L'authentification des clients d'accès constitue un problème important en matière de sécurité. En règle générale, les méthodes d'authentification utilisent un protocole d'authentification qui est négocié lors de l'établissement de la connexion. Les méthodes suivantes sont prises en charge par le rôle Accès à distance.

Protocole	Description	Niveau de sécurité
PAP	Mots de passe en clair. Généralement utilisé si le client d'accès à distance et le serveur d'accès à distance ne peuvent pas négocier une forme de validation plus sécurisée	Protocole d'authentification le moins sécurisé. N'offre aucune protection contre les attaques par relecture, l'emprunt d'identité du client distant et l'emprunt d'identité du serveur distant
CHAP	Protocole d'authentification de type demande/réponse qui utilise le schéma de hachage MD5	Sécurité accrue par rapport au protocole PAP dans le sens où le mot de passe n'est pas envoyé sur le lien PPP Une version en clair du mot de passe est requise pour valider la réponse à la demande d'accès. N'offre aucune protection contre l'emprunt d'identité du serveur distant
MS-CHAPv2	Mise à niveau du protocole MS-CHAP. Propose une authentification bidirectionnelle, également appelée authentification mutuelle. Le client d'accès à distance reçoit confirmation que le serveur d'accès à distance auquel il tente d'accéder a accès au mot de passe de l'utilisateur	Assure une plus forte sécurité que le protocole CHAP
EAP	Permet l'authentification arbitraire d'une connexion d'accès à distance en utilisant des modèles d'authentification, appelés types de protocole EAP	Offre la plus forte sécurité en proposant la plus grande flexibilité en termes de solutions d'authentification

PAP

Le protocole PAP (Password Authentication Protocol) utilise des mots de passe en clair et est le moins sécurisé des protocoles d'authentification. Il est généralement négocié si le client et le serveur d'accès à distance ne parviennent pas à négocier une forme plus sécurisée de validation. Le protocole PAP, inclus dans Microsoft Windows Server 2012, prend en charge des systèmes d'exploitation clients antérieurs ne prenant en charge aucune autre méthode d'authentification.

CHAP

Le protocole CHAP (Challenge Handshake Authentication Protocol) est un protocole d'authentification par demande d'accès/réponse qui utilise le schéma de hachage MD5 standard pour chiffrer la réponse. Plusieurs fournisseurs de clients et serveurs d'accès réseau utilisent le protocole CHAP. Dans la mesure où le protocole CHAP requiert l'utilisation d'un mot de passe chiffré réversible, vous devez envisager d'utiliser un autre protocole d'authentification, comme Microsoft® Challenge Handshake Authentication Protocol (MS-CHAP) version 2.

MS-CHAP V2

Le protocole MS-CHAP v2 est un processus d'authentification mutuelle par mot de passe chiffré à sens unique. Il fonctionne comme suit :

1. L'authentificateur (serveur d'accès à distance ou ordinateur qui exécute NPS) envoie au client d'accès à distance une demande d'accès. Celle-ci se compose d'un identificateur de session et d'une chaîne de demande d'accès arbitraire.
2. Le client d'accès à distance envoie une réponse qui contient un chiffrement à sens unique de la chaîne de demande d'accès reçue, la chaîne de demande d'accès de l'homologue arbitraire, l'identificateur de session et le mot de passe de l'utilisateur.
3. L'authentificateur vérifie la réponse du client et renvoie une réponse contenant une indication de la réussite ou de l'échec de la tentative de connexion et une réponse authentifiée reposant sur la chaîne de demande d'accès envoyée, la chaîne de demande d'accès de l'homologue, la réponse chiffrée du client et le mot de passe de l'utilisateur.
4. Le client d'accès à distance vérifie la réponse d'authentification et utilise la connexion si celle-ci est valide. Si la réponse d'authentification est incorrecte, le client d'accès à distance met fin à la connexion.

EAP

Le protocole EAP (Extensible Authentication Protocol) est un mécanisme d'authentification arbitraire qui permet d'authentifier une connexion d'accès à distance. Le client d'accès à distance et l'authentificateur (le serveur d'accès à distance ou le serveur RADIUS) négocient le modèle d'authentification exact à utiliser. Le service Routage et accès distant inclut la prise en charge du protocole EAP-TLS (EAP-Transport Layer Security) par défaut. Vous pouvez de ce fait connecter d'autres modules EAP au serveur exécutant le service Routage et accès distant de manière à fournir d'autres méthodes EAP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

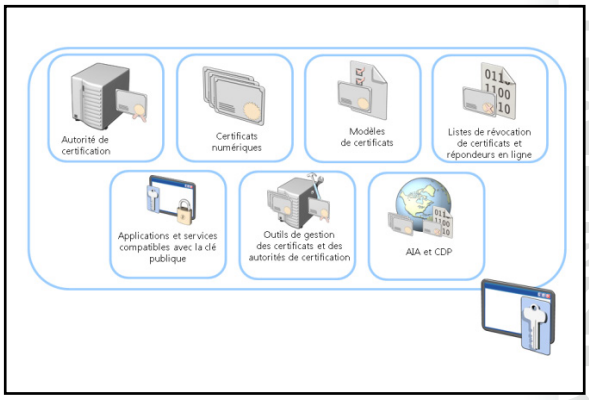
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Autres options

Outre les méthodes d'authentification précédemment mentionnées, il existe deux autres options que vous pouvez activer lors de la sélection d'une méthode d'authentification :

- Accès non authentifié. Il ne s'agit pas d'une méthode d'authentification à proprement parler, mais plutôt de l'absence d'une méthode. L'accès non authentifié permet aux systèmes distants de se connecter sans authentification. Toutefois, cette option ne doit en aucun cas être activée dans un environnement de production, car elle constitue un risque pour votre réseau. Néanmoins, elle peut parfois s'avérer utile pour résoudre les problèmes d'authentification dans un environnement de test.
- Certificat d'ordinateur pour IKEv2 (Internet Key Exchange version 2). Sélectionnez cette option pour utiliser la Reconnexion VPN.

Qu'est-ce qu'une infrastructure à clé publique ?



Une infrastructure à clé publique se compose de plusieurs composants qui permettent de sécuriser les communications et transactions de l'entreprise, notamment celles utilisées dans des scénarios d'accès à distance. Différents composants fonctionnent ensemble pour fournir une solution PKI complète. Les composants PKI de Windows Server 2012 sont les suivants :

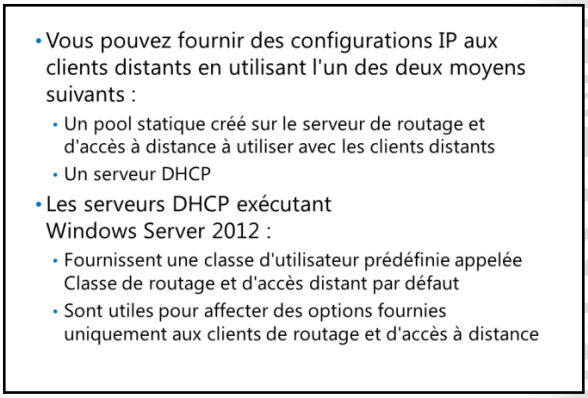
- *Autorité de certification (CA)*. L'autorité de certification émet et gère les certificats numériques pour les utilisateurs, les ordinateurs et les services. En déployant l'autorité de certification, vous établissez l'infrastructure à clé publique dans votre organisation.
- *Certificats numériques*. Les certificats numériques s'apparentent à un passeport électronique. Un certificat numérique est utilisé pour justifier l'identité de l'utilisateur (ou de toute autre entité). Il contient des informations d'identification électroniques associées à une clé publique et à une clé privée, utilisées pour authentifier des utilisateurs et d'autres périphériques tels que des serveurs Web et des serveurs de messagerie. Les certificats numériques garantissent également qu'un logiciel ou du code est exécuté à partir d'une source approuvée. Ils contiennent différents champs, tels que **Objet**, **Émetteur** et **Nom commun**. Ces champs sont utilisés pour déterminer l'utilisation spécifique du certificat. Par exemple, un certificat de serveur Web peut comporter le champ **Nom commun** de **web01.contoso.com**, ce qui rendrait ce certificat valide uniquement pour ce serveur Web. Si une tentative venait à être effectuée pour utiliser ce certificat sur un serveur Web nommé **web02.contoso.com**, l'utilisateur de ce serveur recevrait alors un avertissement.
- *Modèles de certificats*. Ce composant décrit le contenu ainsi que l'objectif d'un certificat numérique. Lors de la demande d'un certificat auprès d'une autorité de certification d'entreprise AD CS, le demandeur de certificat peut, en fonction de ses droits d'accès, faire un choix parmi plusieurs types de certificats basés sur des modèles de certificats, tels que les modèles Utilisateur et Signature du code. Le modèle de certificat enregistre les utilisateurs de bas niveau et les décisions techniques relatives au type de certificat dont ils ont besoin. En outre, il permet aux administrateurs d'identifier le demandeur et le type de certificat demandé.

- *Listes de révocation de certificats et répondeurs en ligne*.
  - Les listes de révocation de certificats consistent en des listes complètes numériquement signées de certificats révoqués. Ces listes sont publiées périodiquement et peuvent être récupérées et mises en cache par les clients, selon la durée de vie configurée de la liste de révocation de certificats. Elles sont utilisées pour vérifier l'état de la révocation d'un certificat.
  - Les répondeurs en ligne font partie du service de rôle OCSP (Online Certificate Status Protocol) de Windows Server 2008 et Windows Server 2012. Un répondeur en ligne peut recevoir une demande de vérification de la révocation d'un certificat sans que le client ait besoin de télécharger la liste de révocation de certificats complète. Cette opération accélère le processus de vérification de la révocation de certificats et réduit la bande passante réseau. Elle améliore également l'évolutivité et la tolérance de panne en permettant la configuration de groupe des répondeurs en ligne.
- *Applications et services basés sur une clé publique*. Il s'agit des applications ou des services qui prennent en charge le chiffrement par clé publique. En d'autres termes, l'application ou les services doivent pouvoir prendre en charge les implémentations de clé publique pour en tirer profit.
- *Outils de gestion des certificats et des autorités de certification*. Les outils de gestion fournissent les outils basés sur l'interface graphique utilisateur et sur la ligne de commande pour :
  - configurer les autorités de certification ;
  - récupérer les clés privées archivées ;
  - importer et exporter les certificats et les clés ;
  - publier les certificats des autorités de certification et les listes de révocation de certificats ;
  - gérer les certificats émis.
- *Accès aux informations de l'autorité (AIA) et points de distribution de la liste de révocation de certificats (CDP)*. Les points d'accès aux informations de l'autorité déterminent l'emplacement de recherche et de validation des certificats des autorités de certification, et les emplacements de points de distribution de la liste de révocation de certificats déterminent les points de recherche des listes de révocation de certificats pendant le processus de validation du certificat. Dans la mesure où les listes de révocation de certificats peuvent devenir volumineuses (en fonction du nombre de certificats émis et révoqués par une autorité de certification), vous pouvez également publier des listes de révocation de certificats temporaires plus limitées appelées *listes de révocation de certificats delta*. Les listes de révocation de certificats delta contiennent uniquement les certificats révoqués depuis la publication de la dernière liste CRL standard. Cela permet aux clients de récupérer les listes de révocation de certificats delta plus petites et d'établir plus rapidement la liste complète des certificats révoqués. Les listes de révocation de certificats delta permettent également de publier plus fréquemment les données de révocation, dans la mesure où leur transfert s'effectue plus rapidement que celui des listes CRL complètes.
- *Module de sécurité matériel (HSM, Hardware security module)*. Un module de sécurité matériel est un périphérique matériel de chiffrement sécurisé facultatif qui accélère le traitement du chiffrement en vue de gérer les codes numériques. Ce matériel de stockage spécialisé hautement sécurisé est connecté à l'autorité de certification afin de gérer les certificats. En règle générale, le module de sécurité matériel est physiquement raccordé à un ordinateur. Il consiste en un module complémentaire facultatif de l'infrastructure à clé publique, et est plus fréquemment utilisé dans les environnements de haute sécurité dans lesquels les répercussions seraient importantes si une clé venait à être compromise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Intégration du protocole DHCP au service Routage et accès distant

Vous pouvez déployer le rôle DHCP avec le rôle Accès à distance afin de fournir aux clients d'accès à distance une adresse IP affectée de manière dynamique pendant la connexion. Lorsque vous utilisez ces deux services sur le même serveur, les informations fournies pendant la configuration dynamique le sont d'une manière différente par rapport à la configuration DHCP classique des clients de réseau local.



Dans les environnements de réseau local, les clients DHCP négocient et reçoivent les informations de configuration suivantes, en fonction uniquement des paramètres que vous configurez dans la console DHCP du serveur DHCP :

- Une adresse IP allouée extraite du pool d'adresses disponibles d'une portée active sur le serveur DHCP. Le serveur DHCP gère l'adresse et la distribue directement au client DHCP sur le réseau local.
- Des paramètres supplémentaires et d'autres informations de configuration fournis par les options DHCP affectées dans le bail d'adresse. Les valeurs et la liste d'options correspondent aux types d'options que vous configurez et que vous affectez sur le serveur DHCP.

Lorsqu'un serveur d'accès à distance propose une configuration dynamique pour les clients d'accès à distance, il commence par exécuter les étapes suivantes :

1. Lorsque le serveur qui exécute le service d'accès à distance démarre avec l'option Utiliser DHCP pour attribuer des adresses TCP/IP distantes, il indique au client DHCP qu'il doit obtenir 10 adresses IP auprès d'un serveur DHCP.
2. Le serveur d'accès à distance utilise la première des 10 adresses IP obtenues auprès du serveur DHCP pour l'interface du serveur d'accès à distance.
3. Les neuf adresses restantes sont allouées aux clients TCP/IP lorsqu'ils établissent une session sur le serveur d'accès à distance.

Les adresses IP qui sont libérées lorsque les clients d'accès à distance se déconnectent sont réutilisées. Lorsque les 10 adresses IP sont utilisées, le serveur d'accès à distance en obtient 10 de plus auprès d'un serveur DHCP. Lorsque le service Routage et accès distant s'arrête, toutes les adresses IP obtenues via le serveur DHCP sont libérées.

Lorsque le serveur d'accès à distance utilise ce type de mise en cache proactive des baux d'adresses DHCP pour les clients d'accès à distance, il enregistre les informations suivantes pour chaque réponse de bail obtenue du serveur DHCP :

- l'adresse IP du serveur DHCP ;
- l'adresse IP allouée par le client (pour une distribution ultérieure au client du service de routage et d'accès à distance) ;
- l'heure à laquelle le bail a été obtenu ;
- l'heure à laquelle le bail expire ;
- la durée du bail.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Toutes les autres informations renvoyées par le serveur DHCP relatives aux options DHCP comme les options de serveur, de portée ou de réservation, sont ignorées. Lorsque le client se connecte au serveur et demande une adresse IP (autrement dit, lorsque Adresse IP attribuée par serveur est sélectionné), il utilise un bail DHCP mis en cache pour fournir au client d'accès à distance une configuration d'adresse IP dynamique.

Lorsque l'adresse IP est fournie au client d'accès à distance, le client ne sait pas que cette adresse a été obtenue via ce processus intermédiaire entre le serveur DHCP et le serveur d'accès à distance. Le serveur d'accès à distance maintient le bail au nom du client. Par conséquent, la seule information que le client reçoit du serveur DHCP est l'adresse IP.

Dans les environnements d'accès à distance, les clients DHCP négocient et reçoivent la configuration dynamique de la manière suivante, qui est légèrement différente :

- Une adresse IP allouée provenant du cache d'adresses de portée DHCP sur le serveur de routage et d'accès à distance. Le serveur de routage et d'accès à distance obtient et renouvelle son pool d'adresses mis en cache sur le serveur DHCP.
- Si le serveur DHCP fournit normalement les paramètres supplémentaires et les autres informations de configuration fournis grâce à des options DHCP affectées dans le bail d'adresse, ces informations sont renvoyées au client d'accès à distance en fonction des propriétés TCP/IP configurées sur le serveur d'accès à distance.

 **Remarque :** Les serveurs DHCP qui exécutent Windows Server 2012 fournissent une classe d'utilisateur prédéfinie (la Classe de routage et d'accès distant par défaut) pour affecter des options fournies uniquement aux clients de routage et d'accès à distance. Pour affecter ces options, vous devez créer une stratégie DHCP avec la condition selon laquelle **la classe d'utilisateur équivaut à la classe de routage et d'accès distant par défaut**. Configurez ensuite les options requises.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration de l'accès VPN

Pour implémenter correctement et prendre en charge un environnement VPN au sein de votre organisation, il est important de comprendre comment sélectionner un protocole de tunneling approprié, configurer l'authentification VPN et configurer le rôle serveur Services de stratégie et d'accès réseau pour prendre en charge la configuration de votre choix.

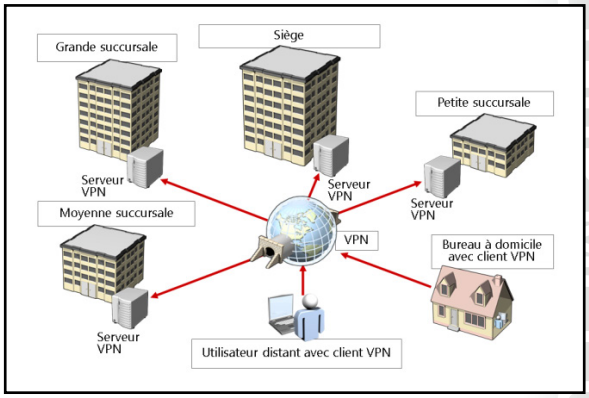
Objectifs de la leçon

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

- décrire ce qu'est une connexion VPN et la manière dont elle est utilisée pour connecter des clients de réseau distant ;
- décrire les protocoles de tunneling utilisés pour une connexion VPN ;
- décrire la reconnexion VPN ;
- décrire les conditions requises de la configuration liées à une connexion VPN ;
- expliquer comment configurer un accès VPN ;
- décrire les tâches supplémentaires qui peuvent être exécutées à l'issue de la configuration d'un serveur VPN ;
- décrire les fonctionnalités et les avantages du Kit d'administration du Gestionnaire des connexions ;
- expliquer comment créer un profil de connexion à l'aide du Kit d'administration du Gestionnaire des connexions.

Qu'est-ce qu'une connexion VPN ?

Pour émuler une liaison point à point, les données sont encapsulées (ou enrobées) et préfixées à l'aide d'un en-tête qui contient les informations de routage, lesquelles permettent aux données de traverser le réseau partagé ou public jusqu'à leur destination finale.



Pour émuler une liaison privée, les données sont chiffrées afin d'assurer la confidentialité. Les paquets qui sont interceptés sur le réseau partagé ou public sont indéchiffrables sans clé de chiffrement. La liaison dans laquelle les données privées sont encapsulées et chiffrées est appelée *connexion VPN*.

Il existe deux types de connexions VPN :

- accès à distance ;
- de site à site.

VPN d'accès à distance

Les connexions VPN d'accès à distance permettent aux utilisateurs qui travaillent hors site (par exemple, à la maison, chez un client, ou à partir d'un point d'accès sans fil public) d'accéder à un serveur sur le réseau privé de votre organisation en utilisant l'infrastructure mise à disposition par un réseau public, comme Internet. Du côté de l'utilisateur, la connexion VPN est une connexion point à point entre l'ordinateur, le client VPN et le serveur de votre organisation. L'infrastructure exacte du réseau partagé ou public n'a pas d'importance car cette connexion fonctionne logiquement comme si les données étaient envoyées sur une liaison privée dédiée.

Connexion VPN de site à site

Les connexions VPN de site à site (également appelées connexions VPN routeur à routeur) permettent à votre organisation d'utiliser des connexions routées entre des bureaux éloignés les uns des autres (ou avec d'autres organisations) sur un réseau public tout en assurant la sécurité des communications. Une connexion VPN routée sur Internet fonctionne logiquement comme une liaison de réseau étendue dédiée. Lorsque des réseaux se connectent via Internet, un routeur transmet les paquets à un autre routeur par l'intermédiaire d'une connexion VPN. Du côté des routeurs, la connexion VPN fonctionne comme une liaison de couche de liaison de données.

Une connexion VPN de site à site connecte deux segments d'un réseau privé. Le serveur VPN fournit une connexion routée vers le réseau auquel le serveur VPN est rattaché. Le routeur appelant (le client VPN) s'authentifie auprès du routeur répondant (le serveur VPN) et, réciproquement, le routeur répondant s'authentifie auprès du routeur appelant. Dans une connexion VPN de site à site, les paquets envoyés par l'un ou l'autre des routeurs via la connexion VPN ne proviennent généralement pas des routeurs.

Propriétés des connexions VPN

Les connexions VPN qui utilisent le protocole PPTP (Point-to-Point Tunneling Protocol), le protocole L2TP/IPsec (Layer Two Tunneling Protocol/Internet Protocol security) ou le protocole SSTP (Secure Socket Tunneling Protocol), ont les propriétés suivantes :

- Encapsulation. Avec la technologie VPN, les données privées sont encapsulées avec un en-tête contenant les informations de routage permettant aux données d'être transmises sur le réseau de transit.
- Authentification. L'authentification des connexions VPN prend les trois formes suivantes :
    - Authentification au niveau utilisateur à l'aide de l'authentification PPP (Point-to-Point Protocol). Pour établir la connexion VPN, le serveur VPN authentifie le client VPN qui essaie de se connecter à l'aide d'une méthode d'authentification PPP au niveau utilisateur et vérifie que le client VPN possède l'autorisation appropriée. Si vous utilisez l'authentification mutuelle, le client VPN authentifie également le serveur VPN, ce qui permet d'assurer une protection contre les ordinateurs qui se font passer pour des serveurs VPN.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

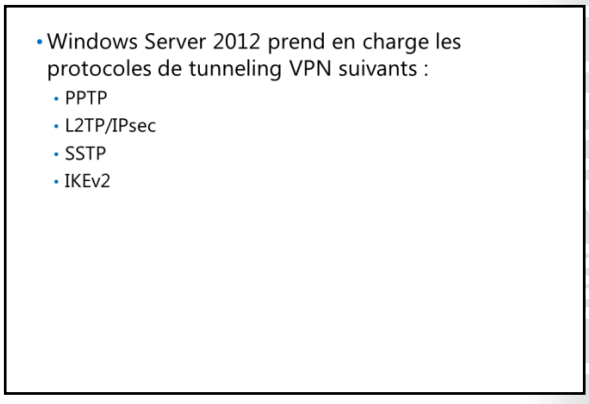
  - Authentification au niveau ordinateur à l'aide du protocole IKE (Internet Key Exchange). Pour établir une association de sécurité IPsec, le client VPN et le serveur VPN utilisent le protocole IKE pour échanger des certificats d'ordinateur ou une clé prépartagée. Dans l'un ou l'autre cas, le client et le serveur VPN s'authentifient l'un l'autre au niveau de l'ordinateur. Nous recommandons l'authentification par certificat d'ordinateur car il s'agit d'une méthode d'authentification beaucoup plus puissante. L'authentification de niveau ordinateur est exécutée uniquement pour les connexions L2TP/IPsec.
  - Authentification de l'origine des données et intégrité des données. Pour vérifier que les données envoyées sur la connexion VPN proviennent bien de l'autre extrémité de la connexion et qu'elles n'ont pas été modifiées pendant leur transit, les données contiennent une somme de contrôle de chiffrement basée sur une clé de chiffrement connue uniquement de l'expéditeur et du destinataire. L'authentification de l'origine des données et l'intégrité des données sont uniquement disponibles pour les connexions L2TP/IPsec.

- Chiffrement des données. Pour assurer la confidentialité des données transmises sur le réseau de transit partagé ou public, l'expéditeur chiffre les données et le destinataire les déchiffre. Les processus de chiffrement et de déchiffrement reposent sur l'expéditeur et sur le destinataire qui utilisent tous les deux une clé de chiffrement commune.

  Les paquets interceptés sur le réseau de transit sont inintelligibles pour quiconque ne possède pas la clé de chiffrement commune. La longueur de la clé de chiffrement est un paramètre de sécurité important. Vous pouvez utiliser des techniques de calcul pour déterminer la clé de chiffrement. Toutefois, plus cette clé est longue, plus la puissance et le temps de calcul nécessaires seront élevés. Par conséquent, il est important d'utiliser la plus grande taille de clé possible pour assurer la confidentialité des données.

Protocoles de tunneling pour les connexions VPN

Les protocoles PPTP, L2TP et SSTP dépendent largement des fonctionnalités spécifiées à l'origine pour le protocole PPP. Le protocole PPP a été conçu pour envoyer des données via des connexions point à point d'accès à distance ou dédiées. Dans le cadre des paquets IP, le protocole PPP encapsule les paquets IP dans des trames PPP, puis transmet les paquets PPP encapsulés via une liaison point à point. Le protocole PPP a été défini à l'origine comme le protocole à utiliser entre un client d'accès à distance et un serveur d'accès réseau.



PPTP

Le protocole PPTP vous permet de chiffrer et d'encapsuler dans un en-tête IP le trafic multiprotocole qui est ensuite envoyé sur un réseau IP ou sur un réseau IP public comme Internet. Vous pouvez utiliser le protocole PPTP pour les connexions d'accès à distance et les connexions VPN de site à site. Si vous utilisez Internet comme réseau public VPN, le serveur PPTP est un serveur VPN PPTP avec une interface sur Internet et une seconde interface sur le réseau intranet.

- Encapsulation. Le protocole PPTP encapsule des trames PPP dans des datagrammes IP en vue de la transmission sur le réseau. Le protocole PPTP utilise une connexion TCP (Transmission Control Protocol) pour gérer les tunnels et une version modifiée du protocole GRE (Generic Route Encapsulation) afin d'encapsuler des trames PPP pour les données en tunnel. Les charges utiles des trames PPP encapsulées peuvent être chiffrées et/ou compressées.
- Chiffrement. La trame PPP est chiffrée avec le chiffrement Microsoft Point-to-Point (MPPE, Microsoft Point-to-Point Encryption) à l'aide des clés de chiffrement générées par le processus d'authentification MS-CHAPv2 ou EAP-TLS. Les clients VPN doivent utiliser le protocole d'authentification MS-CHAPv2 ou EAP-TLS pour que les charges utiles des trames PPP soient chiffrées. Le protocole PPTP utilise le chiffrement PPP sous-jacent et de l'encapsulation d'une trame PPP précédemment chiffrée.

L2TP

Le protocole L2TP vous permet de chiffrer le trafic multiprotocole qui doit être envoyé via tout support prenant en charge la remise de datagramme point à point, comme le trafic IP ou le mode de transfert asynchrone. Le protocole L2TP est une combinaison des protocoles PPTP et L2F (Layer 2 Forwarding). Il regroupe les meilleures fonctionnalités des deux.

À la différence du protocole PPTP, l'implémentation Microsoft du protocole L2TP n'utilise pas le chiffrement MPPE pour chiffrer les datagrammes PPP. Le protocole L2TP s'appuie sur IPsec en mode transport pour les services de chiffrement. La combinaison des protocoles L2TP et IPsec est appelée L2TP/IPsec.

Pour utiliser les protocoles L2TP et IPsec, le client et le serveur VPN doivent tous deux prendre en charge les protocoles L2TP et IPsec. La prise en charge des clients pour le protocole L2TP est intégrée dans les clients d'accès à distance Windows XP, Windows Vista®, Windows 7 et Windows 8. La prise en charge du serveur VPN pour le protocole L2TP est intégrée dans les produits des familles Windows Server 2012, Windows Server 2008 et Windows Server 2003.

- Encapsulation : l'encapsulation pour les paquets L2TP/IPsec est formée de deux couches, l'encapsulation L2TP et l'encapsulation IPsec. L2TP encapsule et chiffre les données de la manière suivante :
    - Première couche. La première couche est l'encapsulation L2TP. Une trame PPP (datagramme IP) est encapsulée avec un en-tête L2TP et un en-tête UDP (User Datagram Protocol).
    - Seconde couche. La seconde couche est l'encapsulation IPsec. Le message L2TP résultant est encapsulé avec un en-tête et un code de fin ESP (Encapsulating Security Payload) IPsec, un code de fin d'authentification IPsec qui fournit l'intégrité et l'authentification des messages, et un en-tête IP final. L'en-tête IP contient les adresses IP source et de destination qui correspondent au client et au serveur VPN.
- Chiffrement : le message L2TP est chiffré avec l'algorithme AES (Advanced Encryption Standard) ou 3DES (Triple Data Encryption Standard) en utilisant les clés de chiffrement générées par le processus de négociation IKE.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

SSTP

Le protocole SSTP est un nouveau protocole de tunneling qui utilise le protocole HTTPS (HTTP Secure) sur le port TCP 443 pour faire transiter le trafic à travers des pare-feux et des proxys Web qui peuvent bloquer le trafic PPTP et L2TP/IPsec. Le protocole SSTP propose un mécanisme permettant d'encapsuler le trafic PPP sur le canal SSL (Secure Sockets Layer) du protocole HTTPS. L'utilisation du protocole PPP permet la prise en charge de méthodes d'authentification fortes, telles qu'EAP-TLS. Le protocole SSL offre une sécurité de niveau du transport avec une négociation des clés améliorée, le chiffrement et le contrôle d'intégrité.

Lorsqu'un client essaie d'établir une connexion VPN basée sur le protocole SSTP, ce dernier commence par établir une couche HTTPS bidirectionnelle avec le serveur SSTP. Sur cette couche HTTPS, les paquets du protocole sont transmis comme charge utile des données à l'aide des méthodes suivantes d'encapsulation et de chiffrement :

- Encapsulation. Le protocole SSTP encapsule des trames PPP dans des datagrammes IP en vue de la transmission sur le réseau. Le protocole SSTP utilise une connexion TCP (sur le port 443) pour la gestion des tunnels et comme trames de données PPP.
- Chiffrement. Le message SSTP est chiffré avec le canal SSL du protocole HTTPS.

IKEv2

IKEv2 utilise le protocole Mode de tunnel IPsec sur port UDP 500. IKEv2 prend en charge la mobilité, ce qui en fait le choix idéal pour la main d'œuvre mobile. Les connexions VPN basées sur IKEv2 permettent aux utilisateurs de se déplacer plus facilement entre les zones d'accès sans fil et les connexions câblées.

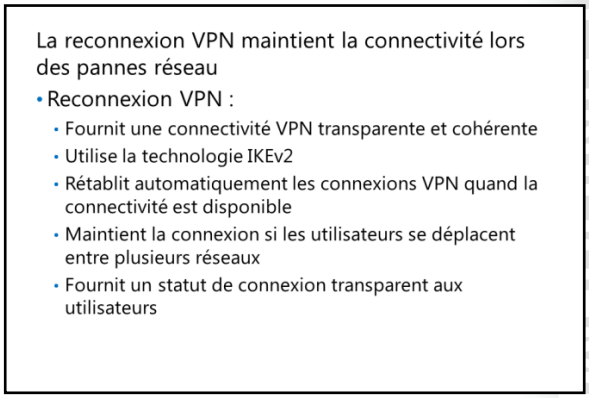
L'utilisation des protocoles IKEv2 et IPsec permet la prise en charge des méthodes de chiffrement et d'authentification forte.

- Encapsulation. Le protocole IKEv2 encapsule des datagrammes en utilisant les modes AH (Authentication Header) ou ESP IPsec pour la transmission sur le réseau.
- Chiffrement. Le message est chiffré avec un des protocoles suivants à l'aide des clés de chiffrement générées à partir du processus de négociation IKEv2 : algorithmes de chiffrement AES 256, AES 192, AES 128 et 3DES.

IKEv2 est pris en charge uniquement sur les ordinateurs avec les systèmes d'exploitation suivants : Windows 7, Windows 8, Windows Server 2008 R2 et Windows Server 2012. IKEv2 est le protocole de tunneling VPN par défaut dans Windows 7 et Windows 8.

Qu'est-ce qu'une Reconnexion VPN ?

Dans les scénarios d'entreprise dynamiques, les utilisateurs doivent être en mesure d'accéder en toute sécurité aux données, à tout moment, partout, et de manière continue, sans interruption. Par exemple, les utilisateurs peuvent souhaiter accéder en toute sécurité aux données figurant sur le serveur de la société, à partir d'une succursale ou lors d'un déplacement.



Pour répondre à cette exigence, vous pouvez configurer la fonctionnalité Reconnexion VPN disponible dans Windows Server 2012, Windows Server 2008 R2, Windows 8 et Windows 7. Grâce à cette fonctionnalité, les utilisateurs peuvent accéder aux données de la société à l'aide d'une connexion VPN, qui se reconnectera automatiquement en cas d'interruption de la connectivité. La Reconnexion VPN permet également le déplacement entre différents réseaux.

La Reconnexion VPN utilise la technologie IKEv2 pour fournir une connectivité VPN transparente et cohérente. Les utilisateurs qui se connectent via une large bande mobile sans fil tireront davantage parti de cette fonctionnalité. Prenons l'exemple d'un utilisateur avec un ordinateur portable équipé de Windows 8. Lorsque ce dernier emprunte le train pour se rendre sur son lieu de travail, il se connecte à Internet via une carte large bande mobile sans fil, puis établit une connexion VPN au réseau de l'entreprise. Quand le train passe dans un tunnel, la connexion Internet s'interrompt. Dès que le train sort du tunnel, la carte large bande mobile sans fil se reconnecte automatiquement au réseau Internet. Avec les versions précédentes des systèmes d'exploitation serveur et client Windows, VPN ne se reconnectait pas automatiquement. C'est pourquoi l'utilisateur devait répéter le processus en plusieurs étapes de connexion au VPN manuellement. C'était long et frustrant pour les utilisateurs mobiles avec une connectivité par intermittence.

Avec la Reconnexion VPN, Windows Server 2012 et Windows 8 rétablissent les connexions VPN actives de manière automatique lorsque la connectivité Internet est rétablie. Même si la reconnexion peut prendre plusieurs secondes, les utilisateurs n'ont pas besoin de relancer manuellement la connexion, ou de s'authentifier à nouveau pour accéder aux ressources du réseau.

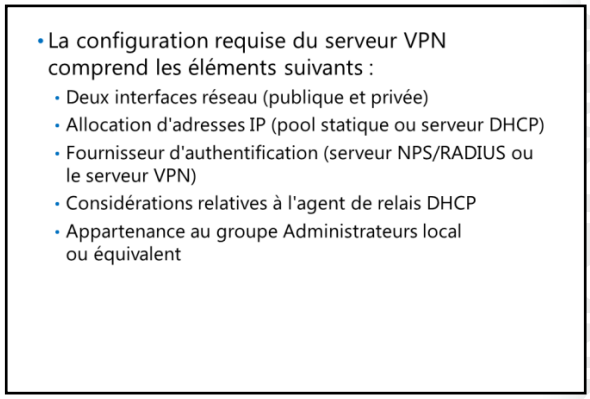
Les conditions requises du système pour utiliser la fonctionnalité Reconnexion VPN sont les suivantes :

- Windows Server 2008 R2 ou Windows Server 2012 en tant que serveur VPN.
- Client Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012.
- Infrastructure à clé publique (PKI), car un certificat informatique est indispensable pour une connexion à distance avec la Reconnexion VPN. Vous pouvez utiliser les certificats émis par une autorité de certification interne ou publique.

Configuration requise

Avant de déployer la solution VPN de votre organisation, il convient de tenir compte des configurations requises suivantes en matière de configuration :

- Votre serveur VPN a besoin de deux interfaces réseau. Vous devez identifier quelle interface réseau se connectera à Internet et quelle interface réseau se connectera au réseau privé. Durant la configuration, vous serez invité à choisir l'interface réseau qui assure la connexion à Internet. Si vous n'indiquez pas l'interface appropriée, le serveur VPN d'accès à distance ne fonctionnera pas correctement.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Déterminez si les clients distants reçoivent des adresses IP d'un serveur DHCP situé sur votre réseau privé ou du serveur VPN d'accès à distance en cours de configuration. Si le réseau privé comporte un serveur DHCP, le serveur VPN d'accès à distance peut à tout moment réserver simultanément dix adresses auprès du serveur DHCP, puis les attribuer aux clients distants. Dans le cas contraire, le serveur VPN d'accès à distance peut générer et attribuer automatiquement des adresses IP aux clients distants. Si vous voulez que le serveur VPN d'accès à distance attribue des adresses IP dans une plage déterminée, vous devez spécifier cette dernière.
- Précisez si les demandes de connexion des clients VPN doivent être authentifiées par un serveur RADIUS ou par le serveur VPN d'accès à distance en cours de configuration. L'ajout d'un serveur RADIUS est utile si vous envisagez d'installer plusieurs serveurs VPN d'accès à distance, points d'accès sans fil ou autres clients RADIUS sur votre réseau privé.

Remarque : Pour activer une infrastructure RADIUS, installez le rôle serveur Services de stratégie et d'accès réseau. Le NPS peut agir soit en tant que proxy RADIUS, soit en tant que serveur RADIUS.

- Déterminez si les clients VPN peuvent envoyer des messages DHCPINFORM au serveur DHCP sur votre réseau privé. Si un serveur DHCP se trouve sur le même sous-réseau que votre serveur VPN d'accès à distance, les messages DHCPINFORM des clients VPN seront en mesure d'atteindre le serveur DHCP une fois la connexion VPN établie. Si un serveur DHCP se trouve sur un sous-réseau différent de votre serveur VPN d'accès à distance, assurez-vous que le routeur entre les sous-réseaux peut relayer des messages DHCP entre clients et le serveur. Si votre routeur exécute Windows Server 2008 R2 ou Windows Server 2012, vous pouvez configurer le service Agent relais DHCP sur le routeur de sorte que les messages DHCPINFORM soient transférés entre les sous-réseaux.
- Veillez à vous assurer que le responsable du déploiement de votre solution VPN dispose des appartenances au groupe d'administration requises pour installer les rôles serveur et configurer les services nécessaires ; l'appartenance au groupe Administrateurs local est requise pour effectuer ces tâches.

Démonstration : Procédure de configuration d'un accès VPN

Cette démonstration montre comment :

- configurer l'accès à distance en tant que serveur VPN ;
- configurer un client VPN.

Procédure de démonstration

Configurer l'accès à distance en tant que serveur VPN

1. Ouvrez une session sur LON-RTR en tant qu'ADATUM\Administrateur avec le mot de passe Pa$$w0rd.
2. Sur LON-RTR, ouvrez le Gestionnaire de serveur, puis ajoutez le rôle Services de stratégie et d'accès réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Fermez le Gestionnaire de serveur.
4. Ouvrez la console Serveur NPS.
5. Enregistrez le serveur dans AD DS.
6. Laissez la fenêtre Serveur NPS (Network Policy Server) ouverte.
7. Ouvrez Routage et accès distant.
8. Désactivez la configuration existante.
9. Reconfigurez LON-RTR en tant que serveur VPN à l'aide des paramètres suivants :
   - **Connexion au réseau local 2** correspond à l'interface publique.
   - Le serveur VPN alloue des adresses du pool : **172.16.0.100 - 172.16.0.111**.
   - Le serveur est configuré avec l'option Non, utiliser Routage et accès distant pour authentifier les **demandes** de connexion.
10. Démarrez le service VPN.

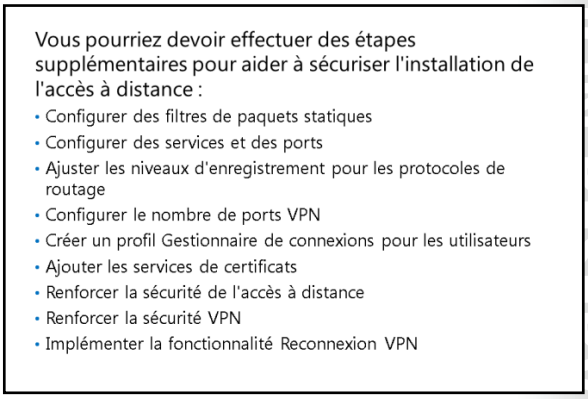
Configurer un client VPN

1. Basculez vers LON-CL2, puis ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Créez une connexion VPN avec les propriétés suivantes :
   - Adresse Internet de connexion : **10.10.0.1**.
   - Nom de la destination : **VPN Adatum**
   - Autoriser d'autres personnes à utiliser cette connexion : **true**.
3. Une fois le VPN créé, modifiez ses paramètres en affichant les propriétés de la connexion, puis sélectionnez l'onglet **Sécurité** pour reconfigurer le VPN à l'aide des paramètres suivants :
   - Type de réseau VPN : **Protocole PPTP (Point to Point Tunneling Protocol)**.
   - Authentification : **Autoriser ces protocoles = Protocole Microsoft CHAP Version 2 (MS-CHAP v2)**.
4. Testez la connexion VPN à l'aide des informations d'identification suivantes :
   - Nom d'utilisateur : ADATUM\administrateur
   - Mot de passe : **Pa$$w0rd**
5. Attendez que la connexion VPN soit établie. La connexion échoue. Vous recevez une erreur relative aux problèmes d'authentification.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Réalisation de tâches de configuration supplémentaires

À l'issue de ces étapes de déploiement et de configuration initiale de votre solution d'accès à distance, votre serveur est prêt à être utilisé en tant que serveur VPN d'accès à distance. Cependant, vous trouverez ci-après les tâches supplémentaires que vous pouvez également effectuer sur votre serveur VPN/d'accès à distance :

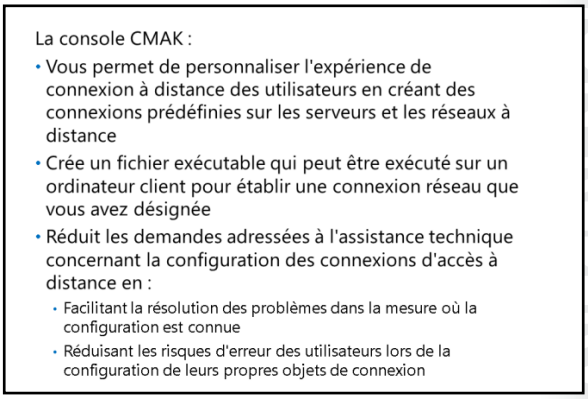


- Configurer des filtres de paquets statiques. Ajoutez des filtres de paquets statiques afin de mieux protéger votre réseau.
- Configurer des services et des ports. Choisissez quels services du réseau privé vous souhaitez rendre disponibles pour les utilisateurs d'accès à distance.
- Régler les niveaux d'enregistrement. Configurez le niveau de détails des événements que vous souhaitez enregistrer. Vous pouvez décider quelles informations vous souhaitez suivre dans les fichiers journaux.
- Configurer le nombre de ports VPN. Ajoutez ou supprimez des ports VPN.
- Créer un profil Gestionnaire des connexions pour les utilisateurs. Gérez l'expérience de connexion cliente des utilisateurs et simplifiez la configuration et le dépannage de ces connexions.
- Ajouter AD CS. Configurez et gérez une autorité de certification (CA) sur un serveur en vue de l'utiliser dans une infrastructure à clé publique (PKI).
- Renforcer la sécurité de l'accès à distance. Protégez les utilisateurs distants et le réseau privé en appliquant des méthodes d'authentification sécurisées, en exigeant des niveaux supérieurs de chiffrement des données, etc.
- Renforcer la sécurité VPN. Protégez les utilisateurs distants et le réseau privé en exigeant l'utilisation de protocoles de tunneling sécurisés, en configurant le verrouillage de compte, etc.
- Implémenter la fonctionnalité Reconnexion VPN. Ajoutez la Reconnexion VPN pour rétablir les connexions VPN automatiquement pour les utilisateurs qui perdent temporairement leurs connexions Internet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que le Kit d'administration du Gestionnaire des connexions ?

Le Kit d'administration du Gestionnaire des connexions (CMAK, Connection Manager Administration Kit) vous permet de personnaliser les options de connexion à distance des utilisateurs en créant des connexions prédéfinies aux serveurs et aux réseaux à distance. L'Assistant Kit d'administration du Gestionnaire des connexions crée un fichier exécutable que vous pouvez distribuer de différentes manières ou intégrer dans l'image du système d'exploitation dans le cadre des activités de déploiement.



Connection Manager est un outil de connexion réseau client qui permet à un utilisateur de se connecter à un réseau distant, tel qu'un fournisseur de services Internet ou un réseau d'entreprise protégé par un serveur VPN.

Le Kit d'administration du Gestionnaire des connexions (CMAK) est un outil que vous pouvez utiliser pour personnaliser l'expérience de connexion à distance des utilisateurs de votre réseau en créant des connexions prédéfinies à des serveurs et des réseaux à distance. Utilisez l'Assistant Kit d'administration du Gestionnaire des connexions pour créer et personnaliser une connexion pour vos utilisateurs.

Le Kit d'administration du Gestionnaire des connexions est un composant facultatif qui n'est pas installé par défaut. Vous devez l'installer avant de pouvoir créer des profils de connexion que vos utilisateurs pourront installer pour accéder aux réseaux à distance.

Distribution du profil de connexion

L'Assistant Kit d'administration du Gestionnaire des connexions compile le profil de connexion dans un fichier exécutable unique portant l'extension de nom de fichier .exe. Vous pouvez distribuer ce fichier aux utilisateurs par toute méthode à votre disposition. Différentes méthodes à considérer :

- Inclure le profil de connexion dans l'image qui est fournie avec les nouveaux ordinateurs.

  Vous pouvez installer votre profil de connexion avec les images d'ordinateur client installées sur les nouveaux ordinateurs de votre organisation.

- Distribuer le profil de connexion sur un média amovible afin que l'utilisateur puisse l'installer manuellement.

  Vous pouvez distribuer le programme d'installation du profil de connexion sur un CD-DVD, un lecteur flash USB ou tout autre média amovible auquel vous autorisez les utilisateurs à accéder. Un certain nombre de médias amovibles prennent en charge la fonction de démarrage automatique qui permet de lancer l'installation dès que l'utilisateur insère le média dans l'ordinateur.

- Remettre le profil de connexion à l'aide d'outils de distribution de logiciels automatisés.

  De nombreuses organisations utilisent un outil de gestion du bureau ou de gestion des logiciels tel que Microsoft System Center Configuration Manager (auparavant appelé Systems Management Server). Configuration Manager permet de mettre le package en logiciel et de le distribuer aux ordinateurs clients. L'installation peut être invisible pour vos utilisateurs et vous pouvez la configurer pour signaler son succès ou son échec dans la console de gestion.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Procédure de création d'un profil de connexion

Cette démonstration montre comment :

- installer les services CMAK ;
- créer un profil de connexion ;
- examiner le profil.

Procédure de démonstration

Installer les services CMAK

1. Au besoin, ouvrez une session sur LON-CL2 en tant qu'ADATUM\Administrateur avec le mot de passé Pa$$w0rd.
2. Ouvrez le Panneau de configuration, puis activez la nouvelle fonctionnalité Windows appelée Kit d'administration du Gestionnaire des connexions Microsoft (CMAK) RAS.

Créer un profil de connexion

1. Dans Outils d'administration, ouvrez le Kit d'administration du Gestionnaire des connexions.
2. Suivez les instructions de l'Assistant Kit d'administration du Gestionnaire des connexions pour créer le profil de connexion.

Examiner le profil créé

- Utilisez l'Explorateur de fichiers pour examiner le contenu du dossier que vous avez créé à l'aide de l'Assistant Kit d'administration du Gestionnaire des connexions pour créer le profil de connexion. Normalement, vous devriez à présent distribuer ce profil à vos utilisateurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Vue d'ensemble des stratégies réseau

Les stratégies réseau déterminent si une tentative de connexion aboutit. Si la tentative de connexion aboutit, la stratégie réseau définit également des caractéristiques de connexion, telles que des restrictions de jour et d'heure, des déconnexions de session en cas d'inactivité ainsi que d'autres paramètres.

La compréhension du mode de configuration des stratégies réseau est essentielle si vous voulez implémenter avec succès des connexions VPN basées sur le rôle serveur Services de stratégie et d'accès réseau dans votre organisation.

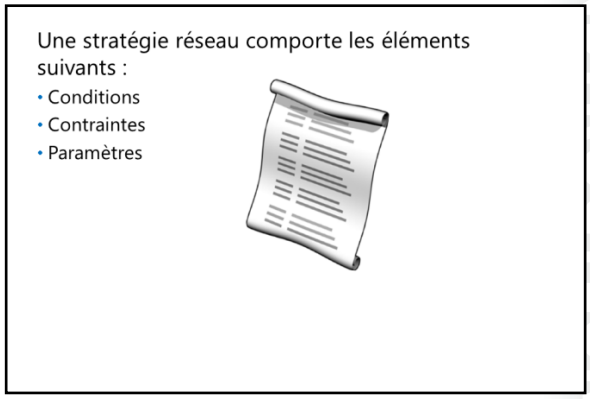
Objectifs de la leçon

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

- définir une stratégie réseau ;
- décrire le traitement d'une stratégie réseau ;
- décrire le processus de création d'une stratégie réseau ;
- expliquer comment créer une stratégie réseau pour les connexions VPN.

Qu'est-ce qu'une stratégie réseau ?

Une stratégie réseau est un ensemble de conditions, de contraintes et de paramètres qui vous permettent de désigner les personnes autorisées à se connecter au réseau et les circonstances dans lesquelles elles peuvent, ou non, se connecter. De plus, lorsque vous déployez la protection d'accès réseau NAP, la stratégie de contrôle d'intégrité est ajoutée à la configuration de la stratégie réseau afin que le serveur NPS puisse effectuer des contrôles d'intégrité des clients pendant le processus d'autorisation.



Vous pouvez envisager les stratégies réseau comme des règles : chaque règle regroupe un ensemble de conditions et de paramètres. Le serveur NPS compare les conditions de la règle aux propriétés des demandes de connexion. En cas de correspondance entre la règle et la demande de connexion, les paramètres définis dans la règle sont alors appliqués à la connexion.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous configurez plusieurs stratégies réseau sur le serveur NPS, elles constituent un jeu ordonné de règles. Le serveur NPS vérifie chaque demande de connexion par rapport à la première règle de la liste, puis à la deuxième, et ainsi de suite, jusqu'à ce qu'une correspondance soit trouvée.

Remarque : Une fois qu'une règle de correspondance est déterminée, les autres règles sont ignorées. Par conséquent, il est important que vous commandiez vos stratégies réseau de manière appropriée, par ordre d'importance.

Chaque stratégie réseau possède un paramètre État de la stratégie qui vous permet d'activer ou de désactiver la stratégie. Si vous désactivez une stratégie réseau, le serveur NPS ne l'évalue pas lors du processus d'autorisation des demandes de connexion.

Propriétés des stratégies réseau

Chaque stratégie réseau possède quatre catégories de propriétés :

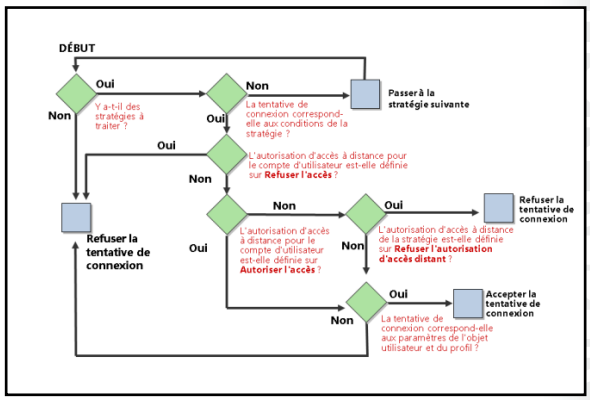
- *Vue d'ensemble*. Les propriétés de vue d'ensemble vous permettent de spécifier si la stratégie est activée, si elle accorde ou refuse l'accès et si une méthode de connexion réseau ou un type de serveur d'accès réseau spécifique est requis pour les demandes de connexion. Ces propriétés vous permettent également de spécifier si les propriétés de numérotation des comptes d'utilisateurs dans AD DS doivent être ignorées. Si vous sélectionnez cette option, le serveur NPS utilise uniquement les paramètres de la stratégie réseau pour déterminer si la connexion doit être autorisée.
- *Conditions*. Ces propriétés vous permettent de spécifier les conditions que la demande de connexion doit réunir pour être conforme à la stratégie réseau. Si les conditions configurées dans la stratégie sont réunies dans la demande de connexion, le serveur NPS applique les paramètres de la stratégie réseau à la connexion. Par exemple, si vous spécifiez l'adresse IPv4 du serveur d'accès réseau (adresse IPv4 NAS) comme condition de la stratégie réseau et que le serveur NPS reçoit une demande de connexion d'un serveur d'accès réseau ayant cette adresse IP, la demande de connexion est conforme à la condition de la stratégie.
- *Contraintes*. Les contraintes sont des paramètres supplémentaires de la stratégie réseau auxquels les demandes de connexion doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS rejette automatiquement cette demande. À la différence de la réponse du serveur NPS à des conditions de la stratégie réseau auxquelles la demande de connexion ne se conforme pas, si une demande de connexion ne répond pas à une contrainte, le serveur NPS n'évalue pas les stratégies réseau supplémentaires, et la demande de connexion est refusée.
- *Paramètres*. Les propriétés de paramètres vous permettent de spécifier les paramètres que le serveur NPS applique à la demande de connexion dès lors que toutes les conditions de la stratégie réseau sont réunies et que la demande est acceptée.

Lorsque vous ajoutez une nouvelle stratégie réseau à l'aide du composant logiciel enfichable MMC (Microsoft Management Console) Serveur NPS, vous devez utiliser l'Assistant Nouvelle stratégie réseau. Après avoir créé une stratégie réseau à l'aide de l'Assistant Nouvelle stratégie réseau, vous pouvez la personnaliser en double-cliquant dessus dans le serveur NPS de manière à afficher ses propriétés.

Remarque : Les stratégies par défaut du serveur NPS bloquent l'accès au réseau. Une fois vos propres stratégies créées, vous devez modifier la priorité, désactiver ou supprimer ces stratégies par défaut.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

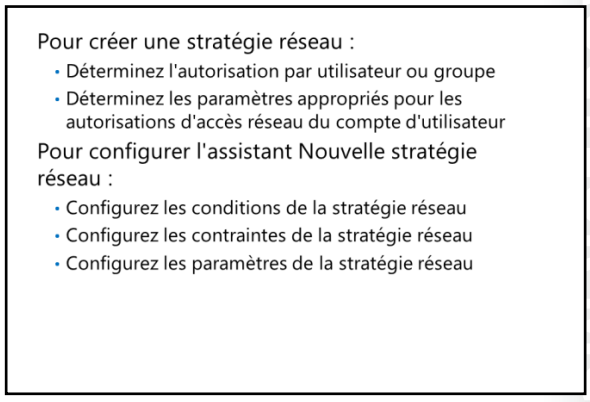
Traitement des stratégies réseau



Lorsque le serveur NPS exécute le processus d'autorisation d'une demande de connexion, il compare la demande à chaque stratégie réseau de la liste triée de stratégies, en commençant par la première stratégie. S'il trouve une stratégie dont les conditions correspondent à la demande de connexion, le serveur NPS utilise la stratégie correspondante et les propriétés de numérotation du compte d'utilisateur pour réaliser l'autorisation. Si vous configurez les propriétés de numérotation du compte d'utilisateur de manière à accorder ou à contrôler l'accès à l'aide d'une stratégie réseau, et si la demande de connexion est autorisée, le serveur NPS applique les paramètres configurés dans la stratégie réseau à la connexion :

- Si le serveur NPS ne trouve pas de stratégie réseau qui corresponde à la demande de connexion, il refuse la connexion, sauf si les propriétés de numérotation du compte d'utilisateur sont configurées pour accorder l'accès.
- Si les propriétés de numérotation du compte d'utilisateur sont configurées pour refuser l'accès, le serveur NPS rejette la demande de connexion.

Processus de création et de configuration d'une stratégie réseau



Le serveur NPS utilise des stratégies réseau et les propriétés de numérotation des comptes d'utilisateurs pour déterminer si une demande de connexion réseau peut être autorisée. Vous pouvez configurer une nouvelle stratégie réseau dans le composant logiciel enfichable MMC Serveur NPS ou Service de routage et d'accès à distance.

Création de votre stratégie

Lorsque vous utilisez l'Assistant Nouvelle stratégie réseau pour créer une stratégie réseau, la valeur spécifiée comme méthode de connexion réseau est utilisée automatiquement pour configurer la condition Type de stratégie. Si vous conservez la valeur par défaut Non spécifié, le serveur NPS évalue la stratégie réseau que vous créez pour tous les types de connexion réseau via tout type de serveur d'accès réseau. Si vous spécifiez une méthode de connexion réseau, le serveur NPS évalue la stratégie réseau uniquement si la demande de connexion émane du type de serveur d'accès réseau que vous spécifiez.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Par exemple, si vous spécifiez Passerelle des services Bureau à distance, le serveur NPS évalue la stratégie réseau uniquement pour les demandes de connexion qui proviennent de serveurs de passerelle des services Bureau à distance.

Sur la page **Spécifier l'autorisation d'accès**, vous devez sélectionner **Accès accordé** si vous souhaitez que la stratégie autorise les utilisateurs à se connecter à votre réseau. Si vous souhaitez que la stratégie empêche les utilisateurs de se connecter à votre réseau, sélectionnez **Accès refusé**. Si vous souhaitez que les propriétés de numérotation des comptes d'utilisateurs dans AD DS déterminent l'autorisation d'accès, vous pouvez activer la case à cocher **L'accès est déterminé par les propriétés de numérotation des utilisateurs**. Ce paramètre remplace la stratégie NPS.

Configuration de votre stratégie

Une fois que vous avez créé votre stratégie réseau, vous pouvez utiliser la boîte de dialogue **Propriétés** de la stratégie réseau pour afficher ou modifier ses paramètres.

Propriétés de Stratégie réseau - Onglet Vue d'ensemble

Sous l'onglet **Vue d'ensemble** de la boîte de dialogue **Propriétés** de la stratégie réseau, ou dans l'Assistant Nouvelle stratégie réseau, vous pouvez configurer les paramètres suivants :

- **Nom de la stratégie**. Spécifiez un nom convivial et pertinent pour la stratégie réseau.
- **État de la stratégie**. Indiquez s'il convient d'activer la stratégie.
- **Autorisation d'accès**. Indiquez si la stratégie autorise ou refuse l'accès. Indiquez également si le serveur NPS doit ignorer les propriétés de numérotation des comptes d'utilisateurs dans AD DS lorsqu'il utilise la stratégie pour autoriser la tentative de connexion.
- La méthode de connexion réseau à utiliser pour la demande de connexion :
    - **Non spécifié**. Si vous sélectionnez **Non spécifié**, le serveur NPS évalue la stratégie réseau pour toutes les demandes de connexion ayant pour origine tout type de serveur d'accès réseau et pour toute méthode de connexion.
    - **Passerelle des services Bureau à distance**. Si vous spécifiez **Passerelle des services Bureau à distance**, le serveur NPS évalue la stratégie réseau pour les demandes de connexion qui proviennent de serveurs exécutant la passerelle des services Bureau à distance.
    - **Serveur d'accès à distance (VPN-Dial up)**. Si vous sélectionnez **Serveur d'accès à distance (VPN-Dial up)**, le serveur NPS évalue la stratégie réseau pour les demandes de connexion ayant pour origine un ordinateur qui exécute le service de routage et d'accès à distance configuré en tant que serveur d'accès à distance ou VPN. Si un autre serveur d'accès à distance ou VPN est utilisé, le serveur doit prendre en charge le protocole RADIUS et les protocoles d'authentification fournis par le serveur NPS pour les connexions d'accès à distance et les connexions VPN.
    - **Serveur DHCP**. Si vous spécifiez **Serveur DHCP**, le serveur NPS évalue la stratégie réseau pour les demandes de connexion ayant pour origine des serveurs exécutant le protocole DHCP.
    - **Autorité d'inscription d'intégrité**. Si vous sélectionnez **Autorité d'inscription d'intégrité**, le serveur NPS évalue la stratégie réseau pour les demandes de connexion ayant pour origine des serveurs exécutant l'autorité HRA.
    - **Serveur HCAP**. Si vous spécifiez Serveur HCAP, le serveur NPS évalue la stratégie réseau pour les demandes de connexion ayant pour origine des serveurs exécutant le protocole HCAP.

Propriétés de Stratégie réseau - Onglet Conditions

Vous devez configurer au moins une condition pour chaque stratégie réseau. Cette opération s'effectue dans l'onglet **Conditions** de la boîte de dialogue **Propriétés** de la stratégie réseau. Dans cet onglet, le serveur NPS propose de nombreux groupes de conditions qui vous permettent de définir avec précision les propriétés que doivent présenter les demandes de connexion pour être conformes à la stratégie.

Les groupes de conditions disponibles que vous pouvez sélectionner sont les suivants :

- *Groupes*. Ces conditions spécifient les groupes d'utilisateurs ou d'ordinateurs que vous configurez dans AD DS et auxquels vous souhaitez que les autres règles de la stratégie réseau s'appliquent lorsque des membres du groupe essaient de se connecter au réseau.
- *HCAP (Host Credential Authorization Protocol)*. Ces conditions sont utilisées uniquement lorsque vous souhaitez intégrer votre solution NAP NPS à la solution Contrôle d'admission au réseau de Cisco. Pour utiliser ces conditions, vous devez déployer le Contrôle d'admission au réseau de Cisco, ainsi que la Protection d'accès réseau (NAP). Vous devez également déployer un serveur HCAP qui exécute les Services Internet (IIS) et le serveur NPS.
- *Restrictions relatives aux jours et aux heures*. Ces conditions vous permettent de spécifier de manière hebdomadaire si les connexions doivent être autorisées des jours et à des heures spécifiques de la semaine.
- *NAP*. Les paramètres incluent Type d'identité, Classe MS-Service, Ordinateurs compatibles avec la p d'accès réseau (NAP), Système d'exploitation et Expiration de la stratégie.
- *Propriétés de la connexion*. Les paramètres incluent Adresse IPv4 du client d'accès, Adresse IPv6 du client d'accès, Type d'authentification, Types de protocoles EAP autorisés, Protocole de trames, Type de service et Type de tunnel.
- *Propriétés du client RADIUS*. Les paramètres incluent ID de la station appelante, Nom convivial du client, Adresse IPv4 du client, Adresse IPv6 du client, Fournisseur du client et Fournisseur MS-RAS.
- *Passerelle*. Les paramètres incluent ID de la station appelée, Identificateur NAS, Adresse IPv4 NAS, Adresse IPv6 NAS et Type de port NAS.

Propriétés de Stratégie réseau - Onglet Contraintes

Les contraintes sont des paramètres supplémentaires facultatifs de la stratégie réseau qui sont très différents de ses conditions : lorsqu'une demande de connexion ne répond pas à une condition, le serveur NPS continue à évaluer les autres stratégies réseau configurées afin de trouver une stratégie à laquelle la demande de connexion est conforme. Lorsqu'une demande de connexion ne répond pas à une contrainte, le serveur NPS n'évalue pas les autres stratégies réseau, mais rejette la demande de connexion et l'accès de l'utilisateur ou de l'ordinateur au réseau est refusé.

La liste suivante décrit les contraintes que vous pouvez configurer dans l'onglet **Contraintes** de la boîte de dialogue **Propriétés** de la stratégie réseau :

- *Méthodes d'authentification*. Permet de spécifier les méthodes d'authentification requises pour que la demande de connexion soit conforme à la stratégie réseau.
- *Délai d'inactivité*. Permet de spécifier la durée maximale (en minutes) pendant laquelle le serveur d'accès réseau peut rester inactif avant que la connexion ne soit rompue.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Délai d'expiration de session*. Permet de spécifier la durée maximale (en minutes) pendant laquelle un utilisateur peut rester connecté au réseau.
- *ID de la station appelée*. Permet de spécifier le numéro de téléphone du serveur d'accès à distance que les clients utilisent pour accéder au réseau.
- *Restrictions relatives aux jours et aux heures*. Permet de spécifier à quel moment les utilisateurs peuvent se connecter au réseau.
- *Type de port NAS*. Permet de spécifier les types de support d'accès qui sont autorisés pour la connexion des utilisateurs au réseau.

Propriétés de Stratégie réseau - Onglet Paramètres

Si les propriétés de la demande de connexion répondent à toutes les conditions et contraintes configurées dans la stratégie, le serveur NPS applique les paramètres configurés dans l'onglet **Paramètres** de la boîte de dialogue **Propriétés** de la stratégie réseau à la connexion. Ces paramètres sont notamment :

- *Attributs RADIUS*. Ce paramètre permet de définir des attributs RADIUS supplémentaires à envoyer au serveur RADIUS.
- *NAP*. Ce paramètre permet de configurer les paramètres de protection d'accès réseau (NAP), pour notamment indiquer si les clients qui se connectent disposent d'un accès total ou limité au réseau, ou encore si la mise à jour automatique est activée.
- *Routage et accès distant*. Ce paramètre permet de configurer des paramètres de liaisons multiples et de protocole BAP, des filtres IP, des paramètres de chiffrement et d'autres paramètres IP pour les connexions.

Démonstration : Procédure de création d'une stratégie réseau

Cette démonstration montre comment :

- créer une stratégie VPN basée sur la condition Groupes Windows ;
- tester la stratégie VPN.

Procédure de démonstration

Créer une stratégie VPN basée sur la condition Groupes Windows

1. Sur LON-RTR, basculez vers la console Serveur NPS (Network Policy Server).
2. Désactivez les deux stratégies réseau existantes ; elles empêcheraient le traitement de la stratégie que vous êtes sur le point de créer.
3. Créez une stratégie réseau à l'aide des propriétés ci-dessous :
    - Nom de la stratégie : **Stratégie VPN Adatum**
    - Type de serveur d'accès réseau : **Serveur d'accès à distance (VPN-Dial up)**
    - Condition : **Groupes Windows = Admins du domaine**
    - Autorisation : **Accès accordé**
    - Méthodes d'authentification : valeur par défaut
    - Contraintes : valeur par défaut
    - Paramètres : valeur par défaut

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Tester la stratégie VPN

1. Basculez vers LON-CL2.
2. Testez la connexion VPN Adatum. Utilisez les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\administrateur**
   - Mot de passe : **Pa$$w0rd**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4

Résolution des problèmes du service de routage et d'accès à distance

Le dépannage du service de routage et d'accès à distance peut prendre du temps. Les problèmes peuvent en effet être très différents et difficilement identifiables. Par ailleurs, sachant que vous pouvez utiliser des réseaux distants, dédiés, réservés ou publics selon la solution de connectivité à distance choisie, vous devez effectuer le dépannage en suivant une procédure systématique méthodique.

Dans certains cas, vous pouvez identifier et résoudre rapidement le problème. Dans d'autres, vous devrez mettre à l'épreuve vos connaissances sur tous les outils disponibles afin de déterminer la source du problème et pouvoir le résoudre dans les temps impartis.

Objectifs de la leçon

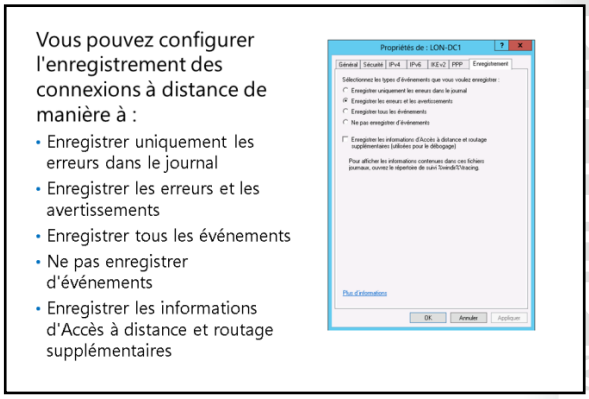
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire comment configurer l'enregistrement des connexions d'accès à distance ;
- décrire comment configurer le suivi de l'accès à distance ;
- expliquer comment résoudre les problèmes généraux de connectivité VPN ;
- expliquer comment résoudre les autres problèmes courants d'accès à distance.

Configuration de l'enregistrement des connexions d'accès à distance

Pour configurer l'enregistrement des connexions d'accès à distance, ouvrez la console **Routage et accès distant**, cliquez avec le bouton droit sur le **nom du serveur**, puis cliquez sur **Propriétés**. Cliquez sur l'onglet **Enregistrement** pour afficher les options disponibles pour le journal de suivi et connaître son emplacement.

Pour commencer, il est préférable de spécifier plus d'options d'enregistrement que nécessaire, plutôt que pas assez. Une fois que vous aurez déterminé le niveau d'enregistrement optimal pour dépanner votre infrastructure, vous pourrez modifier les options et/ou le niveau d'enregistrement.



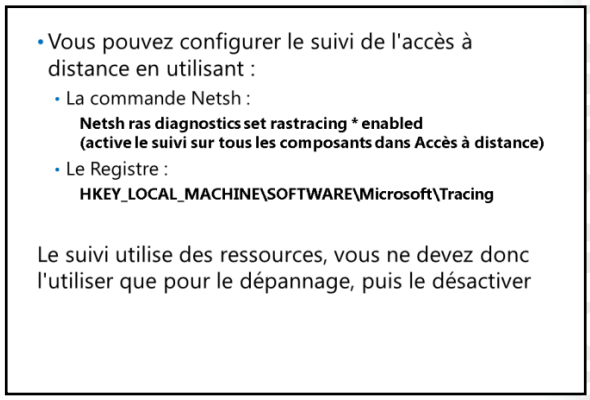
Quatre niveaux d'enregistrement sont disponibles dans l'onglet **Enregistrement**, comme décrit dans le tableau suivant.

Option de la boîte de dialogue	Description
Enregistrer uniquement les erreurs dans le journal	Indique que seules les erreurs sont enregistrées dans le journal système dans l'Observateur d'événements.
Enregistrer les erreurs et les avertissements	Indique que les erreurs et les avertissements sont enregistrés dans le journal système dans l'Observateur d'événements.
Enregistrer tous les événements	Indique que la quantité maximale d'informations est enregistrée dans le journal système dans l'Observateur d'événements.
Ne pas enregistrer d'événements	Indique qu'aucun événement n'est enregistré dans le journal système dans l'Observateur d'événements.

La case à cocher **Enregistrer les informations d'Accès à distance et routage supplémentaires (utilisées pour le débogage)** vous permet de spécifier si les événements du processus d'établissement de la connexion PPP sont consignés dans le fichier PPP.LOG. Ce fichier journal est stocké dans le dossier systemroot\Tracing (emplacement par défaut).

Configuration du suivi de l'accès à distance

Le service de routage et d'accès à distance de Windows Server 2012 propose une fonction de suivi étendue que vous pouvez utiliser pour résoudre les problèmes réseau complexes. À l'aide de la commande Netsh ou à l'aide du Registre, vous pouvez activer l'enregistrement des informations de suivi dans des fichiers par les composants de Windows Server 2012.



Activation du suivi à l'aide de la commande Netsh

La commande Netsh vous permet d'activer et de désactiver le suivi pour des composants spécifiques ou pour tous les composants. Pour activer et désactiver le suivi pour un composant spécifique, utilisez la syntaxe suivante :

```
netsh ras set tracing composant enabled|disabled
```

Où *composant* est un composant figurant dans la liste des composants du service de routage et d'accès à distance qui se trouve dans le Registre sous HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing. Par exemple, pour activer le suivi du composant RASAUTH, la commande est la suivante :

```
netsh ras set tracing rasauth enabled
```

Pour activer le suivi pour tous les composants, utilisez la commande suivante :

```
netsh ras set tracing * enabled
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Activation du suivi à l'aide du Registre

Vous pouvez également configurer la fonction de suivi en modifiant les paramètres du Registre sous le chemin suivant :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing
```

Vous pouvez activer le suivi pour chaque composant du service d'accès à distance en définissant les valeurs de Registre appropriées. Vous pouvez activer et désactiver le suivi de composants même si le service de routage et d'accès à distance est en cours d'exécution. Chaque composant peut être suivi et apparaît sous la forme d'une sous-clé sous la clé de Registre précédente.

Pour activer le suivi pour chaque composant, vous pouvez configurer les entrées de Registre suivantes pour chaque clé de protocole :

```
EnableFileTracing REG_DWORD Flag
```

Vous pouvez activer l'enregistrement des informations de suivi dans un fichier en attribuant la valeur 1 à EnableFileTracing, la valeur par défaut étant 0.

Vous pouvez modifier l'emplacement par défaut des fichiers de suivi en indiquant le chemin d'accès de votre choix dans FileDirectory. Le nom du fichier journal est le nom du composant faisant l'objet du suivi. Par défaut, les fichiers journaux sont placés dans le dossier SystemRoot\Tracing.

```
Chemin d'accès FileDirectory REG_EXPAND_SZ
```

FileTracingMask détermine le volume d'informations de suivi stockées dans le fichier. La valeur par défaut est 0xFFFF0000.

```
FileTracingMask REG_DWORD LevelOfTracingInformationLogged
```

Vous pouvez modifier la taille du fichier journal en attribuant des valeurs différentes à MaxFileSize. La valeur par défaut est 0x10000 (64 Ko).

```
MaxFileSize REG_DWORD SizeOfLogFile
```

 **Remarque :** Le suivi utilise des ressources système et doit être utilisé avec modération pour tenter d'identifier les problèmes réseau. Une fois le suivi enregistré ou le problème identifié, désactivez immédiatement le suivi. Ne le laissez pas activé sur des ordinateurs multiprocesseurs.

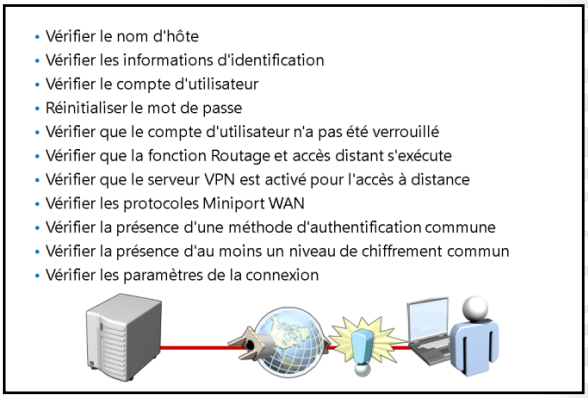
Les informations de suivi peuvent être complexes et détaillées. C'est pourquoi elles ne sont généralement utiles qu'aux professionnels du support technique Microsoft ou aux administrateurs réseau ayant une expérience avec le service de routage et d'accès à distance.

Vous pouvez enregistrer les informations de suivi sous forme de fichiers et les envoyer au support technique Microsoft pour analyse.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Résolution des problèmes VPN généraux

Pour résoudre les problèmes généraux d'établissement d'une connexion VPN d'accès à distance, effectuez les tâches suivantes :

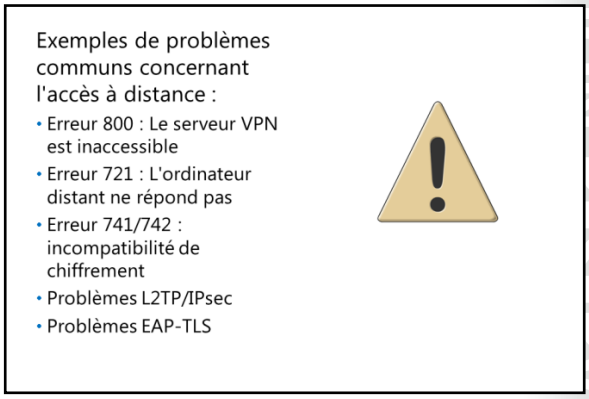


- À l'aide de la commande **ping**, vérifiez que le nom d'hôte est résolu en adresse IP correcte. Il est possible que la commande ping elle-même échoue en raison du filtrage de paquets qui peut empêcher la remise de messages ICMP (Internet Control Message Protocol) au serveur VPN ou depuis ce dernier.
- Vérifiez que les informations d'identification du client VPN (nom d'utilisateur, mot de passe et nom de domaine) sont correctes et que le serveur VPN peut les valider.
- Vérifiez que le compte d'utilisateur du client VPN n'est pas verrouillé, arrivé à expiration ou désactivé, ou bien encore que l'heure à laquelle la connexion est établie ne correspond pas aux heures de connexion configurées. Si le mot de passe du compte a expiré, vérifiez que le client VPN d'accès à distance utilise le protocole MS-CHAP v2. MS-CHAP v2 est le seul protocole d'authentification fourni par Windows Server 2012 qui vous permet de modifier un mot de passe arrivé à expiration au cours du processus de connexion.
- Réinitialisez les mots de passe arrivés à expiration des comptes de niveau administrateur à l'aide d'un autre compte de niveau administrateur.
- Vérifiez que le compte d'utilisateur n'a pas été verrouillé en raison du verrouillage d'un compte d'accès à distance.
- Vérifiez que le service de routage et d'accès à distance est en cours d'exécution sur le serveur VPN.
- Vérifiez que le serveur VPN est activé pour l'accès à distance dans l'onglet **Général** de la boîte de dialogue **Propriétés** du serveur VPN.
- Vérifiez que les périphériques Miniport WAN (PPTP) et Miniport WAN (L2TP) sont activés pour l'accès à distance entrant dans les propriétés de l'objet Ports dans le composant logiciel enfichable Routage et accès à distance.
- Vérifiez que le client VPN, le serveur VPN et la stratégie réseau correspondant aux connexions VPN sont configurés pour utiliser au moins une méthode d'authentification commune.
- Vérifiez que le client VPN et la stratégie réseau correspondant aux connexions VPN sont configurés pour utiliser au moins un niveau de chiffrement commun.
- Vérifiez que les paramètres de la connexion sont autorisés au moyen de stratégies réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dépannage des autres problèmes

Cette rubrique répertorie les autres problèmes courants que vous pouvez rencontrer lors de l'utilisation de la fonctionnalité d'accès à distance dans Windows Server 2012.



Erreur 800 : Le serveur VPN est inaccessible

- Cause : Les paquets PPTP/L2TP/SSTP provenant du client VPN ne peuvent pas atteindre le serveur VPN.
- Solution : Assurez-vous que les ports appropriés sont ouverts sur le pare-feu.
    - PPTP. Pour le trafic PPTP, configurez le pare-feu du réseau de sorte qu'il ouvre le port TCP 1723 et qu'il transmette le protocole IP 47 pour le trafic GRE vers le serveur VPN.
    - L2TP. Pour le trafic L2TP, configurez le pare-feu du réseau de sorte qu'il ouvre le port UDP 1701 et qu'il autorise les paquets au format ESP IPsec (protocole IP 50).
    - SSTP. Pour SSTP, activez le port TCP 443.

Erreur 721 : L'ordinateur distant ne répond pas

- Cause : Ce problème peut se produire si le pare-feu du réseau n'autorise pas le trafic GRE (protocole IP 47). Le protocole PPTP utilise le protocole GRE pour les données en tunnel.
- Solution : Configurez le pare-feu du réseau entre le client VPN et le serveur de sorte qu'il autorise le trafic GRE. De plus, assurez-vous que le pare-feu du réseau autorise le trafic TCP sur le port 1723. Ces deux conditions doivent être réunies pour établir la connectivité VPN à l'aide du protocole PPTP.

Remarque : Le pare-feu peut se trouver sur ou devant le client VPN, ou devant le serveur VPN.

Erreur 741/742 : Erreur d'incompatibilité de chiffrement

- Cause : Ces erreurs se produisent si le client VPN demande un niveau de chiffrement non valide ou si le serveur VPN ne prend pas en charge un type de chiffrement demandé par le client.
- Solution : Vérifiez les propriétés de la connexion VPN sur le client VPN sous l'onglet **Sécurité**. Si l'option **Exiger le chiffrement des données (sinon, déconnecter)** est sélectionnée, effacez la sélection et réessayez d'établir la connexion. Si vous utilisez un serveur NPS, vérifiez le niveau de chiffrement dans la stratégie réseau de la console NPS ou les stratégies sur les autres serveurs RADIUS. Vérifiez que le niveau de chiffrement demandé par le client VPN est sélectionné sur le serveur VPN.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Problèmes d'authentification L2TP/IPsec

La liste qui suit décrit les causes les plus communes d'échec des connexions L2TP/IPsec :

- Absence de certificat. Par défaut, les connexions L2TP/IPsec exigent pour l'authentification de l'homologue IPsec qu'un échange de certificats d'ordinateur ait lieu entre le serveur d'accès à distance et le client d'accès à distance. Vérifiez qu'un certificat approprié existe dans les magasins de certificats de l'ordinateur local du client d'accès à distance et du serveur d'accès à distance utilisant le composant logiciel enfichable Certificats.
- Certificat incorrect. Un certificat d'ordinateur valide émis par une autorité de certification qui suit une chaîne de certificats valide depuis l'autorité de certification émettrice jusqu'à une autorité de certification racine approuvée par le serveur VPN doit être installé sur le client VPN. Par ailleurs, un certificat d'ordinateur valide émis par une autorité de certification qui suit une chaîne de certificats valide depuis l'autorité de certification émettrice jusqu'à une autorité de certification racine approuvée par le client VPN doit être installée sur le serveur VPN.
- Un périphérique NAT existe entre le client d'accès à distance et le serveur d'accès à distance. S'il existe un service de routage NAT entre un client L2TP/IPsec Windows 2000 Server, Windows Server 2003 ou Windows XP et un serveur L2TP/IPsec Windows Server 2008, vous ne pouvez pas établir de connexion L2TP/IPsec, sauf si le client et le serveur prennent en charge IPSec NAT-T (IPSec NAT Traversal).
- Un pare-feu existe entre le client d'accès à distance et le serveur d'accès à distance. S'il existe un pare-feu entre un client L2TP/IPsec Windows et un serveur L2TP/IPsec Windows Server 2012 et si vous ne parvenez pas à établir une connexion L2TP/IPsec, vérifiez que le pare-feu autorise le transfert du trafic L2TP/IPsec.

Problèmes d'authentification EAP-TLS

Lorsque vous utilisez le protocole EAP-TLS pour l'authentification, le client VPN envoie un certificat utilisateur et le serveur d'authentification (le serveur VPN ou le serveur RADIUS) soumet un certificat d'ordinateur. Pour que le serveur d'authentification puisse valider le certificat du client VPN, les assertions suivantes doivent être vraies dans chacun des certificats de la chaîne de certificats envoyée par le client VPN :

- La date actuelle doit être comprise dans les dates de validité du certificat. Lorsque des certificats sont émis, ils sont assortis d'une plage de dates valides, avant laquelle ils ne peuvent pas être utilisés et après laquelle ils sont considérés comme étant arrivés à expiration.
- Le certificat n'a pas été révoqué. Les certificats émis peuvent être révoqués à tout moment. Chaque autorité de certification émettrice gère une liste de certificats qui ne sont pas considérés comme valides, et publie une liste de révocation de certificats. Par défaut, le serveur d'authentification vérifie chacun des certificats de la chaîne de certificats des clients VPN (la série de certificats entre le certificat du client VPN et l'autorité de certification racine) afin de voir s'il n'a pas été révoqué. Si l'un des certificats de la chaîne a été révoqué, la validation du certificat échoue.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Le certificat est assorti d'une signature numérique valide. Les autorités de certification signent numériquement les certificats qu'elles émettent. Le serveur d'authentification vérifie la signature numérique de chaque certificat de la chaîne (à l'exception du certificat d'autorité de certification racine) en obtenant la clé publique auprès de l'autorité de certification émettrice des certificats et en validant mathématiquement la signature numérique.

  Pour que le client VPN valide le certificat du serveur d'authentification pour l'authentification EAP-TLS, les assertions suivantes doivent être vraies pour chaque certificat de la chaîne de certificats envoyée par le serveur d'authentification :

  - La date actuelle doit être comprise dans les dates de validité du certificat.
  - Le certificat doit avoir une signature numérique valide.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique A : Configuration de l'accès à distance

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

La direction de A. Datum souhaite implémenter une solution d'accès à distance pour ses employés afin que les utilisateurs puissent se connecter au réseau d'entreprise en dehors du bureau. Vous décidez de déployer un projet pilote qui permettra aux utilisateurs du service informatique de se connecter à l'aide d'une connexion VPN à l'intranet d'entreprise.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

1. configurer un serveur VPN ;
2. configurer des clients VPN.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-RTR 22411B-LON-CL2
Nom d'utilisateur	**Administrateur**
Mot de passe	**Pa$$w0rd**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
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. Effectuez les étapes 2 à 4 pour **22411B-LON-RTR** et **22411B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configurer un serveur de réseau privé virtuel

Scénario

A. Datum Corporation souhaite implémenter une solution d'accès à distance pour ses employés afin qu'ils puissent se connecter au réseau d'entreprise en dehors du bureau. Vous devez activer et configurer les services de serveur nécessaires pour établir cet accès à distance. Pour que la solution VPN soit prise en charge, vous devez configurer une stratégie réseau qui reflète la stratégie de connexion à distance de l'entreprise. Pour le pilote, seul le groupe de sécurité informatique doit pouvoir utiliser la solution VPN. Les conditions requises comprennent le besoin d'un certificat client ; les heures de connexion sont fixées à tout moment, du lundi au vendredi uniquement.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les certificats serveur et client
2. Configurer le rôle Accès à distance
3. Créer une stratégie réseau pour les clients d'un réseau privé virtuel (VPN)

▶ Tâche 1 : Configurer les certificats serveur et client

1. Basculez vers LON-DC1.
2. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Ouvrez l'**Autorité de certification**.
4. Dans la Console des modèles de certificat, ouvrez les propriétés du modèle de certificat **Ordinateur**.
5. Sous l'onglet **Sécurité**, accordez l'autorisation **Autoriser l'inscription** au groupe **Utilisateurs authentifiés**.
6. Redémarrez l'Autorité de certification.
7. Fermez l'Autorité de certification.
8. Ouvrez la **Console de gestion des stratégies de groupe**.
9. Naviguez jusqu'à **Forêt : Adatum.com\Domaines\Adatum.com**.
10. Modifiez la **stratégie de domaine par défaut**.
11. Naviguez jusqu'au dossier **Configuration ordinateur\Stratégies\Paramètres Windows\ Paramètres de sécurité\Stratégies de clé publique**.
12. Créez des **Paramètres de demande automatique de certificat** pour le modèle de certificat **Ordinateur**.
13. Fermez l'Éditeur et la Console de gestion des stratégies de groupe.
14. Basculez vers l'ordinateur LON-RTR.
15. Créez une console de gestion à l'aide de **mmc.exe**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Ajoutez le composant logiciel enfichable **Certificats** en mettant l'accent sur le compte d'ordinateur local.
17. Naviguez jusqu'à la banque de **certificats personnels** et sélectionnez **Demander un nouveau certificat**.
18. Sur la page **Sélectionner la stratégie d'inscription de certificat**, cliquez sur **Stratégie d'inscription à Active Directory**, puis sur **Suivant**.
19. Inscrivez le certificat **Ordinateur** répertorié.
20. Fermez la console sans enregistrer ses paramètres.
21. Basculez vers l'ordinateur LON-CL2, puis ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
22. Ouvrez une invite de commandes et exécutez la commande **gpupdate /force** pour actualiser les paramètres de stratégie de groupe.
23. Créez une console de gestion à l'aide de **mmc.exe**.
24. Ajoutez le composant logiciel enfichable **Certificats** en mettant l'accent sur le compte d'ordinateur local.
25. Naviguez jusqu'à la banque de certificats **Personnel**.
26. Vérifiez qu'un certificat émis par Adatum-LON-DC1-CA existe pour LON-CL2.
27. Fermez la console sans enregistrer ses paramètres.

▶ Tâche 2 : Configurer le rôle Accès à distance

1. Sur LON-RTR, ouvrez le **Gestionnaire de serveur**, puis ajoutez le rôle **Services de stratégie et d'accès réseau**.
2. Fermez le Gestionnaire de serveur.
3. Ouvrez la console Serveur NPS.
4. Enregistrez le serveur dans AD DS.
5. Laissez la fenêtre Serveur NPS (Network Policy Server) ouverte.
6. Ouvrez Routage et accès distant.
7. Désactivez la configuration existante.
8. Reconfigurez LON-RTR en tant que serveur VPN à l'aide des paramètres suivants :
   a. **Connexion au réseau local 2** correspond à l'interface publique.
   b. Le serveur VPN alloue des adresses du pool : **172.16.0.100** - **172.16.0.111**
   c. Le serveur est configuré avec l'option **Non, utiliser Routage et accès distant pour authentifier les demandes de connexion**.
9. Démarrez le service VPN.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Créer une stratégie réseau pour les clients d'un réseau privé virtuel (VPN)

1. Sur LON-RTR, basculez vers la console Serveur NPS (Network Policy Server).
2. Désactivez les deux stratégies réseau existantes ; elles empêcheraient le traitement de la stratégie que vous êtes sur le point de créer.
3. Créez une stratégie réseau à l'aide des propriétés ci-dessous :
   a. Nom de la stratégie : **Stratégie VPN pilote informatique**
   b. Type de serveur d'accès réseau : **Serveur d'accès à distance (VPN-Dial up)**
   c. Condition : **Groupes Windows = IT**
   d. Autorisation : **Accès accordé**
   e. Méthodes d'authentification : **Authentification cryptée Microsoft version 2 (MS-CHAP-v2)**
   f. Contraintes : **Restrictions relatives aux jours et aux heures = toute la journée du lundi au vendredi accordée**.
   g. Paramètres : valeur par défaut

Résultats : À la fin de cet exercice, vous devriez avoir déployé un serveur VPN et configuré l'accès pour les membres du groupe de sécurité global informatique.

Exercice 2 : Configuration de clients VPN

Scénario

Vous devez maintenant fournir une solution cliente simple de sorte que les utilisateurs puissent installer une connexion VPN L2TP préconfigurée pour se connecter au réseau d'entreprise.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer et distribuer un profil Kit d'administration du Gestionnaire des connexions
2. Vérifier l'accès au client
3. Pour préparer l'atelier suivant

▶ Tâche 1 : Configurer et distribuer un profil Kit d'administration du Gestionnaire des connexions

1. Basculez vers LON-CL2.
2. Dans le Panneau de configuration, installez la fonctionnalité **Kit d'administration du Gestionnaire des connexions Microsoft (CMAK) RAS**.
3. Dans **Outils d'administration**, ouvrez le **Kit d'administration du Gestionnaire des connexions**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Suivez les instructions de l'Assistant Kit d'administration du Gestionnaire des connexions à l'aide des valeurs par défaut, à l'exception de ce qui suit :
   a. Page Sélectionner le système d'exploitation cible : **Windows Vista ou version ultérieure**
   b. Page Créer ou modifier un profil Gestionnaire des connexions : **Nouveau profil**
   c. Page Spécifier les noms de service et de fichier :
      - Nom du service : **VPN pilote Adatum**
      - Nom du fichier : **Adatum**
   d. Page Spécifier un nom de domaine : **Ne pas ajouter de nom de domaine Kerberos au nom d'utilisateur**
   e. Page Ajouter une prise en charge des connexions VPN :
      - Annuaire de ce profil : activé
      - Nom de serveur VPN ou adresse IP : **10.10.0.1**
   f. Page Créer ou modifier une entrée VPN : **Modifier** l'entrée VPN répertoriée. Dans l'onglet **Sécurité** :
      - Stratégie VPN : Utiliser uniquement le protocole L2TP (Protocole Layer two Tunneling Protocol).
   g. Page Ajouter un annuaire téléphonique personnalisé : **Téléchargement automatique des mises à jour de l'annuaire téléphonique** désélectionné.
5. Ouvrez l'Explorateur de fichiers et naviguez jusqu'au dossier **C:\Programmes\CMAK\Profils\Windows Vista and above\Adatum**.
6. Double-cliquez sur **Adatum.exe**, puis suivez les instructions de l'Assistant VPN pilote Adatum :
   - Rendre cette connexion disponible pour : **Tous les utilisateurs**
7. Dans la fenêtre de connexion, cliquez sur **Annuler**.

▶ Tâche 2 : Vérifier l'accès au client

1. Déconnectez-vous de LON-CL2.
2. Ouvrez une session en tant qu'**ADATUM\April** avec le mot de passe **Pa$$w0rd**.
3. Ouvrez le dossier Connexions réseau.
4. Testez la connexion VPN pilote Adatum. Utilisez les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\April**
   - Mot de passe : **Pa$$w0rd**

▶ Pour préparer l'atelier suivant

- Une fois l'atelier terminé, rétablissez l'état initial de tous les ordinateurs virtuels.

Résultats : À la fin de cet exercice, vous aurez distribué avec succès un profil CMAK et testé l'accès VPN.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 5
Configuration de DirectAccess

Les organisations comptent souvent sur les connexions VPN pour fournir à des utilisateurs distants l'accès sécurisé aux données et aux ressources sur le réseau d'entreprise. Les connexions VPN sont faciles à configurer et sont prises en charge par différents clients. Cependant, elles doivent d'abord être initialisées par l'utilisateur, et peuvent requérir une configuration supplémentaire au niveau du pare-feu de l'entreprise. En outre, les connexions VPN permettent généralement d'accéder à distance à l'ensemble du réseau d'entreprise. De plus, les organisations ne peuvent pas gérer efficacement les ordinateurs distants, à moins qu'ils ne soient connectés. Pour aller au-delà de telles restrictions sur ces connexions VPN, les organisations peuvent implémenter DirectAccess pour fournir une connexion transparente entre le réseau interne et l'ordinateur distant sur Internet. DirectAccess permet aux organisations de gérer les ordinateurs distants plus efficacement, car ils sont considérés comme faisant partie du réseau d'entreprise.

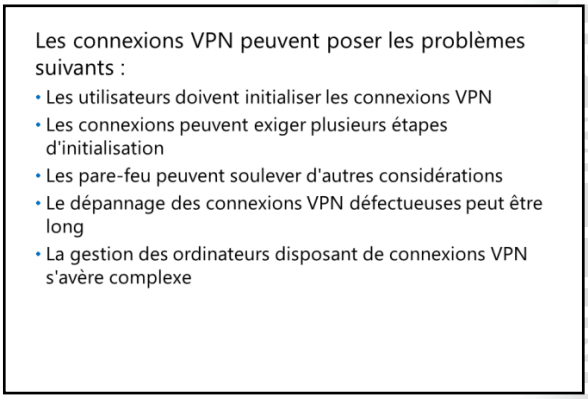
Objectifs de la leçon

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

- débattre de la complexité des connexions VPN typiques ;
- décrire DirectAccess ;
- décrire les composants requis pour implémenter DirectAccess ;
- expliquer comment utiliser la Table de stratégie de résolution de noms ;
- expliquer comment DirectAccess fonctionne pour les clients connectés en interne ;
- expliquer comment DirectAccess fonctionne pour les clients connectés en externe ;
- lister la configuration requise pour DirectAccess ;
- expliquer comment configurer DirectAccess.

Complexités liées à la gestion des connexions VPN

Bon nombre d'organisations comptent souvent sur les connexions VPN pour fournir à leurs utilisateurs l'accès à distance sécurisé aux ressources sur le réseau interne d'entreprise. Ces connexions VPN doivent bien souvent être configurées manuellement, ce qui peut entraîner des problèmes d'interopérabilité lorsque les utilisateurs utilisent différents clients VPN. En outre, les connexions VPN peuvent poser les problèmes suivants :



- Les utilisateurs doivent initialiser les connexions VPN.
- Les connexions peuvent requérir plusieurs étapes pour s'initialiser, et la procédure de connexion peut prendre plusieurs secondes voire plus.

- Les pare-feu peuvent soulever d'autres considérations. Si elles ne sont pas correctement configurées sur le pare-feu, les connexions VPN peuvent échouer, voire permettre l'accès à distance à la totalité du réseau d'entreprise.
- Le dépannage des problèmes liés aux échecs de connexions VPN peut souvent représenter une importante partie des appels au support technique pour de nombreuses organisations.
- La gestion des ordinateurs disposant de connexions VPN s'avère complexe. Les ordinateurs clients distants basés sur VPN représentent un défi pour les professionnels de l'informatique, car ces ordinateurs ne peuvent pas se connecter au réseau interne pendant des semaines à la fois, ce qui les empêche de télécharger des objets de stratégie de groupe (GPO, Group Policy Objects) et les mises à jour logicielles.

Extension du réseau pour atteindre les ordinateurs et les utilisateurs connectés à distance

Pour aller au-delà de ces restrictions sur ces connexions VPN traditionnelles, les organisations peuvent implémenter DirectAccess pour fournir une connexion transparente entre le réseau interne et l'ordinateur distant sur Internet. DirectAccess permet aux organisations de gérer plus facilement des ordinateurs distants car ils sont toujours connectés.

Qu'est-ce que DirectAccess ?

La fonctionnalité DirectAccess dans Windows Server 2012 active l'accès à distance transparent aux ressources intranet sans établir de connexion VPN au préalable. La fonctionnalité DirectAccess garantit également une connectivité transparente à l'infrastructure d'applications pour les utilisateurs internes et les utilisateurs distants.

Fonctionnalités de DirectAccess :

- Se connecte automatiquement au réseau d'entreprise sur le réseau public
- Utilise plusieurs protocoles, notamment HTTPS, pour établir une connectivité IPv6
- Prend en charge l'accès au serveur sélectionné et l'authentification IPsec
- Prend en charge l'authentification de bout en bout et le chiffrement
- Prend en charge la gestion des ordinateurs clients distants
- Permet la connexion directe des utilisateurs distants aux serveurs intranet

À la différence des VPN traditionnels qui nécessitent l'intervention de l'utilisateur pour établir une connexion à un intranet, DirectAccess permet à toutes les applications compatibles avec IPv6 sur l'ordinateur client d'avoir un accès complet aux ressources intranet. DirectAccess vous permet également de spécifier les ressources et les applications côté client qui sont limitées en ce qui concerne l'accès à distance.

DirectAccess profite aux organisations en permettant à leur personnel informatique de gérer des ordinateurs distants comme il gèrerait des ordinateurs locaux. L'utilisation des mêmes serveurs de gestion et de mise à jour garantit que les ordinateurs distants sont toujours mis à jour et conformes aux stratégies de contrôle d'intégrité système et de sécurité. Vous pouvez également définir des stratégies d'accès plus détaillées pour l'accès à distance par rapport aux stratégies de contrôle d'accès définies dans les solutions VPN.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

DirectAccess présente les fonctionnalités suivantes :

- connexion automatique à l'intranet d'entreprise lorsque connecté à Internet ;
- utilisation de divers protocoles, y compris HTTPS, pour établir une connectivité IPv6. HTTPS est généralement autorisé via les pare-feu et les serveurs proxy ;
- prise en charge de l'accès au serveur sélectionné et authentification IPsec de bout en bout avec les serveurs du réseau intranet ;
- prise en charge de l'authentification de bout en bout et du chiffrement avec les serveurs du réseau intranet ;
- prise en charge de la gestion des ordinateurs clients distants ;
- connexion directe des utilisateurs distants aux serveurs intranet.

DirectAccess présente également les avantages ci-dessous :

- Connectivité toujours activée. Lorsque l'utilisateur connecte l'ordinateur client à Internet, l'ordinateur client est également connecté à l'intranet. Cette connectivité permet aux ordinateurs clients distants d'accéder aux applications, et de les mettre à jour, plus facilement. Les ressources intranet demeurent ainsi toujours disponibles, permettant aux utilisateurs de se connecter à l'intranet d'entreprise depuis n'importe quel endroit, à tout moment, améliorant par conséquent leur productivité et leurs performances.
- Connectivité transparente. DirectAccess fournit une expérience de connectivité cohérente, que l'ordinateur client soit local ou distant. Grâce à cela, les utilisateurs délaissent les options et la procédure de connectivité au profit de la productivité. Cette cohérence peut réduire les frais de formation pour les utilisateurs, avec moins d'incidents de support.
- Accès bidirectionnel. Vous pouvez configurer DirectAccess de manière à ce que les clients DirectAccess aient accès aux ressources intranet et de sorte que vous puissiez également avoir accès à ces clients DirectAccess depuis l'intranet. Par conséquent, DirectAccess peut être bidirectionnel. Cela garantit la mise à jour constante des ordinateurs clients avec les dernières mises à jour de sécurité, l'application du domaine Stratégie de groupe et une expérience identique, que l'utilisateur soit sur l'intranet d'entreprise ou sur le réseau public. Cet accès bidirectionnel a également les consequences suivantes :
  - délai des mises à jour réduit ;
  - renforcement de la sécurité ;
  - taux d'échec des mises à jour réduit ;
  - amélioration de l'analyse de la conformité.
- Prise en charge de la gestion sortante. Cette nouvelle fonctionnalité de Windows Server 2012 permet d'activer uniquement la fonctionnalité de gestion à distance dans le client DirectAccess. Cette nouvelle sous-option de l'Assistant de configuration des clients DirectAccess automatise le déploiement des stratégies qui sont utilisées pour la gestion des ordinateurs clients. La prise en charge de la gestion sortante n'assure aucune option de stratégie permettant aux utilisateurs de se connecter au réseau pour accéder à un fichier ou une application. Unidirectionnelle, elle fournit un accès entrant à des fins administratives uniquement.

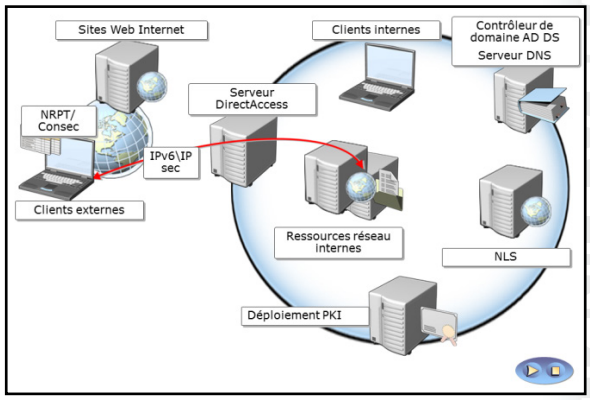
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Sécurité optimisée. Contrairement aux VPN traditionnels, DirectAccess offre plusieurs niveaux de contrôle d'accès aux ressources du réseau. Ce contrôle avancé permet aux architectes de la sécurité de contrôler de manière précise les utilisateurs distants qui accèdent aux ressources spécifiées. Vous pouvez utiliser une stratégie granulaire pour définir les utilisateurs pouvant utiliser DirectAccess ainsi que l'emplacement à partir duquel ils peuvent y accéder. Le chiffrement IPsec est utilisé pour protéger le trafic DirectAccess, de telle sorte que les utilisateurs peuvent garantir la fiabilité de la sécurité de leur communication.
- Solution intégrée. DirectAccess s'intègre pleinement aux solutions NAP et d'isolation de serveur et de domaine, entraînant ainsi l'intégration transparente des stratégies de spécification d'intégrité, d'accès et de sécurité entre l'intranet et les ordinateurs distants.

Composants de DirectAccess

Pour déployer et configurer DirectAccess, votre organisation doit prendre en charge les composants d'infrastructure suivants :

- serveur DirectAccess ;
- clients DirectAccess ;
- Serveur d'emplacement réseau
- ressources internes ;
- domaine AD DS ;
- Stratégie de groupe
- PKI (en option pour le réseau interne) ;
- Serveur DNS (Domain Name System)
- Serveur NAP



Serveur DirectAccess

Le serveur DirectAccess peut être n'importe quel serveur Windows Server 2012 connecté à un domaine ; il accepte les connexions à partir des clients DirectAccess et établit la communication avec les ressources intranet. Ce serveur fournit les services d'authentification pour les clients DirectAccess et agit comme point de terminaison de mode de tunnel IPsec pour le trafic externe. Le nouveau rôle du serveur d'accès à distance permet l'administration centralisée, la configuration et l'analyse à la fois de la connectivité DirectAccess et de la connectivité VPN.

Par rapport à la précédente implémentation dans Windows Server 2008 R2, la nouvelle installation sous la forme d'un Assistant simplifie la gestion DirectAccess pour les petites et moyennes organisations. L'Assistant simplifie la gestion en supprimant le recours au déploiement complet PKI ainsi que le besoin de deux adresses IPv4 publiques consécutives pour la carte physique connectée à Internet. Dans Windows Server 2012, l'Assistant d'installation DirectAccess détecte l'état réel de l'implémentation du serveur DirectAccess et sélectionne automatiquement le meilleur déploiement. Cela épargne ainsi à l'administrateur la complexité d'une configuration manuelle des technologies de transition IPv6.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Clients DirectAccess

Les clients DirectAccess peuvent être tout ordinateur connecté à un domaine fonctionnant sous Windows 8 Enterprise, Windows 7 Enterprise ou Windows 7 Ultimate.

Remarque : Avec la mise en service hors site, vous pouvez associer l'ordinateur client Windows 8 Enterprise à un domaine sans le connecter en interne.

L'ordinateur client DirectAccess se connecte au serveur DirectAccess à l'aide d'IPv6 et IPsec. Si un réseau IPv6 natif n'est pas disponible, le client établit alors un tunnel IPv6/IPv4 à l'aide des technologies de transition 6to4 ou Teredo. Notez que l'exécution de cette étape ne requiert pas que l'utilisateur soit connecté à l'ordinateur.

Si un pare-feu ou un serveur proxy empêche l'ordinateur client utilisant 6to4 ou Teredo de se connecter au serveur DirectAccess, l'ordinateur client essaie automatiquement de se connecter à l'aide du protocole IP-HTTPS qui utilise une connexion SSL pour garantir la connectivité. Le client a accès aux règles de Table de stratégie de résolution de noms et de tunnel de sécurité de connexion.

Serveur d'emplacement réseau

Les clients DirectAccess utilisent le serveur d'emplacement réseau (NLS) pour déterminer leur emplacement. Si l'ordinateur client peut se connecter avec HTTPS, il suppose alors qu'il est sur l'intranet et il désactive les composants DirectAccess. S'il est impossible de contacter le serveur NLS, le client suppose qu'il est sur Internet. Le serveur NLS est installé avec le rôle serveur Web.

Remarque : L'URL pour le serveur NLS est distribuée à l'aide d'un objet de stratégie de groupe.

Ressources internes

Vous pouvez configurer n'importe quelle application compatible avec IPv6 qui s'exécute sur les serveurs internes ou les ordinateurs clients de manière à la rendre disponible pour les clients DirectAccess. Pour les applications et serveurs plus anciens, notamment ceux qui ne sont pas basés sur les systèmes d'exploitation Windows et qui ne prennent pas en charge IPv6, Windows Server 2012 inclut désormais la prise en charge native d'une passerelle de traduction de protocole (NAT64) et de résolution de noms (DNS64) pour convertir les communications IPv6 provenant d'un client DirectAccess vers IPv4 pour les serveurs internes.

Remarque : Comme dans le passé, cette fonctionnalité peut être également accomplie en passant par le déploiement de Microsoft Forefront® Unified Access Gateway. De même, comme dans les versions antérieures, ces services de traduction ne prennent pas en charge les sessions lancées par les périphériques internes, mais uniquement les demandes en provenance de DirectAccess IPv6.

Domaine Active Directory

Vous devez déployer au moins un domaine Active Directory doté, au minimum, du niveau fonctionnel du domaine Windows Server 2003. Windows Server 2012 DirectAccess offre une prise en charge intégrée de plusieurs domaines, ce qui permet aux ordinateurs clients provenant de différents domaines d'accéder aux ressources qui peuvent être situées dans différents domaines approuvés.

Stratégie de groupe

La stratégie de groupe est nécessaire à l'administration centralisée et au déploiement des paramètres DirectAccess. L'Assistant Installation DirectAccess crée un ensemble d'objets de stratégie de groupe et les paramètres des clients DirectAccess, le serveur DirectAccess ainsi que les serveurs sélectionnés.

PKI

Le déploiement de l'infrastructure PKI est facultatif pour la configuration et la gestion simplifiées. DirectAccess sous Windows Server 2012 permet l'envoi des demandes d'authentification client vers un service proxy Kerberos basé sur HTTPS qui s'exécute sur le serveur DirectAccess. Cela élimine le besoin d'établir un second tunnel IPsec entre les clients et les contrôleurs de domaine. Le proxy Kerberos envoie alors les demandes Kerberos aux contrôleurs de domaine de la part du client.

Cependant, pour une configuration DirectAccess complète qui permet l'intégration de la protection d'accès réseau (NAP), l'authentification à deux facteurs et le tunneling forcé, vous devez encore implémenter les certificats d'authentification pour chaque client qui participera aux communications DirectAccess.

Serveur DNS

Lorsque le protocole ISATAP est exécuté, vous devez utiliser au moins Windows Server 2008 R2, Windows Server 2008 Service Pack 2 (SP2) ou plus récent, ou un serveur DNS non-Microsoft qui prend en charge les échanges de messages DNS sur le protocole ISATAP.

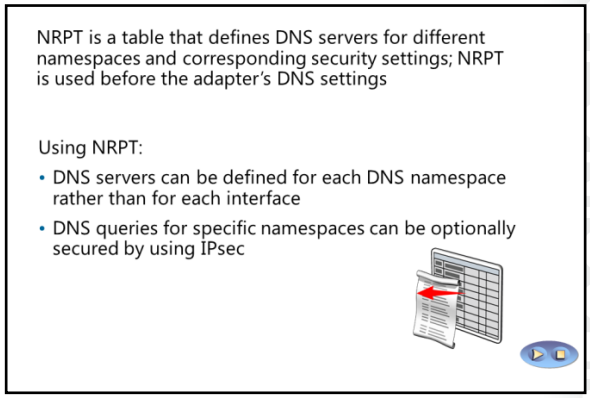
Serveurs NAP

La protection d'accès réseau (NAP) est un composant facultatif de la solution DirectAccess qui permet d'effectuer un contrôle de conformité et d'appliquer la stratégie de sécurité pour les clients DirectAccess sur Internet. DirectAccess sous Windows Server 2012 permet de configurer une vérification d'intégrité NAP directement depuis l'interface utilisateur d'installation plutôt que de modifier manuellement les objets de stratégie de groupe nécessaires avec DirectAccess sous Windows Server 2008 R2.

Qu'est-ce que la Table de stratégie de résolution de noms ?

Intégrée à Windows Server 2012 et Windows 8, la Table de stratégie de résolution de noms (NRPT) permet de séparer le trafic Internet du trafic intranet dans DirectAccess. Cette fonctionnalité permet aux serveurs DNS d'être définis pour un espace de noms DNS plutôt que pour une interface.

La table NRPT stocke une liste de règles. Chaque règle définit un espace de noms DNS et des paramètres de configuration qui décrivent le comportement du client DNS pour cet espace de noms.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsqu'un client DirectAccess est connecté à Internet, chaque demande de requête de nom est comparée aux règles d'espace de noms figurant dans la table NRPT.

- Si une correspondance est trouvée, la demande est traitée selon les paramètres de la règle NRPT.
- Si une demande de requête de nom ne correspond pas à un espace de noms répertorié dans la table NRPT, la demande est envoyée aux serveurs DNS configurés dans les paramètres TCP/IP pour l'interface réseau spécifiée.

Les paramètres DNS sont configurés selon l'emplacement client :

- Pour un ordinateur client distant, les serveurs DNS sont généralement les serveurs DNS Internet configurés via le fournisseur de services Internet (ISP, Internet Service Provider).
- Pour un client DirectAccess sur l'intranet, les serveurs DNS sont généralement les serveurs DNS intranet configurés via le protocole DHCP.

Les noms en une partie, par exemple, http://internal, ont, en général, des suffixes de recherche DNS configurés ajoutés au nom avant qu'ils ne soient contrôlés par rapport à la table NRPT.

Si aucun suffixe de recherche DNS n'est configuré et que le nom en une partie ne correspond à aucune autre entrée de nom en une partie dans la table NRPT, la demande est envoyée aux serveurs DNS spécifiés dans les paramètres TCP/IP du client.

Les espaces de noms, par exemple, internal.adatum.com, sont saisis dans la table NRPT, suivis des serveurs DNS vers lesquels les demandes correspondant à cet espace de noms doivent être dirigées. Si une adresse IP est saisie pour le serveur DNS, toutes les demandes DNS sont envoyées directement au serveur DNS sur la connexion DirectAccess. De telles configurations ne requièrent pas de sécurité supplémentaire. Cependant, si un nom est spécifié pour le serveur DNS (par exemple, dns.adatum.com) dans la table NRPT, ce nom doit pouvoir être publiquement résolu lorsque le client interroge les serveurs DNS spécifiés dans ses paramètres TCP/IP.

La table NRPT permet aux clients DirectAccess d'utiliser les serveurs DNS intranet pour la résolution de noms des ressources internes et les serveurs DNS Internet pour la résolution de noms d'autres ressources. Les serveurs DNS dédiés ne sont pas indispensables à la résolution de nom. DirectAccess est conçu pour empêcher l'exposition de votre espace de noms intranet à Internet.

Il convient de traiter différemment certains noms en ce qui concerne la résolution de nom ; ces noms ne doivent pas être traduits à l'aide des serveurs DNS intranet. Pour garantir la traduction de ces noms avec les serveurs DNS spécifiés dans les paramètres TCP/IP du client, vous devez les ajouter aux exemptions de la table NRPT.

La table NRPT est contrôlée par la stratégie de groupe. Quand l'ordinateur est configuré pour utiliser la table NRPT, le mécanisme de résolution de noms utilise, dans l'ordre :

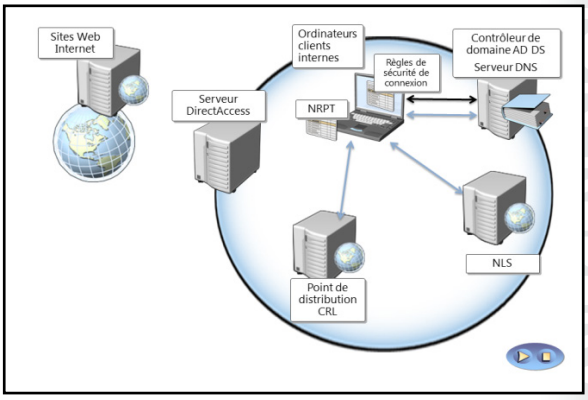
- le cache de noms local ;
- le fichier d'hôtes ;
- la table NRPT.

Puis, le mécanisme de résolution de noms envoie la demande aux serveurs DNS spécifiés dans les paramètres TCP/IP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fonctionnement de DirectAccess pour les clients internes

Un serveur NLS est un serveur de réseau interne qui héberge une URL accessible via HTTPS. Les clients DirectAccess essayent d'accéder à l'URL du serveur NLS pour déterminer s'ils sont situés sur l'intranet ou sur un réseau public. Le serveur DirectAccess peut également être le serveur NLS. Dans quelques organisations dans lesquelles DirectAccess est un service vital pour l'entreprise, le serveur NLS doit être maintenu à un haut niveau de disponibilité. En général, le serveur Web sur le serveur NLS ne doit pas être dédié uniquement à la prise en charge des clients DirectAccess.



Il est vital que le serveur NLS soit disponible depuis chaque site de l'entreprise, car le comportement du client DirectAccess dépend de la réponse du serveur NLS. Les emplacements des succursales peuvent requérir un serveur NLS distinct sur chaque site pour garantir que le serveur NLS reste accessible même en cas de défaillance de liaison entre les succursales.

Fonctionnement de DirectAccess pour les clients internes

La procédure de connexion DirectAccess se produit automatiquement, sans intervention de l'utilisateur. Les clients DirectAccess utilisent la procédure suivante pour se connecter aux ressources de l'intranet :

1. Le client DirectAccess tente de résoudre le nom de domaine complet (FQDN) d'une URL du serveur NLS. Puisque le nom de domaine complet (FQDN) de l'URL du serveur NLS correspond à une règle d'exemption dans la table NRPT, le client DirectAccess envoie à la place la requête DNS à un serveur DNS configuré localement (un serveur DNS basé sur l'intranet). Le serveur DNS basé sur l'intranet résout le nom.
2. Le client DirectAccess accède à l'URL accessible via HTTPS du serveur NLS, procédure au cours de laquelle il obtient le certificat du serveur NLS.
3. Selon le champ Points de distribution de la liste de révocation des certificats du certificat du serveur NLS, le client DirectAccess vérifie les fichiers de révocation de la liste de révocation de certificats dans le point de distribution CRL pour déterminer si le certificat du serveur NL a été révoqué.
4. Lorsque le code de réponse HTTP est 200, le client DirectAccess détermine le succès de l'URL du serveur NLS (accès, authentification de certificat et test de vérification de révocation réussis). Le client DirectAccess bascule vers le profil du pare-feu du domaine et ignore les stratégies DirectAccess ; il suppose qu'il se situe sur le réseau interne jusqu'à la prochaine modification réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. L'ordinateur client DirectAccess tente de localiser et de se connecter au domaine AD DS à l'aide de son compte d'ordinateur.

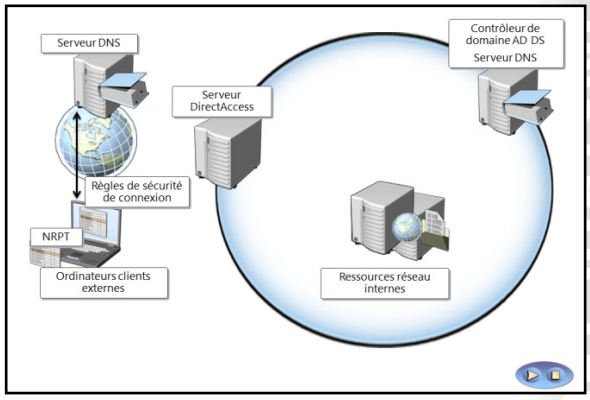
   Puisque le client ne référence plus aucune règle DirectAccess dans la table NRPT pendant le reste de la session connectée, toutes les demandes DNS sont envoyées via les serveurs DNS configurés sur l'interface (serveurs DNS basés sur l'intranet). Avec l'association de la détection d'emplacement réseau et la connexion au domaine d'ordinateurs, le client DirectAccess se configure pour un accès normal à l'intranet.

6. Selon la réussite de la connexion de l'ordinateur au domaine, le client DirectAccess attribue le profil de domaine (réseau de pare-feu) au réseau associé.

Normalement, les règles du tunnel de sécurité de connexion DirectAccess s'étendent aux profils de pare-feu privés et publics ; elles sont désactivées à partir de la liste des règles actives de sécurité de connexion.

Le client DirectAccess a déterminé avec succès qu'il est connecté à son intranet, et n'utilise pas de paramètres DirectAccess (règles de la table NRPT ou règles de tunnel de sécurité de connexion). Le client DirectAccess peut à présent accéder normalement à des ressources intranet. Il peut également accéder à des ressources Internet par des moyens normaux, tels qu'un serveur proxy.

Fonctionnement de DirectAccess pour les clients externes



Lorsqu'un client DirectAccess démarre, il tente d'accéder à l'adresse URL spécifiée pour le serveur NLS et suppose qu'il n'est pas connecté à l'intranet car il ne parvient pas à communiquer avec le serveur NLS. Il commence alors à utiliser la table NRPT et les règles de sécurité de connexion. La table NRPT a des règles basées sur DirectAccess en ce qui concerne la résolution de noms, et les règles de sécurité de connexion définissent les tunnels IPsec DirectAccess pour la communication avec les ressources intranet. Les clients DirectAccess connectés à Internet utilisent les étapes générales suivantes pour se connecter aux ressources intranet.

- Tout d'abord, le client DirectAccess tente d'accéder au serveur NLS.
- Puis, le client tente de trouver un contrôleur de domaine.
- Enfin, le client tente d'accéder aux ressources intranet, puis aux ressources Internet.

Le client DirectAccess tente d'accéder au serveur d'emplacement réseau (NLS)

Le client DirectAccess essaie d'accéder au serveur NLS comme suit :

1. Le client essaie de résoudre le nom de domaine complet de l'URL du serveur NLS. Puisque le nom de domaine complet de l'URL du serveur NLS correspond à une règle d'exemption de la table NRPT, le client DirectAccess n'envoie pas de demande DNS à un serveur DNS configuré au niveau local (serveur DNS basé sur Internet). Un serveur DNS externe basé sur Internet ne parviendrait pas à résoudre le nom.
2. Le client DirectAccess traite la demande de résolution de noms comme défini dans les règles d'exemption de DirectAccess dans la table NRPT.

3. Puisque le serveur NLS est introuvable sur le même réseau sur lequel le client DirectAccess se trouve actuellement, le client DirectAccess applique au réseau associé un profil réseau de pare-feu privé ou public.
4. Les règles de tunnel de sécurité de connexion pour DirectAccess, étendues aux profils privés et publics, fournissent le profil réseau de pare-feu privé ou public.

Le client DirectAccess utilise à la fois les règles NRPT et les règles de sécurité de connexion pour trouver les ressources intranet et y accéder à travers Internet via le serveur DirectAccess.

Le client DirectAccess tente de trouver un contrôleur de domaine

Après la détermination de son emplacement réseau, le client DirectAccess tente de trouver un contrôleur de domaine et de s'y connecter. Cette procédure génère un tunnel IPsec ou un tunnel d'infrastructure à l'aide du mode de tunnel IPsec et du mode ESP vers le serveur DirectAccess. Le processus se déroule comme suit :

1. Le nom DNS pour le contrôleur de domaine correspond à la règle d'espace de noms intranet dans la table NRPT, qui spécifie l'adresse IPv6 du serveur DNS intranet. Le service client DNS établit la demande de nom DNS adressée à l'adresse IPv6 du serveur DNS intranet et la fait suivre à la pile TCP/IP du client DirectAccess pour envoi.
2. Avant de procéder à l'envoi du paquet, la pile TCP/IP effectue une vérification et détermine si des règles sortantes du Pare-feu Windows ou des règles de sécurité de connexion pour le paquet existent.
3. Puisque l'adresse IPv6 de destination dans la demande de nom DNS correspond à une règle de sécurité de connexion qui correspond elle-même au tunnel de l'infrastructure, le client DirectAccess utilise les protocoles AuthIP (Authenticated IP) et IPsec pour négocier et authentifier un tunnel IPsec chiffré vers le serveur DirectAccess. Le client DirectAccess (à la fois l'ordinateur et l'utilisateur) s'authentifie respectivement avec son certificat d'ordinateur installé et ses informations d'identification Microsoft Windows NT® LAN Manager (NTLM).

 **Remarque :** AuthIP améliore l'authentification dans IPsec en ajoutant la prise en charge de l'authentification basée sur l'utilisateur avec Kerberos v5 ou les certificats SSL. AuthIP prend également en charge la négociation efficace de protocole et l'utilisation de plusieurs jeux d'informations d'identification pour authentification.

4. Le client DirectAccess envoie la demande de nom DNS via le tunnel IPsec d'infrastructure vers le serveur DirectAccess.
5. Le serveur DirectAccess transmet la demande de nom DNS au serveur DNS intranet. La réponse à la demande de nom DNS est renvoyée au serveur DirectAccess, puis vers le client DirectAccess via le tunnel IPsec d'infrastructure.

Le trafic de connexions au domaine ultérieur passe par le tunnel IPsec d'infrastructure. Lorsque l'utilisateur sur le client DirectAccess se connecte, le trafic de connexions du domaine se passe via le tunnel IPsec d'infrastructure.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le client DirectAccess tente d'accéder aux ressources intranet

La première fois que le client DirectAccess envoie le trafic à un emplacement intranet qui ne figure pas sur la liste de destinations pour le tunnel d'infrastructure (tel qu'un site Web interne), le processus suivant se produit :

1. L'application ou le processus qui tente d'établir une communication élabore un message ou une charge utile, puis le/la transfère vers la pile TCP/IP pour envoi.
2. Avant de procéder à l'envoi du paquet, la pile TCP/IP effectue une vérification et détermine si des règles sortantes du Pare-feu Windows ou des règles de sécurité de connexion pour le paquet existent.
3. Puisque l'adresse IPv6 de destination correspond à la règle de sécurité de connexion qui correspond au tunnel intranet (qui spécifie l'espace d'adressage IPv6 de l'intranet tout entier), le client DirectAccess utilise AuthIP et IPsec pour négocier et authentifier un tunnel IPsec supplémentaire vers le serveur DirectAccess. Le client DirectAccess s'authentifie avec son certificat d'ordinateur installé et les informations d'identification Kerberos de son compte d'utilisateur.
4. Le client DirectAccess envoie le paquet via le tunnel intranet vers le serveur DirectAccess.
5. Le serveur DirectAccess transmet le paquet vers les ressources intranet. La réponse est renvoyée au serveur DirectAccess, puis vers le client DirectAccess via le tunnel intranet.

Tout trafic d'accès intranet ultérieur qui ne correspond pas à une destination intranet dans la règle de sécurité de connexion du tunnel d'infrastructure passe via le tunnel intranet.

Le client DirectAccess tente d'accéder aux ressources Internet

Quand l'utilisateur ou un processus sur le client DirectAccess tente d'accéder à une ressource Internet (telle qu'un serveur Web), le processus suivant se produit :

1. Le service client DNS transmet le nom DNS pour la ressource Internet via la table NRPT. Il n'existe aucune correspondance. Le service client DNS établit la demande de nom DNS adressée à l'adresse IP d'un serveur DNS Internet configuré sur l'interface et la fait suivre à la pile TCP/IP pour envoi.
2. Avant de procéder à l'envoi du paquet, la pile TCP/IP effectue une vérification et détermine si des règles sortantes du Pare-feu Windows ou des règles de sécurité de connexion pour le paquet existent.
3. Parce que l'adresse IP de destination dans la demande de nom DNS ne correspond pas aux règles de sécurité de connexion pour les tunnels vers le serveur DirectAccess, le client DirectAccess envoie normalement la demande de nom DNS.
4. Le serveur DNS Internet répond avec l'adresse IP de la ressource Internet.
5. L'application de l'utilisateur ou le processus établit le premier paquet à envoyer vers la ressource Internet. Avant de procéder à l'envoi du paquet, la pile TCP/IP effectue une vérification et détermine si des règles sortantes du Pare-feu Windows ou des règles de sécurité de connexion pour le paquet existent.
6. Parce que l'adresse IP de destination dans la demande de nom DNS ne correspond pas aux règles de sécurité de connexion pour les tunnels vers le serveur DirectAccess, le client DirectAccess envoie normalement le paquet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

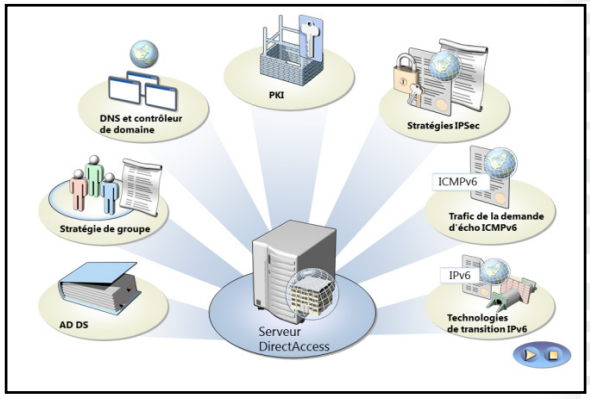
Tout trafic d'accès Internet ultérieur, qui ne correspond pas à une destination dans les règles soit du tunnel Internet d'infrastructure, soit de sécurité de connexion, transite normalement.

La procédure d'accès au contrôleur de domaine et aux ressources intranet est très similaire à la procédure de connexion, parce que les deux utilisent les tables NRPT pour trouver le serveur DNS approprié afin de résoudre les demandes de nom. La différence réside dans le fait que le tunnel IPsec est établi entre le client et le serveur DirectAccess. En accédant au contrôleur de domaine, toutes les demandes DNS sont envoyées par le tunnel IPsec d'infrastructure, et lors de l'accès aux ressources intranet, un deuxième tunnel IPsec (intranet) est établi.

Conditions prérequises pour l'implémentation de DirectAccess

Conditions requises pour le serveur DirectAccess

Pour déployer DirectAccess, vous devez vous assurer que le serveur répond aux conditions requises pour le matériel et le réseau suivantes :



- Le serveur doit être joint à un domaine AD DS.
- Le serveur doit être doté du système d'exploitation Windows Server 2012 ou Windows Server 2008 R2.
- Une seule carte réseau peut être installée sur le système d'exploitation Windows Server 2012 installé en tant que serveur DirectAccess. Elle doit être connectée à l'intranet et publiée sur Microsoft Forefront Threat Management Gateway (TMG) 2010 ou Microsoft Forefront Unified Access Gateway (UAG) 2010 pour connexion Internet. Dans le scénario de déploiement selon lequel DirectAccess est installé sur un serveur Edge, deux cartes réseau doivent être disponibles : l'une étant connectée au réseau interne et l'autre, au réseau externe. Un serveur Edge correspond à n'importe quel serveur qui réside à la périphérie entre deux, voire plusieurs, réseaux ; en général, il s'agit d'un réseau privé et d'Internet.
- L'implémentation de DirectAccess dans Windows Server 2012 ne requiert pas que deux adresses IPv4 publiques, statiques consécutives soient attribuées à la carte réseau.
- Vous pouvez contourner le besoin d'une adresse publique supplémentaire en déployant Windows Server 2012 DirectAccess derrière un périphérique NAT, avec prise en charge pour une, voire plusieurs, interface(s). Dans cette configuration, seul le protocole IP-HTTPS (IP sur HTTPS) est déployé ; il permet l'établissement d'un tunnel IP sécurisé à l'aide d'une connexion HTTP sécurisée.
- Sur le serveur DirectAccess, vous pouvez installer le rôle d'accès à distance pour configurer les paramètres DirectAccess pour le serveur et les clients DirectAccess et surveiller l'état du serveur DirectAccess. L'Assistant Accès à distance fournit la possibilité de configurer des scénarios DirectAccess uniquement, VPN uniquement, ou les deux à la fois sur le même serveur exécutant Windows Server 2012. Cela n'était pas possible dans le déploiement Windows Server 2008 R2 de DirectAccess.
- Pour la prise en charge de l'équilibrage de charge, Windows Server 2012 peut utiliser l'équilibrage de la charge réseau (jusqu'à 8 nœuds) pour obtenir une haute disponibilité et l'évolutivité à la fois pour DirectAccess et RAS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Conditions requises pour le client DirectAccess

Pour déployer DirectAccess, vous devez également vous assurer que l'ordinateur client répond à certaines exigences :

- L'ordinateur client doit être joint à un domaine Active Directory.
- Le nouveau scénario 2012 de DirectAccess permet de fournir hors connexion l'appartenance au domaine aux ordinateurs client Windows 8 sans que ceux-ci se trouvent sur le site.
- L'ordinateur client peut être chargé avec Windows 8 Enterprise, Windows 7 Enterprise, Windows 7 Ultimate, Windows Server 2012 ou Windows Server 2008 R2. Il est impossible de déployer DirectAccess sur des clients exécutant Windows Vista, Windows Server 2008 ou d'autres versions antérieures des systèmes d'exploitation Windows.

Éléments prérequis pour l'infrastructure

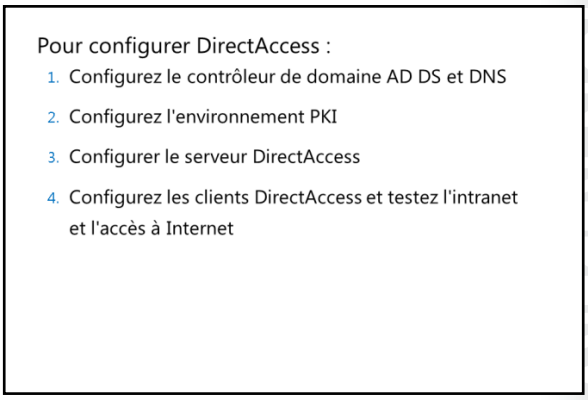
Vous trouverez ci-après les conditions requises d'infrastructure pour déployer DirectAccess :

- AD DS. Vous devez déployer au moins un domaine Active Directory. Les groupes de travail ne sont pas pris en charge.
- Stratégie de groupe. La stratégie de groupe est nécessaire à l'administration centralisée et au déploiement des paramètres du client DirectAccess. L'Assistant Installation DirectAccess crée un ensemble d'objets de stratégie de groupe et les paramètres des clients DirectAccess, des serveurs DirectAccess ainsi que des serveurs de gestion.
- DNS et contrôleur de domaine. Vous devez avoir au moins un contrôleur de domaine et un serveur DNS exécutant Windows Server 2012, Windows Server 2008 SP2 ou Windows Server 2008 R2.
- PKI. Si vous disposez uniquement d'ordinateurs client Windows 8, vous n'avez pas besoin de PKI. Les ordinateurs client Windows 7 requièrent une installation plus complexe et donc une PKI.
- Stratégies IPSec. DirectAccess utilise les stratégies IPsec configurées et administrées dans le cadre du pare-feu Windows avec fonctions avancées de sécurité.
- Trafic de requêtes d'écho ICMPv6. Vous devez créer des règles de trafic entrant et de trafic sortant distinctes qui autorisent les messages de requêtes d'écho ICMPv6. La règle de trafic entrant est requise pour permettre les messages de requêtes d'écho ICMPv6, et doit être étendue à tous les profils. La règle de trafic sortant pour autoriser les messages de requêtes d'écho ICMPv6 doit être étendue à tous les profils, et est requise uniquement si le bloc sortant est activé. Les clients DirectAccess qui utilisent Teredo pour la connectivité IPv6 à l'intranet utilisent le message ICMPv6 pour établir la communication.
- Technologies de transition IPv6. Les technologies de transition IPv6 doivent être disponibles sur le serveur DirectAccess. Pour chaque serveur DNS exécutant Windows Server 2008 ou Windows Server 2008 R2, vous devez supprimer le nom ISATAP de la liste rouge de requêtes globale.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de DirectAccess

Pour configurer DirectAccess, procédez comme suit :



1. Configurez les configurations requises d'AD DS et de DNS :
   - Créez un groupe de sécurité dans AD DS, et ajoutez tous les comptes d'ordinateur client qui accéderont à l'intranet par DirectAccess.
   - Configurez les serveurs DNS à la fois internes et externes avec les noms d'hôtes et les adresses IP appropriés.
2. Configurez l'environnement PKI :
   - Ajoutez et configurez le rôle serveur Autorité de certification, créez le modèle de certificat et le point de distribution de la liste de révocation de certificats, publiez la liste CRL et distribuez les certificats d'ordinateur. Cette opération n'est pas requise si l'installation est lancée à partir de l'Assistant Mise en route.
3. Configurez le serveur DirectAccess.
   - Installez Windows Server 2012 sur un ordinateur serveur doté d'une ou deux cartes réseau physiques (selon le scénario de conception DirectAccess).
   - Associez le serveur DirectAccess à un domaine Active Directory.
   - Installez le rôle d'accès à distance et configurez le serveur DirectAccess de manière à ce qu'il présente l'une des configurations suivantes :
     - Le serveur DirectAccess est sur le réseau de périmètre avec une carte réseau connectée au réseau de périmètre, et au moins une autre carte réseau connectée à l'intranet. Dans ce scénario de déploiement, le serveur DirectAccess est placé entre un pare-feu frontal et le pare-feu principal.
     - Le serveur DirectAccess est publié à l'aide de TMG, d'UAG, ou d'autres pare-feux tiers. Dans ce scénario de déploiement, DirectAccess est placé derrière un pare-feu frontal et il dispose d'une carte réseau connectée au réseau interne.
     - Le serveur DirectAccess est installé sur un serveur Edge (en général, un pare-feu frontal), avec une carte réseau connectée à Internet, et au moins une autre carte réseau connectée à l'intranet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Une autre possibilité consiste en ce que le serveur DirectAccess dispose d'une interface réseau uniquement, et non de deux. Pour cette approche, procédez comme suit :

- Vérifiez que les ports et les protocoles nécessaires pour DirectAccess et la requête d'écho ICMP sont autorisés dans les exceptions du pare-feu et ouverts sur les pare-feux Internet et de périmètre.
- Dans le cadre d'une implémentation simplifiée, le serveur DirectAccess peut utiliser une adresse IP publique unique en association avec les services proxy Kerberos pour authentifier le client au niveau des contrôleurs de domaine. Dans le cadre de l'authentification à deux facteurs et de l'intégration de protection d'accès réseau (NAP), vous devez configurer au moins deux adresses IPv4 publiques, statiques consécutives pouvant être résolues en externe via le serveur DNS. Assurez-vous que vous avez une adresse IPv4 disponible et que vous pouvez la publier dans votre serveur DNS externe.
- Si vous avez désactivé IPv6 sur les clients et les serveurs, vous devez le réactiver car il est indispensable pour DirectAccess.
- Installez un serveur Web sur le serveur DirectAccess pour permettre aux clients DirectAccess de déterminer s'ils se trouvent sur ou en dehors de l'intranet. Vous pouvez installer ce serveur Web sur un serveur interne distinct pour déterminer l'emplacement réseau.
- Selon le scénario de déploiement, vous devez indiquer une des cartes réseau de serveur comme l'interface Internet (dans un déploiement avec deux cartes réseau), ou publier le serveur DirectAccess déployé derrière un périphérique NAT pour l'accès à Internet.
- Sur le serveur DirectAccess, assurez-vous que l'interface Internet est configurée pour être une interface publique ou privée, selon la conception de votre réseau. Configurez les interfaces d'intranet comme interfaces de domaine. Si vous disposez de plus de deux interfaces, vérifiez que seuls deux types de classification sont sélectionnés au maximum.

4. Configurez les clients DirectAccess et testez l'accès à l'intranet et à Internet.
   - Vérifiez que la stratégie de groupe DirectAccess a été appliquée et que des certificats ont été distribués aux ordinateurs clients :
   - Testez si vous pouvez vous connecter au serveur DirectAccess depuis l'intranet.
   - Testez si vous pouvez vous connecter au serveur DirectAccess à partir d'Internet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique B : Configuration de DirectAccess

Scénario

Puisque A. Datum Corporation s'est développée, plusieurs employés sont maintenant fréquemment hors du bureau, travaillant depuis leur domicile ou en voyageant. A. Datum souhaite implémenter une solution d'accès à distance pour ses employés afin qu'ils puissent se connecter au réseau d'entreprise tout en étant en dehors du bureau. Bien que la solution VPN implémentée fournisse un haut niveau de sécurité, la gestion d'entreprise est préoccupée par la complexité de l'environnement pour les utilisateurs finaux. En outre, les responsables informatiques sont également préoccupés par le fait de ne pas être en mesure de gérer efficacement les clients distants. Pour aborder ces problèmes, A. Datum a décidé d'implémenter DirectAccess en fonction des ordinateurs clients exécutant Windows 8.

En tant qu'administrateur réseau senior, vous devez déployer et valider le déploiement DirectAccess. Vous configurerez l'environnement DirectAccess et validerez que les ordinateurs clients peuvent se connecter au réseau interne en fonctionnant à distance.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- configurer l'infrastructure de serveur pour déployer DirectAccess ;
- configurer les clients DirectAccess ;
- valider l'implémentation DirectAccess.

Configuration de l'atelier pratique

Durée approximative : 90 minutes

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-SVR1 22411B-LON-RTR 22411B-LON-CL1
Nom d'utilisateur	**Administrateur**
Mot de passe	**Pa$$w0rd**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.

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. Effectuez les étapes 2 à 4 pour **22411B-LON-SVR1** et **22411B-LON-RTR**.
6. Ne démarrez pas **22411B-LON-CL1** tant que vous n'avez pas été invité à le faire.

Exercice 1 : Configuration de l'infrastructure DirectAccess

Scénario

Vous avez décidé d'implémenter DirectAccess en tant que solution pour les ordinateurs clients distants incapables de se connecter via VPN. En outre, vous souhaitez aborder des problèmes de gestion, tels que l'application d'objets de stratégie de groupe pour les ordinateurs clients distants. À cet effet, vous configurerez les composants nécessaires de DirectAccess, et configurez le serveur DirectAccess.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les services de domaine Active Directory (AD DS) et du système DNS (Domain Name System)
2. Configurer les certificats
3. Configurer les ressources internes
4. Configurer le serveur DirectAccess

▶ Tâche 1 : Configurer les services de domaine Active Directory (AD DS) et du système DNS (Domain Name System)

1. Créez un groupe de sécurité pour les ordinateurs clients DirectAccess en procédant comme suit :
   a. Basculez vers **LON-DC1**.
   b. Ouvrez la console **Utilisateurs et ordinateurs Active Directory** et créez une unité d'organisation nommée **DA_Clients OU**.
   c. Au sein de cette unité d'organisation, créez un **groupe de sécurité global** nommé **DA_Clients**.
   d. Modifiez les membres du groupe **DA_Clients** pour intégrer **LON-CL1**.
   e. Fermez la fenêtre Utilisateurs et ordinateurs Active Directory.
2. Configurez les règles de pare-feu pour le trafic ICMPv6 en exécutant les étapes suivantes :
   a. Ouvrez la console Gestion de stratégie de groupe, puis ouvrez **Default Domain Policy**.
   b. Dans l'Éditeur de gestion des stratégies de groupe, naviguez jusqu'à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Pare-feu Windows avec les fonctions de sécurité avancées\Pare-feu Windows avec fonctions avancées de sécurité**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

c. Créez une règle de trafic entrant avec les paramètres suivants :

- Type de règle : **Personnalisée**
- Type de protocole : **ICMPv6**
- Types d'ICMP spécifiques : **Requête d'écho**
- Nom : **Demandes Echo ICMPv6 entrantes**

d. Créez une règle de trafic sortant avec les paramètres suivants :

- Type de règle : **Personnalisée**
- Type de protocole : **ICMPv6**
- Types d'ICMP spécifiques : **Requête d'écho**
- Action : **Autoriser la connexion**
- Nom : **Demandes Echo ICMPv6 sortantes**

e. Fermez l'Éditeur et la Console de gestion des stratégies de groupe**.**

3. Créez les enregistrements DNS requis en procédant comme suit :

a. Ouvrez la console du **Gestionnaire DNS**, puis créez de nouveaux enregistrements hôte avec les paramètres suivants :

- Nom : **nls**
  - Adresse IP : **172.16.0.21**
- Nom : **crl**
  - Adresse IP : **172.16.0.1**

b. Fermez la console du Gestionnaire DNS.

4. Supprimez le nom ISATAP de la liste rouge de requêtes globale DNS en procédant comme suit :

a. Ouvrez la fenêtre d'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
dnscmd /config /globalqueryblocklist wpad
```

b. Vérifiez que le message **La commande a été correctement exécutée** s'affiche.

c. Fermez la fenêtre d'invite de commandes.

5. Basculez vers LON-RTR et configurez le suffixe DNS en procédant comme suit :

a. Dans la boîte de dialogue **Propriétés** de **Connexion au réseau local**, dans la boîte de dialogue **Protocole Internet Version 4 (TCP/IPv4)**, ajoutez le suffixe DNS **Adatum.com**.

b. Fermez la boîte de dialogue **Propriétés de Connexion au réseau local**.

6. Configurez les propriétés de la connexion au réseau local 2 comme suit :

a. Modifiez la configuration **Connexion au réseau local 2\ Protocole Internet version 4 (TCP/IPv4)** à l'aide des paramètres de configuration suivants :

- Adresse IP : **131.107.0.2**
- Masque de sous-réseau : **255.255.0.0**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer les certificats

1. Configurez les paramètres de distribution de la liste de révocation de certificats en exécutant les étapes suivantes :

   a. Basculez vers LON-DC1 et ouvrez la console Autorité de certification.

   b. Configurez l'autorité de certification **Adatum-LON-DC1-CA** avec les paramètres d'extension suivants :

      - Ajouter un emplacement : **http://crl.adatum.com/crld/**
      - Variable : <**NomAutoritéCertification>**, **<SuffixeNomListeRévocationCertificats>**, <**ListeRévocationCertificatsDeltaAutorisée>**
      - Emplacement : **.crl**
      - Sélectionnez les éléments suivants :
        - **Inclure dans les listes de révocation de certificats. afin de pouvoir rechercher les listes de révocation des certificats delta**
        - **Inclure dans l'extension CDP des certificats émis**
      - Ne redémarrez pas les services de certificats.
      - Ajouter un emplacement : **\\LON-RTR\crldist$**
      - Variable : <**NomAutoritéCertification>**, **<SuffixeNomListeRévocationCertificats>**, **<ListeRévocationCertificatsDeltaAutorisée>**
      - Emplacement : **.crl**
      - Sélectionnez les éléments suivants :
        - **Inclure dans les listes de révocation de certificats. afin de pouvoir rechercher les listes de révocation des certificats delta**
        - **Inclure dans l'extension CDP des certificats émis**

   c. Redémarrez les services de certificats.

   d. Fermez la console Autorité de certification.

2. Pour dupliquer le modèle de certificat Web et configurer une autorisation appropriée, procédez comme suit :

   a. Dans la Console des modèles de certificat, dans le volet du contenu, dupliquez le modèle **Serveur Web** en utilisant les options suivantes :

      - Nom complet du modèle **: Certificat de serveur Web Adatum**
      - Traitement de la demande : **Autoriser l'exportation de la clé privée**
      - Autorisations Utilisateurs authentifiés : sous **Autoriser**, cliquez sur **Inscrire**

   b. Fermez la Console des modèles de certificat.

   c. Dans la console Autorité de certification, choisissez de délivrer un nouveau modèle de certificat et sélectionnez le modèle **Certificat de serveur Web Adatum**.

   d. Redémarrez l'Autorité de certification.

   e. Fermez la console Autorité de certification.

3. Configurez l'inscription automatique de certificat de l'ordinateur en exécutant les étapes suivantes :
   a. Sur LON-DC1, ouvrez la **Console de gestion des stratégies de groupe**.
   b. Dans la Console de gestion des stratégies de groupe, naviguez jusqu'à **Forêt : Adatum.com\Domaines\Adatum.com**.
   c. Modifiez la **stratégie de domaine par défaut**.
   d. Dans l'Éditeur de gestion des stratégies de groupe, naviguez jusqu'à **Configuration ordinateur \Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique**.
   e. Sous **Paramètres de demande automatique de certificat**, configurez **Demande automatique de certificat** pour délivrer le certificat d'**ordinateur**.
   f. Fermez l'Éditeur et la Console de gestion des stratégies de groupe.

▶ Tâche 3 : Configurer les ressources internes

1. Demandez un certificat pour LON-SVR1 en procédant comme suit :
   a. Sur LON-SVR1, ouvrez une invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

   b. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
mmc
```

2. Ajoutez le composant logiciel enfichable **Certificats** pour l'**ordinateur local**.
3. Dans l'arborescence de la console du composant logiciel enfichable Certificats, naviguez jusqu'à Certificats (ordinateur local) **\Personnel\Certificats**, et demandez un nouveau certificat.
4. Sous **Demander des certificats**, sélectionnez **Certificat de serveur Web Adatum** avec le paramètre suivant :
   - Nom de sujet : Sous **Nom commun**, saisissez **nls.adatum.com**
5. Dans le volet d'informations du composant logiciel enfichable de certificats, vérifiez qu'un nouveau certificat avec le nom **nls.adatum.com** a été inscrit avec **Rôles prévus** de **Authentification du serveur**.
6. Fermez la fenêtre de la console. Lorsque vous êtes invité à enregistrer les paramètres, cliquez sur **Non**.
7. Pour changer les liaisons HTTPS, procédez comme suit :
   a. Ouvrez le Gestionnaire des services Internet (IIS).
   b. Dans la console Gestionnaire des services Internet IIS, naviguez jusqu'à et cliquez sur **Site Web par défaut**.
   c. Configurez les liaisons de site en sélectionnant **nls.adatum.com** pour **Certificat SSL**.
   d. Fermez la console Gestionnaire des services Internet (IIS).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer le serveur DirectAccess

1. Demandez les certificats nécessaires pour LON-RTR en procédant comme suit :
   a. Basculez vers LON-RTR.
   b. Ouvrez une fenêtre d'invite de commandes et actualisez la stratégie de groupe en tapant la commande suivante :

```
gpupdate /force
```

   c. Ouvrez la console MMC en tapant **mmc** à l'invite de commandes.
   d. Ajoutez le composant logiciel enfichable **Certificats** pour l'**ordinateur local**.
   e. Dans le composant logiciel enfichable **Certificats**, dans la console MMC, demandez un nouveau certificat avec les paramètres suivants :
      - Modèle de certificat : **Certificat de serveur Web Adatum**
      - Nom commun : **131.107.0.2**
      - Nom convivial : **Certificat IP-HTTPS**
   f. Fermez la console MMC.
2. Créez le point de distribution de liste de révocation de certificats sur LON-RTR en procédant comme suit :
   a. Basculez vers Gestionnaire de serveur.
   b. Dans le Gestionnaire des services Internet (IIS), créez un répertoire virtuel appelé **CRLD** et attribuez **c:\crldist** comme répertoire d'accueil.
   c. Activez l'exploration de répertoire et la fonctionnalité Autoriser le double-échappement.
3. Partagez et sécurisez le point de distribution de la liste de révocation de certificats en exécutant l'étape suivante :

Remarque Vous effectuez cette étape pour attribuer des autorisations au point de distribution de liste de révocation de certificats.

   - Dans le volet d'informations de l'Explorateur de fichiers, cliquez avec le bouton droit sur le dossier **CRLDist**, cliquez sur **Propriétés**, et accordez les autorisations de **partage Contrôle total** et **NTFS**.

4. Publiez la liste de révocation de certificats vers LON-RTR en suivant la procédure ci-dessous :

Remarque : cette étape rend la liste de révocation de certificats disponible sur le serveur Edge pour les clients DirectAccess basés sur Internet.

   a. Basculez vers LON-DC1.
   b. Démarrez la console **Autorité de certification**.
   c. Dans l'arborescence de la console, ouvrez **Adatum-LON-DC1-CA**, cliquez avec le bouton droit sur **Certificats révoqués**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Publier**.

5. Terminez la procédure avec l'Assistant de configuration DirectAccess sur LON-RTR en procédant comme suit :
   a. Sur LON-RTR, ouvrez le **Gestionnaire de serveur**.
   b. Dans le Gestionnaire de serveur, dans **Outils**, sélectionnez **Routage et accès distant**.
   c. Dans Routage et accès distant, désactivez la configuration existante et fermez la console.
   d. Dans la console Gestionnaire de serveur, lancez la console **Gestion à distance**, cliquez sur **Configuration**, et démarrez l'**Assistant Activation DirectAccess**.

 **Remarque :** Si vous obtenez une erreur à ce stade, redémarrez LON-RTR, connectez-vous en tant qu'ADATUM\administrateur, puis recommencez la procédure à partir de l'étape c).

   e. Suivez les instructions de l'Assistant avec les paramètres suivants :
      - Topologie du réseau : **Edge** est sélectionné
      - **131.107.0.2** est utilisé par les clients pour se connecter au serveur d'accès à distance.
   f. Dans la console Gestion de l'accès à distance, sous Étape 1, cliquez sur **Modifier**.
   g. Ajoutez le groupe **DA_Clients**.
   h. Désactivez la case à cocher Activer DirectAccess pour les ordinateurs portables uniquement.
   i. Supprimez le groupe Ordinateurs du domaine.
   j. Dans le volet d'informations de la console Gestion de l'accès à distance, sous **Étape 2**, cliquez sur **Modifier**.
   k. Sur la page **Topologie du réseau**, vérifiez que **Edge** est sélectionné, et saisissez **131.107.0.2**.
   l. Sur la page **Cartes réseau**, vérifiez que **CN=131.107.0.2** est utilisé comme certificat d'authentification de la connexion IP-HTTPS.
   m. Sur la page **Authentification**, cliquez sur **Utiliser les certificats d'ordinateur**, cliquez sur **Parcourir**, puis sur **Adatum Lon-Dc1 CA**.
   n. Sur la page **Configuration VPN**, cliquez sur **Terminer**.
   o. Dans le volet d'informations de la console Gestion de l'accès à distance sous **Étape 3**, cliquez sur **Modifier**.
   p. Sur la page **Serveur Emplacement réseau**, cliquez sur **Le serveur Emplacement réseau est déployé sur un serveur Web distant (recommandé)**, et dans l'URL du serveur NLS, saisissez **https://nls.adatum.com**, et cliquez sur **Valider**.
   q. Assurez-vous que l'URL est validée.
   r. Sur la page **DNS**, examinez les valeurs, puis cliquez sur **Suivant**.
   s. Dans la **Liste de recherche de suffixes DNS**, cliquez sur **Suivant**.
   t. Sur la page **Gestion**, cliquez sur **Terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

u. Dans le volet d'informations de la console Gestion de l'accès à distance, passez en revue le paramètre pour l'**Étape 4**.

v. Dans **Vérification de l'accès à distance**, cliquez sur **Appliquer**.

w. Sous **Application des paramètres de l'Assistant Configuration de l'accès à distance**, cliquez sur **Fermer**.

6. Mettez à jour les paramètres de la stratégie de groupe sur LON-RTR en exécutant l'étape suivante :

   - Ouvrez l'invite de commandes et saisissez les commandes ci-dessous, en appuyant sur Entrée après chaque ligne :

```
gpupdate /force
Ipconfig
```

Remarque : vérifiez que **LON-RTR** a une adresse IPv6 pour **Interface IPHTTPS de la carte Tunnel** commençant par **2002**.

Résultats : À la fin de cet exercice, vous devez avoir configuré l'infrastructure DirectAccess.

Exercice 2 : Configuration des clients DirectAccess

Scénario

Après la configuration du serveur DirectAccess et de l'infrastructure requise, vous devez configurer les clients DirectAccess. Vous décidez d'utiliser la stratégie de groupe pour appliquer les paramètres DirectAccess aux clients et distribuer les certificats.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les paramètres de stratégie de groupe DirectAccess
2. Vérifier la distribution de certificats d'ordinateurs clients
3. Vérifier la connectivité interne aux ressources

▶ Tâche 1 : Configurer les paramètres de stratégie de groupe DirectAccess

1. Démarrez LON-CL1, et ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**. Ouvrez une fenêtre d'invite de commandes, puis saisissez les commandes ci-dessous, en appuyant sur Entrée à la fin de chaque ligne :

```
gpupdate /force
gpresult /R
```

2. Vérifiez que **l'objet de la stratégie de groupe Paramètres client DirectAccess** s'affiche correctement dans la liste des objets de stratégie de groupe pour les paramètres de l'ordinateur.

▶ Tâche 2 : Vérifier la distribution de certificats d'ordinateurs clients

1. Sur LON-CL1, ouvrez la console MMC **Certificats**.
2. Vérifiez qu'un certificat avec le nom **LON-CL1.adatum.com** s'affiche avec **Rôles prévus** de **Authentification client** et **Authentification serveur**.
3. Fermez la fenêtre de la console sans enregistrer les modifications.

▶ Tâche 3 : Vérifier la connectivité interne aux ressources

1. Sur LON-CL1, ouvrez Windows Internet Explorer® à partir du Bureau, et dans la barre d'adresses, saisissez **http://lon-svr1.adatum.com/**. La page Web par défaut IIS8 pour LON-SVR1 s'affiche.
2. Dans Internet Explorer, naviguez jusqu'à **https://nls.adatum.com/**. La page Web par défaut IIS8 pour LON-SVR1 s'affiche.
3. Ouvrez une fenêtre de l'Explorateur de fichiers, et dans la barre d'adresses, saisissez **\\Lon-SVR1\Files**, puis appuyez sur Entrée. Une fenêtre avec les contenus du dossier partagé **Fichiers** s'affiche.
4. Fermez toutes les fenêtres.

Résultats : À la fin de cet exercice, vous devez avoir configuré les clients DirectAccess.

Exercice 3 : Vérification de la configuration DirectAccess

Scénario

Lorsque la configuration du client est terminée, il est important de vérifier que DirectAccess fonctionne. Pour cela, déplacez le client DirectAccess vers Internet et essayez d'accéder aux ressources internes.

Les tâches principales de cet exercice sont les suivantes :

1. Déplacer l'ordinateur client vers le réseau virtuel Internet
2. Vérifier la connectivité vers le serveur DirectAccess
3. Vérifier la connectivité vers les ressources du réseau interne
4. Pour préparer le module suivant

▶ Tâche 1 : Déplacer l'ordinateur client vers le réseau virtuel Internet

1. Basculez vers LON-CL1.
2. Modifiez la configuration de la carte réseau comme suit :
   - Adresse IP : **131.107.0.10**
   - Masque de sous-réseau : **255.255.0.0**
   - Passerelle par défaut : **131.107.0.2**
3. Désactivez puis réactivez la carte réseau **Connexion au réseau local**.
4. Fermez la fenêtre Connexions réseau.
5. Sur votre hôte, dans Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22411B-LON-CL1**, puis cliquez sur **Paramètres**. Modifiez la carte réseau héritée pour qu'elle soit sur le réseau **Réseau privé 2**, puis cliquez sur **OK**.

▶ Tâche 2 : Vérifier la connectivité vers le serveur DirectAccess

1. Sur LON-CL1, ouvrez une invite de commandes et saisissez la commande suivante :

```
ipconfig
```

2. Notez que l'adresse IP renvoyée commence par **2002**. Il s'agit d'une adresse IP-HTTPS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Netsh name show effectivepolicy
```

4. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
powershell
```

5. Dans l'interface de ligne de commande Windows PowerShell®, saisissez la commande suivante, puis appuyez sur Entrée :

```
Get-DAClientExperienceConfiguration
```

▶ Tâche 3 : Vérifier la connectivité vers les ressources du réseau interne

1. Basculez vers **Internet Explorer** et naviguez jusqu'à **http://lon-svr1.adatum.com/**. La page Web par défaut IIS8 pour LON-SVR1 apparaît.
2. Ouvrez l'**Explorateur de fichiers**, et dans la barre d'adresses, saisissez **\\LON-SVR1\Files**, puis appuyez sur Entrée.
3. Une fenêtre de dossier avec le contenu du dossier partagé Fichiers devrait s'afficher.
4. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
ping lon-dc1.adatum.com
```

5. Vérifiez que vous recevez les réponses de lon-dc1.adatum.com.
6. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

7. Fermez toutes les fenêtres.
8. Basculez vers **LON-RTR**.
9. Lancez la console **Gestion de l'accès à distance** et examinez les informations sur **Statut du client distant**.

Remarque : vous remarquerez que LON-CL1 est connecté via IP-HTTPS. Dans le volet d'informations de connexion en bas à droite de l'écran, observez l'utilisation de Kerberos pour l'ordinateur et l'utilisateur.

10. Fermez toutes les fenêtres.

▶ Pour préparer le module suivant

- Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels.

Résultats : À la fin de cet exercice, vous devez avoir vérifié la configuration DirectAccess.

Contrôle des acquis et éléments à retenir

Outils

Outil	Utilisation	Emplacement
Services.msc	Gestion des services Windows	Outils d'administration Lancé de puis le menu Exécuter
Gpedit.msc	Modification de la stratégie de groupe locale	Lancé de puis le menu Exécuter
Mmc.exe	Création et gestion de la MMC	Lancé de puis le menu Exécuter
Gpupdate.exe	Gestion de l'application de la stratégie de groupe	Exécuté à partir d'une ligne de commande

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 8

Installation, configuration et résolution des problèmes du rôle de serveur NPS

Table des matières :

Vue d'ensemble du module **8-1**

Leçon 1 : Installation et configuration d'un serveur NPS **8-2**

Leçon 2 : Configuration de clients et de serveurs RADIUS **8-7**

Leçon 3 : Méthodes d'authentification NPS **8-14**

Leçon 4 : Analyse et résolution des problèmes d'un serveur NPS **8-24**

Atelier pratique : Installation et configuration d'un serveur NPS **8-30**

Contrôle des acquis et éléments à retenir **8-34**

Vue d'ensemble du module

Le rôle de serveur NPS (Network Policy Server) dans Windows Server® 2012 fournit la prise en charge du protocole RADIUS (Remote Authentication Dial-In User Service), et peut être configuré comme une serveur RADIUS ou proxy. En outre, NPS fournit une fonctionnalité qui est essentielle pour l'implémentation de la protection d'accès réseau (NAP). Pour prendre en charge des clients distants et implémenter la protection d'accès réseau (NAP), il est important que vous sachiez installer, configurer et résoudre NPS.

Objectifs

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

- installer et configurer le système NPS ;
- configurer des clients et des serveurs RADIUS ;
- expliquer les méthodes d'authentification NPS ;
- analyser le service NPS et résoudre les problèmes éventuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Installation et configuration d'un serveur NPS

NPS est implémenté en tant que rôle serveur dans Windows Server 2012. Quand vous installez le rôle NPS, vous devez décider d'utiliser NPS en tant que serveur RADIUS, proxy RADIUS ou serveur de stratégie NAP. Après l'installation, vous pouvez configurer le rôle NPS à l'aide de divers outils. Vous devez comprendre comment installer et configurer le rôle NPS afin de prendre en charge votre infrastructure RADIUS.

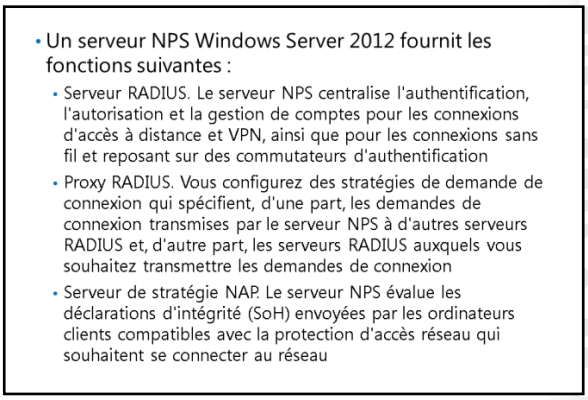
Objectifs de la leçon

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

- décrire le service de rôle NPS ;
- expliquer comment installer NPS ;
- décrire les outils utilisés pour configurer un NPS ;
- expliquer comment configurer les paramètres NPS généraux.

Qu'est-ce qu'un serveur NPS ?

Le serveur NPS vous permet de créer et de mettre en œuvre des stratégies d'accès réseau à l'échelle d'une entreprise pour assurer l'intégrité des clients, l'authentification des demandes de connexion et l'autorisation des demandes de connexion. Vous pouvez également utiliser le serveur NPS en tant que proxy RADIUS pour transmettre les demandes de connexion au serveur NPS ou à d'autres serveurs RADIUS que vous configurez dans des groupes de serveurs RADIUS distants.



Vous pouvez utiliser NPS pour configurer et gérer de manière centralisée l'authentification d'accès réseau, l'autorisation et les stratégies de contrôle d'intégrité des clients en combinant une ou plusieurs des fonctionnalités suivantes :

- serveur RADIUS ;
- proxy RADIUS ;
- serveur de stratégie NAP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Serveur RADIUS

NPS réalise, de manière centralisée, des opérations d'authentification, d'autorisation et de gestion des comptes pour les connexions d'accès à distance et VPN, ainsi que pour les connexions sans fil et reposant sur des commutateurs d'authentification. Lorsque vous utilisez le service NPS en tant que serveur RADIUS, vous devez configurer des serveurs d'accès réseau (tels que des points d'accès sans fil et des serveurs VPN) en tant que clients RADIUS dans le service NPS. Vous devez configurer également des stratégies réseau dont le serveur NPS se sert pour autoriser les demandes de connexion, et vous pouvez configurer la gestion de comptes RADIUS de telle sorte que le serveur NPS enregistre les informations de comptes dans des fichiers journaux sur le disque dur local ou dans une base de données Microsoft® SQL Server®.

Le serveur NPS est l'implémentation Microsoft d'un serveur RADIUS. Il permet l'utilisation d'un jeu hétérogène de périphériques sans fil, à commutateur, d'accès à distance ou VPN. Vous pouvez utiliser NPS avec le service de routage et d'accès à distance, qui est disponible dans Windows 2000® et des versions plus récentes de Windows Server.

Quand un serveur NPS est membre d'un domaine des services de domaine Active Directory® (AD DS), NPS utilise AD DS comme base de données de comptes d'utilisateurs et fournit l'authentification unique (SSO), ce qui signifie que les utilisateurs utilisent le même ensemble d'informations d'identification pour le contrôle d'accès réseau (authentification et autorisation de l'accès à un réseau) comme ils le font pour accéder à des ressources dans le domaine AD DS.

Les organisations en charge de l'accès réseau (les fournisseurs de services Internet, par exemple) sont confrontées à un défi croissant, à savoir les différents types d'accès réseau à partir d'un point d'administration unique, indépendamment des types de périphériques d'accès réseau utilisés. La norme RADIUS prend en charge ce besoin. Le service RADIUS est un protocole client-serveur qui permet aux périphériques d'accès réseau (utilisés en tant que clients RADIUS) de soumettre des demandes d'authentification et de comptes à un serveur RADIUS.

Un serveur RADIUS a accès aux informations du compte d'utilisateur et peut vérifier les informations d'authentification d'accès réseau. Si les informations d'identification de l'utilisateur sont authentifiées et que le serveur RADIUS autorise la tentative de connexion, le serveur RADIUS autorise l'accès de l'utilisateur en fonction de conditions spécifiées et enregistre la connexion d'accès réseau dans un journal de gestion. Le service RADIUS vous permet de collecter et de conserver dans un emplacement central, plutôt que sur chaque serveur d'accès, les données d'authentification, d'autorisation et de comptes des utilisateurs relatives à l'accès réseau.

Proxy RADIUS

Lorsque vous utilisez le serveur NPS en tant que proxy RADIUS, vous configurez des stratégies de demande de connexion qui spécifient, d'une part, les demandes de connexion transmises par le serveur NPS à d'autres serveurs RADIUS et, d'autre part, les serveurs RADIUS auxquels vous souhaitez transmettre les demandes de connexion. Vous pouvez également configurer le serveur NPS de manière à ce qu'il transmette les données de comptes à un ou plusieurs ordinateurs dans un groupe de serveurs RADIUS distants à des fins de journalisation.

Avec le serveur NPS, votre organisation peut également sous-traiter l'infrastructure d'accès à distance à un fournisseur de services tout en maintenant le contrôle de l'authentification, de l'autorisation et de la gestion de comptes des utilisateurs.

Vous pouvez créer des configurations NPS différentes pour les solutions suivantes :

- Accès sans fil
- accès à distance ou VPN d'entreprise ;
- Accès à distance ou sans fil sous-traité
- accès Internet ;
- accès authentifié à des ressources extranet pour les partenaires professionnels.

Serveur de stratégie NAP

Lorsque vous configurez le serveur NPS en tant que serveur de stratégie NAP, le serveur NPS évalue les déclarations d'intégrité envoyées par les ordinateurs clients compatibles avec la protection d'accès réseau (NAP) qui tentent de se connecter au réseau. Le serveur NPS agit également en tant que serveur RADIUS lorsqu'il est configuré avec la protection NAP, en assurant l'authentification et l'autorisation des demandes de connexion. Vous pouvez configurer des stratégies NAP et des paramètres dans le serveur NPS, y compris les programmes de validation d'intégrité système, la stratégie de contrôle d'intégrité et les groupes de serveurs de mise à jour qui permettent aux ordinateurs clients de mettre à jour leur configuration afin de se conformer à la stratégie réseau de votre organisation.

Windows® 8 et Windows Server® 2012 intègrent NAP, qui contribue à protéger l'accès aux réseaux privés en vérifiant que les ordinateurs clients sont configurés conformément aux stratégies de contrôle d'intégrité réseau de l'organisation avant qu'ils ne puissent se connecter aux ressources réseau. En outre, la protection d'accès réseau contrôle la conformité des ordinateurs clients à la stratégie de contrôle d'intégrité définie par l'administrateur lorsque l'ordinateur est connecté au réseau. La mise à jour automatique NAP permet de garantir que les ordinateurs non conformes soient mis à jour automatiquement, ce qui assure leur mise en conformité à la stratégie de contrôle d'intégrité afin qu'ils puissent se connecter au réseau.

Les administrateurs système définissent des stratégies de contrôle d'intégrité réseau, puis créent ces stratégies à l'aide de composants NAP fournis soit par le serveur NPS, en fonction de votre déploiement NAP, soit par des sociétés tierces.

Les stratégies de contrôle d'intégrité peuvent inclure les logiciels requis, les mises à jour de sécurité requises et les paramètres de configuration requis. La protection d'accès réseau met en œuvre des stratégies de contrôle d'intégrité en inspectant et en évaluant l'intégrité des ordinateurs clients, en limitant l'accès réseau lorsque des ordinateurs clients sont jugés défectueux et en mettant à jour les ordinateurs clients défectueux pour obtenir un accès réseau complet.

Démonstration : Installation du rôle Serveur NPS (Network Policy Server)

Cette démonstration montre comment :

- installer le rôle NPS ;
- inscrire NPS dans AD DS.

Procédure de démonstration

Installer le rôle NPS

1. Basculez vers **LON-DC1**.
2. Ouvrez le **Gestionnaire de serveur**, puis ajoutez le rôle de **Stratégie réseau et services d'accès**.
3. Fermez le Gestionnaire de serveur.

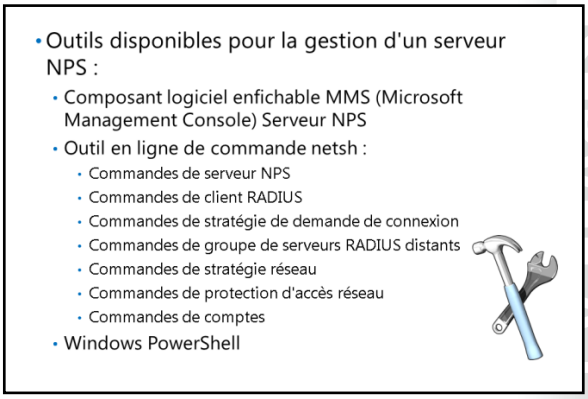
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Inscrire NPS dans AD DS

1. Ouvrez la console **Serveur NPS**.
2. Enregistrez le serveur dans AD DS.
3. Laissez la fenêtre Serveur NPS (Network Policy Server) ouverte.

Outils de configuration d'un serveur NPS

Après avoir installé le rôle Serveur NPS, vous pouvez ouvrir l'outil d'administration NPS dans le menu Outils d'administration, ou ajouter le composant logiciel enfichable pour créer un outil MMC (Microsoft Management Console) personnalisé. Vous pouvez également utiliser des commandes **netsh** pour gérer et configurer le rôle Serveur NPS.



Les outils suivants vous permettent de gérer le rôle serveur Services de stratégie et d'accès réseau :

- Composant logiciel enfichable MMC NP.
  Utilisez le composant logiciel enfichable MMC NPS pour configurer un serveur RADIUS, un proxy RADIUS ou une technologie NAP.
- Commandes netsh pour NPS. Les commandes netsh pour NPS fournissent un jeu de commandes qui est complètement équivalent à tous les paramètres de configuration disponibles à travers le composant logiciel enfichable MMC NPS. Vous pouvez exécuter des commandes **netsh** manuellement à l'invite netsh ou dans des scripts d'administrateur.

  Par exemple, après avoir installé et configuré le serveur NPS, vous pouvez enregistrer la configuration à l'aide de la commande netsh suivante : **netsh nps show config > path\file.txt**. Vous devez alors sauvegarder la configuration NPS avec cette commande chaque fois que vous faites une modification.
- Windows PowerShell®. Vous pouvez également utiliser les applets de commande Windows PowerShell pour configurer et gérer un serveur NPS.

  Par exemple, pour exporter la configuration NPS, vous pouvez utiliser l'applet de commande **Export-NpsConfiguration -Path <filename>**.

Démonstration : Configuration des paramètres NPS généraux

Cette démonstration montre comment :

- configurer un serveur RADIUS pour des connexions VPN ;
- enregistrer la configuration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

Configurer un serveur RADIUS pour des connexions VPN

1. Dans la console Serveur NPS, lancez la configuration VPN ou l'Assistant Accès à distance.
2. Ajoutez **LON-RTR** en tant que client RADIUS.
3. Utilisez un secret partagé **Pa$$word** pour l'authentification entre le client RADIUS et le serveur NPS.
4. Sélectionnez **Authentification chiffrée Microsoft version 2 (MS-CHAPv2)** pour l'authentification.

Enregistrer la configuration

1. Ouvrez Windows PowerShell.
2. Utilisez la commande **Export-NpsConfiguration -Path lon-dc1.xml** pour enregistrer la configuration.
3. Examinez cette configuration avec le Bloc-notes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration de clients et de serveurs RADIUS

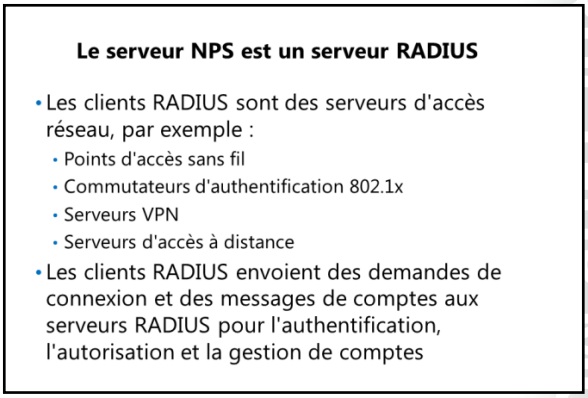
RADIUS est un protocole d'authentification standard que beaucoup de fournisseurs utilisent pour prendre en charge l'échange d'informations d'authentification entre les éléments d'une solution d'accès distant. Pour centraliser les besoins d'authentification distants de votre organisation, vous pouvez configurer NPS comme serveur RADIUS ou proxy RADIUS. Lorsque vous configurez des clients et des serveurs RADIUS, vous devez considérer plusieurs facteurs, notamment les serveurs RADIUS qui authentifieront les demandes de connexion des clients RADIUS et des ports que le trafic de RADIUS utilisera.

Objectifs de la leçon

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

- décrire un client RADIUS ;
- décrire un proxy RADIUS ;
- expliquer comment configurer un client RADIUS ;
- décrire comment utiliser une stratégie de demande de connexion ;
- décrire et configurer le traitement des demandes de connexion pour un environnement de proxy RADIUS ;
- expliquer comment créer une stratégie de demande de connexion.

Qu'est-ce qu'un client RADIUS ?



Un serveur d'accès réseau est un périphérique qui fournit un certain niveau d'accès à un réseau plus important. Un serveur d'accès réseau utilisant une infrastructure RADIUS est également un client RADIUS, à ce titre, il envoie des demandes de connexion et des messages de comptes à un serveur RADIUS à des fins d'authentification, d'autorisation et de gestion de comptes. Les ordinateurs clients, tels que les ordinateurs portables sans fil et d'autres ordinateurs qui exécutent des systèmes d'exploitation clients, ne sont pas des clients RADIUS. Les clients RADIUS sont des serveurs d'accès réseau (y compris des points d'accès sans fil, des commutateurs d'authentification 802.1X, des serveurs VPN et des serveurs d'accès à distance) parce qu'ils utilisent le protocole RADIUS pour communiquer avec les serveurs RADIUS tels que les serveurs NPS.

Pour déployer le serveur NPS en tant que serveur RADIUS, proxy RADIUS ou serveur de stratégie NAP, vous devez configurer des clients RADIUS dans le serveur NPS.

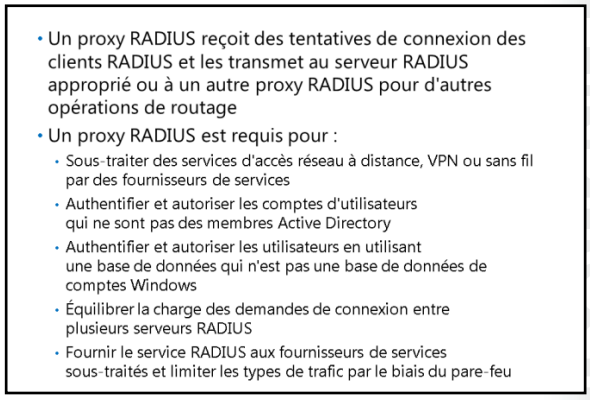
Exemples de clients RADIUS

Voici quelques exemples de serveurs d'accès réseau :

- Des serveurs d'accès réseau qui fournissent la connectivité d'accès à distance à un réseau d'organisation ou Internet, par exemple un ordinateur qui exécute le système d'exploitation Windows Server 2012 et le service de routage et d'accès à distance qui fournit des services d'accès à distance traditionnels ou VPN à l'intranet d'une organisation.
- Des points d'accès sans fil qui fournissent l'accès à la couche physique du réseau d'une organisation à l'aide de technologies de transmission et de réception sans fil.
- Des commutateurs qui fournissent l'accès à la couche physique du réseau d'une organisation à l'aide de technologies de réseau local traditionnelles comme Ethernet.
- Des proxys RADIUS NPS qui transmettent les demandes de connexion aux serveurs RADIUS membres d'un groupe de serveurs RADIUS distants que vous configurez sur le proxy RADIUS ou d'autres proxys RADIUS.

Qu'est-ce qu'un proxy RADIUS ?

Vous pouvez utiliser le serveur NPS en tant que proxy RADIUS pour router les messages RADIUS entre les clients RADIUS (serveurs d'accès réseau) et les serveurs RADIUS qui authentifient les utilisateurs, leur accordent les autorisations et exécutent les opérations de gestion de comptes associées à la tentative de connexion.



Lorsque vous utilisez le serveur NPS en tant que proxy RADIUS, le serveur NPS fait office de point central de commutation ou de routage par lequel transitent les messages d'accès et de comptes RADIUS. Le serveur NPS enregistre les informations sur les messages transmis dans un journal de gestion.

Vous pouvez utiliser le serveur NPS en tant que proxy RADIUS dans les cas suivants :

- Vous êtes un fournisseur de services qui sous-traite des services d'accès réseau à distance, VPN ou sans fil à plusieurs clients.

  Votre NAS envoie des demandes de connexion au proxy RADIUS NPS. En fonction de la partie de domaine du nom d'utilisateur dans la demande de connexion, le proxy RADIUS NPS transmet la demande de connexion à un serveur RADIUS géré par le client, et peut authentifier et autoriser la tentative de connexion.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Vous souhaitez authentifier et autoriser les comptes d'utilisateurs qui ne sont pas membres du domaine dont le serveur NPS est membre ou d'un domaine qui bénéficie d'une approbation bidirectionnelle avec le domaine du membre du serveur NPS.

  Il s'agit notamment des comptes dans des domaines non approuvés, des domaines approuvés à sens unique et d'autres forêts. Au lieu de configurer vos serveurs d'accès pour envoyer leurs demandes de connexion à un serveur RADIUS NPS, vous pouvez les configurer pour envoyer leurs demandes de connexion à un proxy RADIUS NPS. Le proxy RADIUS NPS utilise la partie du nom de domaine du nom de l'utilisateur et transmet la demande à un serveur NPS dans le domaine ou la forêt approprié. Les tentatives de connexion pour les comptes d'utilisateurs dans un domaine ou une forêt peuvent être authentifiées pour NAS dans un autre domaine ou une autre forêt.

- Vous souhaitez effectuer l'authentification et l'autorisation en utilisant une base de données qui n'est pas une base de données de comptes Windows.

  Dans ce cas, le serveur NPS transmet les demandes de connexion qui correspondent à un nom de domaine spécifié à un serveur RADIUS, lequel a accès à une autre base de données de comptes d'utilisateurs et de données d'autorisation. Les bases de données SQL sont un autre exemple de base de données utilisateur.

- Vous souhaitez traiter un grand nombre de demandes de connexion. Dans ce cas, au lieu de configurer vos clients RADIUS de manière à tenter d'équilibrer leurs demandes de connexion et de comptes sur plusieurs serveurs RADIUS, vous pouvez les configurer de telle sorte qu'ils envoient leurs demandes de connexion et de comptes à un proxy RADIUS NPS.

  Le proxy RADIUS NPS équilibre dynamiquement la charge des demandes de connexion et de comptes sur plusieurs serveurs RADIUS et augmente le traitement de grands nombres de clients RADIUS et d'authentifications par seconde.

- Vous souhaitez fournir l'authentification et l'autorisation RADIUS à des sous-traitants de services et réduire les tâches de configuration du pare-feu intranet.

  Un pare-feu intranet se trouve entre votre intranet et votre réseau de périmètre (le réseau entre votre intranet et Internet). En plaçant un serveur NPS sur votre réseau de périmètre, le pare-feu situé entre votre réseau de périmètre et l'intranet doit autoriser le flux de trafic entre le serveur NPS et plusieurs contrôleurs de domaine.

  Si vous remplacez le serveur NPS par un proxy NPS, le pare-feu doit autoriser uniquement le flux de trafic RADIUS entre le proxy NPS et un ou plusieurs serveurs NPS dans votre intranet.

Démonstration : Configuration d'un client RADIUS

Cette démonstration vous indique comment configurer un client RADIUS.

Procédure de démonstration

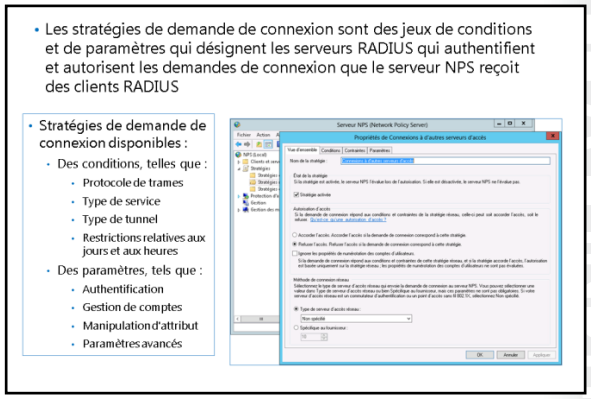
1. Ouvrez **Routage et accès distant**.
2. Désactivez la configuration existante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Reconfigurez LON-RTR en tant que serveur VPN à l'aide des paramètres suivants :
   - Interface publique : **Connexion au réseau local 2**
   - Le serveur VPN alloue des adresses du pool : **172.16.0.100** à **172.16.0.110**
   - Option de configuration du serveur : **Oui, configurer ce serveur pour travailler avec un serveur RADIUS**.
   - Serveur RADIUS principal : **LON-DC1**
   - Secret : **Pa$$w0rd**
4. Démarrez le service VPN.

Qu'est-ce qu'une stratégie de demande de connexion ?

Les stratégies de demande de connexion sont des jeux de conditions et de paramètres qui permettent aux administrateurs réseau de désigner les serveurs RADIUS qui authentifient et autorisent les demandes de connexion que le serveur NPS reçoit des clients RADIUS. Vous pouvez configurer des stratégies de demande de connexion pour désigner les serveurs RADIUS à utiliser pour la gestion de comptes RADIUS.



Remarque : Lorsque vous déployez la protection d'accès réseau à l'aide des méthodes de contrainte de mise en conformité VPN ou 802.1X avec l'authentification PEAP (Protected Extensible Authentication Protocol), vous devez configurer l'authentification PEAP dans la stratégie de demande de connexion même lorsque les demandes de connexion sont traitées localement.

Vous pouvez créer une série de stratégies de demande de connexion de sorte que quelques messages de demande RADIUS envoyés des clients RADIUS sont traités localement (NPS est un serveur RADIUS) et d'autres types de messages sont transférés à un autre serveur RADIUS (NPS est un proxy RADIUS).

Avec des stratégies de demande de connexion, vous pouvez utiliser NPS en tant que serveur RADIUS ou proxy RADIUS, selon un grand choix de facteurs, notamment :

- l'heure et le jour de la semaine ;
- le nom de domaine dans la demande de connexion ;
- le type de connexion que vous demandez ;
- l'adresse IP du client RADIUS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Conditions

Les conditions de la stratégie de demande de connexion se composent d'un ou plusieurs attributs RADIUS qui sont évalués par rapport aux attributs du message de demande d'accès RADIUS entrant. Si plusieurs conditions existent, NPS applique la stratégie uniquement si toutes les conditions dans le message de demande de connexion et dans la stratégie de demande de connexion correspondent.

Paramètres

Les paramètres de la stratégie de demande de connexion sont un jeu de propriétés qui sont appliquées à un message RADIUS entrant. Les paramètres sont constitués des groupes de propriétés suivants :

- Authentification
- Gestion
- Manipulation d'attribut
- Avancé

Stratégie de demande de connexion par défaut

Lorsque vous installez le serveur NPS, une stratégie de demande de connexion par défaut est créée avec les conditions suivantes :

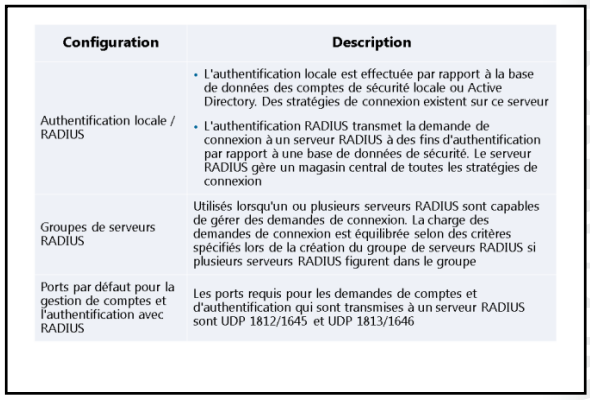
- L'authentification n'est pas configurée.
- La gestion de comptes n'est pas configurée de manière à transmettre les informations de comptes à un groupe de serveurs RADIUS distants.
- La manipulation d'attribut n'est pas configurée avec des règles qui modifient les attributs dans les demandes de connexion transmises.
- La transmission de la demande est activée, ce qui signifie que le serveur NPS local authentifie et autorise les demandes de connexion.
- Les attributs avancés ne sont pas configurés.

La stratégie de demande de connexion par défaut utilise le serveur NPS en tant que serveur RADIUS. Pour configurer un serveur NPS pour agir en tant que proxy RADIUS, vous devez également configurer un groupe de serveurs RADIUS distants. Vous pouvez créer un groupe de serveurs RADIUS distants au cours du processus la création d'une stratégie de demande de connexion à l'aide de l'Assistant Nouvelle stratégie de demande de connexion. Vous pouvez soit supprimer la stratégie de demande de connexion par défaut, soit vérifier que la stratégie de demande de connexion par défaut est la dernière stratégie traitée.

 **Remarque :** Si le serveur NPS et le service de routage et d'accès à distance sont installés sur le même ordinateur, et que le service de routage et d'accès à distance est configuré pour l'authentification et la gestion de comptes Windows, il est possible que les demandes d'authentification et de gestion du service de routage et d'accès à distance soient transmises à un serveur RADIUS. Cela peut se produire lorsque les demandes d'authentification et de comptes du service de routage et d'accès à distance correspondent à une stratégie de demande de connexion configurée pour les transmettre à un groupe de serveurs RADIUS distants.

Configuration du traitement des demandes de connexion

La stratégie de demande de connexion par défaut utilise le serveur NPS en tant que serveur RADIUS et traite toutes les demandes d'authentification localement.



Configuration	Description
Authentification locale / RADIUS	• L'authentification locale est effectuée par rapport à la base de données des comptes de sécurité locale ou Active Directory. Des stratégies de connexion existent sur ce serveur • L'authentification RADIUS transmet la demande de connexion à un serveur RADIUS à des fins d'authentification par rapport à une base de données de sécurité. Le serveur RADIUS gère un magasin central de toutes les stratégies de connexion
Groupes de serveurs RADIUS	Utilisés lorsqu'un ou plusieurs serveurs RADIUS sont capables de gérer des demandes de connexion. La charge des demandes de connexion est équilibrée selon des critères spécifiés lors de la création du groupe de serveurs RADIUS si plusieurs serveurs RADIUS figurent dans le groupe
Ports par défaut pour la gestion de comptes et l'authentification avec RADIUS	Les ports requis pour les demandes de comptes et d'authentification qui sont transmises à un serveur RADIUS sont UDP 1812/1645 et UDP 1813/1646

Éléments à prendre en considération pour la configuration du traitement des demandes de connexion

Lorsque vous configurez le traitement des demandes de connexion, prenez en compte les éléments suivants :

- Pour configurer un serveur NPS pour agir en tant que proxy RADIUS et transmettre les demandes de connexion à d'autres serveurs NPS ou RADIUS, vous devez configurer un groupe de serveurs RADIUS distants, puis ajouter une nouvelle stratégie de demande de connexion qui spécifie les conditions et les paramètres auxquels doivent satisfaire les demandes de connexion.
- Vous pouvez utiliser l'Assistant Nouvelle stratégie de demande de connexion pour créer un groupe de serveurs RADIUS distants lors de la demande de connexion.
- Si vous ne souhaitez pas que le serveur NPS agisse en tant que serveur RADIUS et traite les demandes de connexion localement, vous pouvez supprimer la stratégie de demande de connexion par défaut.
- Si vous souhaitez que le serveur NPS agisse en tant que serveur RADIUS (pour traiter les demandes de connexion localement) et en tant que proxy RADIUS (pour transmettre certaines demandes de connexion à un groupe de serveurs RADIUS distants), ajoutez une nouvelle stratégie, puis vérifiez que la stratégie de demande de connexion par défaut est la dernière stratégie traitée.

Ports pour le trafic RADIUS et la journalisation

Par défaut, le serveur NPS écoute le trafic RADIUS sur les ports 1812, 1813, 1645 et 1646 pour le protocole IPv6 (Internet version 6) et IPv4 sur toutes les cartes réseau installées.

Remarque : Si vous désactivez le protocole IPv4 ou IPv6 sur une carte réseau, le serveur NPS ne contrôle pas trafic RADIUS pour le protocole désinstallé.

Les valeurs 1812 pour l'authentification et 1813 pour la gestion de comptes sont des ports RADIUS standard définis dans les documents RFC 2865 et 2866. Toutefois, de nombreux serveurs d'accès utilisent par défaut le port 1645 pour les demandes d'authentification et le port 1646 pour les demandes de comptes. Lorsque vous déterminez les numéros de port à utiliser, assurez-vous de configurer le serveur NPS et le serveur d'accès pour utiliser les mêmes numéros de port. si vous n'utilisez pas les numéros de port RADIUS par défaut, vous devez configurer des exceptions sur le pare-feu pour l'ordinateur local de manière à activer le trafic RADIUS sur les nouveaux ports.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des informations de port UDP NPS

Vous pouvez utiliser la procédure suivante pour configurer les ports UDP utilisés par le serveur NPS pour le trafic d'authentification et de gestion de comptes RADIUS.

Remarque : Pour effectuer cette procédure, vous devez être membre du groupe Admins du domaine, Administrateurs de l'entreprise ou Administrateurs sur l'ordinateur local.

Pour configurer les informations des ports UDP NPS à l'aide de l'interface Windows :

1. Ouvrez la console **NPS**.
2. Cliquez avec le bouton droit sur **Serveur NPS**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Ports**, puis examinez les paramètres des ports. Si vos ports UDP d'authentification RADIUS et de gestion de comptes RADIUS ont des valeurs différentes des valeurs par défaut fournies (1812 et 1645 pour l'authentification, et 1813 et 1646 pour la gestion de comptes), tapez vos paramètres de port dans **Authentification et Gestion**.

Remarque : Pour utiliser plusieurs paramètres de port pour des demandes d'authentification ou de comptes, séparez les numéros des ports par des virgules.

Démonstration : Création d'une stratégie de demande de connexion

Cette démonstration montre comment créer une stratégie de demande de connexion VPN.

Procédure de démonstration

1. Sur LON-DC1, basculez vers la console Serveur NPS (Network Policy Server).
2. Affichez les **Stratégies de demande de connexion** existantes. L'Assistant a créé ces derniers automatiquement quand vous avez spécifié le rôle NPS de ce serveur.
3. Créez une **stratégie de demande de connexion** avec les paramètres suivants :
   - Type de serveur d'accès réseau : **Serveur d'accès à distance (VPN-Dial up)**
   - Condition : **Type de port de NAS** en tant que **Virtuel (VPN)**
   - Autres paramètres : valeurs par défaut
4. Attribuez la priorité la plus élevée à la nouvelle stratégie.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Méthodes d'authentification NPS

NPS authentifie et autorise la demande de connexion avant d'autoriser ou de refuser l'accès lorsque des utilisateurs tentent de se connecter à votre réseau par l'intermédiaire de serveurs d'accès réseau (aussi appelés clients RADIUS), tels que des points d'accès sans fil, des commutateurs d'authentification 802.1X, des serveurs d'accès à distance et des serveurs VPN.

L'authentification étant le processus de vérification de l'identité de l'utilisateur ou de l'ordinateur qui essaie de se connecter au réseau, le serveur NPS doit recevoir une preuve d'identité de l'utilisateur ou de l'ordinateur sous forme d'informations d'identification.

Certaines méthodes d'authentification implémentent l'utilisation d'informations d'identification basées sur un mot de passe. Le serveur d'accès réseau passe ensuite ces informations d'identification au serveur NPS qui vérifie les informations d'identification dans la base de données des comptes d'utilisateurs.

D'autres méthodes d'authentification implémentent l'utilisation d'informations d'identification basées sur des certificats pour l'utilisateur, l'ordinateur client, le serveur NPS ou une combinaison de ces éléments. Les méthodes d'authentification basées sur les certificats offrent une sécurité forte et sont préférables aux méthodes d'authentification par mot de passe.

Lorsque vous déployez le serveur NPS, vous pouvez spécifier le type de méthode d'authentification à utiliser pour l'accès à votre réseau.

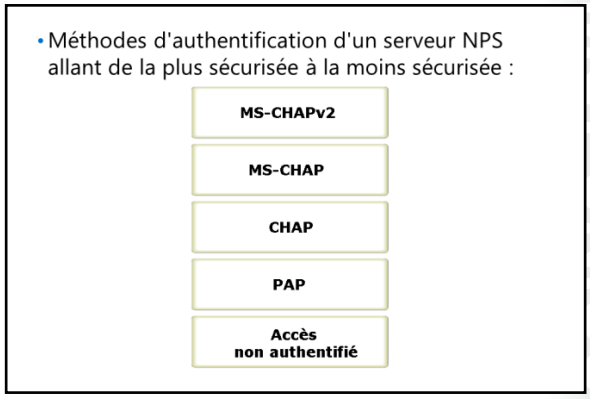
Objectifs de la leçon

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

- Décrivez les méthodes d'authentification basées sur un mot de passe pour un serveur NPS.
- Décrivez la manière dont les certificats sont utilisés pour fournir l'authentification pour des clients réseau.
- Décrivez les types de certificats requis pour différentes méthodes d'authentification.
- Décrivez comment déployer des certificats pour PEAP et EAP.

Méthodes d'authentification par mot de passe

Chaque méthode d'authentification présente des avantages et des inconvénients en termes de sécurité, de facilité d'utilisation et d'étendue de la prise en charge. Toutefois, nous déconseillons les méthodes d'authentification par mot de passe car elles ne garantissent pas une sécurité renforcée. Nous recommandons plutôt l'utilisation d'une méthode d'authentification basée sur les certificats pour toutes les méthodes d'accès réseau qui prennent en charge l'utilisation de certificats. Cela s'applique particulièrement aux connexions sans fil pour lesquelles nous recommandons l'utilisation de la méthode PEAP-MS-CHAP v2 ou PEAP-TLS.



La méthode d'authentification dont vous avez besoin est déterminée par la configuration du serveur d'accès réseau, de l'ordinateur client et de la stratégie réseau sur le serveur NPS. Consultez la documentation de votre serveur d'accès pour déterminer les méthodes d'authentification qui sont prises en charge.

Vous pouvez configurer le serveur NPS de telle sorte qu'il accepte plusieurs méthodes d'authentification. Vous pouvez également configurer vos serveurs d'accès réseau, aussi appelés clients RADIUS, de manière à ce qu'ils tentent de négocier une connexion avec les ordinateurs en utilisant différents protocoles, du plus sécurisé au moins sécurisé. Par exemple, le service de routage et d'accès à distance essaie de négocier une connexion à l'aide des protocoles suivants dans l'ordre indiqué :

1. Protocole EAP (Extensible Authentication Protocol)
2. MS-CHAP v2
3. MS-CHAP
4. Protocole CHAP (Challenge Handshake Authentication Protocol)
5. Protocole SPAP (Shiva Password Authentication Protocol)
6. Protocole PAP (Password Authentication Protocol)

Lorsque le protocole EAP est choisi comme méthode d'authentification, la négociation du type EAP se produit entre le client d'accès et le serveur NPS.

MS-CHAP Version 2

Le protocole MS-CHAP v2 offre une sécurité renforcée pour les connexions d'accès réseau par rapport à son prédécesseur (MS-CHAP). Le protocole MS-CHAP v2 est un processus d'authentification mutuelle par mot de passe chiffré à sens unique. Il fonctionne comme suit :

1. L'authentificateur (serveur d'accès réseau ou serveur NPS) envoie au client distant une demande d'accès qui se compose d'un identificateur de session et d'une chaîne de demande d'accès arbitraire.
2. Le client d'accès envoie une réponse qui contient :
    - le nom d'utilisateur ;
    - une chaîne de demande d'accès de l'homologue arbitraire ;
    - un chiffrement à sens unique de la chaîne de demande d'accès reçue, la chaîne de demande d'accès de l'homologue arbitraire, l'identificateur de session et le mot de passe de l'utilisateur.
3. L'authentificateur vérifie la réponse du client et émet une réponse contenant :
    - une indication de la réussite ou de l'échec de la tentative de connexion ;
    - une réponse authentifiée basée sur la chaîne de demande d'accès envoyée, la chaîne de demande d'accès de l'homologue, la réponse chiffrée du client et le mot de passe de l'utilisateur.
4. Le client d'accès vérifie la réponse d'authentification et utilise la connexion si celle-ci est valide. Si la réponse d'authentification est incorrecte, le client d'accès met fin à la connexion.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

MS-CHAP

Le protocole MS-CHAP, aussi appelé MS-CHAP version 1, est un protocole d'authentification par mot de passe irréversible et chiffré.

Le processus de demande d'accès fonctionne comme suit :

1. L'authentificateur (serveur d'accès réseau ou serveur NPS) envoie au client distant une demande d'accès qui se compose d'un identificateur de session et d'une chaîne de demande d'accès arbitraire.
2. Le client d'accès envoie une réponse qui contient le nom de l'utilisateur ainsi qu'un chiffrement irréversible de la chaîne de demande d'accès, l'identificateur de la session et le mot de passe.
3. L'authentificateur vérifie la réponse et, si elle est valide, authentifie les informations d'identification de l'utilisateur.

Remarque : Si vous utilisez le protocole MS-CHAP, MS-CHAP v2 ou EAP-TLS comme protocole d'authentification, vous pouvez utiliser le chiffrement MPPE (Microsoft Point-to-Point Encryption) pour chiffrer les données envoyées sur la connexion PPP (Point-to-Point Protocol) ou PPTP (Point-to-Point Tunneling Protocol).

Le protocole MS-CHAP v2 offre une sécurité renforcée pour les connexions d'accès réseau par rapport au protocole MS-CHAP. Il est recommandé d'utiliser le protocole MS-CHAP v2 à la place du protocole MS-CHAP.

CHAP

Le protocole CHAP (Challenge Handshake Authentication Protocol) est un protocole d'authentification par demande d'accès/réponse qui utilise le schéma de hachage MD5 (Message Digest 5) standard pour chiffrer la réponse.

Plusieurs fournisseurs de clients et serveurs d'accès réseau utilisent le protocole CHAP. Un serveur qui exécute le service de routage et d'accès à distance prend en charge le protocole CHAP, ce qui permet aux clients d'accès qui requièrent le protocole CHAP d'être authentifiés. Le protocole CHAP nécessitant l'utilisation d'un mot de passe chiffré réversible, songez à utiliser un autre protocole d'authentification, par exemple MS-CHAP v2.

Autres aspects à prendre en considération

Tenez compte des points suivants lors de l'implémentation de CHAP :

- Lorsque les mots de passe des utilisateurs expirent, le protocole CHAP ne permet pas aux utilisateurs de modifier leurs mots de passe au cours du processus d'authentification.
- Vérifiez que votre serveur d'accès réseau prend en charge le protocole CHAP avant de l'activer sur une stratégie réseau d'un serveur NPS. Pour plus d'informations, consultez la documentation de votre serveur d'accès réseau.
- Vous ne pouvez pas utiliser MPPE avec le protocole CHAP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

PAP

Ce protocole utilise des mots de passe en clair et constitue le protocole d'authentification le moins sûr. Il est négocié en général si le client d'accès et serveur d'accès réseau ne peuvent négocier aucune autre méthode d'authentification plus sécurisée. Lorsque vous activez le protocole PAP comme protocole d'authentification, les mots de passe des utilisateurs sont envoyés sous forme de texte en clair. Toute personne capturant les paquets du processus d'authentification peut aisément lire le mot de passe, puis l'utiliser pour accéder à votre intranet de façon non autorisée. L'utilisation du protocole PAP est fortement déconseillée, surtout pour les connexions VPN.

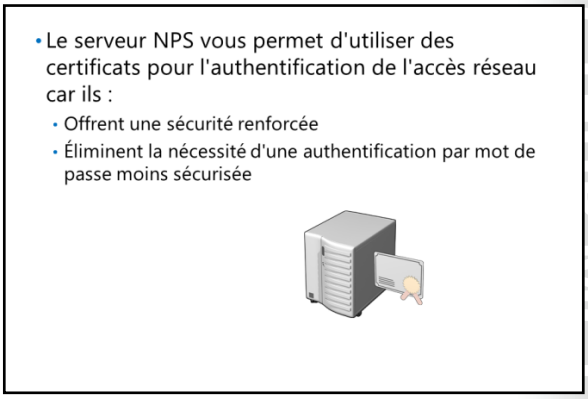
Accès non authentifié

Dans le cadre d'un accès non authentifié, les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) ne sont pas requises. Bien que l'accès non authentifié soit utile dans certains cas, nous déconseillons en général son déploiement dans le réseau de votre organisation.

Lorsque vous activez l'accès non authentifié, les utilisateurs peuvent accéder à votre réseau sans envoyer d'informations d'identification de l'utilisateur. En outre, les clients d'accès non authentifiés ne négocient pas l'utilisation d'un protocole d'authentification commun pendant le processus d'établissement de la connexion et n'envoient pas de nom d'utilisateur ni de mot de passe au serveur NPS.

Si vous autorisez l'accès non authentifié, les clients peuvent se connecter sans être authentifiés si les protocoles d'authentification configurés sur le client d'accès ne correspondent pas aux protocoles d'authentification configurés sur le serveur d'accès réseau. Dans ce cas, l'utilisation d'un protocole d'authentification commun n'est pas négociée, et le client d'accès n'envoie pas de nom d'utilisateur ni de mot de passe. Cette circonstance pose un sérieux problème de sécurité. Par conséquent, l'accès non authentifié ne doit pas être autorisé sur la plupart des réseaux.

Utilisation de certificats pour l'authentification



Les certificats sont des documents numériques émis par les autorités de certification (CA), par exemple les services de certificats Active Directory (AD CS) ou l'autorité de certification publique Verisign. Les applications des certificats sont nombreuses, notamment la signature de code et la sécurisation des communications par messagerie électronique. Toutefois, avec le serveur NPS, les certificats sont utilisés pour l'authentification d'accès réseau car ils fournissent une sécurité forte pour authentifier les utilisateurs et les ordinateurs, et vous évitent d'avoir recours à des méthodes d'authentification basées sur un mot de passe moins sécurisées.

Les serveurs NPS utilisent les protocoles EAP-TLS et PEAP pour effectuer l'authentification basée sur les certificats pour de nombreux types d'accès réseau, y compris les connexions VPN et sans fil.

Méthodes d'authentification

Deux méthodes d'authentification, lorsque vous les configurez avec des types d'authentification basée sur les certificats, utilisent des certificats : EAP et PEAP. Avec le protocole EAP, vous pouvez configurer le type d'authentification TLS (EAP-TLS) ; et avec le protocole PEAP, vous pouvez configurer les types d'authentification TLS (PEAP-TLS) et MS-CHAP v2 (PEAP-MS-CHAP v2). Ces méthodes d'authentification utilisent toujours des certificats pour l'authentification serveur. En fonction du type d'authentification que vous configurez avec la méthode d'authentification, vous pouvez également utiliser des certificats pour l'authentification d'utilisateurs et l'authentification d'ordinateurs clients.

 **Remarque :** L'utilisation de certificats dans le cadre de l'authentification de connexion VPN constitue la forme d'authentification la plus puissante dans Windows Server 2008 R2. Vous devez utiliser des certificats pour l'authentification d'IPsec sur les connexions VPN qui sont basés sur le protocole L2TP/IPsec (Layer Two Tunneling protocol over Internet protocol security). Les connexions PPTP ne requièrent pas de certificats, bien que vous puissiez configurer des connexions PPTP de manière à utiliser des certificats pour l'authentification d'ordinateur lorsque vous utilisez la méthode d'authentification EAP-TLS. Pour les clients sans fil (appareils informatiques avec des cartes réseau sans fil, tels qu'un ordinateur portable ou un assistant numérique personnel), utilisez la méthode d'authentification PEAP avec EAP-TLS et des cartes à puce ou des certificats.

 **Remarque :** Vous pouvez déployer des certificats en vue d'une utilisation avec le serveur NPS en installant et en configurant le rôle serveur AD CS.

Authentification mutuelle

Lorsque vous utilisez le protocole EAP avec un type EAP fort (par exemple la sécurité TLS avec des cartes à puce ou des certificats), le client et le serveur utilisent des certificats pour vérifier leurs identités les uns par rapports aux autres, cette procédure est également appelée authentification mutuelle. Les certificats doivent répondre à des exigences spécifiques pour que le serveur et le client puissent les utiliser pour l'authentification mutuelle.

Entre autres, le certificat doit être configuré avec un ou plusieurs rôles dans les extensions d'utilisation améliorée de la clé (EKU) qui correspondent à l'utilisation du certificat. Par exemple, vous devez configurer un certificat que vous utilisez pour l'authentification d'un client avec le rôle Authentification du client. De la même façon, vous devez configurer un certificat que vous utilisez pour l'authentification d'un serveur avec le rôle Authentification du serveur. Lorsque vous utilisez des certificats pour l'authentification, l'authentificateur examine le certificat client à la recherche de l'identificateur d'objet de rôle correct dans les extensions EKU. Par exemple, l'identificateur d'objet pour le rôle Authentification du client est 1.3.6.1.5.5.7.3.2. Lorsque vous utilisez un certificat pour l'authentification d'ordinateur client, cet identificateur d'objet doit être présent dans les extensions EKU du certificat ; sinon, l'authentification échoue.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Modèles de certificats

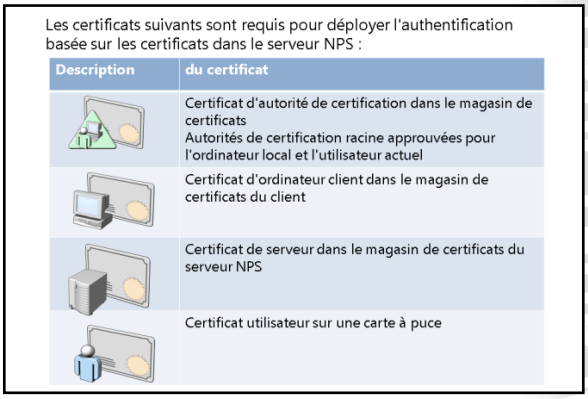
Modèles de certificats est un composant logiciel enfichable MMC qui permet la personnalisation de certificats émis par les services AD CS. Il est possible de personnaliser le mode d'émission des certificats et leur contenu, y compris leurs rôles. Dans Modèles de certificats, vous pouvez utiliser un modèle par défaut, tel que le modèle Ordinateur, pour définir le modèle utilisé par l'autorité de certification pour affecter des certificats aux ordinateurs. Vous pouvez également créer un modèle de certificat et lui affecter des rôles dans les extensions EKU. Par défaut, le modèle Ordinateur inclut les rôles Authentification du client et Authentification du serveur dans les extensions EKU.

Le modèle de certificat que vous créez peut inclure le rôle de votre choix. Par exemple, si vous utilisez des cartes à puce pour l'authentification, vous pouvez inclure le rôle Ouverture de session par carte à puce en plus du rôle Authentification du client. Lorsque vous utilisez le serveur NPS, vous pouvez le configurer pour vérifier les rôles du certificat avant d'accorder l'autorisation réseau. Le serveur NPS peut vérifier des rôles EKU et de stratégie d'émission supplémentaires (aussi appelés stratégies de certificat).

Remarque : Certains logiciels d'autorité de certification non-Microsoft peuvent contenir un rôle nommé Tout, celui-ci représentant tous les rôles possibles. Cela est indiqué par une extension EKU vide (ou nulle). Bien que Tout signifie *« tous les rôles possibles »*, vous ne pouvez pas remplacer le rôle Authentification du client, le rôle Authentification du serveur ou tout autre rôle en rapport à l'authentification d'accès réseau par le rôle Tout.

Certificats requis pour l'authentification

Le tableau suivant fournit le détail des certificats requis pour déployer correctement chacune des méthodes d'authentification basées sur les certificats répertoriées.



Certificat	Requis pour l'authentification EAP-TLS et PEAP-TLS ?	Requis pour l'authentification PEAP-MS-CHAP v2 ?	Détails
Certificat d'autorité de certification dans le magasin de certificats Autorités de certification racine approuvées pour l'ordinateur local et l'utilisateur actuel	Oui. Le certificat d'autorité de certification est inscrit automatiquement pour les ordinateurs membres du domaine. Pour les ordinateurs qui ne sont pas membres du domaine, vous devez importer manuellement le certificat dans le magasin de certificats.	Oui. Ce certificat est inscrit automatiquement pour les ordinateurs membres du domaine. Pour les ordinateurs qui ne sont pas membres du domaine, vous devez importer manuellement le certificat dans le magasin de certificats.	Pour l'authentification PEAP-MS-CHAP v2, ce certificat est requis pour l'authentification mutuelle entre le client et le serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR UNIQUEMENT

(suite)

Certificat	Requis pour l'authentification EAP-TLS et PEAP-TLS ?	Requis pour l'authentification PEAP-MS-CHAP v2 ?	Détails
Certificat d'ordinateur client dans le magasin de certificats du client	Oui. Les certificats d'ordinateur client sont requis à moins que les certificats utilisateur ne soient distribués sur des cartes à puce. Les certificats clients sont inscrits automatiquement pour les ordinateurs membres du domaine. Pour les ordinateurs qui ne sont pas membres du domaine, vous devez importer le certificat manuellement ou l'obtenir avec l'outil d'inscription via le Web.	Non. L'authentification utilisateur est effectuée avec des informations d'identification basées sur un mot de passe, et non avec des certificats.	Si vous déployez des certificats utilisateur sur des cartes à puce, les ordinateurs clients n'ont pas besoin de certificats clients.
Certificat de serveur dans le magasin de certificats du serveur NPS	Oui. Vous pouvez configurer les éléments suivants : AD CS de manière à inscrire automatiquement les certificats de serveur auprès des membres du groupe de serveurs RAS et IAS dans AD DS.	Oui. Outre l'utilisation des services AD CS pour les certificats de serveur, vous pouvez acheter des certificats de serveur auprès d'autres autorités de certification que les ordinateurs clients approuvent déjà.	Le serveur NPS envoie le certificat de serveur à l'ordinateur client. L'ordinateur client utilise le certificat pour authentifier le serveur NPS.
Certificat utilisateur sur une carte à puce	AD CS de manière à inscrire automatiquement les certificats de serveur auprès des membres du groupe de serveurs RAS et IAS dans AD DS.	Non. L'authentification utilisateur est effectuée avec des informations d'identification basées sur un mot de passe, et non avec des certificats.	Pour EAP-TLS et PEAP-TLS, si vous n'inscrivez pas automatiquement les certificats d'ordinateur client, des certificats utilisateur sur les cartes à puce sont requis.

L'authentification 802.1X de l'institut IEEE (Institute of Electrical and Electronics Engineers, Inc.) offre un accès authentifié aux réseaux sans fil 802.11 et aux réseaux Ethernet câblés. 802.1X prend en charge les types EAP sécurisés, tels que la sécurité TLS avec les cartes à puce ou les certificats. Vous pouvez configurer l'authentification 802.1X avec EAP-TLS de plusieurs manières.

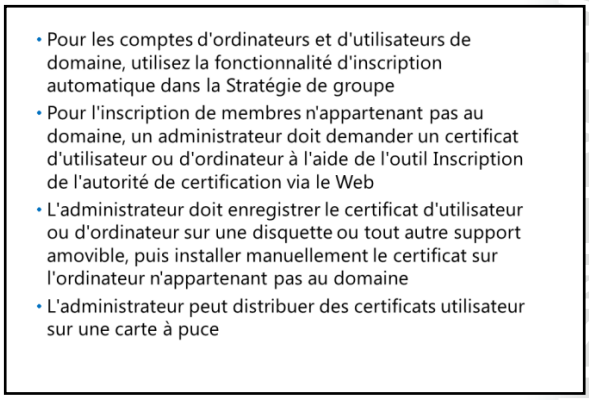
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si vous configurez l'option **Valider le certificat du serveur** sur le client, le client authentifie le serveur en utilisant son certificat. L'authentification de l'ordinateur client et de l'utilisateur est accomplie à l'aide de certificats du magasin de certificats client ou d'une carte à puce, garantissant une authentification mutuelle.

Avec les clients sans fil, vous pouvez utiliser la méthode d'authentification PEAP-MS-CHAP v2. Cette dernière est une méthode d'authentification utilisateur basée sur mot de passe qui utilise la sécurité TLS avec les certificats de serveur. Pendant l'authentification PEAP-MS-CHAP v2, le serveur NPS fournit un certificat pour valider son identité au client (si l'option Valider le certificat du serveur est configurée sur le client Windows 8). L'authentification de l'ordinateur client et de l'utilisateur est accomplie à l'aide de mots de passe, ce qui simplifie en partie le déploiement de certificats vers les ordinateurs clients sans fil.

Déploiement de certificats pour l'authentification PEAP et EAP

Tous les certificats que vous utilisez pour l'authentification d'accès réseau avec les méthodes EAP-TLS et PEAP doivent satisfaire aux exigences des certificats X.509 et fonctionner avec des connexions SSL/TLS (Secure Sockets Layer-Transport Layer Security). Lorsque ces conditions sont remplies, les certificats client et serveur imposent des exigences supplémentaires.



Exigences relatives aux certificats de serveur

Vous pouvez configurer des clients pour valider des certificats de serveur à l'aide de l'option Valider le certificat du serveur dans les propriétés du protocole d'authentification. Avec la méthode d'authentification PEAP-MS-CHAP v2, PEAP-TLS ou EAP-TLS, le client accepte la tentative d'authentification serveur lorsque le certificat satisfait aux conditions suivantes :

- Le nom du sujet contient une valeur. Si vous émettez un certificat à votre serveur NPS avec un sujet vide, le certificat n'est pas disponible pour authentifier votre serveur NPS. Pour configurer le modèle de certificat avec un nom de sujet :
  a. Ouvrez **Modèles de certificats**.
  b. Dans le volet d'informations, cliquez avec le bouton droit sur le modèle de certificat à modifier, puis cliquez sur **Propriétés**.
  c. Cliquez sur l'onglet **Nom du sujet** , puis sur **Construire à partir de ces informations Active Directory**.
  d. Dans **Format du nom du sujet**, sélectionnez une valeur autre que **None**.
- Le certificat d'ordinateur sur le serveur est lié à une autorité de certification racine de confiance et satisfait à tous les contrôles effectués par CryptoAPI ou spécifiés par les stratégies d'accès à distance ou réseau.
- Le certificat de serveur NPS ou VPN est configuré avec le rôle Authentification du serveur dans les extensions EKU (l'identificateur d'objet pour le rôle Authentification du serveur est 1.3.6.1.5.5.7.3.1).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Le certificat de serveur est configuré avec la valeur d'algorithme requise RSA. Pour configurer le paramètre de chiffrement requis :
  a. Ouvrez **Modèles de certificats**.
  b. Dans le volet d'informations, cliquez avec le bouton droit sur le modèle de certificat à modifier, puis cliquez sur **Propriétés**.
  c. Cliquez sur l'onglet **Chiffrement**. Dans **Nom de l'algorithme**, cliquez sur **RSA**. Vérifiez que **Taille de clé minimale** est définie sur **2048**.
- L'extension Autre nom de l'objet (SubjectAltName), si vous l'utilisez, doit contenir le nom de domaine pleinement qualifié (FQDN, Fully Qualified Domain Name) du serveur. Pour configurer le modèle de certificat avec le nom DNS (Domain Name System) du serveur d'inscription :
  a. Ouvrez **Modèles de certificats**.
  b. Dans le volet d'informations, cliquez avec le bouton droit sur le modèle de certificat à modifier, puis cliquez sur **Propriétés**.
  c. Cliquez sur l'onglet **Nom du sujet** , puis sur **Construire à partir de ces informations Active Directory**.
  d. Dans **Inclure cette information dans le nom de substitution du sujet**, sélectionnez **Nom DNS**.

Avec les méthodes PEAP-TLS et EAP-TLS, les serveurs affichent une liste de tous les certificats installés dans le composant logiciel enfichable Certificats, avec les exceptions suivantes :

- les certificats qui ne contiennent pas le rôle Authentification du serveur dans les extensions EKU ;
- les certificats qui ne contiennent pas de nom de sujet ;
- les certificats basés sur le Registre et d'ouverture de session par carte à puce.

Exigences relatives aux certificats clients

Avec la méthode d'authentification EAP-TLS ou PEAP-TLS, le serveur accepte la tentative d'authentification du client lorsque le certificat satisfait aux conditions suivantes :

- Une autorité de certification d'entreprise a émis le certificat client ou est mappée à un compte d'utilisateur ou d'ordinateur Active Directory.
- Le certificat utilisateur ou d'ordinateur sur le client est lié à une autorité de certification racine de confiance. Il inclut le rôle Authentification du client dans les extensions EKU (l'identificateur d'objet pour le rôle Authentification du client est 1.3.6.1.5.5.7.3.2) ; et satisfait aux contrôles effectués par CryptoAPI, spécifiés par les stratégies d'accès à distance ou réseau, et aux contrôles d'identificateur d'objet Certificat, spécifiés par les stratégies d'accès à distance IAS ou réseau NPS.
- Le client 802.1X n'utilise pas les certificats basés sur le Registre qui sont des certificats d'ouverture de session par carte à puce ou des certificats protégés par un mot de passe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Pour les certificats utilisateur, l'extension Autre nom de l'objet (SubjectAltName) dans le certificat contient le nom principal de l'utilisateur. Pour configurer le nom principal de l'utilisateur dans un modèle de certificat :

  a. Ouvrez **Modèles de certificats**.

  b. Dans le volet d'informations, cliquez avec le bouton droit sur le modèle de certificat à modifier, puis cliquez sur **Propriétés**.

  c. Cliquez sur l'onglet **Nom du sujet** , puis sur **Construire à partir de ces informations Active Directory**.

  d. Dans **Inclure cette information dans le nom de substitution du sujet**, sélectionnez **User principal name (UPN)**.

- Pour les certificats d'ordinateur, l'extension Autre nom de l'objet (SubjectAltName) dans le certificat doit contenir le nom de domaine complet du client, aussi appelé « nom DNS ». Pour configurer ce nom dans le modèle de certificat :

  a. Ouvrez **Modèles de certificats**.

  b. Dans le volet d'informations, cliquez avec le bouton droit sur le modèle de certificat à modifier, puis cliquez sur **Propriétés**.

  c. Cliquez sur l'onglet **Nom du sujet** , puis sur **Construire à partir de ces informations Active Directory**.

  d. Dans **Inclure cette information dans le nom de substitution du sujet**, sélectionnez **Nom DNS**.

Avec les méthodes PEAP-TLS et EAP-TLS, les clients affichent une liste de tous les certificats installés dans le composant logiciel enfichable Certificats, avec les exceptions suivantes :

- Les clients sans fil n'affichent pas les certificats basés sur le Registre ni les certificats d'ouverture de session par carte à puce.
- Les clients sans fil et les clients VPN n'affichent pas les certificats protégés par un mot de passe.
- Les certificats qui ne contiennent pas le rôle Authentification du client dans les extensions EKU.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Analyse et résolution des problèmes d'un serveur NPS

Vous pouvez analyser le serveur NPS en configurant et en utilisant la journalisation des événements et les demandes d'authentification et de comptes d'utilisateurs. La journalisation des événements vous permet d'enregistrer des événements NPS dans les journaux système et les journaux des événements de sécurité. Vous pouvez utiliser la journalisation des demandes pour l'analyse des connexions et la facturation. Les informations collectées dans les fichiers journaux sont utiles pour résoudre les problèmes de tentatives de connexion et pour étudier la sécurité.

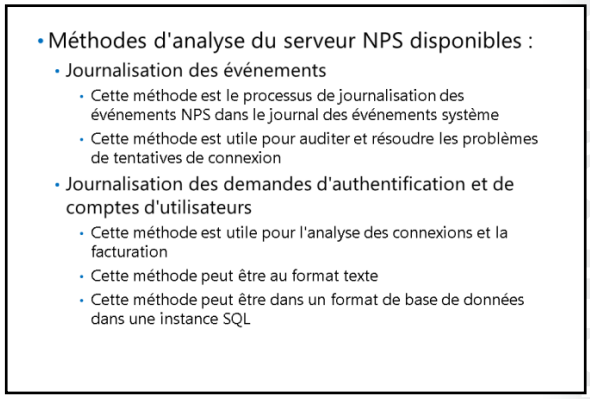
Objectifs de la leçon

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

- décrire les méthodes d'analyse du protocole NPS :
- expliquer comment configurer des propriétés des fichiers journaux ;
- expliquer comment configurer la journalisation SQL Server sur le serveur NPS ;
- expliquer configurer l'enregistrement d'événements NPS dans l'Observateur d'événements.

Méthodes d'analyse du serveur NPS

Deux méthodes de gestion de comptes, ou journalisation, s'offrent à vous pour analyser le serveur NPS :



- *Journalisation des événements pour le serveur NPS*. Vous pouvez utiliser la journalisation des événements pour enregistrer les événements NPS dans les journaux système et les journaux des événements de sécurité. Ce type de journalisation est principalement utilisé pour auditer et dépanner les tentatives de connexion.
- *Journalisation des demandes d'authentification et de comptes d'utilisateurs*. Vous pouvez enregistrer les demandes d'authentification et de comptes d'utilisateurs dans des fichiers journaux au format texte ou base de données, ou encore dans une procédure stockée dans une base de données SQL Server. La journalisation des demandes est particulièrement utile pour l'analyse des connexions et la facturation. Vous pouvez aussi vous en servir comme outil pour étudier la sécurité puisqu'elle permet d'identifier l'activité d'un intrus.

Pour utiliser le plus efficacement possible la journalisation NPS :

- Activez la journalisation (au départ) pour les enregistrements d'authentification et de comptes. Modifiez ces choix après avoir déterminé ce qui convient à votre environnement.
- Vérifiez que vous configurez la journalisation des événements avec une capacité suffisante pour prendre en charge vos journaux.
- Sauvegardez régulièrement tous les fichiers journaux car il vous sera impossible de les recréer si vous les endommagez ou les supprimez.

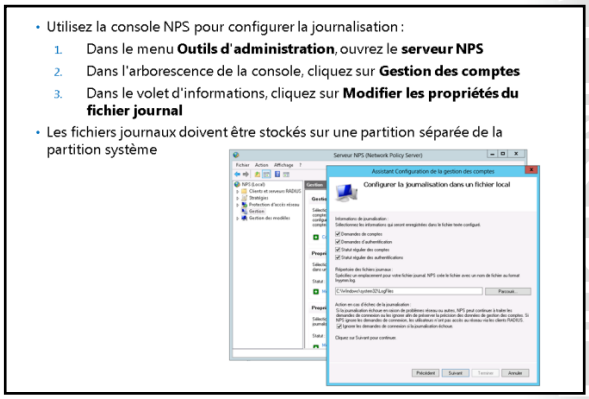
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Utilisez l'attribut Class **RADIUS** pour suivre l'emploi et simplifier l'identification des services ou des utilisateurs à facturer. Bien que l'attribut **Class**, qui est généré automatiquement, soit unique pour chaque demande, des enregistrements dupliqués peuvent exister lorsque la réponse au serveur d'accès est perdue et que la demande est renvoyée. Vous devrez peut-être supprimer les demandes dupliquées dans vos journaux pour obtenir un suivi précis de l'utilisation.
- Pour générer un basculement et une redondance dans le cadre de la journalisation SQL Server, placez deux ordinateurs équipés de SQL Server sur des sous-réseaux différents. Utilisez l'Assistant Création d'une publication de SQL Server pour configurer la réplication de la base de données entre les deux serveurs. Pour plus d'informations, consultez la documentation SQL Server.

Remarque : Pour interpréter des données journalisées, consultez les informations du site Web Microsoft TechNet :
Interpréter les fichiers journaux au format de base de données NPS
http://go.microsoft.com/fwlink/?LinkID=214832&clcid=0x409

Enregistrement de la gestion des comptes NPS

Vous pouvez configurer le serveur NPS pour effectuer la gestion de comptes RADIUS pour les demandes d'authentification utilisateur, les messages d'acceptation d'accès, les messages de rejet d'accès, les demandes et les réponses de comptes, et les mises à jour de statut périodique. Vous pouvez utiliser cette procédure pour configurer les fichiers journaux où vous souhaitez stocker les données de comptes.



Éléments à prendre en considération pour la configuration de la gestion de comptes pour NPS

La liste suivante fournit plus d'informations sur la configuration de la gestion de comptes NPS :

- Pour envoyer les données du fichier journal afin d'être collectées par un autre processus, vous pouvez configurer le service NPS de manière à écrire dans un canal nommé. Pour utiliser des canaux nommés, définissez le dossier du fichier journal comme suit : \\.\canal ou \\ComputerName\canal. Le programme serveur de canal nommé crée un canal nommé appelé \\.\canal\iaslog.log pour accepter les données. Dans la boîte de dialogue **Propriétés de Fichier local**, dans **Créer un fichier journal**, sélectionnez **Jamais (taille de fichier non limitée)** lorsque vous utilisez des canaux nommés.
- Pour créer le répertoire du fichier journal, utilisez des variables d'environnement système (au lieu de variables utilisateur), telles que %systemdrive%, %systemroot% et %windir%. Par exemple, le chemin d'accès suivant, qui utilise la variable d'environnement %windir%, localise le fichier journal dans le répertoire système du sous-dossier \System32\Logs (c'est-à-dire %windir%\System32\Logs\).
- Le fait de changer de formats de fichier journal n'entraîne pas la création d'un nouveau journal. Si vous modifiez les formats de fichier journal, le fichier actif au moment de la modification contient un mélange des deux formats. Les enregistrements en début de journal appliqueront l'ancien format, tandis que les enregistrements en fin de journal auront le nouveau format.

- Si vous gérez un serveur NPS à distance, vous ne pouvez pas parcourir la structure de répertoires. Pour journaliser des informations de comptes sur un serveur distant, spécifiez le nom du fichier journal en tapant un nom UNC (Universal Naming Convention), par exemple \\MyLogServer\LogShare.
- Si la gestion de comptes RADIUS échoue en raison d'un lecteur de disque dur plein ou pour d'autres motifs, le serveur NPS cesse de traiter les demandes de connexion, ce qui empêche les utilisateurs d'accéder aux ressources réseau.
- Le serveur NPS vous permet d'enregistrer des journaux dans une base de données SQL Server en plus, ou à la place, de l'enregistrement dans un fichier local.

Remarque : Si vous ne spécifiez pas un chemin d'accès complet dans le répertoire du fichier journal, le chemin par défaut est utilisé. Par exemple, si vous tapez NPSLogFile dans le répertoire du fichier journal, le fichier se trouve à l'emplacement %systemroot%\System32\NPSLogFile.

Configuration des propriétés des fichiers journaux

Pour configurer les propriétés des fichiers journaux à l'aide de l'interface Windows, procédez comme suit :

1. Ouvrez le composant logiciel enfichable **MMC Serveur NPS**.
2. Dans l'arborescence de la console, cliquez sur **Gestion**.
3. Dans le volet d'informations, cliquez sur **Modifier les propriétés du fichier journal**.
4. Dans **Propriétés du fichier journal**, sur l'onglet **Fichier journal**, dans **Répertoire**, tapez l'emplacement où vous souhaitez stocker les fichiers journaux NPS. L'emplacement par défaut est le dossier systemroot\System32\LogFiles.
5. Dans **Format**, sélectionnez **Compatible DTS**, **ODBC (hérité)** et **IAS (hérité)**.
6. Pour configurer le serveur NPS de manière à démarrer de nouveaux fichiers journaux à des intervalles spécifiés, cliquez sur l'intervalle que vous souhaitez utiliser :

- Pour un volume de transaction lourd et des activités de journalisation importantes, cliquez sur **Chaque jour**.
- Pour des volumes de transaction et des activités de journalisation moindres, cliquez sur **Hebdomadaire** ou **Tous les mois**.
- Pour stocker toutes les transactions dans un fichier journal, cliquez sur **Jamais (taille de fichier non limitée)**.
- Pour limiter la taille de chaque fichier journal, cliquez sur **Lorsque le fichier journal atteint cette taille**, puis tapez une taille de fichier. La taille par défaut est de 10 mégaoctets (Mo).

7. Pour configurer le serveur NPS de manière à supprimer automatiquement des fichiers journaux lorsque le disque est plein, cliquez sur **Lorsque le disque est plein, supprimer les anciens fichiers journaux**. Si le fichier journal le plus ancien est le fichier journal actif, il n'est pas supprimé.

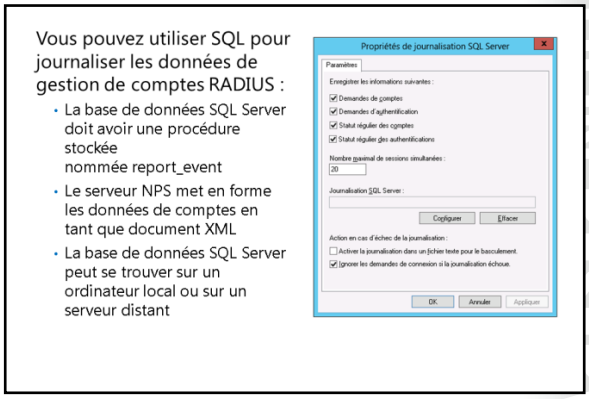
Remarque : Pour effectuer cette procédure, vous devez être membre du groupe Admins du domaine, Administrateurs de l'entreprise ou Administrateurs sur l'ordinateur local.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de la journalisation SQL Server

Vous pouvez configurer NPS pour exécuter la gestion de comptes RADIUS dans une base de données SQL Server. Vous pouvez utiliser cette procédure pour configurer les propriétés de journalisation et la connexion au serveur, exécutant SQL Server, qui stocke vos données de comptes. La base de données SQL Server peut se trouver sur l'ordinateur local ou sur un serveur distant.



Remarque : Le serveur NPS met en forme les données de comptes en tant que document XML, puis envoie ce document à la procédure stockée report_event dans la base de données SQL Server que vous désignez dans le serveur NPS. Pour que la journalisation SQL Server fonctionne correctement, vous devez avoir une procédure stockée nommée report_event dans la base de données SQL Server qui peut recevoir les documents XML du serveur NPS et les analyser.

Configuration de la journalisation SQL Server dans le serveur NPS

Pour configurer la journalisation SQL Server dans le serveur NPS à l'aide de l'interface Windows, procédez comme suit :

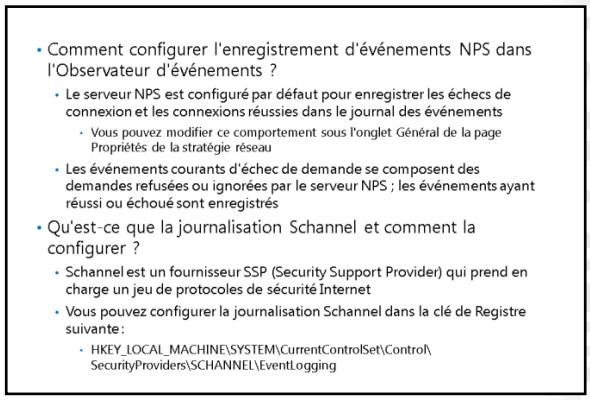
1. Ouvrez le composant logiciel enfichable MMC **Serveur NPS**.
2. Dans l'arborescence de la console, cliquez sur **Gestion**.
3. Dans le volet d'informations, cliquez sur **Modifier les propriétés de journalisation SQL Server**. La boîte de dialogue **Propriétés de journalisation SQL Server** s'ouvre.
4. Dans Enregistrer les informations suivantes, sélectionnez les informations à enregistrer :
   - Pour journaliser toutes les demandes de comptes, cliquez sur **Demandes de comptes**.
   - Pour journaliser les demandes d'authentification, cliquez sur**Demandes d'authentification**.
   - Pour journaliser le statut périodique, tel que les demandes de comptes intérimaires, cliquez sur **Statut de gestion de compte périodique**.
   - Pour journaliser le statut périodique, tel que les demandes d'authentification intérimaires, cliquez sur **Statut d'authentification périodique**.
5. Pour configurer le nombre de sessions simultanées que vous souhaitez autoriser entre le serveur NPS et la base de données SQL Server, tapez un nombre dans **Nombre maximal de sessions simultanées**.

6. Cliquez sur **Configurer** pour configurer la source de données SQL Server. La boîte de dialogue **Propriétés de liaison de données** s'ouvre. Sous l'onglet **Connexion**, indiquez les informations suivantes :
   - Pour spécifier le nom du serveur sur lequel la base de données est stockée, tapez ou sélectionnez un nom dans **Sélectionnez un serveur ou entrez un nom de serveur.**
   - Pour spécifier la méthode d'authentification avec laquelle se connecter au serveur, cliquez sur **Sécurité intégrée de Windows NT** ou sur **Utiliser un nom d'utilisateur et mot de passe spécifiques**, puis saisissez vos informations d'identification **Nom d'utilisateur** et **Mot de passe**.
   - Pour autoriser un mot de passe vide, cliquez sur **Mot de passe vide**.
   - Pour stocker le mot de passe, cliquez sur **Autoriser l'enregistrement du mot de passe**.
   - Pour spécifier à quelle base de données se connecter sur l'ordinateur SQL Server, cliquez sur **Sélectionnez la base de données sur le serveur**, puis sélectionnez un nom de base de données dans la liste.
7. Pour tester la connexion entre le serveur NPS et l'ordinateur sur lequel s'exécute SQL Server, cliquez sur **Tester la connexion**.

Remarque : Pour effectuer cette procédure, vous devez être membre du groupe Admins du domaine, Administrateurs de l'entreprise ou Administrateurs sur l'ordinateur local.

Configuration des événements NPS à enregistrer dans l'Observateur d'événements

Vous pouvez configurer la journalisation des événements NPS de manière à enregistrer les événements d'échec et de réussite des demandes de connexion dans le journal système Observateur d'événements.



Configuration de la journalisation des événements NPS

Pour configurer la journalisation des événements NPS à l'aide de l'interface Windows, procédez comme suit :

1. Ouvrez le composant logiciel enfichable Serveur NPS (Network Policy Server).
2. Cliquez avec le bouton droit sur **NPS (Local)**, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Général**, cochez la case des deux options suivantes, selon les besoins, puis cliquez sur **OK**:
   - Demandes d'authentification rejetées
   - Demandes d'authentification réussies

Remarque : pour effectuer cette procédure, vous devez être membre du groupe Admins du domaine ou du groupe Administrateurs de l'entreprise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

À l'aide des journaux des événements dans l'Observateur d'événements, vous pouvez analyser les erreurs NPS et d'autres événements enregistrés par le serveur NPS selon vos spécifications.

Le serveur NPS enregistre les événements d'échec des demandes de connexion dans les journaux système et les journaux des événements de sécurité par défaut. Les événements d'échec des demandes de connexion se composent des demandes refusées ou ignorées par le serveur NPS. D'autres événements d'authentification NPS sont enregistrés dans le journal système de l'Observateur d'événements en fonction des paramètres que vous spécifiez dans le composant logiciel enfichable Serveur NPS. Par conséquent, le journal de sécurité de l'Observateur d'événements peut enregistrer certains événements qui contiennent des données sensibles.

Événements d'échec des demandes de connexion

Bien que le serveur NPS enregistre les événements d'échec des demandes de connexion par défaut, vous pouvez modifier la configuration en fonction de vos besoins de journalisation. Le serveur NPS refuse ou ignore des demandes de connexion pour diverses raisons, en particulier :

- La mise en forme du message RADIUS n'est pas conforme au document RFC 2865 ou 2866.
- Le client RADIUS est inconnu.
- Le client RADIUS a plusieurs adresses IP et a envoyé la demande sur une adresse autre que celle définie dans NPS.
- L'authentificateur de message (aussi appelé signature numérique) que le client a envoyé n'est pas valide car le secret partagé n'est pas valide.
- Le serveur NPS n'a pas pu localiser le domaine du nom d'utilisateur.
- Le serveur NPS n'a pas pu se connecter au domaine du nom d'utilisateur.
- Le serveur NPS n'a pas pu accéder au compte d'utilisateur dans le domaine.

Lorsque le serveur NPS refuse une demande de connexion, les informations dans le texte d'événement contiennent le nom d'utilisateur, les identificateurs de serveur d'accès, le type d'authentification, le nom de la stratégie réseau correspondante, la raison du refus et d'autres informations.

Événements de réussite des demandes de connexion

Bien que le serveur NPS enregistre les événements de réussite des demandes de connexion par défaut, vous pouvez modifier la configuration en fonction de vos besoins de journalisation.

Lorsque le serveur NPS accepte une demande de connexion, les informations dans le texte d'événement contiennent le nom de l'utilisateur, les identificateurs de serveur d'accès, le type d'authentification et le nom de la première stratégie réseau correspondante.

Journalisation des événements Schannel

Schannel (Secure channel) est un fournisseur SSP (Security Support Provider) qui prend en charge un jeu de protocoles de sécurité Internet, notamment SSL et TLS. Ces protocoles assurent l'authentification des identités et garantissent des communications sécurisées et privées grâce au chiffrement.

La journalisation d'échecs de la validation de certificats clients est un événement de canal sécurisé et n'est pas activé par défaut sur le serveur NPS. Vous pouvez activer des événements de canal sécurisé supplémentaires en remplaçant la valeur 1 (type REG_DWORD, données 0x00000001) de la clé de Registre suivante par la valeur 3 (type REG_DWORD, données 0x00000003) :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\EventLogg
ing
```

Atelier pratique : Installation et configuration d'un serveur NPS

Scénario

A. Datum est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à London pour assister le bureau de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

A. Datum développe sa solution d'accès distant dans toute l'organisation. Cette opération nécessite la mise en place de plusieurs serveurs VPN situés à différents endroits pour assurer la connectivité des employés. Vous êtes chargé de mettre en place les tâches nécessaires pour prendre en charge ces connexions VPN.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- installer et configurer NPS pour prendre en charge RADIUS ;
- configurer et tester un client RADIUS.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-RTR 22411B-LON-CL2
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
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. Effectuez les étapes 2 à 4 pour **22411B-LON-RTR** et **22411B-LON-CL2**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Installation et configuration de NPS pour prendre en charge RADIUS

Scénario

Vous êtes chargé d'installer un NPS dans l'infrastructure existante avec pour fonction les services RADIUS. Dans cet exercice, vous allez configurer le serveur RADIUS avec les modèles appropriés pour faciliter la gestion de toutes les implémentations futures. Vous devez également configurer la gestion de comptes pour enregistrer les informations d'authentification dans un fichier texte local sur le serveur.

Les tâches principales de cet exercice sont les suivantes :

1. Installer et configurer le Serveur NPS
2. Configurer des modèles NPS
3. Configurer la gestion de comptes RADIUS

▶ Tâche 1 : Installer et configurer le Serveur NPS

1. Basculez vers LON-DC1.
2. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. À l'aide du **Gestionnaire de serveurs**, installez le rôle **Services de stratégie et d'accès réseau** à l'aide des valeurs par défaut pour exécuter l'Assistant d'installation.
4. Ouvrez la console **Serveur NPS**, puis inscrivez le serveur dans Active Directory.
5. Laissez la console Serveur NPS ouverte.

▶ Tâche 2 : Configurer des modèles NPS

1. Créez un modèle **Secrets partagés** avec les propriétés suivantes :
   - Nom : **Secret Adatum**
   - Secret partagé : **Pa$$w0rd**
2. Créez un modèle **Clients RADIUS** avec les propriétés suivantes :
   - Nom convivial : **LON-RTR**
   - Adresse (IP ou DNS) : **LON-RTR**
   - Secret partagé : Utilisez le modèle **Secret d'Adatum**.
3. Laissez la console Serveur NPS ouverte.

▶ Tâche 3 : Configurer la gestion de comptes RADIUS

1. Dans la console Serveur NPS, lancez l'Assistant Configuration de la gestion des comptes.
2. Choisissez l'option **Enregistrer les données dans un fichier texte sur l'ordinateur local**, puis utilisez les valeurs par défaut pour exécuter l'Assistant.
3. Laissez la console Serveur NPS ouverte.

Résultats : À la fin de cet exercice, vous devez avoir activé et configuré NPS pour prendre en charge l'environnement requis.

Exercice 2 : Configuration et test d'un client RADIUS

Scénario

Vous devez configurer un serveur en tant que serveur VPN et client RADIUS, y compris la configuration client, puis modifier les paramètres de stratégie réseau.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer un client RADIUS
2. Configurez une stratégie réseau pour RADIUS
3. Tester la configuration RADIUS
4. Pour préparer le module suivant

▶ Tâche 1 : Configurer un client RADIUS

1. Créez un client RADIUS à l'aide des propriétés suivantes :
   - Modèle : **LON-RTR**
2. Laissez la console ouverte, puis basculez vers LON-RTR.
3. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Ouvrez Routage et accès distant et **Désactiver le routage et l'accès à distance**.
5. Sélectionnez **Configurer et activer le routage et l'accès à distance**.
6. Reconfigurez LON-RTR en tant que serveur VPN :
   - **Connexion au réseau local 2** correspond à l'interface publique.
   - Le serveur VPN alloue des adresses du pool : **172.16.0.100 > 172.16.0.110**
   - Le serveur est configuré avec l'option **Oui, configurer ce serveur pour travailler avec un serveur RADIUS**.
   - Serveur RADIUS principal : **LON-DC1**
   - Secret : **Pa$$w0rd**

   Le service VPN démarre.

▶ Tâche 2 : Configurez une stratégie réseau pour RADIUS

1. Basculez vers LON-DC1.
2. Basculez vers la console Serveur NPS (Network Policy Server).
3. Désactivez les deux stratégies réseau existantes ; elles empêcheraient le traitement de la stratégie que vous êtes sur le point de créer.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Créez une stratégie réseau à l'aide des propriétés ci-dessous :
   - Nom de la stratégie : **Stratégie VPN Adatum**
   - Type de serveur d'accès réseau : **Serveur d'accès à distance (VPN-Dial up)**
   - Condition : **Type de port NAS = Virtuel (VPN)**
   - Autorisation : **Accès accordé**
   - Méthodes d'authentification : valeur par défaut
   - Contraintes : valeur par défaut
   - Paramètres : valeur par défaut

▶ Tâche 3 : Tester la configuration RADIUS

1. Basculez vers LON-CL2, puis connectez-vous avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Créez une connexion VPN avec les propriétés suivantes :
   - Adresse Internet de connexion : **10.10.0.1**
   - Nom de la destination : **VPN Adatum**
   - Autoriser d'autres personnes à utiliser cette connexion : **true**
3. Une fois le VPN créé, modifiez ses paramètres en affichant les propriétés de la connexion, puis sélectionnez l'onglet **Sécurité**. Utilisez les paramètres suivants pour reconfigurer VPN :
   - Type de réseau VPN : **Protocole PPTP (Point to Point Tunneling Protocol)**
   - Authentification : **Autoriser ces protocoles = Protocole Microsoft CHAP Version 2 (MS-CHAP v2)**
4. Testez la connexion VPN. Utilisez les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**

Résultats : À la fin de cet exercice, vous devriez avoir déployé un serveur VPN, et l'avoir configuré en tant que client RADIUS.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial de tous les ordinateurs virtuels. Pour cela, 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 **22411B-LON-CL2**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22411B-LON-RTR** et **22411B-LON-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR – MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Comment pouvez-vous tirer pleinement parti des fonctionnalités de journalisation NPS ?

Question : Que devez-vous prendre en compte si vous choisissez d'utiliser une attribution de port non standard pour le trafic RADIUS ?

Question : Pourquoi devez-vous inscrire le serveur NPS dans Active Directory ?

Outils

Outil	Utilisation	Emplacement
Serveur NPS	Gestion et création de la stratégie réseau	Serveur NPS (Network Policy Server) dans le menu Outils d'administration
Outil en ligne de commande netsh	Création de scripts d'administration pour configurer et gérer le rôle Serveur NPS	À partir d'une fenêtre d'invite de commandes, tapez **netsh –c nps** pour effectuer l'administration via une fenêtre d'invite de commandes
Observateur d'événements	Consultation d'informations journalisées provenant d'événements d'applications, système et de sécurité	Observateur d'événements dans le menu Outils d'administration

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 9

Implémentation de la protection d'accès réseau

Table des matières :

Vue d'ensemble du module **9-1**

Leçon 1 : Vue d'ensemble de la protection d'accès réseau **9-2**

Leçon 2 : Vue d'ensemble des processus de contrainte de mise en conformité NAP **9-8**

Leçon 3 : Configuration de NAP **9-16**

Leçon 4 : Analyse et résolution des problèmes du système NAP **9-22**

Atelier pratique : Implémentation de la protection d'accès réseau **9-27**

Contrôle des acquis et éléments à retenir **9-34**

Vue d'ensemble du module

La sécurité de votre réseau n'est pas meilleure que celle de l'ordinateur le moins sécurisé connecté. Beaucoup de programmes et d'outils existent pour vous aider à sécuriser les ordinateurs connectés au réseau, tels que des logiciels de détection de programme malveillant ou antivirus. Cependant, si le logiciel sur certains de vos ordinateurs n'est pas à jour, ou n'est pas activé ou configuré correctement, ces ordinateurs présentent alors un risque de sécurité.

Il est relativement facile de maintenir la configuration et la mise à jour des ordinateurs qui restent dans l'environnement de bureau et qui sont toujours connectés au même réseau. Il est moins facile de contrôler les ordinateurs qui se connectent à différents réseaux, en particulier les réseaux non gérés. Il est par exemple difficile de contrôler les ordinateurs portables que les utilisateurs utilisent pour se connecter aux réseaux des clients ou aux points d'accès Wi-Fi publics. En outre, les ordinateurs non gérés qui cherchent à se connecter à distance à votre réseau (les utilisateurs se connectant à partir de leurs ordinateurs personnels, par exemple) posent également une difficulté.

La protection d'accès réseau (NAP) vous permet de créer des stratégies personnalisées de spécifications d'intégrité pour valider l'intégrité des ordinateurs avant de permettre l'accès ou la communication. En outre, la protection d'accès réseau (NAP) met automatiquement à jour les ordinateurs pour vérifier leur conformité, et peut limiter l'accès aux ordinateurs non conformes à un réseau restreint jusqu'à ce qu'ils deviennent conformes.

Objectifs

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

- décrire comment la protection d'accès réseau (NAP) peut aider à protéger votre réseau ;
- décrire les divers processus de contrainte de mise en conformité NAP ;
- configurer les services NAP ;
- analyser le service NAP et résoudre les problèmes éventuels.

Leçon 1
Vue d'ensemble de la protection d'accès réseau

NAP est une plateforme d'application de stratégies qui est intégrée aux systèmes d'exploitation Windows® 8, Windows 7, Windows Vista®, Windows XP avec Service Pack 3 (SP3), Windows Server® 2008, Windows Server 2008 R2 et Windows Server 2012. NAP vous permet de protéger plus efficacement les ressources du réseau en mettant en œuvre la conformité à des spécifications d'intégrité système. NAP fournit les composants logiciels nécessaires pour garantir que les ordinateurs qui sont connectés ou qui se connectent au réseau restent gérables, afin qu'ils n'entraînent aucun risque de sécurité pour le réseau de l'entreprise ou les autres ordinateurs connectés.

Le fait de comprendre la fonctionnalité et les limitations de la protection d'accès réseau (NAP) vous aide à protéger votre réseau contre les risques de sécurité posés par les ordinateurs non conformes.

Objectifs de la leçon

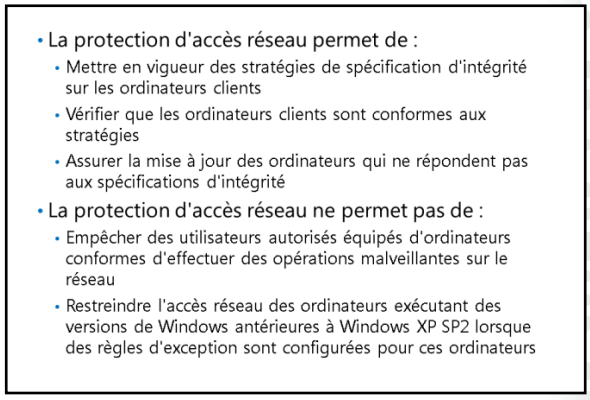
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Expliquez comment vous pouvez utiliser la protection d'accès réseau (NAP) pour appliquer les exigences d'intégrité des ordinateurs.
- Décrivez les scénarios dans lesquels vous utiliseriez la protection d'accès réseau (NAP).
- Décrivez les méthodes de contrainte de mise en conformité NAP.
- Décrivez l'architecture d'une infrastructure–réseau qui prend en charge la protection d'accès réseau (NAP).

Qu'est-ce que la protection d'accès réseau ?

NAP fournit des composants et une interface de programmation d'applications (API) qui permettent d'imposer la conformité aux stratégies de spécification d'intégrité de l'entreprise pour la communication ou l'accès réseau.

NAP vous permet de créer des solutions de validation des ordinateurs qui se connectent à vos réseaux, et de fournir les mises à jour nécessaires ou l'accès aux ressources de mise à jour de l'intégrité. En outre, NAP vous permet de limiter l'accès ou la communication des ordinateurs non conformes.



Vous pouvez intégrer les fonctionnalités de contrainte de mise en conformité de la protection d'accès réseau (NAP) à des logiciels d'autres fournisseurs ou à des programmes personnalisés.

Il est important de garder à l'esprit que NAP ne protège pas un réseau des utilisateurs malveillants. Elle vous permet plutôt d'assurer automatiquement l'intégrité des ordinateurs en réseau de votre organisation, ce qui contribue à garantir l'intégrité générale du réseau. Par exemple, si un ordinateur inclut tous les logiciels et les paramètres de configuration qu'impose la stratégie de contrôle d'intégrité, l'ordinateur est conforme et bénéficie alors d'un accès illimité au réseau. Toutefois, la protection d'accès réseau n'empêche pas un utilisateur autorisé équipé d'un ordinateur conforme de télécharger un programme malveillant sur le réseau ou d'entreprendre d'autres actions inappropriées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

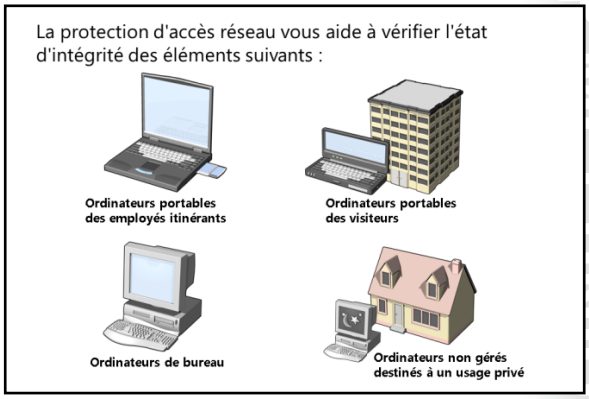
Procédure d'utilisation de NAP

Vous pouvez utiliser NAP de trois façons différentes :

- Pour valider l'état d'intégrité. Lorsqu'un ordinateur tente de se connecter au réseau, NAP valide son état d'intégrité par rapport aux stratégies de spécification d'intégrité que l'administrateur définit. Vous pouvez également définir l'action à entreprendre en cas de non-conformité d'un ordinateur. Dans un environnement d'analyse uniquement, l'état d'intégrité de tous les ordinateurs est évalué, et l'état de conformité de chaque ordinateur est consigné par NAP à des fins d'analyse. Dans un environnement avec accès limité, les ordinateurs qui répondent aux stratégies de spécification d'intégrité bénéficient d'un accès réseau illimité. Quant aux ordinateurs qui ne répondent pas aux stratégies de spécification d'intégrité, leur accès peut être limité à un réseau restreint.
- Pour appliquer les stratégies de contrôle d'intégrité. pour garantir la conformité aux stratégies de spécification d'intégrité, vous pouvez choisir de mettre automatiquement à jour les ordinateurs non conformes en leur appliquant les mises à jour logicielles manquantes ou les modifications de configuration par le biais de logiciels de gestion, tels que Microsoft® System Center Configuration Manager. Dans un environnement d'analyse uniquement, NAP garantit que les ordinateurs peuvent mettre à jour l'accès au réseau avant de recevoir les modifications de configuration ou les mises à jour requises. Dans un environnement avec accès limité, les ordinateurs non conformes bénéficient d'un accès limité tant que les mises à jour et les modifications de configuration n'ont pas été effectuées. Dans les deux environnements, les ordinateurs compatibles avec NAP peuvent devenir conformes automatiquement, et vous pouvez définir des exceptions pour les ordinateurs non compatibles avec NAP.
- Pour limiter l'accès réseau. Vous pouvez protéger vos réseaux en limitant l'accès des ordinateurs non conformes. Vous pouvez spécifier un accès réseau limité en fonction d'une durée spécifique ou des ressources auxquelles l'ordinateur non conforme peut accéder. Dans ce dernier cas, vous devez définir un réseau restreint contenant les ressources de mise à jour de l'intégrité, et l'accès restera limité tant que l'ordinateur non conforme n'aura pas atteint un état de conformité. Vous pouvez également configurer des exceptions afin que l'accès réseau des ordinateurs non compatibles avec NAP ne soit pas limité.

Scénarios de protection d'accès réseau

La protection d'accès réseau (NAP) fournit une solution pour les scénarios courants, tels que les ordinateurs portables d'employés itinérants, les ordinateurs de bureau, les ordinateurs portables de visiteurs et des ordinateurs non gérés. En fonction de vos besoins, vous pouvez configurer pour votre réseau une solution adaptée à certains ou à tous ces scénarios.



Ordinateurs portables des employés itinérants

La portabilité et la souplesse constituent deux avantages essentiels d'un ordinateur portable, mais ces caractéristiques génèrent également un risque en termes d'intégrité du système. En effet, les utilisateurs connectent souvent leurs ordinateurs portables à d'autres réseaux. Lorsque les utilisateurs sont loin de l'organisation, leurs ordinateurs portables ne peuvent pas forcément recevoir les mises à jour logicielles ou les modifications de configuration les plus récentes. En outre, l'exposition à des réseaux non protégés, tels qu'Internet, peut introduire des risques liés à la sécurité dans les ordinateurs portables. NAP vous permet de vérifier l'état d'intégrité de n'importe quel ordinateur portable lorsqu'il est reconnecté au réseau de l'organisation, que ce soit via une connexion VPN, une connexion Windows 8 DirectAccess ou une connexion réseau sur le lieu de travail.

Ordinateurs de bureau

Bien que les ordinateurs de bureau restent en général dans l'enceinte de l'entreprise, ils peuvent tout de même présenter un risque pour le réseau. Pour minimiser ce risque, vous devez garder ces ordinateurs à jour en installant les mises à jour et les logiciels requis les plus récents. Dans le cas contraire, ces ordinateurs sont susceptibles d'être infectés par des sites Web, des messages électroniques, des fichiers de dossiers partagés et d'autres ressources auxquelles tous les utilisateurs peuvent accéder. Vous pouvez utiliser NAP pour automatiser les contrôles de l'état d'intégrité afin de vérifier la conformité de chaque ordinateur de bureau aux stratégies de spécification d'intégrité. Vous pouvez consulter les fichiers journaux pour identifier les ordinateurs qui ne sont pas conformes. En outre, l'utilisation de logiciels de gestion vous permet de générer des rapports automatiques et d'assurer automatiquement la mise à jour des ordinateurs non conformes. Lorsque vous modifiez des stratégies de spécification d'intégrité, vous pouvez configurer NAP pour fournir automatiquement les mises à jour les plus récentes aux ordinateurs.

Ordinateurs portables des visiteurs

Les organisations sont fréquemment amenées à autoriser des consultants, des partenaires commerciaux et des invités à se connecter à leurs réseaux privés. Il est possible que les ordinateurs portables que ces visiteurs amènent dans votre organisation ne répondent pas aux spécifications d'intégrité système et présentent des risques d'intégrité. NAP vous permet de déterminer quels ordinateurs portables de visiteurs ne sont pas conformes et de limiter leur accès à un réseau restreint. En règle générale, vous n'exigez ni ne fournissez aucune mise à jour ou modification de configuration pour les ordinateurs portables de visiteurs. Vous pouvez configurer un accès Internet pour ces ordinateurs portables, mais pas pour d'autres ordinateurs d'organisation bénéficiant d'un accès limité.

Ordinateurs non gérés destinés à un usage privé

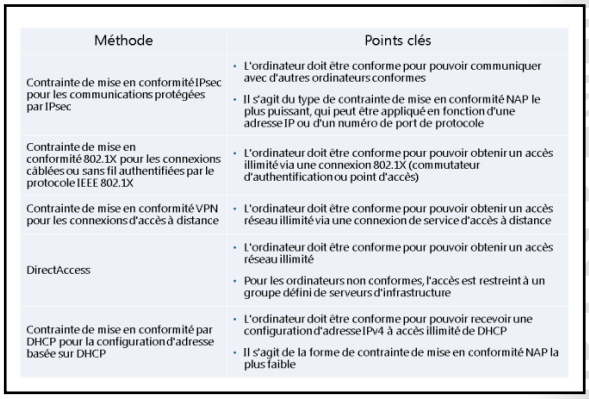
Les ordinateurs « privés » non gérés qui n'appartiennent pas au domaine Active Directory® de la société peuvent se connecter à un réseau d'entreprise géré par le biais d'une connexion VPN. Les ordinateurs « privés » non gérés constituent une difficulté supplémentaire car vous ne pouvez pas y accéder physiquement. Du fait de l'absence d'accès physique, la mise en conformité aux spécifications d'intégrité (comme l'utilisation d'un antivirus) se révèle plus difficile. Toutefois, NAP vous permet de vérifier l'état d'intégrité d'un ordinateur destiné à un usage privé chaque fois qu'il établit une connexion VPN au réseau de l'entreprise, et de limiter son accès à un réseau restreint jusqu'à ce qu'il réponde aux spécifications d'intégrité du système.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Méthodes de contrainte de mise en conformité NAP

Les composants de l'infrastructure NAP (appelés « clients de contrainte de mise en conformité » et « serveurs de contrainte de mise en conformité ») requièrent une validation de l'état d'intégrité et appliquent un accès réseau limité pour les ordinateurs non conformes. Windows 8, Windows 7, Windows Vista, Windows XP avec SP3, Windows Server 2008, Windows Server 2008 R2 et Windows Server 2012 comprennent la prise en charge NAP pour l'accès réseau suivant ou les méthodes de communication suivantes :



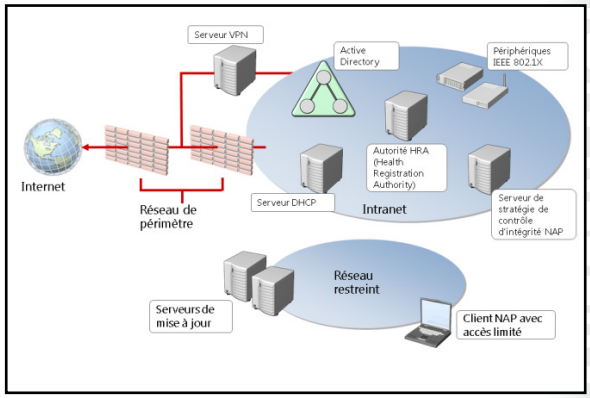
Méthode	Points clés
Contrainte de mise en conformité IPsec pour les communications protégées par IPsec	• L'ordinateur doit être conforme pour pouvoir communiquer avec d'autres ordinateurs conformes • Il s'agit du type de contrainte de mise en conformité NAP le plus puissant, qui peut être appliqué en fonction d'une adresse IP ou d'un numéro de port de protocole
Contrainte de mise en conformité 802.1X pour les connexions câblées ou sans fil authentifiées par le protocole IEEE 802.1X	• L'ordinateur doit être conforme pour pouvoir obtenir un accès illimité via une connexion 802.1X (commutateur d'authentification ou point d'accès)
Contrainte de mise en conformité VPN pour les connexions d'accès à distance	• L'ordinateur doit être conforme pour pouvoir obtenir un accès réseau illimité via une connexion de service d'accès à distance
DirectAccess	• L'ordinateur doit être conforme pour pouvoir obtenir un accès réseau illimité • Pour les ordinateurs non conformes, l'accès est restreint à un groupe défini de serveurs d'infrastructure
Contrainte de mise en conformité par DHCP pour la configuration d'adresse basée sur DHCP	• L'ordinateur doit être conforme pour pouvoir recevoir une configuration d'adresse IPv4 à accès illimité de DHCP • Il s'agit de la forme de contrainte de mise en conformité NAP la plus faible

- *Trafic protégé par le protocole IPsec*. La contrainte de mise en conformité IPsec (Internet Protocol security) restreint la communication aux ordinateurs conformes une fois qu'ils se sont correctement connectés et qu'ils ont obtenu une configuration d'adresse IP valide. La contrainte de mise en conformité IPsec constitue la forme de communication ou d'accès réseau limité la plus puissante de la protection d'accès réseau.
- *Connexions réseau authentifiées par le protocole IEEE (Institute of Electrical and Electronics Engineers) 802.1X*. La contrainte de mise en conformité IEEE 802.1X requiert qu'un ordinateur soit conforme pour obtenir un accès réseau illimité via une connexion réseau authentifiée IEEE 802.1X–. Les exemples de ce type de connexion réseau comprennent un commutateur d'authentification Ethernet ou un point d'accès sans fil IEEE 802.11.
- *Connexions VPN d'accès à distance*. La contrainte de mise en conformité VPN nécessite qu'un ordinateur soit conforme pour pouvoir obtenir un accès réseau illimité via une connexion VPN d'accès à distance. Pour les ordinateurs non conformes, l'accès réseau est limité au moyen d'un jeu de filtres de paquets IP que le serveur VPN applique à la connexion VPN.
- *Connexions DirectAccess*. Les connexions DirectAccess nécessitent qu'un ordinateur soit conforme pour pouvoir obtenir un accès réseau illimité via un serveur DirectAccess. Pour les ordinateurs non conformes, l'accès réseau est limité à l'ensemble d'ordinateurs qui sont définis comme serveurs d'infrastructure à l'aide du tunnel d'infrastructure. Les ordinateurs conformes peuvent créer le tunnel intranet distinct qui offre un accès illimité aux ressources intranet. Les connexions DirectAccess utilisent la mise en conformité IPsec.
- *Configurations d'adresses DHCP (Dynamic Host Configuration Protocol)*. La contrainte de mise en conformité par DHCP nécessite qu'un ordinateur soit conforme pour pouvoir obtenir une configuration IPv4 (Internet Protocol version 4) illimitée à partir d'un serveur DHCP. Pour les ordinateurs non conformes, l'accès réseau est limité par une configuration d'adresse IPv4 qui limite l'accès au réseau restreint.

Ces accès réseau ou ces méthodes de communication, ou ces *méthodes de contrainte de mise en conformité NAP* sont utiles séparément ou ensemble pour limiter l'accès ou la communication des ordinateurs non conformes. Un serveur qui exécute NPS (Network Policy Server) dans Windows Server 2012 agit en tant que serveur de stratégie de contrôle d'intégrité pour toutes ces méthodes de contrainte de mise en conformité NAP.

Architecture de la plateforme NAP

Le tableau suivant décrit les composants d'une infrastructure réseau qui prend en charge la protection d'accès réseau (NAP).



Composants	Description
Clients NAP	Ces ordinateurs prennent en charge la plateforme NAP pour la communication et la validation avant l'accès réseau d'un contrôle d'intégrité système.
Points de contrainte de mise en conformité NAP	• Il s'agit d'ordinateurs ou de périphériques d'accès réseau qui utilisent la protection d'accès réseau (NAP) ou que vous pouvez utiliser avec NAP pour exiger l'évaluation de l'état d'intégrité d'un client NAP et assurer des communications ou un accès réseau restreints. Les points de contrainte de mise en conformité NAP utilisent un serveur NPS qui joue le rôle de serveur de stratégie de contrôle d'intégrité NAP pour évaluer l'état d'intégrité des clients NAP, pour déterminer si la communication ou l'accès réseau sont autorisés et pour définir les actions de mise à jour qu'un client NAP non conforme doit exécuter. • Les points de contrainte de mise en conformité NAP sont les suivants : o *Autorité HRA (Health Registration Authority)*. Ordinateur exécutant Windows Server 2012 et les Services Internet (IIS), et qui obtient des certificats d'intégrité d'une autorité de certification pour les ordinateurs conformes. o *Serveur VPN*. Ordinateur exécutant Windows Server 2012 et le service Routage et accès distant, qui autorise les connexions intranet VPN d'accès à distance via l'accès à distance. o *Serveur DHCP*. Ordinateur exécutant Windows Server 2012 et le service Serveur DHCP, et qui fournit une configuration d'adresse IPv4 (Internet Protocol version 4) automatique aux clients intranet DHCP. o *Périphériques d'accès réseau*. Commutateurs Ethernet ou de points d'accès sans fil qui prennent en charge l'authentification IEEE 802.1X.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Composants	Description
Serveurs de stratégie de contrôle d'intégrité NAP	Ordinateurs exécutant Windows Server 2012 et le service NPS, qui stockent les stratégies de spécification d'intégrité et qui assurent la validation de l'état d'intégrité pour la protection d'accès réseau. Le service NPS remplace le service d'authentification Internet (IAS), ainsi que le serveur et le proxy RADIUS (Remote Authentication Dial-In User Service) de Windows Server 2003. Le service NPS fait également office de serveur d'authentification, d'autorisation et d'administration (AAA) pour l'accès réseau. Lorsqu'il agit en tant que serveur AAA ou serveur de stratégie de contrôle d'intégrité NAP, le service NPS s'exécute généralement sur un serveur indépendant pour permettre la configuration centralisée des stratégies d'accès réseau et de spécification d'intégrité. Le service NPS s'exécute également sur les points de contrainte de mise en conformité NAP (selon Windows Server 2012) qui ne comportent pas d'ordinateur client RADIUS intégré, comme un serveur HRA ou DHCP. Toutefois, dans ces configurations, le service NPS agit en tant que proxy RADIUS pour échanger des messages RADIUS avec un serveur de stratégie de contrôle d'intégrité NAP.
Serveurs de spécification d'intégrité	Ces ordinateurs fournissent l'état d'intégrité système actuel pour les serveurs de stratégie de contrôle d'intégrité NAP. Il peut s'agir, par exemple, d'un serveur de spécification d'intégrité pour un antivirus qui détecte la version la plus récente du fichier de signature antivirus.
AD DS	Ce service d'annuaire Windows stocke les propriétés et les informations d'identification de compte, ainsi que des paramètres de stratégie de groupe. Bien que le service Active Directory ne soit pas requis pour la validation de l'état d'intégrité, il est indispensable pour les communications protégées par la sécurité IPsec, pour les connexions authentifiées par le protocole 802.1X et pour les connexions VPN d'accès à distance.
Périphériques 802.1X	Commutateur d'authentification Ethernet ou point d'accès sans fil IEEE 802.11.
Réseau restreint	• Il s'agit d'un réseau logique ou physique qui contient les éléments suivants : o *Serveurs de mise à jour*. Ces ordinateurs contiennent des ressources de mise à jour d'intégrité auxquelles les clients NAP peuvent accéder pour mettre à jour leur état non conforme. C'est le cas notamment des serveurs de distribution de signatures antivirus et des serveurs de mises à jour de logiciels. o *Clients NAP dotés d'un accès limité*. Ces ordinateurs sont placés sur le réseau restreint lorsqu'ils ne sont pas conformes aux stratégies de spécification d'intégrité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2

Vue d'ensemble des processus de contrainte de mise en conformité NAP

Lorsqu'un client tente d'accéder au réseau ou de communiquer sur ce dernier, il doit présenter son état d'intégrité système ou prouver sa conformité à la stratégie de contrôle d'intégrité. Si un client ne peut pas prouver qu'il est conforme aux spécifications d'intégrité système (qu'il comporte, par exemple, les mises à jour d'antivirus et du système d'exploitation les plus récentes), vous pouvez alors limiter son accès ou sa communication sur le réseau contenant des ressources de serveur. Vous pouvez limiter cet accès jusqu'à ce que les problèmes de conformité soient résolus. Une fois que les mises à jour ont été installées, le client demande l'accès au réseau ou tente d'établir à nouveau la communication. S'il est conforme, le client reçoit alors un accès illimité au réseau, ou les communications sont autorisées.

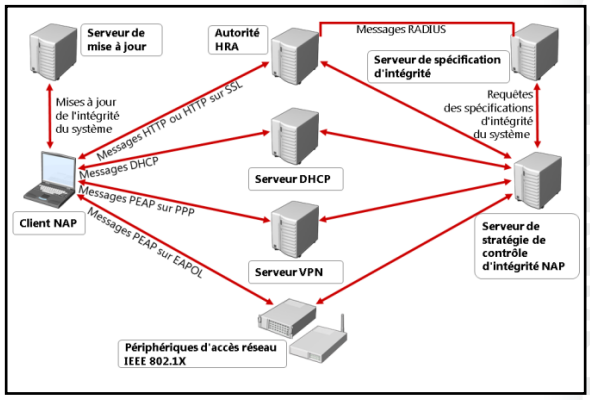
Objectifs de la leçon

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

- décrire les processus de contrainte de mise en conformité NAP généraux ;
- présenter la contrainte de mise en conformité IPsec ;
- décrire la contrainte de mise en conformité 802.1X ;
- expliquer la contrainte de mise en conformité VPN ;
- présenter la contrainte de mise en conformité DHCP ;

Processus de contrainte de mise en conformité NAP

Quelle que soit la contrainte de mise en conformité NAP que vous sélectionnez, plusieurs des communications client/serveur sont courantes. Les points suivants résument ces communications :



- Entre un client NAP et une autorité HRA

  Le client NAP envoie l'état d'intégrité actuel de système au HRA et demande un certificat d'intégrité. Si le client NAP est conforme, l'autorité HRA délivre un certificat d'intégrité au client NAP. Si le client n'est pas conforme, l'autorité HRA délivre des instructions de mise à jour d'intégrité au client NAP.

- Entre un client NAP et un serveur de mise à jour

  Même si le client NAP dispose d'un accès intranet illimité, il accède au serveur de mise à jour pour vérifier qu'il reste conforme. Si le client NAP bénéficie d'un accès limité, il communique avec le serveur de mise à jour pour devenir conforme, en fonction des instructions du serveur de stratégie de contrôle d'intégrité NAP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Entre une autorité HRA et un serveur de stratégie de contrôle d'intégrité NAP

  L'autorité HRA envoie des messages RADIUS qui contiennent l'état d'intégrité système du client NAP au serveur de stratégie de contrôle d'intégrité NAP. Le serveur de stratégie de contrôle d'intégrité NAP envoie des messages RADIUS pour indiquer que le client NAP a :

  - *Un accès illimité parce qu'il est conforme*. En fonction de la réponse, l'autorité HRA obtient un certificat d'intégrité et l'envoie au client NAP.
  - *Un accès limité jusqu'à ce qu'il exécute des fonctions de mise à jour*. En fonction de la réponse, l'autorité HRA ne délivre pas de certificat d'intégrité au client NAP.

- Entre un périphérique d'accès réseau 802.1X et un serveur de stratégie de contrôle d'intégrité NAP

  Le périphérique d'accès réseau 802.1X envoie des messages RADIUS pour transférer les messages PEAP (Protected Extensible Authentication Protocol) envoyés par un client NAP 802.1X. Le serveur de stratégie de contrôle d'intégrité NAP envoie des messages RADIUS pour :

  - indiquer que le client 802.1X dispose d'un accès illimité car il est conforme ;
  - indiquer un profil d'accès limité et placer le client 802.1X sur le réseau restreint jusqu'à ce qu'il exécute des fonctions de mise à jour ;
  - envoyer des messages PEAP au client 802.1X.

- Entre un serveur VPN et un serveur de stratégie de contrôle d'intégrité NAP

  Le serveur VPN envoie des messages RADIUS pour transférer les messages PEAP qui sont envoyés par un client NAP utilisant une connexion VPN. Le serveur de stratégie de contrôle d'intégrité NAP envoie des messages RADIUS pour :

  - indiquer que le client VPN dispose d'un accès illimité car il est conforme ;
  - indiquer que le client VPN dispose d'un accès limité au moyen d'un jeu de filtres de paquets IP appliqués à la connexion VPN ;
  - envoyer des messages PEAP au client VPN.

- Entre un serveur DHCP et un serveur de stratégie de contrôle d'intégrité NAP

  Le serveur DHCP envoie des messages RADIUS qui contiennent l'état d'intégrité système du client DHCP au serveur de stratégie de contrôle d'intégrité NAP. Le serveur de stratégie de contrôle d'intégrité NAP envoie des messages RADIUS au serveur DHCP pour indiquer que le client DHCP a :

  - Un accès illimité parce qu'il est conforme.
  - Un accès limité jusqu'à ce qu'il exécute des fonctions de mise à jour.

- Entre un serveur de stratégie de contrôle d'intégrité NAP et un serveur de spécification d'intégrité :

  Lorsque vous validez l'accès réseau d'un client NAP, le serveur de stratégie de contrôle d'intégrité NAP peut être amené à contacter un serveur de spécification d'intégrité pour obtenir des informations sur les spécifications actuelles de l'intégrité système.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Communication basée sur le type de contrainte

Selon le type de contrainte sélectionné, la communication suivante est établie :

- Entre un client NAP et un périphérique d'accès réseau 802.1X

  Le client NAP effectue l'authentification de la connexion 802.1X, puis fournit l'état actuel de l'intégrité système au serveur de la stratégie de contrôle d'intégrité NAP.

  Le serveur de stratégie de contrôle d'intégrité NAP fournit soit des instructions de mise à jour (car le client 802.1X n'est pas conforme) ou indique que le client 802.1X dispose d'un accès réseau illimité.

  La protection d'accès réseau (NAP) route ces messages par le périphérique d'accès réseau 802.1X.

- Entre un client NAP et un serveur VPN

  Le client NAP qui agit comme un client VPN indique son état d'intégrité système actuel au serveur de stratégie de contrôle d'intégrité NAP.

  Le serveur de stratégie de contrôle d'intégrité NAP répond par des messages pour fournir soit les instructions de mise à jour (car le client VPN n'est pas conforme) soit pour indiquer que le client VPN dispose d'un accès intranet illimité.

  La protection d'accès réseau (NAP) route ces messages par le serveur VPN.

- Entre un client NAP et un serveur DHCP

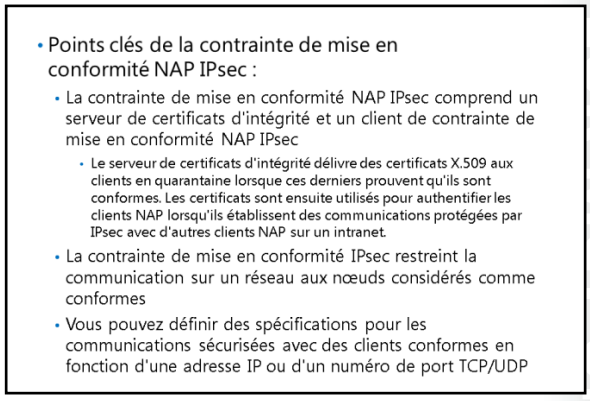
  Le client NAP (également client DHCP) communique avec le serveur DHCP pour obtenir une configuration d'adresse IPv4 valide et pour indiquer son état d'intégrité système actuel.

  Le serveur DHCP alloue une configuration d'adresse IPv4 pour le réseau restreint, puis fournit les instructions de mise à jour (si le client DHCP n'est pas conforme), ou une configuration d'adresse IPv4 pour l'accès illimité (si le client DHCP est conforme).

Contrainte de mise en conformité IPsec

Avec la contrainte de mise en conformité IPsec, un ordinateur doit être conforme pour être en mesure d'établir des communications avec d'autres ordinateurs conformes. La contrainte de mise en conformité IPsec tirant parti de la sécurité IPsec, vous pouvez définir des spécifications pour les communications protégées avec les ordinateurs conformes basées sur l'une des caractéristiques de communication suivantes :

- Adresse IP
- Numéro de port TCP (Transmission Control Protocol)
- Numéro de port UDP (User Datagram Protocol)



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La contrainte de mise en conformité IPsec restreint la communication aux ordinateurs conformes une fois qu'ils se sont correctement connectés et qu'ils ont obtenu une configuration d'adresse IP valide. La contrainte de mise en conformité IPsec constitue la forme de communication ou d'accès réseau limité la plus puissante de la protection d'accès réseau.

Les composants de la contrainte de mise en conformité IPsec se composent d'une autorité HRA qui exécute Windows Server 2012 et d'un client de contrainte de mise en conformité IPSec qui exécute l'un des systèmes d'exploitation suivants :

- Windows XP Service Pack 3
- Windows Vista
- Windows 7
- Windows 8
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

L'autorité HRA obtient des certificats X.509 pour les clients NAP lorsque ces derniers prouvent qu'ils sont conformes. Ces certificats d'intégrité sont alors utilisés pour authentifier les clients NAP lorsqu'ils établissent des communications protégées par la sécurité IPsec avec d'autres clients NAP sur un intranet.

La contrainte de mise en conformité IPsec limite la communication des clients NAP protégés par IPsec en rejetant les tentatives de communications entrantes envoyées par les ordinateurs qui ne peuvent pas négocier la protection IPsec à l'aide de certificats d'intégrité. Avec la contrainte de mise en conformité IPsec, chaque ordinateur exécute la contrainte de mise en conformité IPsec, alors qu'avec la contrainte de mise en conformité 802.1X et VPN, la contrainte de mise en conformité se produit au point d'entrée du réseau. Étant donné que vous pouvez tirer parti des paramètres de stratégie IPsec, la contrainte de mise en conformité de certificats d'intégrité peut concerner :

- tous les ordinateurs d'un domaine ;
- des ordinateurs spécifiques d'un sous-réseau ;
- un ordinateur spécifique ;
- un jeu spécifique de ports TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol) ;
- un jeu de ports TCP ou UDP sur un ordinateur spécifique.

Éléments à prendre en compte pour la contrainte de mise en conformité IPsec

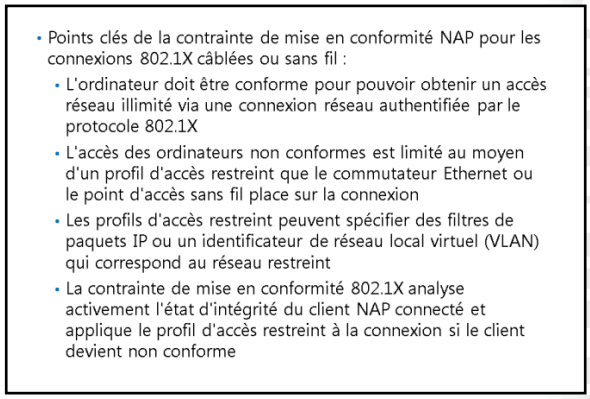
Lorsque vous choisissez une méthode de contrainte de mise en conformité NAP IPsec, tenez compte des éléments ci-dessous :

- La contrainte de mise en conformité IPsec est plus complexe à implémenter que d'autres méthodes, car elle requiert une autorité HRA et une autorité de certification.
- Aucun matériel supplémentaire n'est requis pour implémenter la contrainte de mise en conformité IPsec. Il n'est pas nécessaire de mettre à niveau des commutateurs ou des protocoles WAP, alors que vous devriez le faire si vous sélectionnez la contrainte de mise en conformité 802.1X.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Vous pouvez implémenter la contrainte de mise en conformité IPsec dans n'importe quel environnement.
- La contrainte de mise en conformité IPsec est très sécurisée et difficile à contourner.
- Vous pouvez configurer IPsec pour chiffrer la communication pour plus de sécurité.
- La contrainte de mise en conformité IPsec est appliquée à la communication IPv4 et IPv6.

Contrainte de mise en conformité 802.1X



Avec la contrainte de mise en conformité 802.1X un ordinateur doit être conforme pour pouvoir obtenir un accès réseau illimité via une connexion réseau authentifiée par le protocole 802.1X ; par exemple, un commutateur d'authentification Ethernet ou un point d'accès sans fil IEEE 802.11.

Pour les ordinateurs non conformes, l'accès réseau est limité au moyen d'un profil d'accès restreint que le commutateur Ethernet ou le point d'accès sans fil place sur la connexion. Le profil d'accès restreint peut spécifier soit des filtres de paquets IP, soit un identificateur de réseau local virtuel (VLAN) qui correspond au réseau restreint. La contrainte de mise en conformité 802.1X impose les spécifications des stratégies de contrôle d'intégrité chaque fois qu'un ordinateur tente d'établir une connexion réseau authentifiée par le protocole 802.1X. Qui plus est, la contrainte de mise en conformité 802.1X analyse activement l'état d'intégrité du client NAP connecté, puis applique le profil d'accès restreint à la connexion si le client devient non conforme.

Les composants de la contrainte de mise en conformité 802.1X se composent de NPS dans Windows Server 2012 et d'un client de contrainte d'hôte de programme d'aide au personnel dans Windows 8, Windows 7, Windows Vista, Windows XP Service Pack 3, Windows Server 2008, Windows Server 2008 R2, et Windows Server 2012. La contrainte de mise en conformité 802.1X fournit l'accès réseau limité fort pour tous les ordinateurs qui accèdent au réseau par une connexion 802.1X authentifiée.

Pour implémenter la contrainte de mise en conformité 802.1X, vous devez vérifier que les commutateurs réseau ou les points d'accès sans fil prennent en charge l'authentification 802.1X. Les commutateurs ou les points d'accès sans fil agissent alors en tant que point de contrainte de mise en conformité pour des clients NAP. L'état d'intégrité du client est envoyé dans le cadre de la procédure d'authentification.

Quand un ordinateur n'est pas conforme, le commutateur le place sur un réseau VLAN distinct ou utilise des filtres de paquets pour restreindre l'accès aux serveurs de mise à jour seulement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

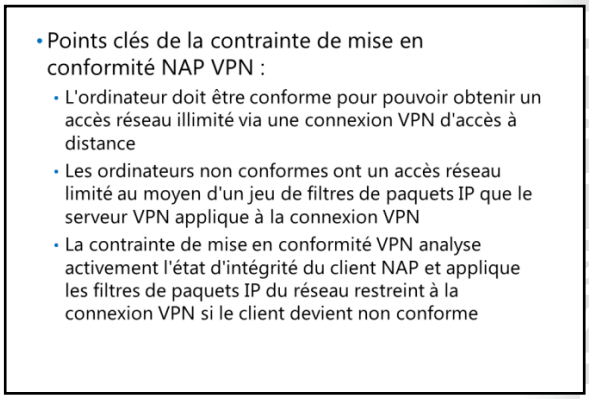
Éléments à prendre en compte pour la contrainte de mise en conformité 802.1X

Lorsque vous choisissez une méthode de contrainte de mise en conformité NAP 802.1X, tenez compte des éléments ci-dessous :

- Le commutateur ou le point d'accès sans fil qui se connecte avec le client isole les ordinateurs non conformes. Ceci est très difficile à contourner, et est par conséquent très sécurisé.
- Utilisez la contrainte de mise en conformité 802.1X pour les ordinateurs internes. Ce type de mise en conformité est approprié pour des ordinateurs du réseau local avec des connexions câblées et sans fil.
- Vous ne pouvez pas utiliser la contrainte de mise en conformité 802.1X si vos commutateurs et points d'accès sans fil ne prennent pas en charge l'utilisation du protocole 802.1X pour l'authentification.

Contrainte de mise en conformité VPN

La contrainte de mise en conformité VPN impose les spécifications des stratégies de contrôle d'intégrité chaque fois qu'un ordinateur tente d'établir une connexion VPN d'accès à distance au réseau. Qui plus est, la contrainte de mise en conformité VPN analyse activement l'état d'intégrité du client NAP, et applique les filtres de paquets IP du réseau restreint à la connexion VPN si le client devient non conforme.



Les composants de la contrainte de mise en conformité VPN comprennent le service NPS dans Windows Server 2012 et un client de contrainte de mise en conformité VPN qui fait partie du client d'accès à distance dans :

- Windows 8
- Windows 7
- Windows Vista
- Windows XP SP3
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

La contrainte de mise en conformité VPN fournit un accès réseau limité puissant pour tous les ordinateurs qui accèdent au réseau via une connexion VPN d'accès à distance. La contrainte de mise en conformité VPN utilise un jeu de filtres de paquets IP d'accès à distance pour limiter le trafic des clients VPN, afin qu'il puisse atteindre uniquement les ressources du réseau restreint. Le serveur VPN applique les filtres de paquets IP au trafic IP qu'il reçoit du client VPN et rejette silencieusement tous les paquets qui ne correspondent pas à un filtre de paquets configuré.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

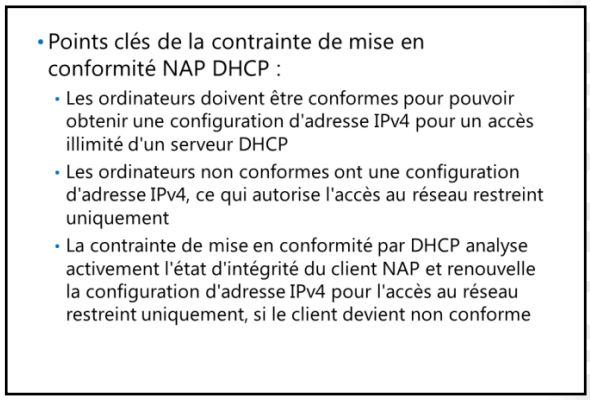
Éléments à prendre en compte pour la contrainte de mise en conformité VPN

Lorsque vous choisissez une méthode de contrainte de mise en conformité NAP VPN tenez compte des éléments ci-dessous :

- La contrainte de mise en conformité VPN est la plus adaptée lorsque vous utilisez déjà VPN. Il est peu probable que vous implémentiez des connexions VPN sur un réseau interne pour utiliser la contrainte de mise en conformité VPN.
- Utilisez la contrainte de mise en conformité VPN pour vous assurer que les membres du personnel se connectant à partir d'ordinateurs personnels n'introduisent pas de programmes malveillants dans votre réseau. Souvent les utilisateurs ne gèrent pas leurs ordinateurs personnels correctement, et ceux-ci peuvent représenter un risque élevé. Beaucoup d'utilisateurs n'ont pas d'antivirus, ou n'appliquent pas les mises à jour Windows régulièrement.
- Utilisez la contrainte de mise en conformité VPN pour vous assurer que les ordinateurs portables d'employés itinérants n'introduisent pas de programmes malveillants dans votre réseau. Les ordinateurs portables d'employés itinérants sont plus sensibles aux attaques malveillantes que les ordinateurs directement connectés au réseau d'entreprise, car ils ne peuvent pas forcément télécharger les mises à jour des virus et les mises à jour Windows en dehors du réseau d'entreprise. Ils sont également plus susceptibles de se trouver dans des environnements où un programme malveillant est présent.

Contrainte de mise en conformité DHCP

Le serveur DHCP applique les spécifications de la stratégie de contrôle d'intégrité chaque fois qu'un client DHCP tente de louer ou de renouveler une configuration d'adresse IP. Qui plus est, la contrainte de mise en conformité par DHCP analyse activement l'état d'intégrité du client NAP et, si le client devient non conforme, renouvelle la configuration d'adresse IPv4 pour l'accès au réseau restreint uniquement, si le client devient non conforme.



Les composants de la contrainte de mise en conformité par DHCP se composent d'un service Contrainte de mise en conformité par DHCP qui fait partie du service Serveur DHCP dans Windows Server 2012 et d'un client de contrainte de mise en conformité par DHCP qui fait partie du service Client DHCP dans :

- Windows 8
- Windows 7
- Windows Vista
- Windows XP SP3
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comme la contrainte de mise en conformité par DHCP repose sur une configuration d'adresse IPv4 limitée qu'un utilisateur (bénéficiant d'un accès administrateur) peut remplacer, il s'agit de la forme d'accès réseau limité la plus faible de la protection d'accès réseau dans NAP.

La configuration d'adresses DHCP limite l'accès réseau du client DHCP via sa table de routage IPv4. Étant donné que la contrainte de mise en conformité par DHCP définit la valeur 0.0.0.0 pour l'option Router DHCP, aucune passerelle par défaut n'est configurée pour l'ordinateur non conforme. La contrainte de mise en conformité par DHCP définit également le masque de sous-réseau pour l'adresse IPv4 allouée à la valeur 255.255.255.255. Il n'existe donc aucun itinéraire vers le sous-réseau lié.

Pour permettre à l'ordinateur non conforme d'accéder aux serveurs de mise à jour du réseau restreint, le serveur DHCP attribue l'option DHCP Itinéraires statiques sans classe. Cette option contient des itinéraires hôtes vers les ordinateurs du réseau restreint, tels que les serveurs DNS (Domain Name System) et de mise à jour. Le résultat final de l'accès réseau limité de DHCP est une table de configuration et de routage qui autorise uniquement la connectivité aux adresses de destination spécifiques correspondant au réseau restreint. Par conséquent, lorsqu'une application tente d'envoyer des données à une adresse IPv4 unicast (monodiffusion) différente de celles fournies via l'option Itinéraires statiques sans classe, le protocole TCP/IP retourne une erreur de routage.

Éléments à prendre en compte pour la contrainte de mise en conformité DHCP

Lorsque vous choisissez une méthode de contrainte de mise en conformité NAP DHCP tenez compte des éléments ci-dessous :

- La contrainte de mise en conformité par DHCP est facile à implémenter, et peut être appliquée à n'importe quel ordinateur avec une adresse IP dynamique.
- Il est facile de contourner la contrainte de mise en conformité par DHCP. Un client peut contourner la contrainte de mise en conformité par DHCP à l'aide d'une adresse IP statique. En outre, un ordinateur non conforme pourrait ajouter des itinéraires hôtes statiques pour atteindre les serveurs qui ne sont pas des serveurs de mise à jour.
- La contrainte de mise en conformité par DHCP n'est pas possible pour des clients IPv6. Si les ordinateurs de votre réseau utilisent les adresses IPv6 pour communiquer, la contrainte de mise en conformité par DHCP est inefficace.

Leçon 3
Configuration de NAP

Si vous souhaitez que votre déploiement de NAP fonctionne de façon optimale, il est important que vous compreniez ce que chacun des composants de protection d'accès réseau (NAP) fait, et comment ils interagissent pour protéger votre réseau. Si vous souhaitez protéger votre réseau à l'aide de la protection d'accès réseau (NAP), vous devez comprendre les impératifs requis en matière de configuration pour le client NAP, comment configurer NPS en tant que serveur de la stratégie de contrôle d'intégrité NAP, configurer des stratégies de contrôle d'intégrité et des stratégies réseau et configurer les paramètres de client et serveur. Il est également important de tester la protection d'accès réseau (NAP) avant de l'utiliser.

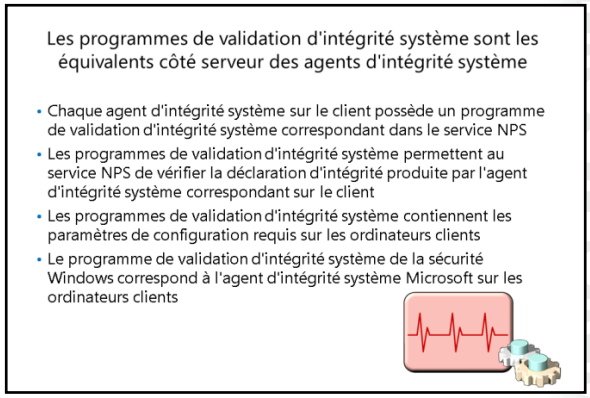
Objectifs de la leçon

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

- décrire les programmes de validation d'intégrité système ;
- expliquer l'utilisation d'une stratégie de contrôle d'intégrité ;
- expliquer l'utilisation des groupes de serveurs de mise à jour ;
- décrire les impératifs requis pour la configuration du client NAP ;
- expliquer comment activer et configurer NAP.

Qu'est-ce que les programmes de validation d'intégrité système ?

Les agents d'intégrité système et les programmes de validation d'intégrité système sont des composants d'infrastructure de protection d'accès réseau (NAP) qui assurent la validation de l'état d'intégrité. Windows 8 inclut un **programme de validation d'intégrité de la sécurité Windows** qui analyse les paramètres du Centre de sécurité Windows. Windows Server 2012 inclut un **programme de validation d'intégrité de la sécurité Windows** correspondant.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

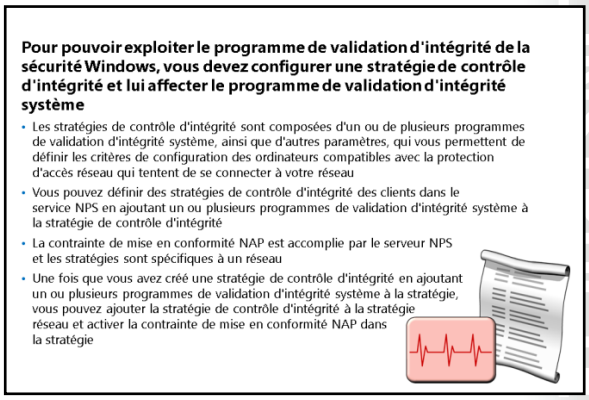
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La protection d'accès réseau est conçue pour être flexible et extensible, et elle peut interagir avec les logiciels de tous les fournisseurs qui proposent des agents d'intégrité système et des programmes de validation d'intégrité système utilisant l'API NAP. Un programme de validation d'intégrité système reçoit une déclaration d'intégrité, puis compare les informations d'état d'intégrité système fournies dans la déclaration d'intégrité à l'état d'intégrité système requis. Par exemple, si la déclaration d'intégrité provient d'un agent d'intégrité système d'antivirus et qu'elle contient le dernier numéro de version du fichier de signature antivirus, le programme de validation d'intégrité système d'antivirus correspondant peut contacter le serveur de spécification d'intégrité d'antivirus afin d'obtenir le numéro de version le plus récent et de valider la déclaration d'intégrité du client NAP.

Le programme de validation d'intégrité système renvoie une réponse à la déclaration d'intégrité au serveur d'administration NAP. Cette réponse peut contenir des informations de mise à jour indiquant comment l'agent d'intégrité système correspondant sur le client NAP peut répondre aux spécifications d'intégrité système actuelles. Par exemple, la réponse SoHR que le programme de validation d'intégrité système d'antivirus envoie peut demander à l'agent d'intégrité système d'antivirus du client NAP de se procurer la version la plus récente (en fonction du nom ou de l'adresse IP) du fichier de signature antivirus auprès d'un serveur de signatures antivirus spécifique.

Qu'est-ce qu'une stratégie de contrôle d'intégrité ?

Les stratégies de contrôle d'intégrité sont composées d'un ou de plusieurs programmes de validation d'intégrité système, ainsi que d'autres paramètres, qui vous permettent de définir les critères de configuration des ordinateurs clients pour les ordinateurs compatibles avec la protection d'accès réseau qui tentent de se connecter à votre réseau.



Lorsque des clients compatibles avec la protection d'accès réseau tentent de se connecter au réseau, l'ordinateur client envoie une déclaration d'intégrité au serveur NPS. La déclaration d'intégrité est un rapport de l'état de configuration du client, et le serveur NPS la compare aux critères définis par la stratégie de contrôle d'intégrité. Si l'état de configuration du client ne répond pas aux critères que la stratégie de contrôle d'intégrité définit, en fonction de la configuration NAP, le serveur NAP effectue l'une des opérations suivantes :

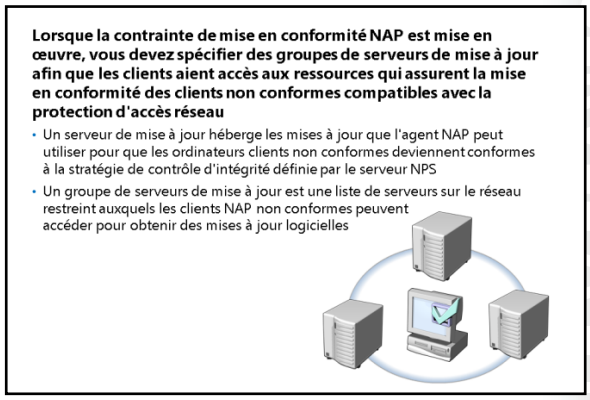
- Il rejette la demande de connexion.
- Il place le client NAP sur un réseau restreint, où il peut recevoir des mises à jour des serveurs de mise à jour qui procèdent à la mise en conformité du client avec la stratégie de contrôle d'intégrité. Une fois que la conformité du client NAP a été vérifiée et son nouvel état d'intégrité soumis à nouveau, NPS lui permet de se connecter.
- Il autorise le client NAP à se connecter au réseau bien qu'il ne soit pas conforme à la stratégie de contrôle d'intégrité.

Vous pouvez définir des stratégies de contrôle d'intégrité des clients dans le service NPS en ajoutant un ou plusieurs programmes de validation d'intégrité système à la stratégie de contrôle d'intégrité.

Une fois que vous avez configuré une stratégie de contrôle d'intégrité avec un ou plusieurs programmes de validation d'intégrité système, vous pouvez l'ajouter à la condition Stratégies de contrôle d'intégrité d'une stratégie réseau que vous souhaitez utiliser pour mettre en application la protection d'accès réseau lorsque des ordinateurs clients tentent de se connecter à votre réseau.

Qu'est-ce que les groupes de serveurs de mise à jour ?

Un groupe de serveurs de mise à jour est une liste de serveurs sur le réseau restreint qui fournissent des ressources permettant de mettre les clients non conformes en conformité avec la stratégie de contrôle d'intégrité client définie par vous.

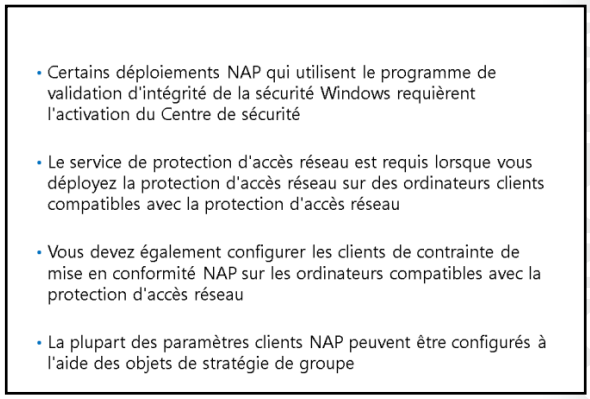


Un serveur de mise à jour héberge les mises à jour qu'un agent NAP peut utiliser pour que les ordinateurs clients non conformes deviennent conformes à la stratégie de contrôle d'intégrité définie par le serveur NPS. Par exemple, un serveur de mise à jour peut héberger des signatures antivirus. Si une stratégie de contrôle d'intégrité impose que les ordinateurs clients incluent les définitions antivirus les plus récentes, la mise à jour des ordinateurs non conformes est assurée grâce à l'interaction des composants suivants :

- un Agent d'intégrité système antivirus ;
- un programme de validation d'intégrité système antivirus ;
- un serveur de stratégie antivirus ;
- le serveur de mise à jour.

Configuration du client NAP

Gardez en mémoire les consignes de base indiquées ci-après lorsque vous configurez des clients NAP :



- Certains déploiements NAP qui utilisent le programme de validation d'intégrité de la sécurité Windows requièrent l'activation du Centre de sécurité. Le centre de sécurité n'est pas compris avec Windows Server 2008, Windows Server 2008 R2 ou Windows Server 2012.
- Vous devez activer le service de protection d'accès réseau lorsque vous déployez desordinateurs clients compatibles avec la protection d'accès réseau.
- Vous devez configurer les clients de contrainte de mise en conformité NAP sur les ordinateurs compatibles avec la protection d'accès réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Activer le Centre de sécurité dans la stratégie de groupe

Vous pouvez utiliser le centre de sécurité d'activation dans la procédure de stratégie de groupe pour activer le centre de sécurité sur les clients compatibles avec la protection d'accès réseau à l'aide de la Stratégie de groupe. Certains déploiements NAP qui utilisent le programme de validation d'intégrité de la sécurité Windows nécessitent le Centre de sécurité.

Remarque : Pour effectuer cette procédure, vous devez être membre du groupe Admins du domaine, Administrateurs de l'entreprise ou Administrateurs sur l'ordinateur local.

Pour activer le Centre de sécurité dans la stratégie de groupe :

1. Ouvrez la console Gestion des stratégies de groupe.
2. Dans l'arborescence de la console, double-cliquez sur **Stratégie Ordinateur Local**, puis sur **Configuration ordinateur**, sur **Modèles d'administration**, sur **Composants Windows**, et enfin sur **Centre de sécurité**.
3. Double-cliquez sur **Activer le Centre de sécurité (ordinateurs appartenant à un domaine uniquement)**, cliquez sur **Activé**, puis sur **OK**.

Activer le service de protection d'accès réseau sur les clients

Vous pouvez utiliser la procédure d'activation du service de protection d'accès réseau sur les clients pour activer et configurer le service de protection d'accès réseau sur des ordinateurs clients compatibles avec la protection d'accès réseau. Lorsque vous déployez la protection d'accès réseau, il est indispensable d'activer ce service.

Remarque : Pour effectuer cette procédure, vous devez être membre du groupe Admins du domaine, Administrateurs de l'entreprise ou Administrateurs sur l'ordinateur local.

Pour activer le service de protection d'accès réseau sur les ordinateurs clients :

1. Ouvrez le Panneau de configuration, cliquez sur **Système et sécurité**, puis sur **Outils d'administration**, et double-cliquez sur **Services**.
2. Dans la liste Services, faites défiler le contenu et double-cliquez sur **Agent de protection d'accès réseau**.
3. Dans la boîte de dialogue **Propriétés de Agent de protection d'accès réseau**, remplacez **Type de démarrage** par **Automatique**, puis cliquez sur **OK**.

Activer et désactiver les clients de contrainte de mise en conformité NAP

Vous pouvez utiliser la procédure d'activation et de désactivation des clients de contrainte de mise en conformité NAP pour activer ou désactiver un ou plusieurs clients de contrainte de mise en conformité NAP sur des ordinateurs compatibles avec la protection d'accès réseau. Il peut s'agir des clients suivants :

- client de contrainte de mise en conformité DHCP ;
- client de contrainte de mise en conformité d'accès à distance ;
- client de contrainte de mise en conformité EAP ;
- client de contrainte de mise en conformité IPsec (également utilisé pour les connexions DirectAccess) ;
- client de contrainte de mise en conformité Passerelle des services Terminal Server.

Pour activer et désactiver les clients de contrainte de mise en conformité NAP :

1. Ouvrez la console **Configuration du client NAP** (NAPCLCFG.MSC).
2. Cliquez sur **Clients de contrainte**. Dans le volet d'informations, cliquez avec le bouton droit sur le client de contrainte que vous souhaitez activer ou désactiver, puis cliquez sur **Activer** ou **Désactiver**.

Remarque : Pour effectuer cette procédure, vous devez être membre du groupe Administrateurs sur l'ordinateur local ou bien disposer des autorisations appropriées. Si l'ordinateur est rattaché à un domaine, les membres du groupe Admins du domaine peuvent peut-être exécuter la procédure. Par mesure de sécurité, il est conseillé d'effectuer cette procédure à l'aide de la commande **Exécuter en tant que**.

Démonstration : Configuration de NAP

Cette démonstration montre comment :

- installer le rôle de serveur NPS ;
- configurer le serveur NPS en tant que serveur de stratégie de contrôle d'intégrité NAP ;
- configurer les stratégies de contrôle d'intégrité ;
- configurer des stratégies réseau pour les ordinateurs conformes ;
- configurer des stratégies réseau pour les ordinateurs non conformes ;
- configurer le rôle de serveur DHCP pour la protection d'accès réseau ;
- configurer les paramètres NAP du client ;
- tester NAP.

Procédure de démonstration

Installer le rôle de serveur NPS

1. Basculez vers LON-DC1 et connectez-vous en tant qu'administrateur de domaine.
2. Ouvrez le Gestionnaire de serveur, puis installez le rôle de **Stratégie réseau et services d'accès**.

Configurer le serveur NPS en tant que serveur de stratégie de contrôle d'intégrité NAP

1. Ouvrez la console Serveur NPS.
2. Configurez le **Programme de validation d'intégrité de la sécurité Windows** pour demander que tous les ordinateurs sous Windows 8 exécutent un pare-feu.

Configurer les stratégies de contrôle d'intégrité

1. Créez une stratégie de contrôle d'intégrité appelée **Conforme** qui spécifier la condition **Réussite de tous les contrôles SHV pour le client**.
2. Créez une autre stratégie de contrôle d'intégrité appelée **Non conforme**qui spécifie la condition **Échec d'un ou de plusieurs contrôles SHV pour le client**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configurer des stratégies réseau pour les ordinateurs conformes

1. Désactivez les deux stratégies réseau existantes ; elles empêcheraient le traitement des stratégies que vous êtes sur le point de créer.
2. Créez une nouvelle stratégie réseau appelée **Conforme – Accès Complet** ayant une condition de stratégie de contrôle d'intégrité **Conforme**. Un accès illimité est accordé aux ordinateurs.

Configurer des stratégies réseau pour les ordinateurs non conformes

- Créez une nouvelle stratégie réseau appelée **Non conforme-restreint** ayant une condition de stratégie de contrôle d'intégrité **Non conforme**. Un accès limité est accordé aux ordinateurs.

Configurer le rôle de serveur DHCP pour la protection d'accès réseau

1. Ouvrez la console DHCP.
2. Modifiez les propriétés de la portée IPv4 pour prendre en charge la protection d'accès réseau.
3. Créez une nouvelle stratégie DHCP qui alloue des options de portée DHCP appropriées aux ordinateurs non conformes. Ces options attribuent un suffixe DNS restricted.Adatum.com.

Configurer les paramètres NAP du client

1. Activez le **Client de contrainte de quarantaine DHCP** sur LON-CL1.
2. Activez le service **Agent de protection d'accès réseau**.
3. Utilisez la console de gestion de stratégie de groupe locale pour activer le centre de sécurité.
4. Reconfigurez LON-CL1 pour obtenir une adresse IP à partir d'un serveur DHCP.

Tester NAP

1. Vérifiez la configuration obtenue avec la commande **ipconfig**.
2. Désactivez et arrêtez **Pare-feu Windows** service.
3. Dans la zone de barre d'état système, cliquez sur la fenêtre contextuelle **Protection d'accès réseau**. Examinez le contenu de la boîte de dialogue **Protection d'accès réseau**. Cliquez sur **Fermer**.
4. Vérifiez la configuration obtenue avec la commande **ipconfig**.
5. Notez que l'ordinateur a un masque de sous-réseau de 255.255.255.255 et un suffixe DNS restricted.Adatum.com. Ne fermez aucune fenêtre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Analyse et résolution des problèmes du système NAP

L'opération de résolution des problèmes et d'analyse de la structure NAP est une tâche d'administration importante en raison des différents niveaux de technologie, notamment de la diversité des compétences et des connaissances préalables indispensables pour chaque méthode de contrainte de mise en conformité NAP. Des journaux de suivi sont disponibles pour la protection d'accès réseau, mais ils sont désactivés par défaut. Ces journaux ont une double utilité : ils permettent de résoudre les problèmes et d'évaluer l'intégrité et la sécurité d'un réseau.

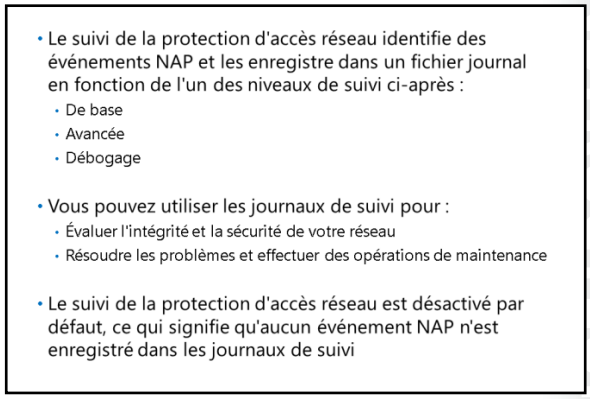
Objectifs de la leçon

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

- Décrivez comment le suivi NAP peut aider à surveiller et résoudre la protection d'accès réseau (NAP).
- Expliquez comment configurer le suivi NAP.
- Dépannez la protection d'accès réseau (NAP) avec Netsh.
- Utilisez le journal des événements NAP pour corriger NAP.

Qu'est-ce que le suivi NAP ?

Outre les recommandations générales précédentes, vous pouvez utiliser la console Configuration du client NAP pour configurer le suivi NAP. Le suivi, qui consiste à enregistrer les événements NAP dans un fichier journal, est utile pour la résolution des problèmes et la maintenance. Vous pouvez aussi utiliser les journaux de suivi pour évaluer l'intégrité et la sécurité de votre réseau. Vous pouvez configurer trois niveaux de suivi : De base, Avancé et Débogage.



Activez le suivi NAP quand :

- Vous souhaitez résoudre des problèmes liés à la protection d'accès réseau.
- Vous souhaitez évaluer l'intégrité et la sécurité globales des ordinateurs de votre organisation.

En plus de la journalisation du suivi, vous pouvez afficher des journaux de gestion de comptes NPS. Ces journaux peuvent contenir des informations utiles sur la protection d'accès réseau (NAP). Par défaut, les journaux de gestion de comptes NPS se trouvent dans %systemroot%\system32\logfiles.

Les journaux suivants peuvent contenir des informations liées à la protection d'accès réseau (NAP) :

- IASNAP.LOG. Ce journal contient des données détaillées au sujet des processus de protection d'accès réseau (NAP), de l'authentification NPS et de l'autorisation NPS.
- IASSAM.LOG. Ce journal contient des données détaillées au sujet de l'authentification utilisateur et des autorisations.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration du suivi NAP

Les deux outils suivants sont disponibles pour configurer le suivi de la protection d'accès réseau : La console Configuration du client NAP, qui fait partie de l'interface utilisateur Windows, et **netsh** qui est un outil de ligne de commande.

Utilisation de l'interface utilisateur Windows

Vous pouvez utiliser l'interface utilisateur Windows afin d'activer ou de désactiver le suivi de la protection d'accès réseau et de spécifier le niveau de détail enregistré en procédant comme suit :

1. Ouvrez la console Configuration du client NAP en exécutant **napclcfg.msc**.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur **Configuration du client NAP (ordinateur local)**, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de Configuration du client NAP (ordinateur local)**, sélectionnez **Activé** ou **Désactivé**.

Remarque : Pour effectuer cette procédure, vous devez être membre du groupe Administrateurs sur l'ordinateur local ou bien disposer des autorisations appropriées. Par mesure de sécurité, il est conseillé d'effectuer cette opération à l'aide de la commande **Exécuter en tant que**.

4. Si l'option Activé est choisie, sous **Spécifier le niveau de détails à inscrire dans les journaux de suivi**, sélectionnez **De base**, **Avancé** ou **Débogage**.

Utilisation d'un outil en ligne de commande

Pour utiliser un outil en ligne de commande afin d'activer ou de désactiver le suivi NAP et de spécifier le niveau de détail enregistré, procédez comme suit :

1. Ouvrez une invite de commandes avec élévation de privilèges.
2. Pour activer ou désactiver le suivi NAP, effectuez l'une des opérations suivantes :
   - Pour activer le suivi NAP et configurer le niveau d'enregistrement de base ou avancé, tapez : **netsh NAP client set tracing state=enable level =[advanced or basic]**
   - Pour activer le suivi NAP afin de consigner des informations de débogage, tapez : **netsh NAP client set tracing state=enable level =verbose**
   - Pour désactiver le suivi NAP, tapez : **netsh NAP client set tracing state=disable**

Remarque : Pour effectuer cette procédure, vous devez être membre du groupe Administrateurs sur l'ordinateur local ou bien disposer des autorisations appropriées. Par mesure de sécurité, il est conseillé d'effectuer cette opération à l'aide de la commande **Exécuter en tant que**.

Affichage des fichiers journaux

Pour afficher les fichiers journaux, accédez au répertoire %systemroot%\tracing\nap, puis ouvrez le journal de suivi que vous souhaitez consulter.

Demonstration

Cette démonstration montre comment :

- configurer le suivi à partir de l'interface utilisateur graphique ;
- configurer le suivi à partir de la ligne de commande.

Procédure de démonstration

Configurer le suivi à partir de l'interface utilisateur graphique

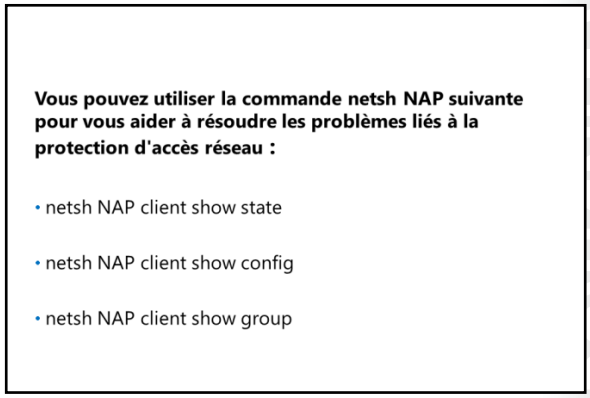
1. Sur LON-CL1, ouvrez la console NAPCLCFG – [Configuration du client NAP (ordinateur local)].
2. À partir des propriétés **Configuration de client NAP (ordinateur local)**, activez le suivi **Avancé**.

Configurer le suivi à partir de la ligne de commande

- À l'invite de commandes, tapez **netsh NAP client set tracing state = enable** et appuyez sur Entrée.

Résolution des problèmes de la protection d'accès réseau

Pour résoudre des problèmes de protection d'accès réseau (NAP), utilisez les outils suivants.



Commandes Netsh

Utilisez la commande de protection d'accès réseau netsh pour résoudre des problèmes de protection d'accès réseau (NAP). La commande suivante affiche l'état d'un client NAP, y compris ce qui suit :

- État de restriction
- État des clients de contrainte
- État des agents d'intégrité système installés
- Groupes de serveurs approuvés qui ont été configurés

```
netsh NAP client show state
```

La commande suivante affiche les paramètres de configuration locaux sur un client NAP, notamment :

- Paramètres de chiffrement
- Paramètres du client de contrainte de mise en conformité
- Paramètres des groupes de serveurs approuvés
- Paramètres du suivi de client qui ont été configurés

```
netsh NAP client show config
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La commande suivante affiche les paramètres de configuration de la stratégie de groupe sur un client NAP, notamment :

- Paramètres de chiffrement
- Paramètres du client de contrainte de mise en conformité
- Paramètres des groupes de serveurs approuvés
- Paramètres du suivi de client qui ont été configurés

```
netsh NAP client show group
```

Résolution des problèmes de la protection d'accès réseau avec les journaux d'événements

Les services NAP enregistrent les événements liés à la protection d'accès réseau dans les journaux des événements Windows. Pour afficher ces événements, ouvrez l'observateur d'événements, sélectionnez **Vues personnalisées**, sélectionnez **Rôles serveur**, puis **Stratégie réseau et services d'accès**. Les événements suivants fournissent des informations au sujet des services de protection d'accès réseau (NAP) qui s'exécutent sur un serveur NPS :

ID d'événement	Signification
6272	L'authentification a réussi
6273	L'authentification n'a pas réussi
6274	Un problème de configuration existe
6276	Le client NAP est mis en quarantaine
6277	Le client NAP est en période d'essai
6278	Le client NAP bénéficie d'un accès complet

- ID d'événement 6272. Accès accordé par serveur NPS à un utilisateur.

  Se produit quand un client NAP authentifie avec succès, et, selon son état d'intégrité, obtient l'accès complet ou limité au réseau.

- ID d'événement 6273. Accès refusé par le serveur NPS à un utilisateur.

  Se produit quand un problème d'authentification ou d'autorisation surgit et qu'il est associé à un code de raison.

- ID d'événement 6274. Le serveur NPS a ignoré la demande d'un utilisateur.

  Se produit quand un problème de configuration surgit, ou si les paramètres de client RADIUS sont incorrects ou si NPS ne peut pas créer des journaux de gestion de comptes.

- ID d'événement 6276. Utilisateur mis en quarantaine par le serveur NPS.

  Se produit quand la demande d'accès client correspond à une stratégie réseau qui est configurée avec un paramètre de contrainte de mise en conformité NAP de type **Autoriser un accès limité**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- ID d'événement 6277. Le serveur NPS a accordé l'accès à un utilisateur, mais l'a mis en période d'essai parce que l'hôte ne respecte pas la stratégie de contrôle d'intégrité définie.

  Se produit quand la demande d'accès client correspond à une stratégie réseau qui est configurée avec un paramètre de contrainte de mise en conformité NAP de type **Autoriser l'accès réseau complet pendant une période limitée quand la date spécifiée dans la stratégie est passée**.

- ID d'événement 6278. Le serveur NPS a accordé l'accès complet à un utilisateur parce que l'hôte respecte la stratégie de contrôle d'intégrité définie.

  Se produit quand la demande d'accès client correspond à une stratégie réseau qui est configurée avec un paramètre de contrainte de mise en conformité NAP de type **Autoriser un accès réseau complet**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation de la protection d'accès réseau

Scénario

A. Datum est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données situés à Londres pour s'occuper du siège social et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

Pour améliorer la sécurité et les exigences de conformité, A. Datum doit étendre sa solution VPN pour inclure la protection d'accès réseau (NAP). Vous devez trouver une manière de le vérifier et, s'il y a lieu, mettre automatiquement les ordinateurs client en conformité chaque fois qu'ils se connectent à distance à l'aide de la connexion VPN. Vous allez réaliser cet objectif à l'aide de NPS pour créer des paramètres de validation d'intégrité système, des stratégies réseau et de contrôle d'intégrité et configurer la protection d'accès réseau (NAP) pour vérifier l'intégrité des clients et y remédier.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- configurer des composants NAP ;
- configurer l'accès VPN ;
- configurer les paramètres clients pour prendre en charge NAP.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-RTR 22411B-LON-CL2
Nom d'utilisateur	**ADATUM\Administrateur**
Mot de passe	**Pa$$w0rd**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
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. Effectuez les étapes 2 à 4 pour **22411B-LON-CL2** et **22411B-LON-RTR**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configuration des composants NAP

Scénario

La première étape pour implémenter la conformité et la sécurité consiste à configurer des composants de protection d'accès réseau (NAP), tels que des exigences relatives aux certificats, des stratégies de réseau et d'intégrité et des stratégies de demande de connexion.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les exigences des certificats clients et de serveur
2. Configurer les stratégies de contrôle d'intégrité
3. Configurer les stratégies réseau
4. Configurer des stratégies de demande de connexion pour VPN

▶ Tâche 1 : Configurer les exigences des certificats clients et de serveur

1. Basculez sur le serveur virtuel LON-DC1.
2. Ouvrez l'outil **Autorité de certification**.
3. Dans la Console des modèles de certificat, ouvrez les propriétés du modèle de certificat **Ordinateur**.
4. Sous l'onglet **Sécurité**, accordez l'autorisation **Autoriser l'inscription** au groupe **Utilisateurs authentifiés**.
5. Redémarrez l'Autorité de certification.
6. Fermez l'outil **Autorité de certification**.

▶ Tâche 2 : Configurer les stratégies de contrôle d'intégrité

1. Basculez vers l'ordinateur LON-RTR.
2. Créez une console de gestion à l'aide de **mmc.exe**.
3. Ajoutez le composant logiciel enfichable **Certificats** en mettant l'accent sur le compte d'ordinateur local.
4. Naviguez jusqu'à **Magasin** de certificats personnel et **Demander un nouveau certificat**.
5. Sur la page **Sélectionner la stratégie d'inscription de certificat**, cliquez sur **Stratégie d'inscription à Active Directory**, puis sur **Suivant**.
6. Inscrivez le certificat **Ordinateur** répertorié.
7. Fermez la console sans enregistrer ses paramètres.
8. Installez le serveur NPS à l'aide du **Gestionnaire de serveur** avec les services de rôle suivants :
   - Serveur NPS
9. Ouvrez la console **Serveur NPS**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Sous **Protection d'accès réseau**, ouvrez la configuration par défaut pour le **Programme de validation d'intégrité de la sécurité Windows**.
11. Sous l'onglet **Windows 8/Windows 7/Windows Vista**, désactivez toutes les cases à cocher à l'exception de **Un pare-feu est activé pour toutes les connexions réseau**.
12. Créez une stratégie de contrôle d'intégrité avec les paramètres suivants :
    - Nom : **Conforme**
    - Contrôles du client par les programmes de validation d'intégrité système (SHV) : **Réussite de tous les contrôles SHV pour le client**
    - Programme de validation d'intégrité système utilisés dans cette stratégie de contrôle d'intégrité : **Programme de validation d'intégrité de la sécurité Windows**
13. Créez une stratégie de contrôle d'intégrité avec les paramètres suivants :
    - Nom : **Non conforme**
    - Contrôles du client par les programmes de validation d'intégrité système (SHV) : **Échec d'un ou de plusieurs contrôles SHV pour le client**
    - Programme de validation d'intégrité système utilisés dans cette stratégie de contrôle d'intégrité : **Programme de validation d'intégrité de la sécurité Windows**

▶ Tâche 3 : Configurer les stratégies réseau

1. Désactivez toutes les stratégies réseau existantes.
2. Configurez une nouvelle stratégie réseau avec les paramètres suivants :
    - Nom : **Compliant-Full-Access**
    - Conditions : **Stratégies de contrôle d'intégrité**, **Conforme**
    - Autorisations d'accès : **Accès accordé**
    - Paramètres : **Contrainte de mise en conformité NAP**, **Autoriser un accès complet au réseau**
3. Configurez une nouvelle stratégie réseau avec les paramètres suivants :
    - Nom : **Non conforme-restreint**
    - Conditions : **Stratégies de contrôle d'intégrité**, **Non Conforme**
    - Autorisations d'accès : **Accès accordé**
    - Paramètres : **Mise en conformité NAP**, **Autoriser un accès limité** est sélectionné et **Activer la mise à jour automatique des ordinateurs clients** n'est pas sélectionné.
    - Filtres IP : **Filtre d'entrée IPv4**
        - Réseau de destination : **172.16.0.10/255.255.255.255**
        - Filtre de sortie IPv4 :
          Réseau source : **172.16.0.10/255.255.255.255**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Configurer des stratégies de demande de connexion pour VPN

1. Désactivez les stratégies de demande de connexion existantes.
2. Créez une **stratégie de demande de connexion** avec les paramètres suivants :
   - Nom de la stratégie : **Connexions VPN**
   - Type de serveur d'accès réseau : **Serveur d'accès à distance (VPN-Dial up)**
   - Conditions, type de tunnel : **L2TP, SSTP et PPTP**
   - Authentifier les demandes sur ce serveur : Activé
   - Sur la page **Spécifier les méthodes d'authentification**, effectuez ce qui suit :
     a. Sélectionnez **Remplacer les paramètres d'authentification de stratégie réseau**.
     b. Ajoutez **Microsoft : PEAP (Protected EAP)**.
     c. Ajoutez **Microsoft : Mot de passe sécurisé (EAP-MSCHAP version 2)**.
     d. Modifiez **Microsoft : PEAP (Protected EAP)** pour vous assurer que l'option **Appliquer la protection d'accès réseau** est activée.

Résultats : À la fin de cet exercice, vous devriez avoir installé et configuré les composants requis de protection d'accès réseau (NAP), créé les stratégies d'intégrité et réseau et créé les stratégies de demande de connexion.

Exercice 2 : Configuration de l'accès VPN

Scénario

Après avoir configuré la protection d'accès réseau (NAP), vous devez configurer un serveur VPN, puis activer le protocole PING via le pare-feu à des fins de test.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer un serveur VPN
2. Autoriser les tests ping à des fins de test

▶ Tâche 1 : Configurer un serveur VPN

1. Sur LON-RTR, ouvrez **Routage et accès distant**.
2. Désactivez le routage et l'accès distant.
3. Sélectionnez **Configurer et activer le routage et l'accès à distance**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR ICT UNIQUEMENT

4. Utilisez les paramètres suivants pour terminer la configuration :
   a. Sélectionnez **Accès à distance (connexion à distance ou VPN)**.
   b. Activer la case à cocher **VPN**.
   c. Sélectionnez l'interface appelée **Public**, et désactivez la case à cocher **Sécuriser l'interface sélectionnée en configurant des filtres de paquet statiques**.
   d. Sous **Attribution d'adresses IP**, À partir d'une plage d'adresses spécifiée : **172.16.0.100** à **172.16.0.110**
   e. Effectuez le processus en acceptant les valeurs par défaut quand vous recevez une invite, puis en cliquant sur **OK** pour confirmer tous les messages.
5. Dans **Serveur NPS**, cliquez sur le nœud **Stratégies de demande de connexion**, et vérifiez que **Stratégie du service Routage et accès à distance Microsoft** est désactivé. Ceci a été créé automatiquement quand le routage et l'accès à distance ont été activés.
6. Fermez la console de gestion NPS, puis la console Routage et accès distant.

▶ Tâche 2 : Autoriser les tests ping à des fins de test

1. Sur LON-RTR, ouvrez **Pare-feu Windows avec fonctions avancées de sécurité**.
2. Créez une règle de trafic entrant ayant les propriétés suivantes :
   - Type : Personnalisée
   - Tous les programmes
   - Type de protocole : Choisissez **ICMPv4**, puis cliquez sur **Perso…**
   - Types d'ICMP spécifiques : **Requête d'écho**
   - Étendue par défaut
   - Action : **Autoriser la connexion**
   - Profil par défaut
   - Nom : **Requête d'écho ICMPv4**
3. Fermez la console Pare-feu Windows avec fonctions avancées de sécurité.

Résultats : À la fin de cet exercice, vous aurez créé un serveur VPN et configuré des communications entrantes.

Exercice 3 : Configuration des paramètres clients pour prendre en charge la protection d'accès réseau (NAP)

Scénario

Dans cet exercice, vous allez activer la connexion d'un client VPN au réseau Adatum. Vous allez ensuite activer et configurer les composants NAP requis côté client.

Les tâches principales de cet exercice sont les suivantes :

1. Activer une méthode de contrainte de mise en conformité NAP d'un client
2. Établir une connexion VPN
3. Pour préparer le module suivant

▶ Tâche 1 : Activer une méthode de contrainte de mise en conformité NAP d'un client

1. Basculez vers l'ordinateur LON-CL2.
2. Exécutez l'outil **Configuration du client NAP** (napclcfg.msc).
3. Sous **Clients de contrainte**, activez **Client de contrainte de quarantaine EAP**.
4. Fermez l'outil Configuration du client NAP.
5. Exécutez **services.msc**, puis configurez le service **Agent de protection d'accès réseau** pour qu'il démarre automatiquement.
6. Démarrez le service.
7. Fermez la console Services.
8. Ouvrez l'**Éditeur de stratégie de groupe locale** (gpedit.msc), puis activez le paramètre **Stratégie Ordinateur local/Configuration ordinateur/Modèles d'administration/ Composants Windows/Centre de sécurité/Activer le Centre de sécurité (ordinateurs appartenant à un domaine uniquement)**.
9. Fermez l'Éditeur de stratégie de groupe locale.

▶ Tâche 2 : Établir une connexion VPN

1. Sur LON-CL2, créez une connexion VPN avec les propriétés suivantes :
   - Adresse Internet de connexion : **10.10.0.1**
   - Nom de la destination : **VPN Adatum**
   - Autoriser d'autres personnes à utiliser cette connexion : **activé**
2. Une fois le VPN créé, modifiez ses paramètres en affichant les propriétés de la connexion, puis sélectionnez l'onglet **Sécurité**. Utilisez les paramètres suivants pour reconfigurer VPN :
   - Type d'authentification : **Microsoft : PEAP (Protected EAP) (chiffrement activé)**
   - Propriétés de ce type d'authentification :
   - Valider le certificat du serveur : **activé**
   - Connexion à ces serveurs **désactivé**
   - Méthode d'authentification : **Mot de passe sécurisé (EAP-MSCHAP v2)**
   - Activer la reconnexion rapide : désactivé
   - Contraindre la mise en conformité NAP : **activé**
3. Testez la connexion VPN :
   - Dans la fenêtre Connexions réseau, connectez la connexion **VPN Adatum**
   - Affichez les détails de la boîte de dialogue Alerte de sécurité Windows. Vérifiez que les informations de certificat de connexion correctes sont affichées, et cliquez sur **Connexion**.
4. À l'invite de commandes, exécutez la commande **ipconfig /all** pour vérifier que l'option **État de quarantaine du système** est **Non restreint**.
5. Ping **172.16.0.10**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Déconnectez le VPN Adatum.
7. Basculez vers LON-RTR.
8. Ouvrez le serveur NPS.
9. Dans la configuration par défaut du programme de validation d'intégrité de la sécurité Windows, activez l'option **Restreindre l'accès des clients qui n'ont pas intallé toutes les mises à jour de sécurité disponibles ne sont pas installées** sur la page **Windows 8/Windows 7/Windows Vista**.
10. Rebasculez vers LON-CL2, puis reconnectez VPN.
11. Exécutez la commande **ipconfig /all** pour vérifier que l'état de l'option **État de quarantaine du système** est **Restreint**.
12. Déconnectez la connexion VPN.

Résultats : À la fin de cet exercice, vous devriez avoir créé une nouvelle connexion VPN sur LON-CL2, et avoir activé et testé NAP sur LON-CL2.

▶ Tâche 3 : Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial de tous les ordinateurs virtuels. Pour cela, 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 **22411B-LON-CL2**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22411B-LON-RTR** et **22411B-LON-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quelles sont les trois principales configurations de client que vous devez configurer pour la plupart des déploiements NAP ?

Question : Vous souhaitez évaluer l'intégrité et la sécurité globales du réseau sur lequel la protection d'accès réseau est mise en œuvre. Que devez-vous faire pour commencer à enregistrer les événements NAP ?

Question : Sur un ordinateur client, quelles étapes devez-vous effectuer pour vérifier que son intégrité est évaluée ?

Outils

Outil	Utilisation	Emplacement
Services	Permet d'activer et de configurer le service NAP sur les ordinateurs clients.	Cliquez sur **Accueil**, sur **Panneau de configuration**, sur **Système et maintenance**, sur **Outils d'administration**, puis double-cliquez sur **Services**.
Netsh NAP	Si vous utilisez **netsh**, vous pouvez créer des scripts pour configurer un ensemble de protection d'accès réseau (NAP) automatiquement, et afficher la configuration et le statut du service client NAP.	Ouvrez une fenêtre de commande avec des droits administratifs, et tapez **netsh –c nap**. Vous pouvez taper **help** pour obtenir la liste complète des commandes disponibles.
Stratégie de groupe	Certains déploiements NAP qui utilisent le programme de validation d'intégrité de la sécurité Windows imposent l'activation du Centre de sécurité.	Activez le paramètre **Activer le Centre de sécurité (ordinateurs appartenant à un domaine uniquement)** dans les sections Configuration de l'ordinateur/Modèles d'administration/Composants Windows/Centre de sécurité de la stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 10

Optimisation des services de fichiers

Table des matières :

Vue d'ensemble du module **10-1**

Leçon 1 : Vue d'ensemble de FSRM **10-3**

Leçon 2 : Utilisation de FSRM pour gérer les quotas, les filtres de fichiers et les rapports de stockage **10-10**

Leçon 3 : Implémentation des tâches de classification et de gestion de fichiers **10-21**

Atelier pratique A : Configuration des quotas et du filtrage des fichiers à l'aide de FSRM **10-28**

Leçon 4 : Vue d'ensemble de DFS **10-32**

Leçon 5 : Configuration des espaces de noms DFS **10-41**

Leçon 6 : Configuration et résolution des problèmes de la réplication DFS **10-46**

Atelier pratique B : Implémentation de DFS **10-50**

Contrôle des acquis et éléments à retenir **10-55**

Vue d'ensemble du module

Les fichiers se trouvant sur vos serveurs changent constamment, en fonction du contenu qui est ajouté, supprimé et modifié.

Le rôle serveur Service de fichiers et de stockage de Windows Server® 2012 est conçu pour aider les administrateurs dans un environnement d'entreprise à gérer le volume de données, qui est en constante augmentation et évolution. Quand les besoins de stockage changent en même temps que les données stockées, vous devez gérer une infrastructure de stockage de plus en plus volumineuse et complexe. Par conséquent, pour répondre aux besoins de votre organisation, vous devez comprendre et déterminer la manière dont les ressources de stockage existantes sont utilisées.

Ce module vous présente le Gestionnaire de ressources du serveur de fichiers (FSRM) et le système de fichiers DFS (Distributed File System), deux technologies que vous pouvez utiliser pour résoudre et gérer ces problèmes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Objectifs

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

- décrire FSRM ;
- utiliser FSRM pour gérer les quotas, les filtres de fichiers et les rapports de stockage ;
- implémenter des tâches de classification et de gestion de fichiers ;
- décrire le système de fichiers DFS ;
- configurer des espaces de noms DFS ;
- configurer et résoudre les problèmes de réplication DFS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble de FSRM

Le Gestionnaire de ressources du serveur de fichiers (FSRM) est un ensemble d'outils qui vous permettent de comprendre, contrôler et gérer la quantité et le type de données enregistrées sur vos serveurs. FSRM vous permet de placer des quotas sur les volumes de stockage, filtrer les fichiers et dossiers, générer des rapports de stockage complets, contrôler l'infrastructure de classification des fichiers, et utiliser des tâches de gestion de fichiers pour réaliser des actions programmées sur des ensembles de fichiers. Ces outils vous aident à surveiller les ressources de stockage existantes et à planifier et implémenter les modifications de stratégie à venir.

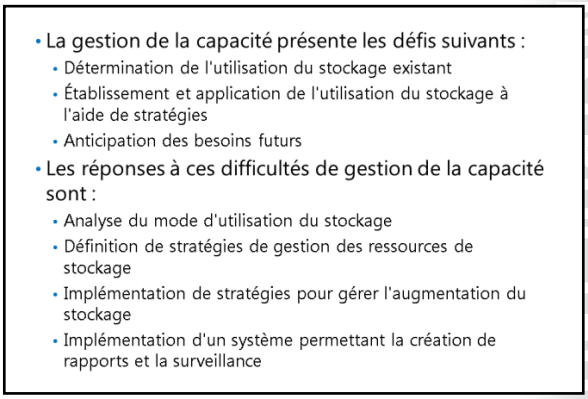
Objectifs de la leçon

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

- décrire les principales difficultés en matière de gestion de la capacité ;
- décrire les fonctionnalités disponibles dans FSRM ;
- expliquer comment installer et configurer le service de rôle FSRM.

Compréhension des défis en matière de gestion de la capacité

La gestion de la capacité est un processus proactif visant à déterminer les besoins actuels et futurs en capacité pour l'environnement de stockage de votre entreprise. À mesure que la taille et la complexité des données augmentent, le besoin de gestion de la capacité croît également. Pour répondre efficacement aux besoins de stockage de votre organisation, vous devez suivre la capacité de stockage disponible, évaluer l'espace de stockage dont vous avez besoin à des fins d'expansion, et déterminer la manière dont vous exploitez le stockage dans votre environnement.



Principales difficultés en matière de gestion de la capacité

La gestion de la capacité implique les difficultés principales suivantes :

- Détermination de l'utilisation du stockage existant. Pour gérer votre environnement de stockage et simplifier au maximum la tâche de gestion de la capacité, vous devez comprendre les besoins de stockage actuels de votre environnement. Le fait de connaître la quantité de données stockées sur vos serveurs et de savoir quels types de données sont stockés et comment ces données sont actuellement utilisées constitue le point de référence pour mesurer les divers aspects de la gestion de la capacité dans votre environnement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Établissement et application de stratégies d'utilisation du stockage. La gestion de la capacité vous garantit que votre environnement de stockage est utilisé au maximum de ses capacités. Il est important de maîtriser la croissance afin de veiller à ne pas submerger l'environnement de stockage par un stockage de données non planifié ou non autorisé sur vos serveurs. Les données de médias modernes telles que l'audio, la vidéo et les fichiers graphiques consomment une grande quantité d'espace de stockage. Si elles ne sont pas contrôlées, le stockage non autorisé de ces types de fichiers peut consommer l'espace qui est requis pour un usage professionnel légitime.
- Anticipation des besoins futurs. Les besoins de stockage changent constamment. Les nouveaux projets et les nouvelles initiatives d'organisation requièrent davantage d'espace de stockage. Il en va de même pour les nouvelles applications et les données importées. Si vous n'êtes pas en mesure d'anticiper ces événements ou de vous y préparer, votre environnement de stockage risque de ne pas pouvoir répondre aux besoins de stockage.

Prise en compte des difficultés en matière de gestion de la capacité

Pour relever ces défis majeurs, vous devez implémenter des mesures basiques de gestion de la capacité afin de gérer de façon proactive l'environnement de stockage et d'éviter que ces défis deviennent des problèmes. Vous trouverez ci-après une liste de mesures de gestion de la capacité qui vous permet de gérer votre environnement de stockage de manière proactive :

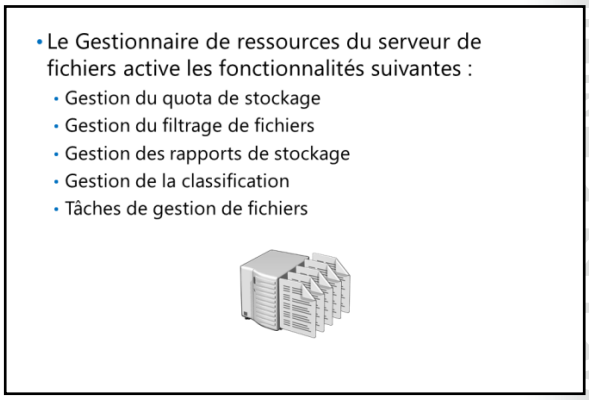
- Analyser le mode d'utilisation du stockage. La première étape en matière de gestion de la capacité consiste à analyser l'environnement de stockage actuel. Une analyse précise commence avec les outils appropriés qui fournissent des informations exploitables et organisées concernant l'état actuel de votre environnement de stockage.
- Définir des stratégies de gestion des ressources de stockage. Il est indispensable de s'appuyer sur un ensemble fiable de stratégies pour gérer l'environnement de stockage actuel et s'assurer que la croissance du stockage progresse de façon maîtrisable et prévisible. Empêcher l'enregistrement des fichiers non autorisés sur vos serveurs, vérifier que les données sont stockées au bon emplacement et que les utilisateurs disposent de l'espace de stockage nécessaire font partie des principales questions auxquelles vos stratégies de gestion de la capacité sont susceptibles de répondre.
- Implémenter des stratégies pour gérer l'augmentation du stockage. Après l'implémentation des stratégies de gestion de la capacité, vous devez disposer d'un outil efficace pour vérifier que ces stratégies sont techniquement appliquées. Les quotas qui sont définis pour le stockage des données d'un utilisateur doivent être gérés, l'enregistrement des fichiers restreints doit être empêché, et les fichiers professionnels doivent être stockés aux emplacements appropriés.
- Implémenter un système permettant la création de rapports et la surveillance. Établissez un système de création de rapports et de notification pour vous informer sur l'application des stratégies. Ces rapports doivent compléter ceux concernant l'état général de votre système de gestion de la capacité et de la situation de stockage des données.

  Question : Quels sont les défis en matière de gestion de la capacité auxquels vous avez été ou êtes confrontés dans votre environnement ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que FSRM ?

FSRM est un service du rôle Services de fichiers dans Windows Server 2012. Vous pouvez l'installer dans le cadre du rôle Services de fichiers via le Gestionnaire de serveur. Ensuite, vous pouvez utiliser la console FSRM pour gérer FSRM sur votre serveur. FSRM est destiné à agir en tant que solution de gestion de la capacité pour votre serveur Windows Server 2012. Il fournit un ensemble fiable d'outils et de fonctionnalités qui vous permettent de gérer et surveiller la capacité de stockage de votre serveur avec efficacité.



FSRM contient cinq composants qui fonctionnent ensemble pour fournir une solution de gestion de la capacité.

Gestion de quota

La gestion de quota est un composant qui vous permet de créer, de gérer et d'obtenir des informations sur les quotas. Ces informations sont ensuite utilisées pour fixer des limites de stockage sur des volumes ou des dossiers (et leur contenu). En définissant des seuils de notification, vous pouvez envoyer des notifications par courrier électronique, enregistrer un événement, exécuter une commande ou un script, ou générer des rapports lorsque les utilisateurs s'approchent d'un quota ou le dépassent. La gestion de quota vous permet également de créer et gérer des modèles de quota afin de simplifier le processus de gestion de quota.

Gestion du filtrage de fichiers

La gestion du filtrage de fichiers est un composant qui vous permet de créer, de gérer et d'obtenir des informations sur les filtres de fichiers. Vous pouvez utiliser ces informations pour empêcher le stockage de types de fichiers spécifiques sur un volume ou un dossier ou pour vous informer quand les utilisateurs enregistrent ces types de fichiers. Lorsque les utilisateurs tentent d'enregistrer des fichiers non autorisés, le filtrage de fichiers peut bloquer le processus et informer les administrateurs pour qu'ils autorisent la gestion proactive.

À l'instar de la gestion de quota, la gestion du filtrage de fichiers vous permet de créer et gérer des modèles de filtre de fichiers pour simplifier la gestion du filtrage de fichiers. Vous pouvez également créer des groupes de fichiers qui vous permettent de déterminer les types de fichiers pouvant être bloqués ou autorisés.

Gestion des rapports de stockage

La gestion des rapports de stockage est un composant qui vous permet de planifier et de configurer des rapports de stockage. Ces rapports fournissent des informations concernant les composants et les aspects de FSRM, notamment :

- l'utilisation de quota ;
- l'activité de filtrage de fichiers ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- les fichiers susceptibles d'avoir un impact négatif sur la gestion de la capacité, tels que les fichiers volumineux, les fichiers en double ou les fichiers inutilisés ;
- l'énumération et le filtrage de fichiers en fonction d'un propriétaire, d'un groupe de fichiers ou d'une propriété de fichier spécifique.

Remarque : Les rapports de stockage peuvent être exécutés selon une planification, ou vous pouvez les générer à la demande.

Gestion de la classification

La gestion de la classification est un composant qui vous permet de créer et gérer des propriétés de classification que vous pouvez ensuite attribuer aux fichiers. Vous pouvez attribuer des valeurs de propriété aux fichiers à l'aide de règles de classification, qui peuvent être appliquées à la demande ou basées sur une planification. La classification vous permet de classer et de gérer des fichiers à l'aide d'un grand nombre de propriétés dans le but d'identifier et de grouper vos fichiers.

Tâches de gestion de fichiers

Le composant de tâches de gestion de fichiers vous permet de planifier et configurer des tâches spécifiques, qui peuvent automatiser l'application ou l'expiration de commandes personnalisées. Ainsi, vous pouvez automatiser les procédures de gestion des fichiers. Les tâches de gestion de fichiers tirent parti des fonctionnalités de gestion de la classification pour vous permettre de supprimer les fichiers anciens ou de les déplacer vers un emplacement spécifique en fonction d'une propriété de fichier (nom de fichier ou type de fichier).

Remarque : Les volumes que FSRM gère doivent être formatés en utilisant le système de fichiers NTFS. FSRM est fourni avec Windows Server 2003 Service Pack 1 (SP1) et versions ultérieures.

Démonstration : Procédure d'installation et de configuration de FSRM

Pour installer FSRM dans Windows 2012, ajoutez le service de rôle FSRM dans le rôle Services de fichiers et de stockage.

FSRM comporte plusieurs options de configuration qui s'appliquent globalement à tous ses composants.

Pour accéder à ces options, procédez comme suit :

1. Ouvrez la console Gestionnaire de ressources du serveur de fichiers.
2. Dans le volet gauche, cliquez avec le bouton droit sur le nœud racine **Gestionnaire de ressources du serveur de fichiers**, puis cliquez sur **Configurer les options**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options FSRM

Dans la boîte de dialogue **Options du Gestionnaire de ressources du serveur de fichiers**, plusieurs onglets vous permettent de configurer les divers aspects de FSRM. Les onglets suivants sont disponibles dans la boîte de dialogue de propriétés **Options du Gestionnaire de ressources du serveur de fichiers** :

- *Onglet Notifications par courrier électronique*. Cet onglet vous permet d'indiquer le nom ou l'adresse d'un serveur SMTP, ainsi que d'autres détails que FSRM utilisera pour envoyer des notifications par courrier électronique.
- *Onglet Limites de notification*. Les limites de notification vous permettent de spécifier une durée pendant laquelle FSRM attend entre chaque envoi de notifications afin d'éviter l'excès de notifications résultant de la répétition d'un dépassement de quota ou d'une détection de fichier non autorisé. Cet onglet vous permet de définir des valeurs distinctes pour les notifications par courrier électronique, les entrées enregistrées dans le journal des événements, les commandes en cours d'exécution ou les rapports en cours de génération. La valeur par défaut de chaque intervalle est de 60 minutes.
- *Onglet Rapports de stockage*. Cet onglet vous permet de configurer et d'afficher les paramètres par défaut de rapports de stockage existants. *Onglet Emplacements des rapports*. Cet onglet vous permet d'afficher et de modifier l'emplacement dans lequel les trois différents types de rapports de stockage sont enregistrés : rapports d'incident, rapports planifiés et rapports à la demande. Par défaut, chaque catégorie est enregistrée dans son propre dossier : %systemdrive%\Rapports de stockage.

 **Remarque :** Si FSRM génère un grand nombre de rapports de stockage, il est possible de déplacer les dossiers de rapport de stockage vers un autre volume physique afin de diminuer les entrées/sorties (E/S) disque sur votre volume système. Vous pouvez également modifier l'emplacement si la taille de vos rapports de stockage provoque un problème de capacité sur votre volume système.

- *Onglet Vérification du filtrage de fichiers*. Sous cet onglet, une case à cocher permet d'activer ou de désactiver l'enregistrement de l'activité de filtrage des fichiers dans la base de données de vérification. Vous pouvez afficher l'activité résultante du filtrage de fichiers quand vous exécutez le rapport de vérification du filtrage des fichiers depuis Gestion des rapports de stockage.
- *Onglet Classification automatique*. Cet onglet vous permet de définir une planification qui régit la classification automatique des fichiers. Vous pouvez spécifier les journaux à générer, puis indiquer s'il faut générer un rapport du processus de classification et comment procéder.
- *Onglet Assistance en cas d'accès refusé*. Cet onglet vous permet de définir un message personnalisé quand FSRM empêche une opération de niveau fichier suite à une restriction de la gestion de quota pour le filtrage de fichiers.

Gestion des services FSRM

La gestion d'un serveur exécutant FSRM se produit en général localement, via la console FSRM Microsoft® Management Console (MMC). Toutefois, vous disposez d'autres options pour gérer un serveur exécutant ce type de service.

Gestion de FSRM à l'aide de Windows PowerShell

Windows PowerShell® 3.0 contient les nouvelles applets de commande pour la gestion de FSRM. Celles-ci étendent les fonctionnalités de gestion à tous les aspects de FSRM. Le module FileServerResourceManager pour Windows PowerShell est installé sur un ordinateur Windows Server 2012 automatiquement quand vous installez le service de rôle FSRM.

Les applets de commande Windows PowerShell3.0 remplacent la fonctionnalité précédemment fournie par les exécutables de ligne de commande dirquota.exe, filescrn.exe et storrpt.exe de FSRM. Bien que ces exécutables soient toujours présents dans Windows Server 2012, ils sont déconseillés et seront supprimés de la future version de Windows Server. Par conséquent, vous devriez utiliser les applets de commande Windows PowerShell pour créer toutes les solutions de gestion impliquant des tâches de ligne de commande.

Pour voir la liste complète des applets de commande FSRM disponibles, exécutez la commande suivante depuis une interface de ligne de commande Windows PowerShell :

```
Get-Command -Module FileServerResourceManager
```

Gestion de FSRM à distance

Vous pouvez vous connecter à distance à un autre serveur qui exécute FSRM à l'aide de la console FSRM. Depuis cette console, vous gérez FSRM de la même manière que vous gérez des ressources sur votre ordinateur local.

Pour gérer FSRM à distance à l'aide de la console FSRM :

- Assurez-vous que les deux serveurs exécutent Windows Server 2008 R2 ou une version plus récente, puis installez FSRM.
- Activez l'exception **Gestion de ressources du serveur de fichiers à distance** manuellement depuis le Pare-feu Windows®, via le Panneau de configuration ou à l'aide d'une stratégie de groupe.
- Autorisez le trafic d'appel de procédure distante (RPC) entre les deux serveurs quel que soit le pare-feu.
- Connectez-vous à l'ordinateur local avec un compte membre du groupe d'administrateurs locaux sur l'ordinateur distant.

Vous pouvez également exécuter les applets de commande Windows PowerShell de FSRM à distance à l'aide des fonctionnalités de communication à distance de Windows PowerShell.

Dans cette démonstration, vous allez apprendre à :

- installer le service de rôle FSRM ;
- spécifier les options de configuration de FSRM ;
- utiliser Windows PowerShell pour gérer FSRM.

Procédure de démonstration

Installer le service de rôle FSRM

1. Connectez-vous à LON-SVR1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez le **Gestionnaire de serveur**.
3. Installez le service de rôle **Gestionnaire de ressources du serveur de fichiers** dans le rôle **Service de fichiers et de stockage (Installé)**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Spécifier les options de configuration de FSRM

1. Ouvrez la console Gestionnaire de ressources du serveur de fichiers.
2. Ouvrez la fenêtre Options du Gestionnaire de ressources du serveur de fichiers pour l'instance locale du **Gestionnaire de ressources du serveur de fichiers**.
3. Activez la vérification du filtrage de fichiers.

Utiliser Windows PowerShell pour gérer FSRM

- À partir d'une invite de commande Windows PowerShell, exécutez la commande suivante :

```
set-FSRMSetting -SMTPServer "server1" -AdminEmailAddress "fileadmin@adatum.com" -
FromEmailAddress "fileadmin@adatum.com"
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2

Utilisation de FSRM pour gérer les quotas, les filtres de fichiers et les rapports de stockage

Les données sont le principal composant de votre infrastructure de serveur. Dans la plupart des circonstances, l'infrastructure de serveur fournit aux utilisateurs ou aux applications les données contenues dans les fichiers sur le serveur.

Que l'ajout de fichiers aux serveurs soit effectué par les utilisateurs ou les applications, la gestion de quota vous permet de vous assurer que ces utilisateurs et ces applications utilisent uniquement l'espace qui leur est alloué. Les filtres de fichiers dans FSRM vous permettent de déterminer quels types de fichiers peuvent être enregistrés dans votre infrastructure de fichiers et de stockage. Par ailleurs, les rapports de stockage vous permettent de fournir des détails sur la gestion de quota, le filtrage de fichiers et plusieurs autres aspects de la fonctionnalité FSRM.

Objectifs de la leçon

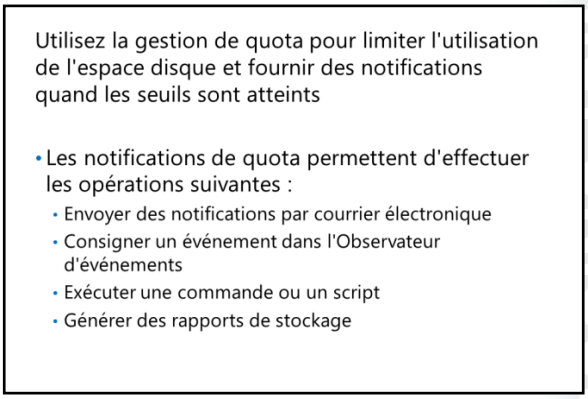
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire la gestion de quota ;
- décrire les modèles de quotas ;
- expliquer comment surveiller l'utilisation des quotas ;
- décrire la gestion du filtrage de fichiers ;
- décrire les groupes de fichiers ;
- décrire les modèles de filtres de fichiers et les exceptions de filtres de fichiers ;
- décrire les rapports de stockage ;
- expliquer une tâche de création de rapport ;
- expliquer comment utiliser FSRM pour gérer les quotas et les filtres de fichiers et pour générer des rapports de stockage.

Qu'est-ce que la gestion de quota ?

Dans FSRM, la gestion de quota vous permet de limiter l'espace disque qui est alloué à un volume ou un dossier. La limite de quota s'applique à l'ensemble de la sous-arborescence d'un dossier.

Les quotas vous permettent de gérer des restrictions de capacité en procédant de différentes manières. Par exemple, vous pouvez utiliser un quota pour vérifier que les utilisateurs individuels ne consomment pas un espace de stockage trop important avec leurs lecteurs de base, ou pour limiter l'espace consommé par les fichiers multimédias dans un dossier spécifique.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Types de quotas

Vous pouvez créer deux types différents de quotas dans la gestion de quota :

- Un quota inconditionnel empêche les utilisateurs d'enregistrer des fichiers une fois que la limite d'espace est atteinte et génère des notifications lorsque le volume de données atteint chaque seuil configuré.
- Un quota conditionnel ne met pas à exécution la limite de quota mais génère des notifications configurées.

Notifications de quotas

Pour déterminer ce qui se produit lorsque la limite de quota est atteinte, vous configurez des seuils de notification. Pour chaque seuil que vous définissez, vous pouvez envoyer des notifications par courrier électronique, enregistrer un événement, exécuter une commande ou un script, ou générer des rapports de stockage. Par exemple, vous pouvez avertir l'administrateur et l'utilisateur lorsqu'un dossier atteint 85 % de sa limite de quota, puis envoyer une autre notification lorsque la limite de quota est atteinte. Parfois, il peut être nécessaire d'exécuter un script qui élève automatiquement la limite de quota lorsqu'un seuil est atteint.

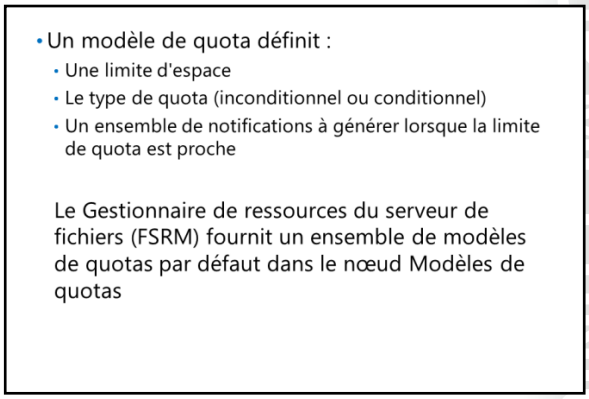
Création de quotas

Quand vous créez un quota sur un volume ou un dossier, vous pouvez le baser sur un modèle de quota ou utiliser des propriétés personnalisées. Autant que possible, basez un quota sur un modèle de quota. Vous pouvez réutiliser un modèle de quota pour créer d'autres quotas ; cela simplifie la gestion actuelle des quotas.

FSRM peut également générer des quotas automatiquement. Quand vous configurez un quota automatique, vous appliquez un modèle de quota à un volume ou à un dossier parent. Ensuite, un quota basé sur ce modèle est créé pour chacun des sous-dossiers existants, et un quota est généré automatiquement pour chaque nouveau sous-dossier créé. Vous pouvez également créer des quotas via l'applet de commande Windows PowerShell, **New-FSRMQuota**.

Que sont les modèles de quotas ?

Les modèles de quotas FSRM vous permettent de créer, d'utiliser et de gérer des modèles pour des quotas. Un modèle de quota définit une limite d'espace, le type de quota (inconditionnel ou conditionnel), et un ensemble de notifications à générer quand la limite de quota est approchée ou dépassée.



Les modèles de quotas simplifient la création et la maintenance des quotas. Vous pouvez utiliser un modèle de quota pour appliquer une limite de stockage standard et un ensemble standard de seuils de notification à un grand nombre de volumes et de dossiers sur les serveurs de votre organisation.

Mise à jour de quota basée sur un modèle

Si vous basez vos quotas sur un modèle, vous pouvez mettre à jour tous les quotas basés sur ce modèle en le modifiant. Cette fonctionnalité simplifie le processus de mise à jour des propriétés de quota en fournissant un point central à partir duquel les administrateurs informatiques peuvent effectuer toutes les modifications.

Par exemple, vous pouvez créer un modèle de quota utilisateur que vous utilisez pour définir une limite de 200 mégaoctets (Mo) sur le dossier personnel de chaque utilisateur. Vous pouvez ensuite créer un quota basé sur ce modèle de quota utilisateur, puis l'attribuer au dossier de chaque utilisateur. Si vous décidez ultérieurement d'attribuer à chaque utilisateur un espace supplémentaire sur le serveur, vous n'avez qu'à modifier la limite d'espace dans le modèle de quota utilisateur, puis à mettre à jour chaque quota basé sur ce modèle de quota.

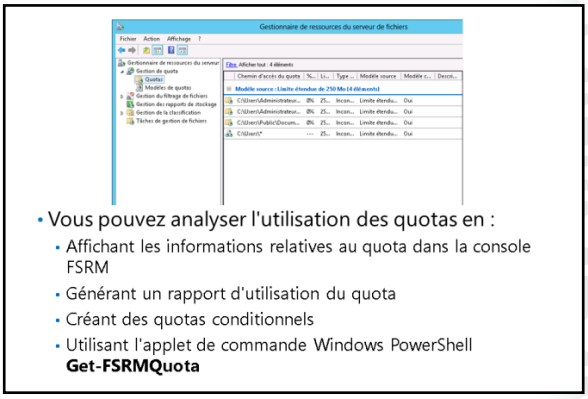
Exemples de modèles de quotas

FSRM fournit plusieurs modèles de quotas. Par exemple :

- Vous pouvez utiliser le modèle Limite de 200 Mo pour les rapports d'utilisateurs pour définir une limite inconditionnelle de 200 Mo sur le dossier personnel de chaque utilisateur, puis envoyer des rapports de stockage aux utilisateurs qui dépassent le quota.
- Pour certains dossiers, vous pouvez utiliser le modèle Limite de 200 Mo avec extension de 50 Mo pour accorder une extension de quota ponctuelle de 50 Mo aux utilisateurs qui dépassent la limite de quota de 200 Mo.
- D'autres modèles par défaut sont conçus pour surveiller l'utilisation du disque par l'intermédiaire de quotas conditionnels, notamment le modèle Analyser l'utilisation de volume de 200 Go et le modèle Analyser un partage de 500 Mo. Quand vous utilisez ces modèles, les utilisateurs peuvent dépasser la limite de quota, mais des notifications par courrier électronique et de journal des événements sont générées le cas échéant.

Analyse du rapport d'utilisation des quotas

En plus des informations figurant dans les notifications envoyées par les quotas, vous disposez d'autres méthodes pour trouver des informations relatives à l'utilisation des quotas. Vous pouvez afficher les quotas dans la fenêtre de gestion des quotas de la console FSRM, générer un rapport d'utilisation des quotas ou créer des quotas conditionnels pour surveiller l'utilisation globale du disque. Vous pouvez également utiliser une applet de commande Windows PowerShell.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Rapport d'utilisation des quotas

Le rapport d'utilisation des quotas vous permet d'identifier les quotas susceptibles d'être bientôt atteints ou dépassés afin que vous puissiez prendre les mesures appropriées. La génération de ce rapport sera abordée en détail dans la leçon Gestion des rapports de stockage.

Modèles pour surveiller l'utilisation du disque

Pour surveiller l'utilisation globale du disque, vous pouvez créer des quotas conditionnels pour des volumes ou des partages. FSRM fournit les modèles par défaut suivants que vous pouvez utiliser (ou adapter) à cette fin :

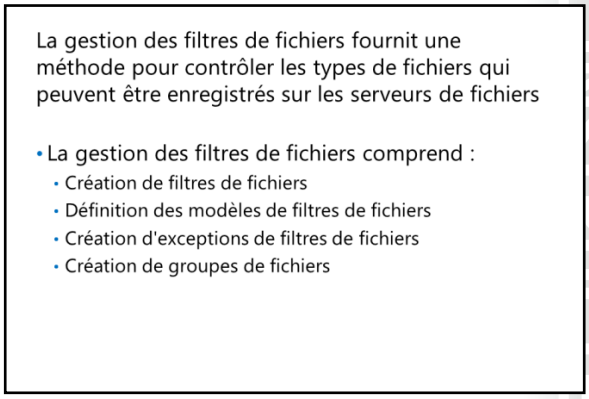
- Analyser l'utilisation de volume de 200 Go
- Analyser un partage de 500 Mo

Windows PowerShell

Vous pouvez utiliser l'applet de commande **Get-FSRMQuota** pour afficher les quotas FSRM qui existent sur le serveur, ainsi que les statistiques de chaque quota.

Qu'est-ce que la gestion du filtrage de fichiers ?

La gestion du filtrage de fichiers vous permet de créer des filtres de fichiers afin d'empêcher l'enregistrement de types de fichiers sur un volume ou dans une arborescence de dossiers. Un filtre de fichiers affecte tous les dossiers dans le chemin d'accès indiqué. Vous utilisez des groupes de fichiers pour contrôler les types de fichiers que les filtres de fichiers gèrent. Par exemple, vous pouvez créer un filtre de fichiers pour empêcher des utilisateurs d'enregistrer des fichiers audio et vidéo dans leurs dossiers personnels sur le serveur. Comme tous les composants de FSRM, vous pouvez choisir de générer des notifications par courrier électronique ou d'autres notifications quand un événement de filtrage de fichiers se produit.



Types de filtre de fichiers

Vous pouvez configurer un filtre de fichiers comme actif ou passif :

- Le filtrage actif empêche les utilisateurs d'enregistrer des types de fichiers non autorisés sur le serveur et génère des notifications configurées lorsqu'ils tentent de le faire.
- Le filtrage passif envoie des notifications configurées aux utilisateurs qui enregistrent des types de fichiers spécifiques, mais il n'empêche pas les utilisateurs d'enregistrer ces fichiers.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte en matière de gestion du filtrage de fichiers

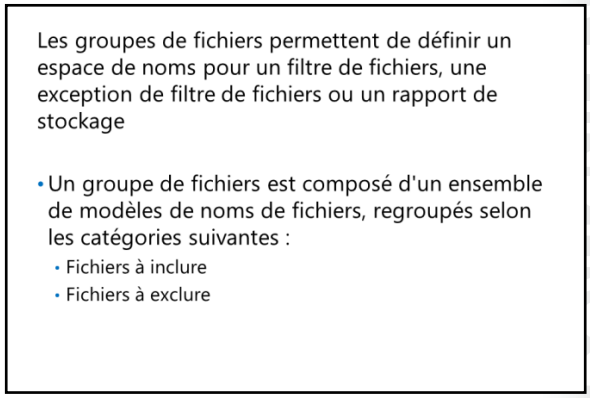
Pour simplifier la gestion des filtres de fichiers, vous pouvez baser vos filtres de fichiers sur les modèles de filtre de fichiers, qui seront présentés ultérieurement dans cette leçon.

Pour davantage de flexibilité, vous pouvez configurer une exception de filtre de fichiers dans un sous-dossier d'un chemin d'accès où vous avez créé un filtre de fichiers. Quand vous placez une exception de filtre de fichiers dans un sous-dossier, vous permettez aux utilisateurs d'enregistrer des types de fichier qui seraient normalement bloqués par le filtre de fichiers appliqué au dossier parent. Vous pouvez également créer des filtres de fichiers dans Windows PowerShell à l'aide de l'applet de commande **New-FSRMFileScreen**.

Remarque : Un filtre de fichiers n'empêche pas les utilisateurs et les applications d'accéder aux fichiers qui ont été enregistrés dans le chemin d'accès avant la création de ce filtre, que ces fichiers appartiennent ou non à des groupes de fichiers bloqués.

Que sont les groupes de fichiers ?

Avant de commencer à utiliser des filtres de fichiers, vous devez comprendre le rôle des groupes de fichiers dans la détermination du filtrage des fichiers. Un groupe de fichiers permet de définir un espace de noms pour un filtre de fichiers ou une exception de filtre de fichiers ou de générer un rapport de stockage Fichiers par groupe de fichiers.



Caractéristiques des groupes de fichiers

Un groupe de fichiers se compose d'un ensemble de modèles de noms de fichiers, qui sont groupés en tant que fichiers à inclure et fichiers à exclure :

- Fichiers à inclure : fichiers auxquels le groupe de fichiers s'applique.
- Fichiers à exclure : fichiers auxquels le groupe de fichiers ne s'applique pas.

Par exemple, un groupe de fichiers appelé Fichiers audio peut contenir les modèles de noms de fichiers suivants :

- Fichiers à inclure : *.mp* : inclut tous les fichiers audio créés dans les formats MPEG actuels et futurs (MP2, MP3, etc.).
- Fichiers à exclure : *.mpp : Exclut les fichiers créés dans Microsoft Project (fichiers .mpp), qui auraient normalement dû être inclus en vertu de la règle d'inclusion *.mp*.

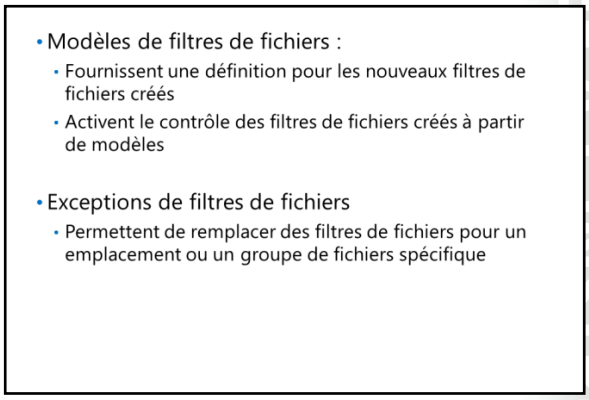
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

FSRM fournit plusieurs groupes de fichiers par défaut, que vous pouvez afficher dans Gestion du filtrage de fichiers en cliquant sur le nœud Groupes de fichiers. Vous pouvez définir d'autres groupes de fichiers ou modifier les fichiers à inclure et à exclure. Toute modification apportée à un groupe de fichiers affecte tous les filtres de fichiers, modèles et rapports existants auxquels le groupe de fichiers a été ajouté.

Remarque : Pour plus de commodité, vous pouvez modifier les groupes de fichiers quand vous modifiez les propriétés d'un filtre de fichiers, d'une exception de filtre de fichiers, d'un modèle de filtre de fichiers, ou le rapport Fichiers par groupe de fichiers. Notez que toutes les modifications que vous apportez à un groupe de fichiers à partir de ces feuilles de propriétés affectent tous les éléments qui utilisent ce groupe de fichiers.

Que sont les modèles de filtres de fichiers et les exceptions de filtres de fichiers ?

Vous utilisez des modèles de filtre de fichiers et des exceptions de filtre de fichiers pour développer les fonctionnalités de la gestion du filtrage de fichiers dans FSRM.



Modèles de filtres de fichiers

Pour simplifier la gestion des filtres de fichiers, vous pouvez les créer en vous basant sur des modèles de filtres de fichiers. Un modèle de filtre de fichiers définit les éléments suivants :

- les groupes de fichiers à bloquer ;
- les types de filtrage à exécuter ;
- les notifications à générer.

Vous pouvez configurer deux types de filtrage dans un modèle de filtre de fichiers. *Le filtrage actif* ne permet pas aux utilisateurs d'enregistrer des fichiers associés aux groupes de fichiers sélectionnés que vous configurez avec le modèle. *Le filtrage passif* permet aux utilisateurs d'enregistrer les fichiers mais envoie des notifications à des fins de surveillance.

FSRM fournit plusieurs modèles de filtres de fichiers par défaut, que vous pouvez utiliser pour bloquer des fichiers audio et vidéo, des fichiers exécutables, des fichiers image et des fichiers de courrier électronique, afin de répondre aux besoins administratifs courants. Pour afficher les modèles par défaut, dans l'arborescence de la console Gestionnaire de ressources du serveur de fichiers, cliquez sur le nœud Modèles de filtres de fichiers.

Le fait de créer des filtres de fichiers exclusivement à partir de modèles vous permet de les gérer de manière centralisée en mettant à jour ces modèles au lieu de modifier les filtres de fichiers un à un.

Remarque : La procédure pour créer des filtres de fichiers à partir de modèles de filtres est identique à celle utilisée pour créer des quotas à partir de modèles de quotas.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exceptions de filtres de fichiers

Il est parfois nécessaire d'autoriser des exceptions au filtrage de fichiers. Par exemple, vous pouvez bloquer les fichiers vidéo provenant d'un serveur de fichiers, mais vous devez autoriser votre groupe de stagiaires à enregistrer les fichiers vidéo dans le cadre de leur formation assistée par ordinateur. Pour autoriser certains fichiers bloqués par d'autres filtres, vous pouvez créer une exception de filtre de fichiers.

Une exception de filtre de fichiers est un type particulier de filtre de fichiers qui remplace tout autre filtre de fichiers qui devrait normalement s'appliquer à un dossier et ses sous-dossiers, dans un chemin d'accès désigné de l'exception. Cela signifie qu'elle crée une exception à toute règle dérivée d'un dossier parent. Pour déterminer quels types de fichier l'exception autorisera, des groupes de fichiers sont attribués.

Pour créer une exception de filtre de fichiers, sous Gestion du filtrage de fichiers dans FSRM, cliquez sur Créer une exception de filtre de fichiers à partir du nœud Filtres de fichiers.



Remarque : Les exceptions de filtres de fichiers remplacent toujours des filtres de fichiers dont les paramètres sont en conflit. Par conséquent, vous devez les organiser et les implémenter avec prudence.

Que sont les rapports de stockage ?

FSRM peut générer des rapports(appelés *rapports de stockage*)qui vous aident à comprendre l'utilisation des fichiers sur votre serveur de stockage. Vous pouvez utiliser des rapports de stockage pour surveiller les modèles d'utilisation du disque (par type de fichier ou utilisateur), pour identifier les fichiers en double et les fichiers dormants, pour suivre l'utilisation du quota et pour auditer le filtrage de fichiers.

Les rapports de stockage fournissent des informations sur l'utilisation des fichiers sur un serveur de fichiers

- Les types de rapports de stockage sont les suivants :
  - Fichiers dupliqués
  - Vérification du filtrage des fichiers
  - Fichiers par groupe de fichiers, propriétaire ou propriété
  - Dossiers par propriété
  - Fichiers volumineux
  - Fichiers ouverts le moins et le plus récemment
  - Utilisation du quota

Dans le nœud Gestion des rapports de stockage, vous pouvez créer des tâches de rapport que vous utiliserez ensuite pour planifier un ou plusieurs rapports périodiques, ou vous pouvez générer des rapports à la demande. Pour les rapports à la demande et les rapports planifiés, les données actuelles sont rassemblées avant la génération du rapport. Vous avez également la possibilité de générer des rapports automatiquement pour vous avertir quand un utilisateur dépasse un seuil de quota ou enregistre un fichier non autorisé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Types de rapports de stockage

Le tableau suivant décrit chaque rapport de stockage disponible.

Rapport	Description
Fichiers dupliqués	Ce rapport répertorie les fichiers qui semblent être des doublons (fichiers avec la même taille et la dernière date de modification). Il permet d'identifier et de récupérer l'espace disque gaspillé en raison de fichiers dupliqués. C'est le seul rapport qui n'est pas configurable.
Vérification du filtrage des fichiers	Ce rapport répertorie les événements de filtrage de fichiers qui se sont produits sur le serveur pendant un nombre de jours déterminé. Il permet d'identifier les utilisateurs ou les applications qui ne respectent pas les stratégies de filtrage de fichiers.
Fichiers par groupe de fichiers	Ce rapport répertorie les fichiers qui appartiennent à des groupes de fichiers spécifiques. Il permet d'identifier les tendances d'utilisation de groupes de fichiers ainsi que les groupes de fichiers qui occupent de grandes quantités d'espace disque. Il peut vous aider à déterminer les filtres de fichiers à configurer sur le serveur.
Fichiers par propriétaire	Ce rapport répertorie les fichiers qui sont groupés par propriétaires. Il permet d'analyser les tendances d'utilisation sur le serveur et d'identifier les utilisateurs qui consomment de grandes quantités d'espace disque.
Fichiers par propriété	Ce rapport répertorie les fichiers en fonction des valeurs d'une propriété particulière de classification. Il permet d'observer des tendances d'utilisation de la classification des fichiers.
Dossiers par propriété	Ce rapport répertorie les dossiers en fonction de la valeur d'une propriété de classification sécurisée donnée. Il permet d'observer des tendances de classification des dossiers.
Fichiers volumineux	Ce rapport répertorie les fichiers d'une taille spécifique ou volumineux. Il permet d'identifier les fichiers qui occupent le plus d'espace disque sur le serveur. Vous pouvez ainsi l'utiliser pour récupérer de grandes quantités d'espace disque.
Fichiers ouverts le moins récemment	Ce rapport répertorie les fichiers qui n'ont pas été ouverts depuis un nombre de jours spécifié. Il peut vous aider à identifier les données rarement utilisées qui peuvent être archivées et supprimées du serveur.
Fichiers ouverts le plus récemment	Ce rapport répertorie les fichiers qui ont été ouverts au cours d'une période en jours spécifiée. Il permet d'identifier les données fréquemment utilisées qui doivent être maintenues à un haut niveau de disponibilité.
Utilisation du quota	Ce rapport répertorie les quotas dont l'utilisation est supérieure au pourcentage spécifié. Il permet d'identifier les quotas présentant des niveaux d'utilisation élevés afin que vous puissiez prendre les mesures appropriées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des paramètres de rapport

Excepté pour le rapport Fichiers dupliqués, tous les rapports ont des paramètres configurables qui déterminent leur contenu. Ces paramètres varient selon le type de rapport. Pour certains rapports, vous pouvez utiliser des paramètres pour sélectionner les volumes et les dossiers particuliers, définir une taille de fichier minimale à inclure ou restreindre leur portée aux fichiers appartenant à des utilisateurs spécifiques.

Enregistrement de rapports

Indépendamment de la façon dont vous le générez, ou que vous choisissiez de l'afficher immédiatement ou non, le rapport est enregistré sur le disque. Les rapports d'incident sont enregistrés au format DHTML (Dynamic HTML). Vous pouvez enregistrer les rapports planifiés et à la demande au format DHTML, HTML, XML, CSV et texte.

Les rapports planifiés, les rapports à la demande et les rapports d'incident sont enregistrés dans des dossiers séparés au sein d'un référentiel de rapports désigné.

Par défaut, les rapports sont enregistrés dans les sous-répertoires du dossier %Systemdrive%\StorageReports\. Pour modifier les emplacements par défaut des rapports, dans la boîte de dialogue **Options du Gestionnaire de ressources du serveur de fichiers**, sous l'onglet **Emplacements des rapports**, indiquez où enregistrer chaque type de rapport de stockage.

Qu'est-ce qu'une tâche de création de rapport ?

Une tâche de création de rapport est un ensemble de rapports de gestion du stockage qui s'exécutent selon une planification.

Elle spécifie les rapports à générer, ceux à utiliser, ainsi que les volumes et les dossiers sur lesquels le rapport doit porter. La tâche de création de rapport indique également à quelle fréquence générer les rapports et dans quels formats les enregistrer.

- Vous pouvez planifier des rapports en créant une tâche de création de rapport qui indique :
  - Les volumes et dossiers sur lesquels porte le rapport
  - Les types de rapports à générer
  - Les paramètres à utiliser
  - La fréquence de génération des rapports
  - Les formats de fichiers sous lesquels enregistrer les rapports

Quand vous planifiez un ensemble de rapports, les rapports sont enregistrés automatiquement dans le référentiel de rapports. Vous pouvez également demander que les rapports soient envoyés par courrier électronique à un groupe d'administrateurs.

Pour planifier des tâches de création de rapport, procédez comme suit dans FSRM.

1. Cliquez sur le nœud **Gestion des rapports de stockage**.
2. Cliquez avec le bouton droit sur **Gestion des rapports de stockage**, puis cliquez sur **Planifier une nouvelle tâche de rapport**. Vous pouvez également cliquer sur **Planifier une nouvelle tâche de rapport** dans le volet Actions.

Remarque : Pour réduire l'impact du traitement des rapports sur les performances du serveur, générez plusieurs rapports selon la même planification de sorte que les données soit collectées une seule fois.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Génération de rapports à la demande

Pendant les opérations quotidiennes, vous pouvez générer des rapports à la demande pour analyser les différents aspects de l'utilisation actuelle du disque sur le serveur. Les données actuelles sont collectées avant la génération des rapports.

Lorsque vous générez des rapports à la demande, ceux-ci sont enregistrés dans le référentiel des rapports, mais aucune tâche de création de rapport n'est créée pour une utilisation ultérieure. Vous pouvez afficher les rapports juste après les avoir générés, ou vous pouvez les envoyer à un groupe d'administrateurs par courrier électronique.

Pour générer des rapports à la demande :

1. Cliquez sur le nœud **Gestion des rapports de stockage**.
2. Cliquez avec le bouton droit sur **Gestion des rapports de stockage**, puis cliquez sur **Générer les rapports maintenant** (ou dans le volet Actions, cliquez sur **Générer les rapports maintenant**).

Remarque : Lorsque vous générez un rapport à la demande, vous pouvez attendre qu'il soit généré et l'afficher immédiatement. Si vous choisissez d'ouvrir les rapports immédiatement, vous devez attendre qu'ils soient générés. Le temps de traitement varie selon les types de rapports et l'étendue des données.

Démonstration : Utilisation de FSRM pour gérer des quotas et des filtres de fichiers et pour générer des rapports de stockage à la demande

Dans cette démonstration, vous allez apprendre à :

- créer un quota ;
- tester un quota ;
- créer un filtre de fichiers ;
- tester un filtre de fichiers ;
- générer un rapport de stockage ;

Procédure de démonstration

Créer un quota

1. Connectez-vous à LON-SVR1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez le **Gestionnaire de serveur**.
3. Ouvrez la console Gestionnaire de ressources du serveur de fichiers**.**
4. Créez un quota basé sur le paramètre **Limite de 100 Mo** dans le dossier **E:\Labfiles\Mod10\Data**.

Tester un quota

1. Ouvrez Windows PowerShell.
2. Créez un nouveau fichier de **130 Mo** dans le dossier **E:\Labfiles\Mod10\Data** à l'aide de la commande suivante :

```
fsutil file createnew largefile.txt 130000000
```

3. Fermez Windows PowerShell.

Créer un filtre de fichiers

- Dans le Gestionnaire de ressources du serveur de fichiers, créez un nouveau filtre de fichiers selon le modèle de filtre de fichiers Bloquer les fichiers image pour E:\Labfiles\Mod10\Data.

Tester un filtre de fichiers

1. Ouvrez l'Explorateur Microsoft Windows.
2. Accédez à **E:\Labfiles\Mod10**.
3. Créez une nouvelle image bitmap (.bmp) nommée **testimage**.
4. Copiez **testimage**, puis collez-la dans le dossier **E:\Labfiles\Mod10\Data**.
5. Affichez et fermez la fenêtre d'erreurs.
6. Fermez la fenêtre de l'Explorateur de fichiers.

Générer un rapport de stockage

1. Générez un rapport à la demande pour **Fichiers volumineux** sur le lecteur **E:**.
2. Affichez le rapport HTML et fermez-le.
3. Fermez le Gestionnaire de ressources du serveur de fichiers.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Implémentation des tâches de classification et de gestion de fichiers

La plupart des applications gèrent des fichiers selon le répertoire dans lequel ils sont stockés. Cela génère des structures de fichiers qui requièrent l'attention des administrateurs. Une telle structure peut également engendrer de la frustration parmi les utilisateurs. Dans Windows Server 2012, les tâches de gestion de la classification et de gestion de fichiers permettent aux administrateurs de gérer des groupes de fichiers selon divers attributs de fichier et de dossier. Avec les tâches de gestion de la classification et de gestion de fichiers, vous pouvez automatiser les tâches de maintenance des fichiers et des dossiers, telles que le nettoyage des données périmées ou la protection des informations sensibles.

Dans cette leçon, vous apprendrez comment les tâches de gestion de la classification et de fichiers fonctionnent ensemble pour faciliter la gestion et l'organisation des fichiers et des dossiers sur vos serveurs.

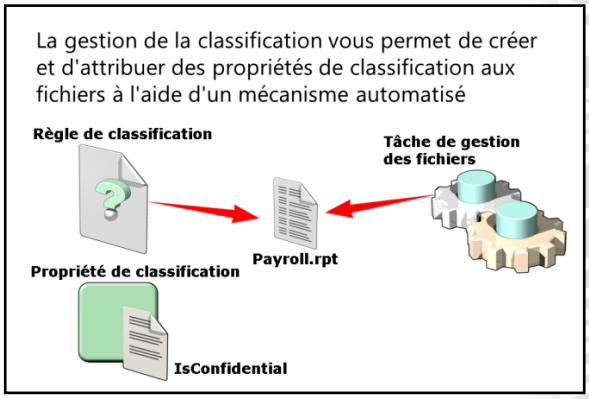
Objectifs de la leçon

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

- décrire la gestion de la classification ;
- décrire les propriétés de la classification ;
- décrire une règle de classification ;
- expliquer comment configurer la gestion de la classification ;
- identifier les éléments à prendre en considération pour l'utilisation de la classification des fichiers ;
- décrire les tâches de gestion de fichiers ;
- expliquer comment configurer les tâches de gestion de fichiers.

Qu'est-ce que la gestion de la classification ?

Pour réduire le coût et le risque associés à la gestion des données, l'infrastructure de classification des fichiers utilise une plateforme qui permet aux administrateurs de classer les fichiers et d'appliquer des stratégies selon cette classification. La disposition du stockage n'est pas modifiée par les exigences en matière de gestion des données, et l'organisation peut s'adapter plus facilement à un changement d'environnement d'entreprise et de réglementation.



La gestion de la classification est conçue pour simplifier la charge et la gestion des données réparties dans l'entreprise. Elle vous permet de classer les fichiers de différentes manières. Dans la plupart des scénarios, vous effectuez la classification manuellement. Dans Windows Server 2012, la fonctionnalité Infrastructure de classification des fichiers permet aux organisations de convertir ces processus manuels en stratégies automatisées. Vous pouvez spécifier des stratégies de gestion des fichiers basées sur la classification d'un fichier, puis appliquer les exigences de l'entreprise pour gérer les données en fonction de la valeur commerciale. Vous pouvez également modifier les stratégies facilement et utiliser des outils qui prennent en charge la classification pour gérer les fichiers.

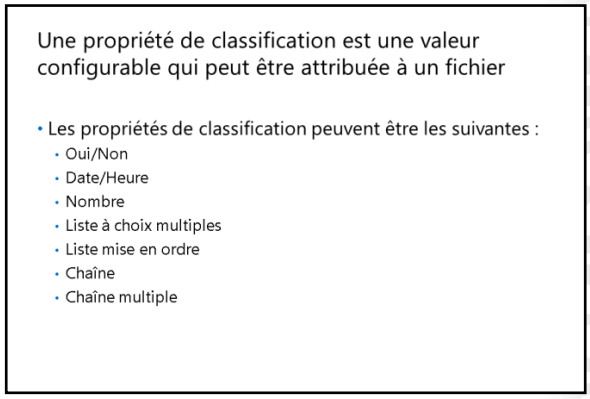
Vous pouvez utiliser la classification des fichiers pour effectuer les actions suivantes :

1. Définir les propriétés et les valeurs de classification pouvant être attribuées aux fichiers en exécutant des règles de classification.
2. Créer, mettre à jour et exécuter des règles de classification. Chaque règle attribue une propriété et une valeur prédéfinies uniques aux fichiers dans un répertoire spécifié, en fonction des plug-ins de classification installés.

Lorsque vous exécutez une règle de classification, vous pouvez réévaluer les fichiers déjà classés. Vous pouvez choisir de remplacer des valeurs de classification existantes ou d'ajouter une valeur aux propriétés qui prennent en charge plusieurs valeurs.

Que sont les propriétés de classification ?

Les propriétés de classification sont utilisées pour attribuer des valeurs aux fichiers. Vous avez le choix entre plusieurs types de propriétés. Vous pouvez définir ces propriétés selon les besoins de votre organisation. Des propriétés de classification sont attribuées aux fichiers qui utilisent les règles de classification, qui sont présentées dans la rubrique suivante.



Le tableau suivant définit les types de propriétés disponibles et la stratégie qui est appliquée quand un fichier est reclassé :

Type de propriété	Description
Oui/Non	Propriété booléenne qui peut avoir la valeur OUI ou NON. Lorsque plusieurs valeurs sont combinées, la valeur NON remplace la valeur OUI.
Date-Heure	Simple propriété de date et d'heure. Lorsque plusieurs valeurs sont combinées, les valeurs en conflit empêchent la reclassification.
Nombre	Simple propriété numérique. Lorsque plusieurs valeurs sont combinées, les valeurs en conflit empêchent la reclassification.

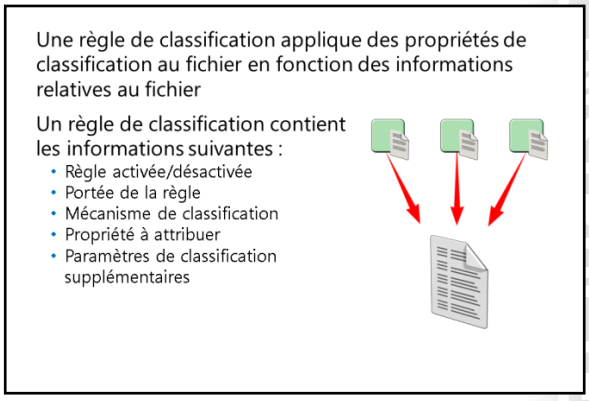
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Type de propriété	Description
Liste à choix multiples	Liste de valeurs qui peuvent être attribuées à une propriété. Plusieurs valeurs à la fois peuvent être attribuées à une propriété. Lorsque plusieurs valeurs sont combinées, chaque valeur dans la liste est utilisée.
Liste mise en ordre	Liste de valeurs fixes. Une seule valeur à la fois peut être attribuée à une propriété. Lorsque plusieurs valeurs sont combinées, c'est la valeur en première position dans la liste qui est utilisée.
Chaîne	Simple propriété de type chaîne. Lorsque plusieurs valeurs sont combinées, les valeurs en conflit empêchent la reclassification.
Chaîne multiple	Liste de chaînes qui peuvent être attribuées à une propriété. Plusieurs valeurs à la fois peuvent être attribuées à une propriété. Lorsque plusieurs valeurs sont combinées, chaque valeur dans la liste est utilisée.

Qu'est-ce qu'une règle de classification ?

Une règle de classification attribue une propriété de classification à un objet du système de fichiers. Elle comprend des informations indiquant à quel moment attribuer une propriété de classification à un fichier.



Principales propriétés des règles de classification

Pour définir le comportement d'une règle de classification, posez-vous les questions suivantes :

- La règle est-elle activée ? Dans la page **Propriétés** de la règle de classification, sous l'onglet **Paramètres de la règle**, la case à cocher **Activé** vous permet précisément de désactiver ou d'activer la règle de classification.
- Quelle est l'étendue de la règle ? Sous l'onglet **Paramètres de la règle**, le paramètre de **Étendue** vous permet de sélectionner un dossier ou des dossiers auxquels la règle de classification s'appliquera. Quand la règle est exécutée, elle traite et tente de classer tous les objets du système de fichiers dans cet emplacement.
- Quel mécanisme de classification la règle utilisera-t-elle ? Dans la page **Propriétés** de règle de classification, sous l'onglet **Classification** de la règle, vous devez choisir une méthode de classification que la règle utilisera pour attribuer à la propriété de classification. Par défaut, vous avez le choix entre deux méthodes :
    - *Classificateur de dossiers*. Le mécanisme de classificateur de dossiers attribue des propriétés à un fichier selon le chemin d'accès au dossier du fichier.
    - *Classifieur de contenus*. Le classifieur de contenus recherche des chaînes ou des expressions régulières dans les fichiers. Cela signifie qu'il classe un fichier en fonction du contenu textuel de ce fichier, par exemple selon qu'il contient un mot, une expression, une valeur numérique ou un type spécifique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Quelle propriété la règle attribuera-t-elle ? La fonction principale de la règle de classification consiste à attribuer une propriété à un objet de fichier selon la façon dont la règle s'applique à cet objet de fichier. Sous l'onglet **Classification**, vous devez spécifier une propriété et la valeur spécifique que la règle attribuera à cette propriété.
- Quels paramètres de classification supplémentaires seront utilisés ? L'essentiel de la logique de la règle tient dans les paramètres supplémentaires de classification. Le fait de cliquer sur le bouton **Avancé** sous l'onglet **Classification** ouvre la fenêtre de paramètres de classification supplémentaires. Dans cette fenêtre, vous pouvez spécifier des paramètres supplémentaires (y compris des chaînes ou des expressions régulières) qui, s'ils sont trouvés dans l'objet du système de fichiers, entraîneront l'application de la règle. Par exemple, ce paramètre pourrait être l'expression « Numéro de sécurité sociale » ou n'importe quel numéro ayant le format 000-00-000. S'il est trouvé, le paramètre de classification appliquera au fichier une valeur OUI pour une propriété de classification **Confidential**. Cette classification pourrait ensuite être exploitée pour effectuer des tâches sur l'objet du système de fichiers, par exemple pour le déplacer vers un emplacement sécurisé.

Un paramètre de classification peut être de l'un des trois types suivants :

- *RegularExpression*. Permet d'établir une correspondance avec une expression régulière à l'aide de la syntaxe Microsoft .NET. Par exemple, **\d\d\d** correspondra à n'importe quelle chaîne à trois chiffres.
- *StringCaseSensitive*. Permet d'établir une correspondance avec une chaîne respectant la casse. Par exemple, Confidential retournera comme correspondance Confidential', et non confidential ou CONFIDENTIAL.
- *String*. Permet d'établir une correspondance avec une chaîne quelle que soit la casse. Par exemple, Confidential retournera comme correspondance Confidential, non confidential et CONFIDENTIAL.

Planification des classifications

Vous pouvez exécuter des règles de classification de deux manières : à la demande ou selon une planification. Quelle que soit la méthode que vous choisissez, chaque fois que vous exécutez la classification, elle utilise toutes les règles que vous avez laissées dans l'état Activé.

La configuration d'une planification de classification vous permet de spécifier un intervalle régulier auquel les règles de classification des fichiers s'exécuteront, ce qui vous garantit que les fichiers de votre serveur sont régulièrement classés et à jour avec les dernières propriétés de classification.

Démonstration : Procédure de configuration de la gestion de la classification

Cette démonstration montre comment :

- créer une propriété de classification ;
- créer une règle de classification ;
- modifier la planification de la classification.

Procédure de démonstration

Créer une propriété de classification

1. Ouvrez le **Gestionnaire de ressources du serveur de fichiers**, puis développez le nœud **Gestion de la classification**.
2. À partir du nœud **Propriétés de classification**, créez un nœud **Propriété de classification** nommé **Confidentiel**, avec **Oui/Non** comme type de propriété.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Créer une règle de classification

1. À partir du nœud **Règles de classification**, créez un nœud **Règle de classification** nommé **Documents de paie confidentiels**.
2. Configurez la règle pour classer les documents en leur attribuant la valeur Oui pour la propriété de classification **Confidentiel** si le fichier contient l'expression de chaîne PAYROLL.

Modifier la planification de la classification

1. Créez une planification de classification qui s'exécute le **dimanche** à **8:30:00**.
2. À partir du nœud **Règle de classification**, lancez manuellement le processus **Exécuter la classification avec toutes les règles maintenant**, puis consultez le rapport.

Éléments à prendre en considération pour l'utilisation de la classification des fichiers

Bien que la gestion de classification fournisse un mécanisme puissant pour cataloguer, classer par catégorie et classer vos objets du système de fichiers, vous devez prendre en considération certains facteurs lorsque vous l'utilisez.

- Lors de l'utilisation de la classification de fichiers, tenez compte des éléments suivants :
  - Mode de stockage des propriétés de classification
  - Déplacement peut affecter les propriétés d'une classification de fichiers
  - Processus de gestion de la classification existe uniquement dans Windows Server 2008 R2 et les versions ultérieures
  - Possibilité des règles de classification d'entrer en conflit
  - Certains fichiers ne peuvent être pris en charge par la gestion de la classification

Mode de stockage des propriétés de classification

Les propriétés de classification sont enregistrées dans un flux de données de substitution, une fonctionnalité de NTFS. Si un fichier est déplacé entre volumes NTFS, les flux de données de substitution sont déplacés avec ce fichier, mais ils n'apparaissent pas dans son contenu. Dans les applications Microsoft Office, les propriétés de classification sont également enregistrées dans des formats de fichier en tant que propriétés de document personnalisé ou propriétés de document du serveur.

Impact du déplacement sur les propriétés de classification

Lorsque vous déplacez un fichier d'un système de fichiers NTFS vers un autre, si vous utilisez un mécanisme standard tel que la copie ou le déplacement, le fichier conserve ses propriétés de classification. En revanche, si vous déplacez un fichier vers un système de fichiers non NTFS, quel que soit le mode de déplacement de ce fichier, les propriétés de classification ne sont pas conservées. Si le fichier est le produit d'une application Microsoft Office, les propriétés de classification restent attachées, quelle que soit la façon dont le fichier est déplacé.

Processus de gestion de la classification dans Windows Server

Les propriétés de classification sont disponibles uniquement sur les serveurs exécutant Windows Server 2008 R2 ou une version ultérieure. Cependant, les documents Microsoft Office conservent les informations de propriétés de classification dans les propriétés des documents, qui sont consultables quel que soit le système d'exploitation utilisé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Règles de classification en conflit

Parfois, il arrive que des règles de classification entrent en conflit. Le cas échéant, l'infrastructure de classification des fichiers tente de combiner les propriétés. Les comportements suivants se produisent lorsque des règles de classification en conflit sont détectées :

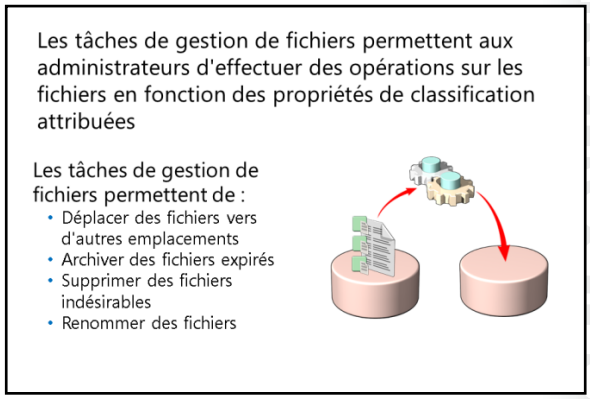
- Pour les propriétés Oui/Non, la valeur OUI est prioritaire sur la valeur NON.
- Pour les propriétés de liste mise en ordre, la valeur de propriété la plus élevée est prioritaire.
- Pour les propriétés de choix multiples, les jeux de propriétés sont combinés un en jeu.
- Pour les propriétés de chaîne multiple, une valeur de chaîne multiple contenant toutes les chaînes uniques des différentes valeurs de propriété est définie.
- Pour les autres types de propriétés, une erreur se produit.

Certains fichiers ne peuvent être pris en charge par la gestion de la classification

L'infrastructure de classification des fichiers n'identifie pas les fichiers individuels dans un conteneur, un fichier tel qu'un fichier .zip ou .vhd. En outre, elle ne permet pas la classification du contenu des fichiers chiffrés.

Que sont les tâches de gestion de fichiers ?

Les tâches de gestion de fichiers automatisent le processus de recherche des sous-ensembles de fichiers sur un serveur et d'application de commandes simples sur une base planifiée. Les fichiers sont identifiés par les propriétés de classification qui ont été attribuées au fichier par une règle de classification.



Les tâches de gestion de fichiers incluent une commande d'expiration de fichier, et vous pouvez également créer des tâches personnalisées. Vous pouvez définir les fichiers qui seront traités par une tâche de gestion de fichiers à l'aide des propriétés suivantes :

- Emplacement
- Propriétés de classification
- Heure de création
- Heure de modification
- Date du dernier accès
- Nom de fichier

Vous pouvez également configurer des tâches de gestion de fichiers afin d'informer les propriétaires de fichiers de toute stratégie imminente qui sera appliquée à leurs fichiers.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Tâches d'expiration de fichier

Les tâches d'expiration de fichier déplacent automatiquement tous les fichiers qui correspondent à certains critères vers un répertoire d'expiration spécifié, où un administrateur peut sauvegarder ces fichiers et les supprimer. Quand vous exécutez une tâche d'expiration de fichier, un nouveau répertoire est créé dans le répertoire d'expiration. Ce nouveau répertoire est groupé d'après le nom du serveur sur lequel la tâche a été exécutée, et son nom est défini en fonction de celui de la tâche de gestion de fichiers et de l'heure à laquelle elle a été exécutée. Quand un fichier expiré est découvert, il est déplacé vers le nouveau répertoire, tout en conservant sa structure de répertoire initiale.

Tâches de gestion de fichiers personnalisées

L'expiration n'est pas toujours une action souhaitable sur les fichiers. Les tâches de gestion de fichiers vous permettent d'exécuter des commandes personnalisées. À partir de la boîte de dialogue **Commandes personnalisées**, vous pouvez exécuter un fichier exécutable, un script ou toute autre commande personnalisée pour exécuter une opération sur les fichiers dans le cadre de la tâche de gestion de fichiers.

 **Remarque :** Pour configurer des tâches personnalisées, sélectionnez le type **Personnalisé** sous l'onglet **Action** de la fenêtre Créer une tâche de gestion de fichiers.

Démonstration : Procédure de configuration des tâches de gestion de fichiers

Dans cette démonstration, vous allez apprendre à :

- créer une tâche de gestion de fichiers ;
- configurer une tâche de gestion de fichiers pour faire expirer des documents.

Procédure de démonstration

Créer une tâche de gestion de fichiers

1. Ouvrez le **Gestionnaire de ressources du serveur de fichiers**, puis développez le nœud **Tâches de gestion de fichiers**.
2. Créez une tâche de gestion de fichiers nommée **Faire expirer les documents confidentiels** avec pour étendue **E:\Labfiles\Mod10\Data**.

Configurer une tâche de gestion de fichiers pour faire expirer des documents

1. Sous l'onglet **Action**, configurez la tâche pour l'expiration de fichiers dans **E:\Labfiles\Mod10\Expired**.
2. Ajoutez une condition indiquant que **Confidentiel** équivaut à **Oui**.
3. **Exécutez la tâche de gestion de fichiers**, puis affichez le rapport.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique A : Configuration des quotas et du filtrage des fichiers à l'aide de FSRM

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, au Royaume-Uni. Un bureau informatique et un centre de données assistent le siège social de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

Chaque client réseau dans le domaine Adatum est fourni avec un dossier de base reposant sur un serveur qui est utilisé pour enregistrer les documents ou fichiers personnels représentant les travaux en cours. Vous avez constaté que les dossiers de base sont de plus en plus volumineux et peuvent contenir des types de fichier tels que les fichiers .MP3 qui ne sont pas approuvés en raison de la stratégie d'entreprise. Vous décidez d'implémenter les quotas et le filtrage de fichiers FSRM pour résoudre ce problème.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- configurer des quotas FSRM ;
- configurer le filtrage de fichiers et générer un rapport de stockage.

Configuration de l'atelier pratique

Durée approximative : 30 minutes

Ordinateur(s) virtuel(s)	22411B-LON-DC1 22411B-LON-SVR1
Nom d'utilisateur	**Administrateur**
Mot de passe	**Pa$$w0rd**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
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. Effectuez les étapes 2 à 4 pour **22411B-LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configuration des quotas FSRM

Scénario

Pour contrôler la taille des dossiers de base, vous implémentez des quotas FSRM. Chaque dossier de base est limité à 100 Mo. Pour vous assurer que les administrateurs sont informés du manque d'espace dans les dossiers de base, un événement est écrit dans le journal d'événements lorsqu'un utilisateur dépasse 85 % de son quota de stockage, ce qui permet aux administrateurs d'effectuer un suivi.

Les tâches principales de cet exercice sont les suivantes :

1. créer un modèle de quota ;
2. configurer un quota à partir du modèle de quota ;
3. vérifier que le quota est fonctionnel.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un modèle de quota
2. Configurer un quota à partir du modèle de quota
3. Vérifier que le quota est fonctionnel

▶ Tâche 1 : Créer un modèle de quota

1. Sur LON-SVR1, depuis le Gestionnaire de serveur, installez le **Gestionnaire de ressources du serveur de fichiers**.
2. Dans la console Gestionnaire de ressources du serveur de fichiers, utilisez le nœud **Modèles de quotas** pour configurer un modèle qui fixe une limite inconditionnelle de **100 Mo** pour la taille maximale des dossiers.
3. Configurez le modèle pour enregistrer un événement dans le **journal des événements** quand la capacité du dossier atteint 85 % et 100 %.

▶ Tâche 2 : Configurer un quota à partir du modèle de quota

1. Utilisez la console Gestionnaire de ressources du serveur de fichiers et le nœud **Quotas** pour créer un quota dans le dossier **E:\Labfiles\Mod10\Users** à l'aide du modèle de quota créé à la tâche 1.
2. Configurez le quota de sorte qu'il s'applique automatiquement sur les sous-dossiers existants et nouveaux.
3. Créez un dossier supplémentaire nommé **Max** dans le dossier **E:\Labfiles\Mod10\Users** et vérifiez que ce nouveau dossier est répertorié dans la liste des quotas du Gestionnaire de ressources du serveur de fichiers.

▶ Tâche 3 : Vérifier que le quota est fonctionnel

1. Ouvrez une fenêtre Windows PowerShell et utilisez les commandes suivantes pour créer un fichier dans le dossier **E:\Labfiles\Mod10\Users\Max**. Appuyez sur Entrée après chaque ligne :

```
E:
cd \Labfiles\Mod10\Users\Max
fsutil file createnew file1.txt 89400000
```

2. Vérifiez l'Observateur d'événements pour **l'ID événement 12325**.

3. Vérifiez le fonctionnement du quota en tentant de créer un fichier dont la taille est égale à **16 400 000 octets**, puis appuyez sur Entrée :

```
fsutil file createnew file2.txt 16400000
```

4. Remarquez que le fichier ne peut pas être créé. Le message retourné par Windows fait référence à l'espace disque, mais la création du fichier a échoué car sa taille dépasserait la limite de quota. Fermez la fenêtre Windows PowerShell.
5. Fermez toutes les fenêtres ouvertes sur LON-SVR1.

Résultats : À la fin de cet exercice, vous devez avoir configuré un quota FSRM.

Exercice 2 : Configuration du filtrage de fichiers et des rapports de stockage

Scénario

Les responsables sont préoccupés par le fait que des fichiers multimédias soient stockés dans les dossiers de base, ce qui constitue une violation de la stratégie d'entreprise. Ils souhaitent empêcher l'enregistrement de ces fichiers, notamment des fichiers vidéo, audio et graphiques. Vous devez implémenter le filtrage de fichiers pour empêcher le stockage des fichiers multimédias dans les dossiers de base. Cependant, vous avez été également informés que plusieurs utilisateurs enregistrent des fichiers Microsoft Project avec l'extension .mpp dans leurs répertoires de base. Vous devez vous assurer que le filtre de fichiers que vous créez ne restreint pas le stockage de ces fichiers.

Vous devez également fournir un rapport à votre responsable documentant toutes les tentatives d'enregistrement de fichiers multimédias restreints sur LON-SVR1.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un filtre de fichiers
2. Créer un groupe de fichiers
3. Tester le filtre de fichiers
4. Générer un rapport de stockage à la demande
5. Pour préparer l'atelier suivant

▶ Tâche 1 : Créer un filtre de fichiers

1. Sur LON-SVR1, ouvrez le Gestionnaire de ressources du serveur de fichiers.
2. Créez un **filtre de fichiers** basé sur le modèle **Bloquer les fichiers audio et vidéo** pour le répertoire **E:\Labfiles\Mod10\Users**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer un groupe de fichiers

1. Sur LON-SVR1, ouvrez la boîte de dialogue **Options de configuration du Gestionnaire de ressources du serveur de fichiers**, puis sous l'onglet **Vérification du filtrage de fichiers**, activez l'option **Enregistrer l'activité de filtrage de fichiers dans la base de données de vérification**.

Remarque : cette étape permet d'enregistrer les événements de filtrage de fichiers. Les enregistrements générés fournissent des données pour un rapport de vérification du filtrage des fichiers, qui sera exécuté ultérieurement dans cet exercice.

2. Créez un nouveau groupe de fichiers avec les propriétés suivantes :
   - Nom du groupe de fichiers : **Fichiers multimédias de multiplexeur**
   - Fichiers à inclure : ***.mp***
   - Fichiers à exclure ***.mpp**
3. Modifiez le modèle **Bloquer les fichiers audio et vidéo** pour n'utiliser que le groupe de fichiers **Fichiers multimédias de multiplexeur**.

▶ Tâche 3 : Tester le filtre de fichiers

1. Dans la barre des tâches, cliquez sur le raccourci de l'**Explorateur de fichiers**.
2. Créez un nouveau document texte dans **E:\Labfiles\Mod10**, puis renommez-le **musicfile.mp3**.
3. Copiez **musicfile.mp3** dans **E:\Labfiles\Mod10\Users**. Vous allez être averti que le système n'a pas pu copier le fichier.

▶ Tâche 4 : Générer un rapport de stockage à la demande

1. Ouvrez la console **Gestionnaire de ressources du serveur de fichiers**.
2. Cliquez avec le bouton droit sur **Gestion des rapports de stockage**, sélectionnez **Générer les rapports maintenant**, puis fournissez les paramètres suivants :
   - Générez seulement le rapport **Vérification du filtrage des fichiers**.
   - Générez un rapport sur **E:\Labfiles\Mod10\Users**
3. Examinez les rapports générés dans Windows Internet Explorer.
4. Fermez toutes les fenêtres ouvertes sur LON-SVR1.

▶ Pour préparer l'atelier suivant

- Une fois l'atelier pratique terminé, n'arrêtez pas les ordinateurs virtuels. Vous allez en avoir besoin pour l'atelier pratique suivant.

Résultats : À la fin de cet exercice, vous aurez configuré des rapports de filtrage de fichiers et de stockage dans FSRM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Vue d'ensemble de DFS

Vous pouvez utiliser DFS pour surmonter les difficultés de gestion des données rencontrées par les succursales en fournissant un accès à tolérance de pannes et une réplication des fichiers sur réseau étendu (WAN) dans l'ensemble de l'entreprise.

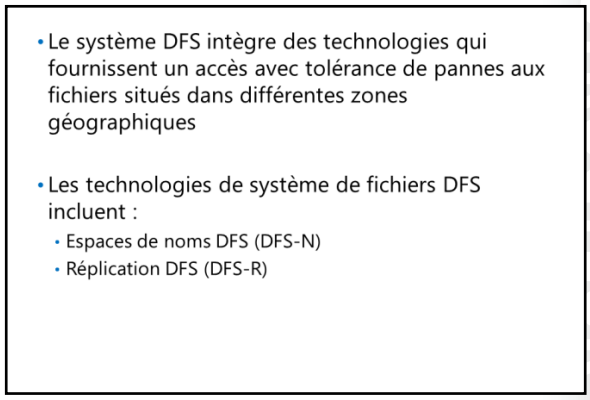
Objectifs de la leçon

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

- décrire le système de fichiers DFS ;
- décrire les espaces de noms DFS ;
- décrire la réplication DFS ;
- expliquer le fonctionnement des espaces de noms DFS et de la réplication DFS ;
- décrire la déduplication des données ;
- décrire les scénarios dans lesquels DFS peut être utilisé ;
- expliquer comment installer le rôle DFS.

Qu'est-ce que DFS ?

Les utilisateurs exigent généralement le nom UNC (Universal Naming Convention) pour accéder au contenu des dossiers partagés. Bon nombre des grandes entreprises possèdent des centaines de serveurs de fichiers qui sont répartis géographiquement au sein de l'organisation. Les utilisateurs sont confrontés à un grand nombre de difficultés lorsqu'ils tentent de rechercher des fichiers et d'y accéder efficacement.



En utilisant un espace de noms, DFS peut simplifier la structure de dossiers UNC. En outre, DFS peut répliquer l'espace de noms virtuel et les dossiers partagés sur plusieurs serveurs au sein de l'organisation. Les partages sont alors situés le plus proche possible des utilisateurs, qui bénéficient d'un avantage supplémentaire, à savoir la tolérance de panne pour les partages réseau.

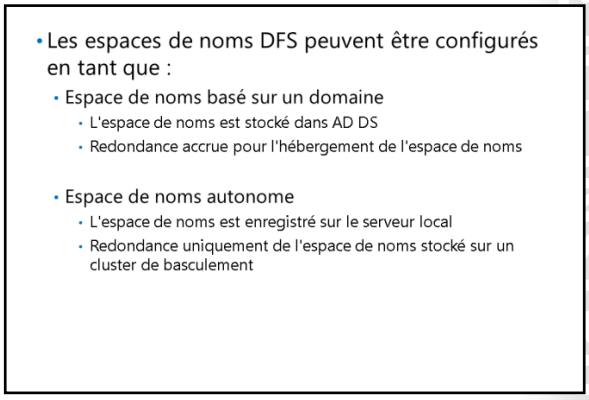
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

DFS comprend deux technologies qui sont implémentées en tant que services de rôle :

- Espace de noms DFS (DFS-N). Permet aux administrateurs de grouper les dossiers partagés se trouvant sur différents serveurs dans un ou plusieurs espaces de noms logiquement structurés. Chaque espace de noms apparaît aux utilisateurs comme un dossier partagé unique avec plusieurs sous-dossiers. Les sous-dossiers indiquent généralement des dossiers partagés qui se trouvent sur plusieurs serveurs dans différents sites géographiques disséminés dans l'organisation.
- DFS-R. Moteur de réplication multimaître qui synchronise les fichiers entre des serveurs pour des connexions à des réseaux locaux et étendus. La réplication DFS prend en charge la planification de réplication et la limitation de bande passante et utilise la compression différentielle à distance pour mettre à jour uniquement les parties de fichiers qui ont changé depuis la dernière réplication. Vous pouvez utiliser la réplication DFS conjointement avec les espaces de noms DFS ou comme un mécanisme de réplication de fichier autonome.

Qu'est-ce qu'un espace de noms DFS ?

Les espaces de noms DFS permettent une représentation virtuelle des structures de dossiers partagées. Vous pouvez créer un espace de noms basé sur un domaine ou autonome. Chaque type possède des caractéristiques différentes.



Espace de noms basé sur un domaine

Un espace de noms basé sur un domaine peut être utilisé dans le cas suivants :

- La haute disponibilité de l'espace de noms est requise, ce qui est garanti en répliquant l'espace de noms sur plusieurs serveurs d'espaces de noms.
- Vous devez masquer le nom des serveurs d'espaces de noms aux utilisateurs. Cela simplifie également le remplacement d'un serveur d'espace de noms ou la migration de l'espace de noms vers un autre serveur. Les utilisateurs accèdent alors au format *nom_domaine**espace_de_noms* au lieu du format *nom_serveur**partage*.

Si vous choisissez de déployer un espace de noms basé sur un domaine, vous devez également choisir entre le mode Microsoft Windows 2000 Server et le mode Windows Server 2008. Le mode Windows Server 2008 fournit d'autres avantages tels que la prise en charge de l'énumération basée sur l'accès, et il augmente le nombre de cibles de dossier de 5 000 à 50 000. Avec l'énumération basée sur l'accès, vous pouvez également masquer des dossiers que les utilisateurs ne sont pas autorisés à afficher.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour utiliser le mode Windows Server 2008, vous devez respecter les exigences suivantes :

- La forêt Active Directory® doit être au niveau fonctionnel de forêt Windows Server 2003 ou à un niveau supérieur.
- Le domaine Active Directory doit être au niveau fonctionnel du domaine Windows Server 2008.
- Tous les serveurs d'espaces de noms doivent fonctionner sous Windows Server 2008.

Espace de noms autonome

Un espace de noms autonome est utilisé dans les cas suivants :

- Une organisation n'a pas implémenté le service de domaine Active Directory (AD DS).
- Une organisation ne répond pas à la configuration requise pour le mode Windows Server 2008, un espace de noms basé sur un domaine, et il existe des besoins concernant plus de 5 000 dossiers DFS. Les espaces de noms DFS autonomes prennent en charge jusqu'à 50 000 dossiers avec des cibles.
- Une organisation héberge un espace de noms DFS dans un cluster de basculement.

Qu'est-ce que la réplication DFS ?

La réplication DFS permet d'assurer la synchronisation des dossiers entre les serveurs via des ordinateurs correctement connectés et des connexions à bande passante limitée. Veuillez prendre en compte les points clés suivants concernant la réplication DFS :

- Les caractéristiques de la réplication DFS sont les suivantes :
  - Utilise RDC
  - Utilise un dossier intermédiaire pour effectuer une copie intermédiaire d'un fichier avant de l'envoyer ou de le recevoir
  - Détecte les modifications sur le volume en surveillant le journal USN
  - Utilise un protocole d'échange de version vectoriel
  - Récupère en cas de défaillance

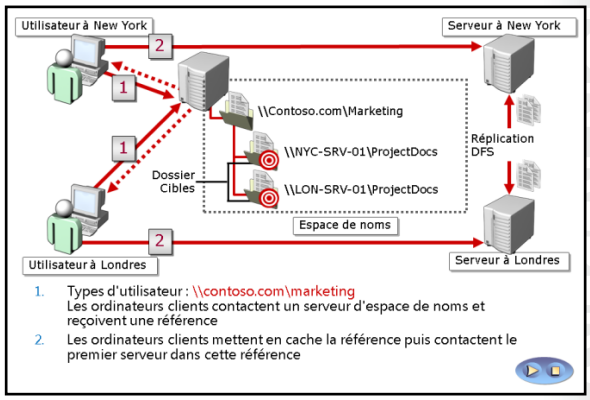
- La réplication DFS utilise la compression différentielle à distance (RDC). La compression différentielle à distance est un protocole client-serveur qui peut servir à mettre à jour des fichiers de manière efficace à travers un réseau à bande passante limitée. Elle détecte les insertions, suppressions ou réorganisations de données dans des fichiers, ce qui permet à la réplication DFS de répliquer uniquement les blocs de fichier modifiés lorsque les fichiers sont mis à jour. La compression différentielle à distance n'est utilisée que pour des fichiers qui ont une taille par défaut de 64 kilo-octets (Ko) ou supérieure. La réplication DFS prend également en charge la compression différentielle à distance entre fichiers, ce qui lui permet de l'utiliser même lorsqu'un fichier portant le même nom n'existe pas sur le poste client. La compression différentielle à distance entre fichiers peut déterminer les fichiers qui sont semblables au fichier qui doit être répliqué, et elle utilise des blocs de fichiers semblables qui sont identiques au fichier de réplication pour réduire la quantité de données à répliquer.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- La réplication DFS utilise un dossier intermédiaire masqué pour effectuer une copie intermédiaire d'un fichier avant de l'envoyer ou de le recevoir. Les dossiers intermédiaires agissent comme des caches pour les fichiers nouveaux et modifiés à répliquer depuis des membres d'envoi vers des membres de réception. Le membre d'envoi commence à créer une copie intermédiaire d'un fichier lorsqu'il reçoit une demande du membre de réception. Le processus implique la lecture du fichier depuis le dossier répliqué et la création d'une représentation compressée du fichier dans le dossier intermédiaire. Après sa création, le fichier intermédiaire est envoyé au membre de réception ; si la compression différentielle à distance est utilisée, seule une partie du fichier intermédiaire peut être répliquée. Le membre de réception télécharge les données et crée le fichier dans son dossier intermédiaire. Une fois le téléchargement du fichier terminé sur le membre de réception, la réplication DFS décompresse le fichier et l'installe dans le dossier répliqué. Chaque dossier répliqué possède son propre dossier intermédiaire, qui, par défaut, se trouve sous le chemin d'accès local du dossier répliqué dans le dossier DFSrPrivate\Staging.
- La réplication DFS détecte des modifications sur le volume en surveillant le journal du nombre de séquences de mise à jour du système de fichiers, puis réplique les modifications uniquement après la fermeture du fichier.
- La réplication DFS utilise une version de protocole d'échange vectoriel pour déterminer les fichiers qui doivent être synchronisés. Le protocole envoie moins d'1 Ko par fichier à travers le réseau pour synchroniser les métadonnées associées aux fichiers modifiés sur les membres d'envoi et de réception.
- La réplication DFS utilise un heuristique de résolution de conflit « le dernier auteur l'emporte » pour les fichiers en conflit (autrement dit, un fichier mis à jour simultanément sur plusieurs serveurs) et « le premier créateur l'emporte » pour les conflits de nom. Les fichiers et les dossiers qui perdent la résolution de conflit sont déplacés vers un dossier appelé dossier des fichiers en conflit et supprimés. Vous pouvez également configurer le service de manière à déplacer des fichiers supprimés vers le dossier des fichiers en conflit et supprimés, en vue d'une récupération en cas de suppression du fichier ou du dossier. Chaque dossier répliqué possède son propre dossier masqué des fichiers en conflit et supprimés, qui se trouve sous le chemin d'accès local du dossier répliqué dans le dossier DFSrPrivate\ConflictandDeleted.
- La réplication DFS s'auto-adapte et peut récupérer automatiquement des dépassements de taille de journal USN, d'une perte du journal USN ou de la perte de la base de données de réplication DFS.
- La réplication DFS utilise un fournisseur Windows Management Instrumentation (WMI) qui fournit des interfaces pour obtenir des informations sur la configuration et l'analyse du service de réplication DFS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fonctionnement des espaces de noms DFS et de la réplication DFS



Bien que les espaces de noms DFS et la réplication DFS soient des services de rôle distincts, vous pouvez les utiliser ensemble pour fournir une haute disponibilité et une redondance des données. Le processus suivant explique comment les espaces de noms DFS et la réplication DFS fonctionnent ensemble :

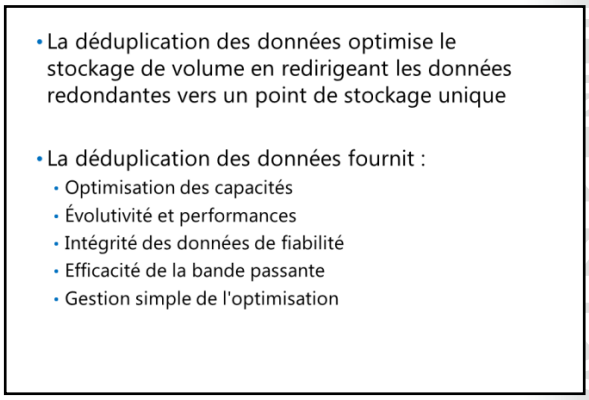
1. Un utilisateur accède à un dossier dans l'espace de noms virtuel. Lorsqu'il essaie d'accéder à un dossier dans un espace de noms, l'ordinateur client contacte le serveur qui héberge la racine d'espace de noms. Le serveur hôte peut être un serveur autonome qui héberge un espace de noms autonome, ou une configuration basée sur un domaine stockée dans les services de domaine Active Directory (AD DS). Il est ensuite répliqué à différents emplacements pour fournir une haute disponibilité. Le serveur d'espace de noms renvoie à l'ordinateur client une référence qui contient une liste de serveurs qui hébergent les dossiers partagés (appelés cibles de dossier) associés au dossier auquel il accède. DFS est une technologie orientée site, par conséquent les ordinateurs clients peuvent être configurés pour accéder d'abord aux espaces de noms se trouvant dans leur site afin de garantir un accès le plus fiable possible.
2. L'ordinateur client accède au premier serveur dans la référence. L'ordinateur client met en cache les informations de référence puis contacte le premier serveur dans la référence. Cette référence correspond en général à un serveur dans le propre site du client, à moins que ce dernier ne comporte aucun serveur. Dans ce cas, l'administrateur peut configurer la priorité cible.

Dans l'exemple de la diapositive, le dossier Marketing publié dans l'espace de noms contient deux cibles de dossier. Un partage se trouve sur un serveur de fichiers à New York, et l'autre partage sur un serveur de fichiers à Londres. La synchronisation des dossiers partagés est assurée par la réplication DFS. Bien que plusieurs serveurs hébergent les dossiers source, ceci est transparent pour les utilisateurs, qui accèdent seulement à un dossier unique dans l'espace de noms. Si l'un des dossiers cibles devient indisponible, les utilisateurs seront redirigés vers les cibles restantes dans l'espace de noms.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que la déduplication des données ?



Dans Windows Server 2012, vous pouvez activer la déduplication des données pour des volumes non-système. La déduplication des données optimise le stockage de volume en recherchant des données redondantes sur un volume et en vérifiant que les données ne sont enregistrées qu'une seule fois sur le volume. Pour ce faire, les données sont stockées à un emplacement unique et une référence est attribuée à cet emplacement pour les autres copies redondantes des données. Les données sont segmentées en blocs de 32 à 218 Ko. La déduplication des données permet donc d'optimiser non seulement les fichiers redondants, mais également les parties de fichiers qui sont redondantes sur le volume.

La déduplication des données peut être implémentée en même temps que la réplication DFS pour fournir une infrastructure de stockage et de réplication encore plus efficace.

Fonctionnement de la déduplication des données

Lorsque la déduplication des données est activée pour un volume, Windows 2012 optimise les volumes en tenant à jour les composants suivants :

- *Fichiers non optimisés*. Il s'agit des fichiers qui ne répondent pas aux critères d'ancienneté pour la déduplication des données. Pour être optimisés par la déduplication des données, les fichiers doivent rester statiques pendant un certain temps. Les fichiers non optimisés peuvent inclure les fichiers d'état du système, les fichiers chiffrés, les fichiers d'une taille inférieure à 32 Ko, les fichiers avec des attributs étendus ou les fichiers utilisés par d'autres applications.
- *Fichiers optimisés*. Ils sont enregistrés en tant que points d'analyse. Un point d'analyse contient un pointeur vers les emplacements des données de bloc dans le magasin de blocs ; les blocs respectifs peuvent donc être récupérés en cas de besoin.
- *Magasin de blocs*. Les données des fichiers optimisés sont situées dans le magasin de blocs.

Avantages de la déduplication des données

La déduplication des données peut vous aider à faire face à la croissance du stockage dans les domaines suivants :

- Optimisation des capacités. La déduplication des données permet à un serveur de stocker davantage de données dans un espace disque physique réduit.
- Évolutivité et performances. Le déduplication des données est très évolutive dans Windows Server 2012. Elle peut fonctionner sur plusieurs volumes sans affecter d'autres services et applications s'exécutant sur le serveur. Il est également possible de la limiter afin de gérer d'autres charges de travail lourdes sur le serveur, de sorte qu'aucune dégradation des performances ne se produise pour les tâches serveur importantes.

- Intégrité des données de fiabilité. Windows Server 2012 utilise une somme de contrôle. Cohérence et validation pour garantir l'intégrité des données affectées par la déduplication. La déduplication de données gère également les copies redondantes des données utilisées le plus souvent sur un volume pour offrir une protection contre la corruption des données.
- Efficacité de la bande passante. Associée à la réplication DFS ou à une autre technologie de réplication de fichier telle que BranchCache, la déduplication des données peut réduire considérablement la bande passante consommée lors de la réplication des données de fichier, à condition que les partenaires de réplication exécutent également Windows Server 2012.
- Gestion simple de l'optimisation. Windows Server 2012 et Windows PowerShell 3.0 offrent une prise en charge intégré de la déduplication des données. L'implémentation et la gestion dans Windows Server 2012 sont effectuées avec des outils familiers.

Implémentation de la déduplication des données

Utilisez le processus suivant pour implémenter la déduplication des données sur un serveur :

1. Installez le service Déduplication des données du rôle Services de fichiers.

   Pour ce faire, utilisez l'Assistant Ajout de rôles et de fonctionnalités dans le Gestionnaire de serveur, ou exécutez les applets de commande Windows PowerShell suivantes :

   ```
   Import-Module ServerManager
   Add-WindowsFeature -name FS-Data-Deduplication
   Import-Module Deduplication
   ```

2. Activez la déduplication des données sur un ou plusieurs volumes.

   Dans le Gestionnaire de serveur, vous pouvez cliquer avec le bouton droit sur un volume et sélectionner Configurer la déduplication des données, ce qui ouvre la page Paramètres de déduplication des données.

   Vous pouvez également utiliser l'applet de commande Windows PowerShell suivante pour activer la déduplication des données (dans le cas présent, pour le volume E:) :

   ```
   Enable-DedupVolume E:
   ```

3. Éventuellement, configurez des travaux de déduplication des données pour un volume.

   Par défaut, des travaux intégrés sont créés et planifiés lorsque vous activez la déduplication des données pour un volume. Si nécessaire, vous pouvez configurer manuellement ces travaux ou en créer d'autres afin de gérer de manière plus approfondie le fonctionnement de la déduplication des données.

 **Documentation supplémentaire :** Vue d'ensemble de la déduplication des données
http://go.microsoft.com/fwlink/?linkID=270996

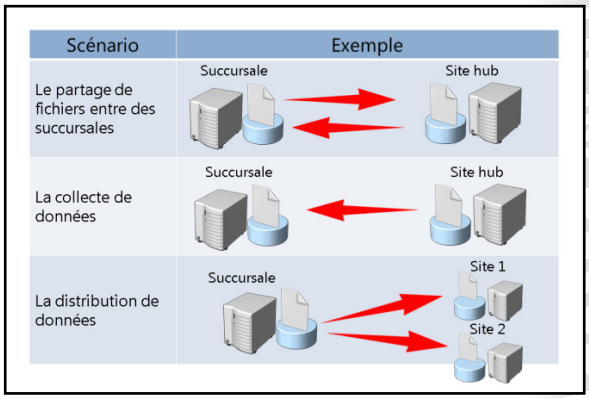
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Scénarios mettant en jeu DFS

Plusieurs scénarios clés peuvent bénéficier des services Espace de noms DFS et Réplication DFS. Ces scénarios incluent :

- le partage de fichiers entre succursales ;
- la collecte de données ;
- la distribution de données.



Partage de fichiers entre succursales

Les grandes organisations qui ont de nombreuses succursales doivent souvent partager des fichiers ou collaborer entre ces différents sites. La réplication DFS peut aider à répliquer des fichiers entre des succursales, ou d'une succursale vers un site concentrateur. Avoir des fichiers dans plusieurs succursales arrange également les utilisateurs qui se déplacent d'une succursale à une autre. Les modifications que les utilisateurs apportent à leurs fichiers dans une succursale sont répliquées à leur succursale.

Remarque : Ce scénario est recommandé uniquement si les utilisateurs peuvent tolérer des incohérences de fichier lorsque les modifications sont répliquées sur l'ensemble des serveurs de succursale. Notez également que la réplication DFS réplique un fichier uniquement après sa fermeture. Par conséquent, elle n'est pas recommandée pour répliquer des fichiers de base de données ou tout fichier maintenu ouvert pendant de longues périodes.

Collecte de données

Les technologies DFS peuvent collecter des fichiers d'une succursale et les répliquer sur un site concentrateur, ce qui permet une utilisation des fichiers à différentes fins. Des données essentielles peuvent être répliquées sur un site concentrateur à l'aide de la réplication DFS, puis sauvegardées sur le site concentrateur à l'aide de procédures de sauvegarde standard. Cela augmente la faculté de récupération des données de la succursale en cas d'échec d'un serveur, car les fichiers seront disponibles depuis deux emplacements séparés et sauvegardés. De plus, les sociétés réduisent les coûts relatifs à leurs succursales, le matériel de sauvegarde et le savoir-faire du personnel informatique n'étant plus nécessaires sur site. Les données répliquées peuvent également être utilisées pour que des partages de fichiers de succursale tolèrent les pannes. Si le serveur de la succursale échoue, les clients dans la succursale peuvent accéder aux données répliquées sur le site concentrateur.

Distribution de données

Vous pouvez utiliser les espaces de noms DFS et la réplication DFS pour publier et répliquer des documents, des logiciels et d'autres données métier à travers votre organisation. Les espaces de noms DFS et les cibles de dossier peuvent accroître la disponibilité des données et répartir la charge du client entre plusieurs serveurs de fichiers.

Démonstration : Procédure d'installation du rôle DFS

La démonstration suivante montre comment installer le rôle DFS.

Procédure de démonstration

Installer le rôle DFS

- Sous le rôle **Service de fichiers et de stockage (Installé)**, installez les rôles de service **Espaces de noms DFS** et **Réplication DFS**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 5
Configuration des espaces de noms DFS

La configuration d'un espace de noms DFS est constituée de plusieurs tâches comprenant la création de la structure d'espace de noms, la création de dossiers dans l'espace de noms et l'ajout de cibles de dossier. Vous pouvez aussi choisir d'effectuer des tâches de gestion supplémentaires, telles que la configuration de l'ordre des références, la restauration du client et l'implémentation de la réplication DFS. Cette leçon fournit des informations sur la manière d'effectuer ces tâches de configuration et de gestion pour déployer une solution DFS efficace.

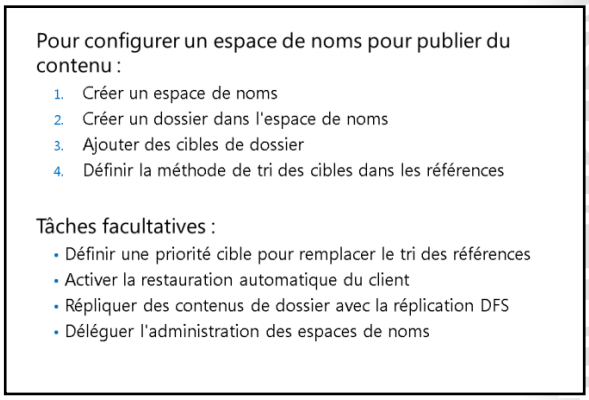
Objectifs de la leçon

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

- décrire le processus de déploiement d'espaces de noms pour publier du contenu ;
- décrire les autorisations requises pour créer et gérer un espace de noms ;
- expliquer comment créer et configurer des espaces de noms et des cibles de dossier DFS ;
- décrire les options d'optimisation d'un espace de noms.

Déploiement d'espaces de noms pour publier du contenu

La plupart des implémentations DFS sont principalement constituées de contenu publié dans l'espace de noms DFS. Pour configurer un espace de noms pour publier du contenu pour les utilisateurs, procédez comme suit :



1. Créer un espace de noms.

   Utilisez l'Assistant Nouvel espace de noms pour créer l'espace de noms à partir de la console Gestion DFS. Lorsqu'un nouvel espace de noms est créé, vous devez fournir le nom du serveur à utiliser comme serveur d'espace de noms, ainsi que le nom de l'espace de noms et son type (basé sur un domaine ou autonome). Vous pouvez également spécifier si l'espace de noms est activé pour le mode Windows Server 2008.

2. Créer un dossier dans l'espace de noms.

   Après avoir créé l'espace de noms, ajoutez-y un dossier pour y placer le contenu que vous souhaitez publier. Au cours de la création de dossier, vous pouvez ajouter des cibles de dossier ou effectuer une autre tâche pour ajouter, modifier ou supprimer des cibles de dossier ultérieurement.

3. Ajouter des cibles de dossier.

   Une fois que vous avez créé un dossier dans l'espace de noms, la tâche suivante consiste à créer des cibles de dossier. La cible de dossier est un chemin d'accès UNC d'un dossier partagé sur un serveur spécifique. Vous pouvez rechercher des dossiers partagés sur des serveurs distants et créer des dossiers partagés si nécessaire. Vous pouvez également ajouter plusieurs cibles de dossier pour augmenter la disponibilité du dossier dans l'espace de noms. Si vous ajoutez plusieurs cibles de dossier, pensez à utiliser la réplication DFS pour vous assurer que le contenu est identique entre les cibles.

4. Définir la méthode de classement des cibles dans les références.

   Une référence est une liste triée de cibles reçues par un ordinateur client à partir du serveur d'espace de noms, lorsqu'un utilisateur accède à une racine d'espace de noms ou à un dossier. Lorsqu'un client reçoit la référence, il essaie d'accéder à la première cible dans la liste. Si la cible n'est pas disponible, la cible suivante est tentée. Par défaut, les cibles dans le site du client sont toujours répertoriées en premier dans la référence. Vous pouvez configurer la méthode pour trier des cibles en dehors du site du client, sous l'onglet **Références** de la boîte de dialogue **Propriétés de espace de noms**. Vous avez le choix entre configurer le coût le plus bas, effectuer un tri de manière aléatoire ou configurer la méthode de tri de manière à exclure les cibles en dehors du site du client.

 **Remarque :** Les dossiers héritent des paramètres de référence à partir de la racine d'espace de noms. Vous pouvez remplacer les paramètres d'espace de noms sous l'onglet **Références** de la boîte de dialogue **Propriétés du dossier**, en excluant des cibles en dehors du site du client.

Tâches de gestion facultatives

Il existe plusieurs tâches de gestion facultatives que vous pouvez prendre en considération :

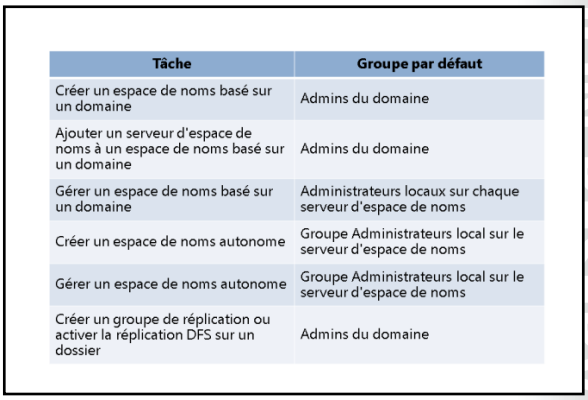
- Définir une priorité cible pour remplacer le tri des références. Vous pouvez disposer d'une cible de dossier spécifique que vous souhaitez que tout le monde utilise depuis tous les emplacements de site, ou définir une cible de dossier spécifique qui doit être utilisée en dernier parmi toutes les cibles. Vous pouvez configurer ces scénarios en remplaçant l'ordre des références sous l'onglet **Avancé** de la boîte de dialogue **Propriétés de cible de dossier**.
- Activer la restauration automatique du client. Si un client ne peut pas accéder à une cible référencée, la cible suivante est sélectionnée. La restauration vérifie que les clients sont restaurés automatiquement à la cible d'origine une fois qu'elle a été restaurée. Vous pouvez configurer la restauration automatique du client sous l'onglet **Références** de la boîte de dialogue **Propriétés de espace de noms**, en activant la case à cocher **Restauration automatique des clients sur les cibles préférées**. Tous les dossiers et cibles de dossier héritent de cette option. Cependant, vous pouvez également remplacer un dossier spécifique pour activer ou désactiver les fonctions de restauration automatique du client, si nécessaire.
- Répliquer des cibles de dossier à l'aide de la réplication DFS. Vous pouvez utiliser la réplication DFS pour assurer la synchronisation du contenu de cibles de dossier. La prochaine rubrique présente la réplication DFS en détail.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Autorisations requises pour créer et gérer un espace de noms

Pour effectuer des tâches de gestion d'espace de noms DFS, un utilisateur doit être membre d'un groupe d'administration ou recevoir une autorisation spécifique. Pour déléguer les autorisations requises, cliquez avec le bouton droit sur l'espace de noms, puis cliquez sur **Déléguer les autorisations de gestion**.

Le tableau suivant décrit les groupes qui peuvent exécuter l'administration de DFS par défaut, ainsi que la méthode pour déléguer la capacité d'effectuer des tâches de gestion DFS.



Tâche	Groupe par défaut
Créer un espace de noms basé sur un domaine	Admins du domaine
Ajouter un serveur d'espace de noms à un espace de noms basé sur un domaine	Admins du domaine
Gérer un espace de noms basé sur un domaine	Administrateurs locaux sur chaque serveur d'espace de noms
Créer un espace de noms autonome	Groupe Administrateurs local sur le serveur d'espace de noms
Gérer un espace de noms autonome	Groupe Administrateurs local sur le serveur d'espace de noms
Créer un groupe de réplication ou activer la réplication DFS sur un dossier	Admins du domaine

Tâche	Groupes qui peuvent effectuer la tâche par défaut	Méthode de délégation
Créer un espace de noms basé sur un domaine	Admins du domaine	Cliquez sur **Déléguer les autorisations de gestion**.
Ajouter un serveur d'espace de noms à un espace de noms basé sur un domaine	Admins du domaine	Ajoutez des utilisateurs au groupe d'administrateurs locaux sur le serveur d'espace de noms.
Gérer un espace de noms basé sur un domaine	Administrateurs locaux sur chaque serveur d'espace de noms	Cliquez sur **Déléguer les autorisations de gestion**.
Créer un espace de noms autonome	Administrateurs locaux sur chaque serveur d'espace de noms	Ajoutez des utilisateurs au groupe d'administrateurs locaux sur le serveur d'espace de noms.
Gérer un espace de noms autonome	Administrateurs locaux sur chaque serveur d'espace de noms	Cliquez sur **Déléguer les autorisations de gestion**.
Créer un groupe de réplication ou activer la réplication DFS sur un dossier	Admins du domaine	Ajoutez des utilisateurs au groupe d'administrateurs locaux sur le serveur d'espace de noms.

Démonstration : Procédure de création des espaces de noms

Cette démonstration montre comment :

- créer un espace de noms ;
- créer un dossier et une cible de dossier.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

Créer un espace de noms

1. Ouvrez la console Gestion du système de fichiers distribués DFS.
2. Sur LON-SVR1, créez un espace de noms basé sur un domaine nommé **Research**.

Créer un dossier et une cible de dossier

1. Créez un dossier nommé **Proposals** dans l'espace de noms **\\Adatum.com\Research**.
2. Créez une cible de dossier pour **Proposals** qui pointe vers **\\LON-SVR1\Proposal_docs**.
3. Vérifiez la fonctionnalité de l'espace de noms en accédant à **\\Adatum.com\Research** et en vous assurant que le dossier **Proposals** s'affiche.

Optimisation d'un espace de noms

Les espaces de noms possèdent plusieurs options de configuration grâce auxquelles vous pouvez optimiser leur facilité d'utilisation et leurs performances.

- Les méthodes pour optimiser un espace de noms sont les suivantes :
  - Renommer ou déplacer un dossier
  - Désactiver des références à un dossier
  - Spécifier la durée du cache de référence
  - Configurer l'interrogation d'espace de noms

Renommer ou déplacer un dossier

Vous pouvez renommer ou déplacer un dossier dans un espace de noms. Cela vous permet de réorganiser la hiérarchie de dossiers pour répondre du mieux possible aux besoins des utilisateurs de votre organisation. Par exemple, lors d'une réorganisation de votre société, vous pouvez réorganiser l'espace de noms pour qu'il corresponde à la nouvelle structure.

Désactiver des références à un dossier

Une référence est une liste de cibles qu'un ordinateur client reçoit d'un contrôleur de domaine ou d'un serveur d'espace de noms lorsque l'utilisateur accède à une racine ou un dossier avec des cibles d'espace de noms. En désactivant la référence d'une cible de dossier, vous empêchez des ordinateurs clients d'accéder à cette cible de dossier dans l'espace de noms. Cela se révèle utile lorsque vous déplacez des données entre serveurs.

Spécifier la durée du cache de référence

Les clients ne contactent pas un serveur d'espace de noms pour obtenir une référence chaque fois qu'ils accèdent à un dossier dans un espace de noms ; au lieu de cela, des références de racine de l'espace de noms sont mises en cache. Les clients qui utilisent une référence mise en cache renouvellent la valeur de durée du cache de la référence à chaque accès à un fichier ou à un dossier à l'aide de cette référence. Cela signifie que les clients utilisent la référence indéfiniment, jusqu'à ce que le cache de la référence soit effacé ou que le client soit redémarré. Vous pouvez personnaliser la durée du cache de référence. La valeur par défaut est de 300 secondes (5 minutes).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configurer l'interrogation d'espace de noms

Pour maintenir la cohérence d'un espace de noms basé sur un domaine entre les serveurs d'espace de noms, ceux-ci doivent interroger périodiquement AD DS pour obtenir les données d'espace de noms les plus récentes. Les deux modes d'interrogation d'espace de noms sont les suivants :

- *Optimiser pour la cohérence*. Les serveurs d'espace de noms interrogent l'émulateur de contrôleur de domaine principal (PDC) chaque fois qu'une modification de l'espace de noms se produit. Il s'agit de la valeur par défaut.
- *Optimiser pour l'évolutivité*. Chaque serveur d'espace de noms interroge son contrôleur de domaine le plus proche à intervalles périodiques.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 6
Configuration et résolution des problèmes de la réplication DFS

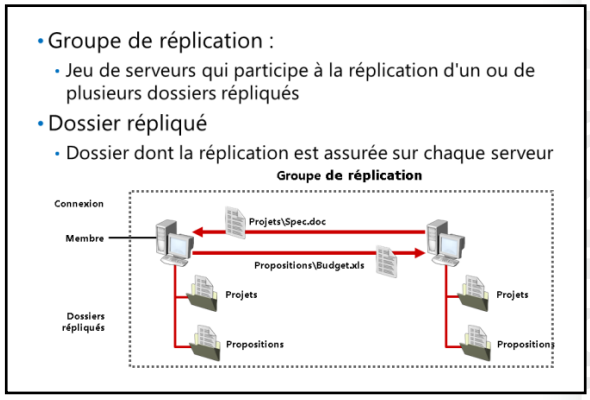
Pour configurer la réplication DFS efficacement, il est important de comprendre la terminologie et les spécifications associées à la fonctionnalité. Cette leçon fournit des informations sur les éléments spécifiques, la configuration requise et les éléments d'évolutivité à prendre en considération lorsqu'ils sont liés à la réplication DFS. Elle fournit également un processus pour configurer une topologie de réplication efficace.

Objectifs de la leçon

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

- décrire les groupes de réplication et les dossiers répliqués ;
- décrire le processus de réplication initiale ;
- expliquer comment configurer les services Espace de noms DFS et Réplication DFS ;
- décrire les options de résolution des problèmes liés à DFS ;

Groupes de réplication et dossiers répliqués



Un groupe de réplication se compose d'un jeu de serveurs membres qui participe à la réplication d'un ou de plusieurs dossiers répliqués. Il existe essentiellement deux types principaux de groupes de réplication :

- Groupe de réplication multi-usage.
  Ce groupe de réplication permet de configurer la réplication entre deux serveurs ou plus pour la publication, le partage de contenu ou d'autres scénarios.
- Groupe de réplication pour la collecte de données. Ce groupe de réplication configure une réplication bidirectionnelle entre deux serveurs, tels qu'un serveur de succursale et un serveur concentrateur. Ce type de groupe est utilisé pour collecter des données depuis le serveur de succursale vers le serveur concentrateur. Vous pouvez utiliser ensuite le logiciel de sauvegarde standard pour sauvegarder les données du serveur concentrateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Un dossier répliqué est synchronisé entre chaque serveur membre. La création de plusieurs dossiers répliqués dans un groupe de réplication unique aide à simplifier les éléments suivants pour la totalité du groupe :

- Type de groupe de réplication
- Topologie
- Configuration hub and spoke
- Planification de la réplication
- Limitation de bande passante

Les dossiers répliqués stockés sur chaque membre peuvent se trouver sur différents volumes dans le membre. Les dossiers répliqués n'ont pas besoin d'être des dossiers partagés ni de faire partie d'un espace de noms, bien que le composant logiciel enfichable Gestion du système de fichiers distribués DFS facilite le partage des dossiers répliqués et les publie éventuellement dans un espace de noms existant.

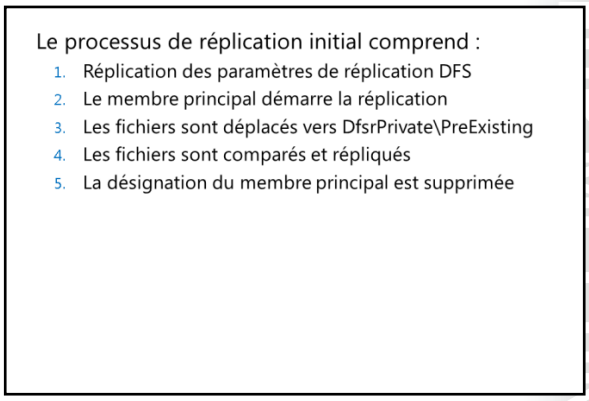
Topologies de réplication

Lorsque vous configurez un groupe de réplication, vous devez définir sa topologie. Vous pouvez choisir entre les éléments suivants :

- Hub and Spoke. Pour sélectionner cette option, vous avez besoin d'au moins trois serveurs membres dans le groupe de réplication. Cette topologie fonctionne bien dans des scénarios de publication où les données proviennent du concentrateur et sont répliquées sur les membres spoke.
- Maille pleine. Si dix membres ou moins font partie du groupe de réplication, cette topologie fonctionne bien, chaque membre effectuant une réplication vers les autres, en fonction des besoins.
- Aucune topologie. Choisissez cette option si vous souhaitez configurer manuellement une topologie personnalisée après avoir créé le groupe de réplication.

Processus de réplication initiale

Lorsque vous configurez la réplication pour la première fois, vous choisissez un membre principal qui dispose des fichiers les plus à jour à répliquer. Ce serveur est considéré comme faisant autorité pour toute résolution de conflit qui se produit lorsque les membres de réception possèdent des fichiers qui sont plus anciens ou plus récents par rapport aux mêmes fichiers sur le membre principal.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Prenez en considération les concepts suivants au sujet du processus de réplication initiale :

- La réplication initiale ne commence pas immédiatement. Les paramètres de topologie et de réplication DFS doivent être répliqués à tous les contrôleurs de domaine, et chaque membre du groupe de réplication doit interroger son contrôleur de domaine le plus proche pour obtenir ces paramètres. La latence de réplication Active Directory et le long intervalle d'interrogation (60 minutes) sur chaque membre déterminent la durée nécessaire.
- La réplication initiale se produit toujours entre le membre principal et ses partenaires de réplication de réception. Après avoir reçu tous les fichiers du membre principal, un membre réplique des fichiers sur ses partenaires de réception. Ainsi, la réplication d'un nouveau dossier répliqué démarre depuis le membre principal puis progresse pour s'étendre aux autres membres du groupe de réplication.
- Lors de la réception de fichiers du membre principal pendant la réplication initiale, les membres de réception qui contiennent des fichiers qui ne figurent pas sur le membre principal déplacent ces fichiers vers leur dossier DFSrPrivate\PreExisting respectif. Si un fichier est physiquement identique à un fichier sur le membre principal, ce fichier n'est pas répliqué. Si la version d'un fichier sur le membre de réception est différente de la version du membre principal, la version du membre de réception est déplacée vers le dossier des fichiers en conflit et supprimés, et la compression différentielle à distance (RDC) peut être utilisée pour télécharger uniquement les blocs modifiés.
- Pour déterminer si des fichiers sont identiques sur le membre principal et le membre de réception, la réplication DFS compare les fichiers à l'aide d'un algorithme de hachage. Si les fichiers sont identiques, seules les métadonnées minimales sont transférées.
- Après l'initialisation du dossier répliqué, la désignation de membre principal est supprimée. (L'initialisation a lieu une fois que tous les fichiers qui existent avant la configuration de la réplication DFS sont ajoutés à la base de données de réplication DFS). Ce membre est ensuite traité comme tout autre membre et ses fichiers ne sont plus considérés comme faisant autorité sur d'autres membres qui ont effectué la réplication initiale. Tout membre qui a effectué la réplication initiale est considéré comme faisant autorité sur les membres qui n'ont pas effectué la réplication initiale.

Démonstration : Procédure de configuration de la réplication DFS

Dans cette démonstration, vous allez apprendre à :

- créer une cible de dossier pour la réplication ;
- créer un groupe de réplication.

Procédure de démonstration

Créer une cible de dossier pour la réplication

- Sur LON-SVR1, créez une cible de dossier pour **\\LON-SVR4\Proposal_docs**.

Créer un groupe de réplication

1. Ajoutez le dossier au groupe de réplication pour **LON-SVR1** et **LON-SVR4**.
2. Déclarez **LON-SVR1** en tant que membre principal et créez une réplication de maille pleine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Résolution des problèmes liés à DFS

Windows Server 2012 fournit plusieurs outils permettant de surveiller et résoudre les problèmes de réplication DFS. Ces outils sont les suivants :

Outil	Utilisation
Rapport d'intégrité	Créer un rapport sur les statistiques de réplication et l'intégrité générale de la topologie
Test de propagation	Générer un fichier de test pour vérifier la réplication
Rapport de propagation	Créer un rapport sur le test de propagation et fournir des statistiques de réplication
Vérifier la topologie	Créer un rapport sur l'état actuel des membres de la topologie
Dfsrdiag.exe	Surveiller l'état de réplication du service de réplication DFS

- *Rapports de diagnostic*. Utilisez cet outil pour exécuter un rapport de diagnostic pour ce qui suit :
  - Rapport d'intégrité. Affiche des statistiques et des rapports complets sur l'intégrité et l'efficacité de la réplication.
  - Test de propagation. Génère un fichier de test dans un dossier répliqué pour vérifier la réplication et fournir des statistiques sur le rapport de propagation.
  - Rapport de propagation. Fournit des informations sur la progression pour le fichier de test qui est généré pendant un test de propagation. Ce rapport permet de s'assurer que la réplication est fonctionnelle.
- *Vérifier la topologie*. Utilisez cet outil pour vérifier le statut de la topologie du groupe de réplication et générer un rapport correspondant. Ce rapport enregistre tous les membres qui sont déconnectés.
- *Dfsrdiag.exe*. Utilisez cet outil de ligne de commande pour surveiller l'état de réplication du service de réplication DFS.

Résolution des problèmes liés à DFS

Les problèmes liés à DFS tombent en général dans une des catégories suivantes :

- Impossibilité d'accéder à l'espace de noms DFS. Assurez-vous que le service Ouverture de session réseau et le service DFS sont en cours d'exécution sur tous les serveurs qui hébergent l'espace de noms.
- Impossibilité de trouver les dossiers partagés. Si les clients ne peuvent pas se connecter à un dossier partagé, utilisez les techniques de résolution des problèmes standard pour vérifier que le dossier est accessible et que les clients disposent d'autorisations. N'oubliez pas que les clients se connectent au dossier partagé directement.
- Impossibilité d'accéder aux liens et aux dossiers partagés DFS. Vérifiez que le dossier sous-jacent est accessible et que le client a des autorisations dessus. Si un réplica existe, déterminez si le problème est lié à la latence de la réplication (reportez-vous à l'entrée de cette liste concernant la latence de la réplication).
- Problème lié à la sécurité. N'oubliez pas que le client accède au dossier partagé directement. Par conséquent, vous devez vérifier le dossier partagé et les autorisations de liste de contrôle d'accès sur le dossier.
- Latence de la réplication. Gardez à l'esprit que la topologie de réplication DFS est enregistrée dans les services AD DS du domaine. Par conséquent, une latence est nécessaire avant qu'une modification apportée à l'espace de noms DFS soit répliquée sur tous les contrôleurs de domaine.

Atelier pratique B : Implémentation de DFS

Scénario

A. Datum Corporation a déployé une nouvelle succursale. Ce bureau a un serveur unique. Pour prendre en charge les exigences liées au personnel de la succursale, vous devez configurer DFS. Pour éviter d'avoir à effectuer des sauvegardes à distance, un partage de fichiers par service dans la succursale sera répliqué au siège social afin de centraliser la sauvegarde, et les fichiers de données de la succursale seront répliqués sur le serveur de la succursale afin de fournir un accès plus rapide.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- installer le service de rôle DFS ;
- configurer un espace de noms DFS ;
- configurer la réplication DFS.

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Configuration de l'atelier pratique

Durée approximative : 30 minutes

Ordinateur(s) virtuel(s)	22411B-LON-DC1 22411B-LON-SVR1 22411B-LON-SVR4
Nom d'utilisateur	**Administrateur**
Mot de passe	**Pa$$w0rd**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
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. Effectuez les étapes 2 à 4 pour **22411B-LON-SVR1** et **22411B-LON-SVR4**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Installation du service de rôle DFS

Scénario

Pour prendre en charge la création d'un espace de noms répliqué, vous avez dû installer le rôle de serveur DFS pour LON-SVR1 et LON-SVR4.

Les tâches principales de cet exercice sont les suivantes :

1. installer le service de rôle DFS sur LON-SVR1 ;
2. installer le service de rôle DFS sur LON-SVR4 ;

▶ Tâche 1 : Installer le service de rôle DFS sur LON-SVR1

- Sur LON-SVR1, dans le Gestionnaire de serveur, sous le rôle Service de fichiers et de stockage (Installé), installez les services de rôle **Espaces de noms DFS** et **Réplication DFS**.

▶ Tâche 2 : Installer le service de rôle DFS sur LON-SVR4

- Sur LON-SVR4, dans le Gestionnaire de serveur, sous le rôle **Service de fichiers et de stockage (Installé)**, installez les services de rôle **Espaces de noms DFS** et **Réplication DFS**.

Résultats : À la fin de cet exercice, vous aurez installé le service de rôle DFS sur LON-SVR1 et sur LON-SVR4.

Exercice 2 : Configuration d'un espace de noms DFS

Scénario

Vous avez dû configurer un espace de noms DFS pour prendre en charge la dernière structure de fichiers demandée. La direction a demandé que la nouvelle structure soit configurée comme suit :

- Espace de noms : \\Adatum.com\BranchDocs
- Partages de fichiers à inclure :
  - \\LON-SVR4\ResearchTemplates
  - \\LON-SVR1\DataFiles

Les tâches principales de cet exercice sont les suivantes :

1. Créer l'espace de noms BranchDocs
2. Activer l'énumération basée sur l'accès pour l'espace de noms BranchDocs
3. Ajouter le dossier ResearchTemplates à l'espace de noms BranchDocs
4. Ajouter le dossier DataFiles à l'espace de noms BranchDocs
5. Vérifier l'espace de noms BranchDocs

▶ Tâche 1 : Créer l'espace de noms BranchDocs

1. Basculez vers LON-SVR1, puis ouvrez le Gestionnaire de serveur.
2. Ouvrez **Gestion du système de fichiers distribués DFS**.

3. Créez un espace de noms avec les propriétés suivantes :
   - Serveur : **LON-SVR1**
   - Nom : **BranchDocs**
   - Type d'espace de noms : **espace de noms de domaine**, puis sélectionnez le mode **Activer le mode Windows Server 2008**
4. Sous le nœud **Espaces de noms**, vérifiez que l'espace de noms a été créé.

▶ Tâche 2 : Activer l'énumération basée sur l'accès pour l'espace de noms BranchDocs

- Dans **Gestion du système de fichiers distribués DFS**, dans la boîte de dialogue **Propriétés de : \\Adatum.com\BranchDocs**, sous l'onglet **Avancé**, activez la case à cocher **Activer l'énumération basée sur l'accès pour cet espace de noms**.

▶ Tâche 3 : Ajouter le dossier ResearchTemplates à l'espace de noms BranchDocs

- Ajoutez un nouveau dossier à l'espace de noms BranchDocs :
  - Nom du dossier : **ResearchTemplates**
  - Ajoutez une cible de dossier :
    - Chemin d'accès : **\\LON-SVR4\ResearchTemplates**
    - Créez un partage
    - Chemin d'accès local : **C:\BranchDocs\ResearchTemplates**
    - Autorisations : **Tous les utilisateurs disposent d'autorisations d'écriture et de lecture**

▶ Tâche 4 : Ajouter le dossier DataFiles à l'espace de noms BranchDocs

- Ajoutez un nouveau dossier à l'espace de noms **BranchDocs** :
  - Nom du dossier : **DataFiles**
  - Ajoutez une cible de dossier :
    - Chemin d'accès : **\\LON-SVR1\DataFiles**
    - Créez un partage
    - Chemin d'accès local : **C:\BranchDocs\DataFiles**
    - Autorisations : **Tous les utilisateurs disposent d'autorisations d'écriture et de lecture**

▶ Tâche 5 : Vérifier l'espace de noms BranchDocs

1. Sur LON-SVR1, ouvrez l'Explorateur de fichiers, puis dans la barre d'adresses, tapez **\\Adatum.com\BranchDocs**, puis appuyez sur Entrée.
2. Vérifiez que **ResearchTemplates** et **DataFiles** s'affichent, puis fermez la fenêtre.

Résultats : À la fin de cet exercice, vous aurez configuré un espace de noms DFS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Configuration de la réplication DFS

Scénario

Vous avez été invité à vérifier que les fichiers figurant dans le nouvel espace de noms DFS sont répliqués sur LON-SVR1 et LON-SVR4 pour garantir la disponibilité des données.

Les tâches principales de cet exercice sont les suivantes :

1. Créer une autre cible de dossier pour DataFiles
2. Configurer la réplication pour l'espace de noms
3. Pour préparer le module suivant

▶ Tâche 1 : Créer une autre cible de dossier pour DataFiles

1. Dans Gestion du système de fichiers distribués DFS, développez **Adatum.com\BranchDocs**, puis cliquez sur **DataFiles**.
2. Dans le volet de détails, vous constatez qu'il n'existe actuellement qu'une seule cible de dossier.
3. Ajoutez une nouvelle cible de dossier :
   - Chemin d'accès de la cible : **\\LON-SVR4\DataFiles**
   - Créez un partage
   - Chemin d'accès local : **C:\BranchDocs\DataFiles**
   - Autorisations : **Tous les utilisateurs disposent d'autorisations d'écriture et de lecture**
   - Créez le dossier
4. Dans la boîte de dialogue **Réplication**, cliquez sur **Oui**. L'Assistant Réplication de dossier démarre.

▶ Tâche 2 : Configurer la réplication pour l'espace de noms

1. Suivez l'Assistant Réplication de dossier :
   - Membre principal : **LON-SVR1**
   - Aucune topologie
   - Laissez les autres valeurs par défaut et acceptez tous les messages.
2. Créez une nouvelle topologie de réplication pour l'espace de noms :
   - **Type** : **Maille pleine**
   - **Planification et bande passante** : utilisez les paramètres par défaut
3. Dans le volet de détails, sous l'onglet **Appartenances**, vérifiez que le dossier répliqué s'affiche à la fois sur LON-SVR4 et LON-SVR1.

▶ Tâche 3 : 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 **22411B-LON-DC1**, puis cliquez sur **Rétablir**.

3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez ces étapes pour **22411B-LON-SVR1** et **22411B-LON-SVR4**.

Résultats : À la fin de cet exercice, vous aurez configuré la réplication DFS.

Question : Quelle est la configuration requise pour déployer un espace de noms en mode Windows Server°2008 ?

Question : Quels avantages procure l'hébergement d'un espace de noms sur plusieurs serveurs d'espace de noms ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Comment les modèles FSRM pour les quotas et les filtres de fichiers rendent-ils l'expérience de gestion de FSRM plus efficace ?

Question : Pourquoi la réplication DFS constitue-t-elle une plateforme de réplication plus efficace que FSRM ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 11

Configuration du chiffrement et de l'audit avancé

Table des matières :

Vue d'ensemble du module **11-1**

Leçon 1 : Chiffrement des fichiers à l'aide du système EFS (Encrypting File System) **11-2**

Leçon 2 : Configuration de l'audit avancé **11-6**

Atelier pratique : Configuration du chiffrement et de l'audit avancé **11-14**

Contrôle des acquis et éléments à retenir **11-18**

Vue d'ensemble du module

En tant qu'administrateur du système d'exploitation Windows Server® 2012, vous devez assurer la sécurité continue des fichiers et des dossiers sur vos serveurs. Vous pouvez chiffrer des fichiers sensibles à l'aide des outils Windows Server 2012 natifs. Cependant, vous devez prendre en compte certains éléments et certaines méthodes d'implémentation afin de fournir un environnement fiable.

En utilisant Windows Server 2012, vous pouvez comprendre comment les fichiers et les dossiers sont utilisés sur vos ordinateurs Windows Server 2012. Vous pouvez également auditer l'accès aux fichiers et dossiers. L'audit de l'accès aux fichiers et dossiers vous donne un aperçu de l'utilisation générale, ainsi que des informations plus critiques, telles que les tentatives d'utilisation non autorisées.

Ce module décrit les outils de Windows Server 2012 qui peuvent vous aider à fournir une sécurité de système de fichiers accrue sur vos serveurs.

Objectifs

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

- chiffrer des fichiers à l'aide du système EFS ;
- configurer l'audit avancé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Chiffrement des fichiers à l'aide du système EFS (Encrypting File System)

Le système EFS est un composant intégré du système de fichiers NTFS qui permet le chiffrement et le déchiffrement du contenu des fichiers et des dossiers sur un volume NFTS. Il est important de comprendre le fonctionnement du système EFS avant de l'implémenter dans votre environnement. Vous devez également savoir comment récupérer les fichiers chiffrés, et résoudre les problèmes quand le chiffrement EFS ne fonctionne pas correctement.

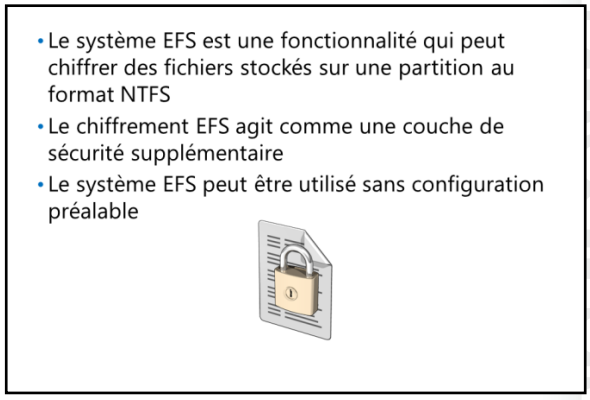
Objectifs de la leçon

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

- décrire EFS ;
- expliquer le fonctionnement du système EFS ;
- expliquer comment récupérer des fichiers chiffrés au format EFS ;
- expliquer comment chiffrer un fichier à l'aide du système EFS.

Qu'est-ce que EFS ?

Le système EFS est une fonctionnalité qui peut chiffrer des fichiers stockés sur une partition au format NTFS. Par défaut, cette option est accessible à tous les utilisateurs. Vous pouvez également utiliser le système EFS pour chiffrer des fichiers sur un partage de fichiers.



Une fois qu'un fichier est chiffré à l'aide du système EFS, seuls les utilisateurs autorisés peuvent y accéder. Si un utilisateur est autorisé, l'accès au fichier est transparent et il peut être ouvert comme un fichier non chiffré. Si un utilisateur n'est pas autorisé, les tentatives d'ouverture du fichier généreront un message d'accès refusé.

Le chiffrement EFS agit comme une couche de sécurité supplémentaire, en plus des autorisations NTFS. Si des utilisateurs reçoivent une autorisation NTFS pour lire un fichier, ils doivent quand même être autorisés par le système EFS pour déchiffrer le fichier.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

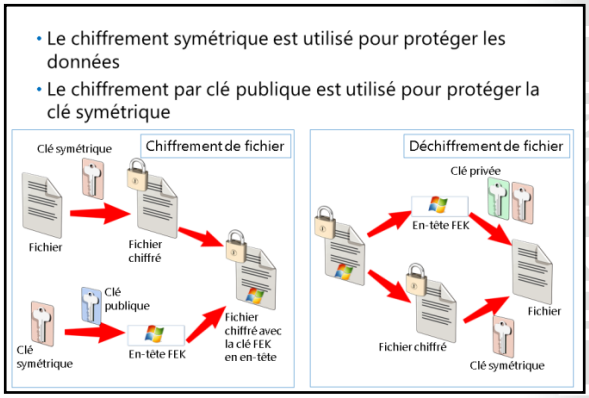
La configuration par défaut du système EFS ne requiert aucune tâche d'administration. Les utilisateurs peuvent commencer à chiffrer immédiatement les fichiers, et le système EFS génère automatiquement un certificat utilisateur avec une paire de clés pour un utilisateur si elle n'existe pas. L'utilisation d'une autorité de certification (CA) pour émettre des certificats utilisateur améliore la facilité de gestion des certificats.

Vous pouvez désactiver le système EFS sur les ordinateurs clients à l'aide de la stratégie de groupe. Dans les propriétés de la stratégie, naviguez jusqu'à Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique\Système de fichiers EFS (Encrypting File System), puis cliquez sur **Ne pas autoriser**.

Remarque : Si vous n'utilisez pas des certificats émanant d'une autorité de certification et souhaitez autoriser l'utilisation du système EFS sur un partage de fichiers, vous devez configurer le compte du serveur de fichiers pour qu'il soit approuvé pour la délégation. Par défaut, les contrôleurs de domaine sont approuvés pour la délégation.

Fonctionnement de la virtualisation des postes de travail (EFS)

Le système EFS utilise une combinaison de chiffrements par clé publique et clé symétrique pour protéger les fichiers contre les attaques. Il utilise une clé symétrique pour chiffrer le fichier, et une clé publique pour protéger la clé symétrique.



Le chiffrement par clé symétrique utilise la même clé pour chiffrer et déchiffrer un fichier. Ce type de chiffrement est plus rapide et performant que le chiffrement par clé publique. Comme il est difficile de sécuriser la clé symétrique pendant un transfert entre réseaux, une sécurité supplémentaire est requise. Le chiffrement par clé symétrique est la méthode standard pour chiffrer de grandes quantités de données.

Le système EFS utilise le chiffrement par clé publique pour protéger la clé symétrique qui est requise pour déchiffrer le contenu des fichiers. Chaque certificat utilisateur contient une clé privée et une clé publique qui est utilisée pour chiffrer la clé symétrique. Seul l'utilisateur disposant du certificat et de sa clé privée peut déchiffrer la clé symétrique.

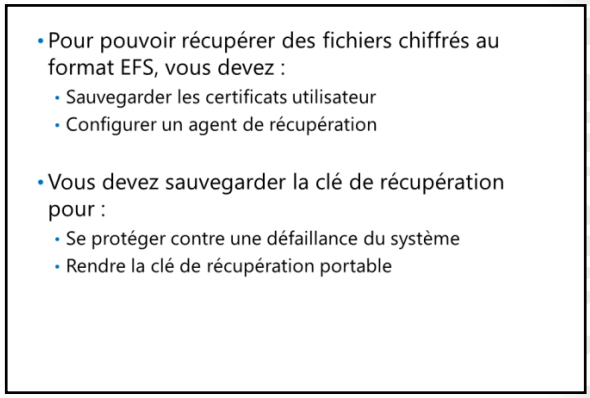
Le processus de chiffrement de fichiers se présente comme suit :

1. Quand un utilisateur chiffre un fichier, le système EFS génère une clé de chiffrement de fichier (FEK, File Encryption Key) pour chiffrer les données. La clé FEK est chiffrée avec la clé publique de l'utilisateur, puis la clé FEK chiffrée est stockée avec le fichier. Ainsi, seul l'utilisateur qui possède la clé privée de chiffrement EFS correspondante peut déchiffrer le fichier. Une fois qu'un utilisateur a chiffré un fichier, ce dernier demeure chiffré tant qu'il est stocké sur le disque.
2. Pour déchiffrer des fichiers, l'utilisateur peut ouvrir le fichier et supprimer l'attribut de chiffrement, ou déchiffrer le fichier à l'aide de la commande cipher. Dans ce cas, le système EFS déchiffre la clé FEK avec la clé privée de l'utilisateur, puis déchiffre les données à l'aide de la clé FEK.

Remarque : En plus de l'utilisateur qui a chiffré le fichier, des copies supplémentaires de la clé symétrique sont chiffrées avec la clé publique de l'agent de récupération, et sont accessibles aux autres utilisateurs autorisés.

Récupération de fichiers chiffrés au format EFS

Si un utilisateur qui a chiffré un fichier à l'aide du système EFS perd la clé privée pour une raison quelconque, une méthode est nécessaire pour récupérer le fichier chiffré au format EFS. La clé privée fait partie d'un certificat utilisateur utilisé pour le chiffrement. La sauvegarde d'un certificat utilisateur est une méthode pour récupérer des fichiers chiffrés au format EFS. Le certificat utilisateur sauvegardé peut être importé dans un autre profil et vous pouvez l'utiliser pour déchiffrer le fichier. Cependant, cette méthode est difficile à implémenter quand les utilisateurs sont nombreux.



Une meilleure méthode pour récupérer des fichiers chiffrés au format EFS consiste à utiliser un agent de récupération. Un agent de récupération est une personne autorisée à déchiffrer tous les fichiers chiffrés au format EFS. L'agent de récupération par défaut est l'administrateur de domaine. Cependant, vous pouvez déléguer le rôle d'agent de récupération à n'importe quel utilisateur.

Quand vous ajoutez un nouvel agent de récupération à l'aide de la stratégie de groupe, il est automatiquement ajouté à tous les nouveaux fichiers chiffrés, mais il n'est pas automatiquement ajouté aux fichiers chiffrés existants. Comme l'agent de récupération d'un fichier est défini au moment où le fichier est chiffré, un fichier chiffré doit être accessible et enregistré pour mettre à jour l'agent de récupération.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour sauvegarder le certificat d'agent de récupération, vous devez toujours exporter le certificat avec la clé privée et le conserver dans un emplacement sécurisé. Deux raisons justifient la sauvegarde de la clé privée pour l'agent de récupération (ou la clé de récupération) :

- Se protéger contre une défaillance du système. La clé d'administrateur de domaine utilisée par défaut pour la récupération EFS n'est stockée que sur le premier contrôleur du domaine. Si ce contrôleur de domaine rencontre un problème, la récupération EFS est impossible.
- Pour rendre la clé de récupération portable. La clé de récupération n'est pas automatiquement accessible à l'agent de récupération sur tous les ordinateurs. Elle doit être installée dans le profil de l'agent de récupération. Si les profils itinérants ne sont pas utilisés, l'exportation et l'importation de la clé de récupération est une méthode pour mettre à jour le profil de l'agent de récupération sur un ordinateur particulier.

Démonstration : Chiffrement d'un fichier à l'aide du système EFS

Cette démonstration montre comment :

- vérifier qu'un compte d'ordinateur prend en charge le système EFS sur un partage réseau ;
- utiliser le système EFS pour chiffrer un fichier sur un partage réseau ;
- afficher le certificat utilisé pour le chiffrement ;
- tester l'accès à un fichier chiffré.

Procédure de démonstration

Vérifier qu'un compte d'ordinateur prend en charge le système EFS sur un partage réseau

1. Sur LON-DC1, ouvrez Utilisateurs et ordinateurs Active Directory.
2. Vérifiez que LON-DC1 est approuvé pour la délégation à un service.

Utiliser le système EFS pour chiffrer un fichier sur un partage réseau

1. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Doug** avec le mot de passe **Pa$$w0rd**.
2. Naviguez jusqu'à **\\LON-DC1\Mod11Share**.
3. Créez un document Microsoft® Word nommé **MonFichierChiffré**.
4. Ouvrez **MonFichierChiffré**, tapez **Mes données secrètes**, puis enregistrez le fichier.
5. Chiffrez **MonFichierChiffré**.
6. Fermez la session sur LON-CL1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Afficher le certificat utilisé pour le chiffrement

1. Sur LON-DC1, naviguez jusqu'à **C:\Utilisateurs**. Notez que Doug a un profil sur l'ordinateur. Il s'agit de l'emplacement de stockage du certificat auto-signé. Il ne peut pas être affiché dans le composant logiciel enfichable Certificats de la console MMC (Microsoft Management Console) à moins que Doug se connecte localement au serveur.
2. Naviguez jusqu'à **C:\Utilisateurs\Doug\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates**. Il s'agit du dossier de stockage du certificat auto-signé pour Doug.

Tester l'accès à un fichier chiffré

1. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Alex**.
2. Tentez d'ouvrir **\\LON-DC1\Mod11Share\MonFichierChiffré** avec Microsoft Word. La tentative échoue car le fichier est chiffré par Doug.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration de l'audit avancé

Les journaux d'audit enregistrent diverses activités de votre entreprise dans le journal de sécurité Windows®. Vous pouvez surveiller ces journaux d'audit pour identifier les problèmes qui nécessitent un examen approfondi. L'audit peut également enregistrer les activités réussies, pour fournir une documentation des modifications. Il peut également enregistrer les tentatives infructueuses et potentiellement malveillantes d'accès aux ressources de l'entreprise. Lors de la configuration de l'audit, vous devez spécifier les paramètres d'audit, activer une stratégie d'audit et surveiller les événements des journaux de sécurité.

Objectifs de la leçon

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

- décrire les stratégies d'audit ;
- expliquer comment spécifier les paramètres d'audit pour un fichier ou un dossier ;
- expliquer comment activer une stratégie d'audit ;
- expliquer comment évaluer les événements du journal de sécurité ;
- décrire la configuration avancée de la stratégie d'audit ;
- expliquer comment configurer l'audit avancé.

Vue d'ensemble des stratégies d'audit

Une stratégie d'audit configure un système pour auditer des catégories d'activités. Si la stratégie d'audit n'est pas activée, un serveur n'audite pas ces activités.

- Auditez les événements dans une catégorie d'activités, telles que :
  - Accès aux fichiers et dossiers NTFS
  - Changements de compte ou d'objet dans AD DS
  - Ouverture de session
  - Attribution de l'utilisation des droits utilisateur
- Par défaut, les contrôleurs de domaine auditent les événements ayant réussi pour la plupart des catégories
- Objectif : aligner les stratégies d'audit sur les stratégies de sécurité de l'entreprise
  - Sur-audit : les journaux sont trop volumineux pour rechercher des événements importants
  - Sous-audit : les événements importants ne sont pas enregistrés

Vous pouvez afficher les stratégies d'audit dans Stratégie de groupe, sous Configuration ordinateur. Dans Configuration ordinateur, développez Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales, puis cliquez sur Stratégie d'audit. Pour configurer l'audit, vous devez définir le paramètre de stratégie. Dans l'Éditeur de gestion des stratégies de groupe, double-cliquez sur un paramètre de stratégie et activez la case à cocher **Définir ces paramètres de stratégie**. Choisissez ensuite si vous souhaitez activer l'audit des événements ayant réussi, des événements ayant échoué ou des deux.

Le tableau suivant définit chaque stratégie d'audit et ses paramètres par défaut sur un contrôleur de domaine Windows Server 2012.

Paramètre de stratégie d'audit	Description	Paramètre par défaut
Auditer les événements de connexion aux comptes	Crée un événement quand un utilisateur ou un ordinateur tente de s'authentifier à l'aide d'un compte Active Directory®. Par exemple, quand un utilisateur se connecte à un ordinateur du domaine, un événement de connexion au compte est généré.	Les connexions au compte réussies sont auditées.
Auditer les événements de connexion	Crée un événement quand un utilisateur se connecte en mode interactif (localement) à un ordinateur ou au réseau (à distance). Par exemple, si une station de travail et un serveur sont configurés pour auditer les événements de connexion, la station de travail audite un utilisateur qui se connecte directement à cette station de travail. Quand l'utilisateur se connecte à un dossier partagé sur le serveur, le serveur enregistre cette connexion distante. Quand un utilisateur se connecte, le contrôleur de domaine enregistre un événement de connexion car les scripts et les stratégies de connexion sont récupérés à partir du contrôleur de domaine.	Les connexions réussies sont auditées.
Auditer la gestion des comptes	Audite les événements, y compris la création, la suppression ou la modification de comptes d'utilisateur, de groupe ou d'ordinateur, et la réinitialisation des mots de passe utilisateur.	Les activités de gestion de compte réussies sont auditées.
Auditer l'accès au service d'annuaire	Audite les événements spécifiés dans la liste de contrôle d'accès système (SACL, System Access Control List), qui s'affiche dans la boîte de dialogue Paramètres de sécurité avancés des propriétés d'un objet Active Directory. Outre la définition de la stratégie d'audit à l'aide de ce paramètre, vous devez également configurer l'audit du ou des objets spécifiques à l'aide de la liste SACL du ou des objets. Cette stratégie est similaire à la stratégie Auditer l'accès aux objets que vous utilisez pour auditer des fichiers et dossiers, mais elle s'applique aux objets Active Directory.	Les événements d'accès au service d'annuaire réussis sont audités, mais les listes SACL de quelques objets spécifient les paramètres d'audit.
Auditer les modifications de stratégie	Audite les modifications apportées aux stratégies d'attribution des droits utilisateur, aux stratégies d'audit ou aux stratégies d'approbation.	Les modifications de stratégie réussies sont auditées.
Auditer l'utilisation des privilèges	Audite l'utilisation d'un privilège ou d'un droit utilisateur. Consultez le texte explicatif de cette stratégie dans l'Éditeur de gestion des stratégies de groupe.	Aucun audit n'est effectué par défaut.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Paramètre de stratégie d'audit	Description	Paramètre par défaut
Auditer les événements système	Audite le redémarrage ou l'arrêt du système, ou les modifications qui affectent les journaux système ou de sécurité.	Les événements système réussis sont audités.
Auditer le suivi des processus	Audite les événements tels que l'activation de programmes et la sortie de processus. Consultez le texte explicatif de cette stratégie dans l'Éditeur de gestion des stratégies de groupe.	Aucun événement n'est audité.
Auditer l'accès aux objets	Audite l'accès aux objets tels que les fichiers, les dossiers, les clés de Registre et les imprimantes qui ont leurs propres listes SACL. Outre l'activation de cette stratégie d'audit, vous devez configurer les entrées d'audit dans les listes SACL des objets.	Aucun événement n'est audité.

Notez que la plupart des principaux événements Active Directory sont déjà audités par les contrôleurs de domaine, dans l'hypothèse où les événements sont réussis. Par conséquent, la création d'un utilisateur, la réinitialisation du mot de passe d'un utilisateur, la connexion au domaine et la récupération des scripts de connexion d'un utilisateur sont toutes enregistrées.

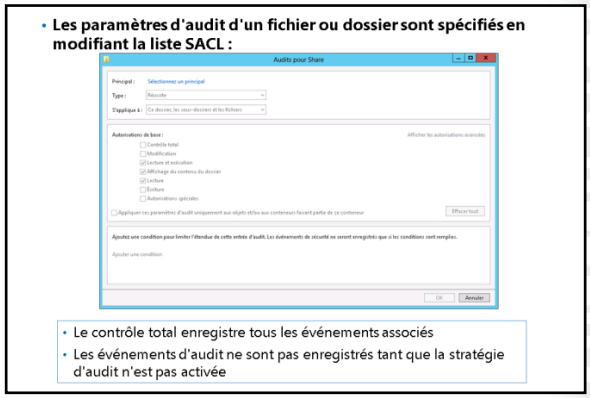
Cependant, tous les événements ayant échoué ne sont pas audités par défaut. Vous devrez peut-être implémenter un audit supplémentaire des échecs en fonction des stratégies et des exigences en matière de sécurité informatique de votre organisation. Par exemple, si vous auditez les échecs de connexion aux comptes, vous pouvez exposer les tentatives malveillantes d'accès au domaine en essayant de façon répétée de vous connecter en tant que compte d'utilisateur du domaine sans connaître le mot de passe du compte. L'audit des échecs de gestion des comptes peut révéler un utilisateur malveillant qui tente de manipuler l'appartenance d'un groupe sensible sur le plan de la sécurité.

L'une des tâches les plus importantes que vous devez effectuer consiste à équilibrer et à aligner la stratégie d'audit sur les stratégies de votre entreprise, et sur ce qui est réaliste. La stratégie de votre entreprise peut stipuler que tous les échecs de connexion et toutes les modifications réussies des utilisateurs et groupes Active Directory doivent être audités. Pour ce faire, il suffit d'utiliser les Services de domaine Active Directory (AD DS). Mais comment, exactement, allez-vous utiliser ces informations ? Les journaux d'audit détaillés sont inutiles si vous ne savez pas comment gérer efficacement ces journaux, ou ne disposez pas des outils nécessaires pour les gérer. Pour implémenter l'audit, vous devez avoir une stratégie d'audit bien configurée et disposer d'outils permettant de gérer les événements audités.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Spécification des paramètres d'audit pour un fichier ou un dossier

De nombreuses organisations choisissent d'auditer l'accès au système de fichiers pour fournir des détails concernant l'utilisation des ressources et les problèmes de sécurité potentiels. Windows Server 2012 prend en charge l'audit granulaire basé sur les comptes d'utilisateurs ou de groupes et les actions spécifiques exécutées par ces comptes. Pour configurer l'audit, vous devez effectuer trois étapes : spécifier les paramètres d'audit, activer la stratégie d'audit et évaluer les événements du journal de sécurité.



Vous pouvez auditer l'accès à un fichier ou un dossier en ajoutant des entrées d'audit à sa liste SACL. Pour cela, procédez comme suit :

1. Ouvrez la boîte de dialogue Propriétés du fichier ou du dossier, puis cliquez sur l'onglet **Sécurité**.
2. Sous l'onglet **Sécurité**, cliquez sur **Avancé**.
3. Cliquez sur **Audit**.
4. Pour ajouter une entrée, cliquez sur **Modifier**. L'onglet **Audit** s'ouvre en mode Édition.
5. Cliquez sur **Ajouter** pour sélectionner l'utilisateur, le groupe ou l'ordinateur à auditer.
6. Dans la boîte de dialogue **Entrée d'audit**, indiquez le type d'accès à auditer.

Éléments à prendre en compte pour configurer l'audit de fichiers et de dossiers

Vous pouvez auditer les succès, les échecs ou les deux lorsque l'utilisateur, le groupe ou l'ordinateur spécifié tente d'accéder à la ressource en utilisant un ou plusieurs niveaux d'accès granulaires.

Vous pouvez auditer les succès aux fins suivantes :

- pour enregistrer l'accès aux ressources pour la création de rapports et la facturation ;
- pour surveiller les accès qui suggéreraient que les utilisateurs exécutent des actions plus importantes que ce que vous aviez prévu, ce qui indiquerait que les autorisations sont trop généreuses ;
- pour identifier les accès inhabituels pour un compte particulier, ce qui pourrait indiquer qu'un compte d'utilisateur a été piraté.

Vous pouvez auditer les échecs aux fins suivantes :

- pour surveiller les tentatives malveillantes d'accès à une ressource dont l'accès a été refusé ;
- pour identifier les tentatives infructueuses d'accès à un fichier ou dossier auquel un utilisateur a besoin d'accéder. Cela indiquerait que les autorisations ne sont pas suffisantes pour répondre aux besoins d'une entreprise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les entrées d'audit demandent aux systèmes d'exploitation Windows d'auditer les activités réussies ou non d'un principal de sécurité (utilisateur, groupe ou ordinateur) pour utiliser une autorisation spécifique. Le contrôle total comprend tous les niveaux d'accès individuels ; par conséquent, cette entrée couvre tout type d'accès. Par exemple, si vous attribuez un contrôle total au groupe Consultant, et si un membre de ce groupe tente un type d'accès et échoue, cette activité est enregistrée.

En général, les entrées d'audit reflètent les entrées d'autorisation de l'objet, mais les entrées d'audit et les entrées d'autorisation peuvent ne pas toujours correspondre. Dans le scénario ci-dessus, gardez à l'esprit qu'un membre du groupe Consultants peut également appartenir à un autre groupe qui est autorisé à accéder au dossier. Comme cet accès est réussi, l'activité n'est pas enregistrée. Par conséquent, si vous souhaitez restreindre l'accès au dossier et en interdire l'accès aux utilisateurs, vous devez surveiller les tentatives d'accès infructueuses. Cependant, vous devez également auditer les accès réussis pour identifier les situations où un utilisateur accède au dossier par le biais d'une autre appartenance de groupe qui est potentiellement incorrecte.

Remarque : Les journaux d'audit peuvent devenir volumineux assez rapidement. Par conséquent, configurez le strict minimum requis pour répondre aux besoins de sécurité de votre société. Quand vous spécifiez d'auditer les succès et les échecs d'un dossier de données actif pour le groupe Tout le monde en utilisant un contrôle total (toutes les autorisations), cela génère des journaux d'audit volumineux qui peuvent affecter les performances du serveur, et rendre presque impossible la localisation d'un événement d'audit spécifique.

Activation de la stratégie d'audit

La configuration des entrées d'audit dans le descripteur de sécurité d'un fichier ou d'un dossier n'active pas en soi l'audit. L'audit doit être activé en définissant le paramètre de stratégie Auditer l'accès aux objets appropriés dans la stratégie de groupe.

Une fois que l'audit est activé, le sous-système de sécurité commence à enregistrer l'accès, comme indiqué par les paramètres d'audit.

Pour activer la stratégie d'audit en configurant les paramètres de stratégie d'audit dans un objet de stratégie de groupe :

- Activez les paramètres appropriés dans l'objet de stratégie de groupe
- Appliquez l'objet de stratégie de groupe à l'emplacement AD DS où vos serveurs sont situés

Le paramètre de stratégie doit être appliqué au serveur qui contient l'objet audité. Vous pouvez configurer le paramètre de stratégie dans l'objet de stratégie de groupe local du serveur, ou vous pouvez utiliser un objet de stratégie de groupe limité en étendue au serveur.

Vous pouvez ensuite définir la stratégie pour auditer les événements ayant réussi, les événements ayant échoué ou les deux. Le paramètre de stratégie doit spécifier l'audit des tentatives ayant réussi ou échoué qui correspondent au type d'entrée d'audit dans la liste SACL de l'objet. Par exemple, pour enregistrer une tentative d'accès infructueuse du groupe Consultants au dossier Données confidentielles, vous devez configurer la stratégie Auditer l'accès aux objets pour auditer les échecs, et vous devez configurer la liste SACL du dossier Données confidentielles pour auditer les échecs. Si la stratégie d'audit audite uniquement les succès, les entrées ayant échoué dans la liste SACL du dossier ne déclenchent pas la journalisation.

Emplacement des paramètres de la stratégie d'audit

Dans la fenêtre Gestion des stratégies de groupe d'AD DS, il existe un groupe de paramètres standard dans un objet de stratégie de groupe qui contrôlent le comportement d'audit. Cet ensemble de paramètres de stratégie d'audit se trouve sous Configuration ordinateur, dans le nœud suivant :

Paramètres Windows\Sécurité\Stratégies locales\Stratégie d'audit. Les paramètres de stratégie d'audit régissent les paramètres de base suivants :

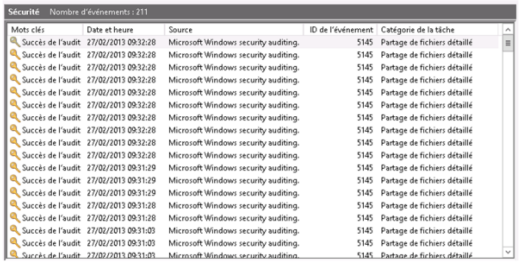
- Auditer les événements de connexion aux comptes
- Auditer la gestion des comptes
- Auditer l'accès au service d'annuaire
- Auditer les événements de connexion
- Auditer l'accès aux objets
- Auditer les modifications de stratégie
- Auditer l'utilisation des privilèges
- Auditer le suivi des processus
- Auditer les événements système

Remarque : Gardez à l'esprit que l'accès audité et consigné est la combinaison des paramètres de la stratégie d'audit et des entrées d'audit de fichiers et dossiers spécifiques. Si vous avez configuré les entrées d'audit pour enregistrer les échecs, mais la stratégie active uniquement l'enregistrement des succès, vos journaux d'audit demeurent vides.

Évaluation des événements du journal de sécurité

Une fois que vous avez activé le paramètre de stratégie Auditer l'accès aux objets et spécifié l'accès que vous souhaitez auditer à l'aide des listes SACL, le système commence à enregistrer l'accès en fonction des entrées d'audit. Vous pouvez afficher les événements obtenus dans le journal de sécurité du serveur. Pour ce faire, dans Outils d'administration, ouvrez la console Observateur d'événements, puis développez Journaux Windows\Sécurité.

Affichez les événements d'audit dans le champ Détails du journal de sécurité, et appliquez un filtre pour réduire le nombre d'événements à examiner :

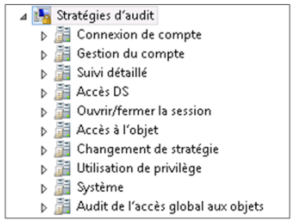


Dans le journal de sécurité, les événements d'audit sont représentés en tant que types d'événement Succès de l'audit et Échec de l'audit. Le champ Détails de chaque événement contient des informations pertinentes, selon le type d'événement audité. De nombreuses catégories d'audit retournent un grand nombre d'événements. Ces événements peuvent être fastidieux à parcourir, par conséquent, leur filtrage est recommandé. Vous pouvez filtrer en fonction du champ Détails, et inclure des informations appropriées, telles que le nom d'un utilisateur ou le nom d'un fichier ou dossier audité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Stratégies d'audit avancées

Windows Server 2012 et Windows Server 2008 R2 fournissent un ensemble supplémentaire de stratégies d'audit à configurer :



Dans Windows Server 2012 et Windows Server 2008 R2, les administrateurs peuvent auditer des aspects plus spécifiques du comportement client sur l'ordinateur ou le réseau. Cela permet à l'administrateur d'identifier plus facilement les comportements présentant le plus d'intérêt. Par exemple, dans Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Stratégie d'audit, il n'existe qu'un seul paramètre de stratégie—Auditer les événements de connexion—pour les événements de connexion. Dans Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Configuration avancée de la stratégie d'audit\Stratégies d'audit, vous pouvez choisir parmi dix paramètres de stratégie différents dans la catégorie Ouverture/Fermeture de session. Cela vous fournit un contrôle plus détaillé des aspects d'ouverture et de fermeture de session que vous pouvez suivre.

Ces améliorations de l'audit de la sécurité peuvent aider à assurer la conformité de l'audit de votre organisation aux règles d'entreprise et de sécurité importantes grâce au suivi précis d'activités définies, telles que :

- Un administrateur de groupe a modifié les paramètres ou données sur les serveurs contenant des informations financières.
- Un employé au sein d'un groupe défini a accédé à un fichier important.
- La liste SACL correcte est appliquée à chaque fichier et dossier ou à la clé de Registre sur un partage d'ordinateurs ou de fichiers, en tant que dispositif de protection vérifiable contre les accès non détectés.

Description des paramètres de stratégie d'audit avancés

Il existe dix groupes de paramètres de stratégie d'audit avancés que vous pouvez configurer dans la stratégie de groupe pour Windows Server 2012 :

- *Connexion de compte*. Ces paramètres activent l'audit de la validation des informations d'identification et d'autres événements de ticket et d'authentification propres à Kerberos.
- *Gestion des comptes*. Vous pouvez activer l'audit des événements relatifs à la modification de comptes d'utilisateur, de comptes d'ordinateur et de groupes avec le groupe de paramètres Gestion des comptes.
- *Suivi détaillé*. Ces paramètres contrôlent l'audit des événements de chiffrement, des événements de création et d'arrêt de processus Windows et des événements d'appel de procédure distante (RPC, Remote Procedure Call).
- *Accès DS*. Ces paramètres d'audit impliquent l'accès aux services d'annuaire, y compris l'accès général, les modifications et la réplication.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Ouverture/Fermeture de session*. Les événements d'ouverture et de fermeture de session standard sont audités par ce groupe de paramètres. D'autres activités propres aux comptes, telles que IPsec (Internet Protocol Security), le serveur NPS (Network Policy Server) et d'autres événements d'ouverture et de fermeture de session non classés sont également audités.
- *Accès à l'objet*. Ces paramètres activent l'audit pour tout accès à AD DS, au Registre, à une application et au stockage de fichiers.
- *Changement de stratégie*. Quand vous configurez ces paramètres, les modifications internes des paramètres de stratégie d'audit sont auditées.
- *Utilisation de privilège*. Dans l'environnement Windows, Windows Server 2012 audite les tentatives d'utilisation de privilèges quand vous configurez ces paramètres.
- *Système*. Les paramètres système sont utilisés pour auditer les modifications de l'état du sous-système de sécurité.
- *Audit de l'accès global aux objets*. Ces paramètres permettent de contrôler les paramètres SACL de tous les objets sur un ou plusieurs ordinateurs. Quand les paramètres de ce groupe sont configurés et appliqués à l'aide de la stratégie de groupe, l'appartenance SACL est déterminée par la configuration du paramètre de stratégie, et les listes SACL sont configurées directement sur le serveur proprement dit. Vous pouvez configurer les listes SACL pour l'accès au système de fichiers et au Registre sous Audit de l'accès global aux objets.

Démonstration : Configuration de l'audit avancé

Cette démonstration montre comment créer et modifier un objet de stratégie de groupe pour la configuration de la stratégie d'audit.

Procédure de démonstration

Créer et modifier un objet de stratégie de groupe pour la configuration de la stratégie d'audit

1. Sur LON-DC1, ouvrez Gestion des stratégies de groupe.
2. Créez un objet de stratégie de groupe appelé **Audit de fichier**.
3. Modifiez l'objet de stratégie de groupe **Audit de fichier** et activez les événements d'audit **Succès** et **Échec** pour les paramètres **Auditer le partage de fichiers détaillé** et **Auditer le stockage amovible**.
4. Fermez Gestion des stratégies de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Configuration du chiffrement et de l'audit avancé

Scénario

A. Datum est une société internationale d'ingénierie et de fabrication, dont le siège social est basé à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

Vous devez configurer l'environnement Windows Server 2012 pour protéger les fichiers sensibles, et vérifier que l'accès aux fichiers sur le réseau est audité convenablement. Vous devez également configurer l'audit du nouveau serveur.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- chiffrer et récupérer des fichiers à l'aide des outils de gestion EFS ;
- configurer l'audit avancé.

Configuration de l'atelier pratique

Durée approximative : 40 minutes

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-CL1 22411B-LON-SVR1
Nom d'utilisateur	**ADATUM\Administrateur**
Mot de passe	**Pa$$w0rd**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Ouvrez une session en utilisant les informations d'authentification suivantes :
    - Nom d'utilisateur : **ADATUM\Administrateur**
    - Mot de passe : **Pa$$w0rd**
5. Effectuez les étapes 2 à 4 pour **22411B-LON-CL1** et **22411B-LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Chiffrement et récupération des fichiers

Scénario

Votre organisation souhaite autoriser les utilisateurs à démarrer le chiffrement des fichiers à l'aide d'EFS. Cependant, il existe des problèmes de capacité de récupération. Pour améliorer la gestion des certificats utilisés pour EFS, vous allez configurer une autorité de certification interne pour émettre des certificats aux utilisateurs. Vous configurerez également un agent de récupération pour EFS, et vérifierez qu'il peut récupérer des fichiers.

Les tâches principales de cet exercice sont les suivantes :

1. Mettre à jour le certificat d'agent de récupération pour le système EFS
2. Mettre à jour la stratégie de groupe sur les ordinateurs
3. Obtenir un certificat pour EFS
4. Chiffrer un fichier
5. Utiliser l'agent de récupération pour ouvrir le fichier

▶ Tâche 1 : Mettre à jour le certificat d'agent de récupération pour le système EFS

1. Sur LON-DC1, à partir du Gestionnaire de serveur, ouvrez l'outil d'administration Gestion des stratégies de groupe.
2. Modifiez la stratégie de domaine par défaut (**Default Domain Policy**) associée à **Adatum.com**.
3. Dans l'Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique\Système de fichiers EFS (Encrypting File System)**.
4. Dans le dossier **Système de fichiers EFS (Encrypting File System)**, supprimez le certificat **Administrateur** existant.
5. Créez un **agent de récupération de données**.
6. Lisez les informations sur le nouveau certificat, et vérifiez qu'il a été émis par AdatumCA.

▶ Tâche 2 : Mettre à jour la stratégie de groupe sur les ordinateurs

1. Sur LON-DC1, utilisez l'interface de ligne de commande Windows PowerShell® pour exécuter **gpupdate /force**.
2. Sur LON-CL1, ouvrez une invite de commandes et exécutez **gpupdate /force**.
3. Fermez la session sur LON-CL1.

▶ Tâche 3 : Obtenir un certificat pour EFS

1. Sur LON-CL1, connectez-vous en tant qu'**ADATUM\Doug** avec le mot de passe **Pa$$w0rd**.
2. Exécutez **mmc.exe** pour ouvrir une console MMC vide.
3. Ajoutez le composant logiciel enfichable **Certificats** à la console MMC.
4. Dans la console MMC, cliquez avec le bouton droit sur **Personnel** et demandez un nouveau certificat.
5. Sélectionnez un certificat **EFS basique**.
6. Vérifiez que le nouveau certificat a été émis par AdatumCA.
7. Fermez la console sans enregistrer les modifications.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Chiffrer un fichier

1. Sur LON-CL1, accédez à **\\LON-DC1\Mod11Share\Marketing**.
2. Ouvrez les propriétés de **DougFile**.
3. Activez le chiffrement dans les attributs avancés pour **DougFile** uniquement.
4. Fermez l'Explorateur de fichiers.
5. Fermez la session sur LON-CL1.

▶ Tâche 5 : Utiliser l'agent de récupération pour ouvrir le fichier

1. Sur LON-DC1, accédez à **E:\Labfiles\Mod11\Mod11Share\Marketing**.
2. Ouvrez **DougFile.txt**, modifiez le contenu, puis enregistrez le fichier.

Résultats : À la fin de cet exercice, vous aurez chiffré et récupéré des fichiers.

Exercice 2 : Configuration de l'audit avancé

Scénario

Votre gestionnaire vous a demandé de suivre tous les accès aux partages de fichiers stockés sur LON-SVR1. Vous devrez également être informé chaque fois qu'un utilisateur accède à un fichier sur un périphérique de stockage amovible rattaché au serveur. Vous avez décidé d'implémenter les paramètres d'accès aux objets appropriés à l'aide de la configuration avancée de la stratégie d'audit.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un objet de stratégie de groupe pour l'audit avancé
2. Vérifier les entrées d'audit

▶ Tâche 1 : Créer un objet de stratégie de groupe pour l'audit avancé

1. Sur LON-DC1, à partir du Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Créez une unité d'organisation dans le domaine **Adatum.com** nommé **Serveurs de fichiers**.
3. Déplacez **LON-SVR1** du conteneur **Computers** vers l'unité d'organisation **Serveurs de fichiers**.
4. Sur LON-DC1, ouvrez Gestion des stratégies de groupe.
5. Créez un objet de stratégie de groupe appelé **Audit de fichier**, puis associez-le à l'unité d'organisation **Serveurs de fichiers**.
6. Modifiez l'objet de stratégie de groupe **Audit de fichier** et, sous Configuration ordinateur, accédez au nœud **Configuration avancée de la stratégie d'audit\Stratégies d'audit\Accès à l'objet**.
7. Configurez les paramètres **Auditer le partage de fichiers détaillé** et **Auditer le stockage amovible** pour enregistrer les événements ayant réussi et échoué.
8. Redémarrez LON-SVR1 et connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

▶ Tâche 2 : Vérifier les entrées d'audit

1. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Allan** avec le mot de passe **Pa$$w0rd**.
2. Ouvrez l'Explorateur de fichiers et naviguez jusqu'à **\\LON-SVR1\Mod11**.
3. Ouvrez **Testfile.txt** dans le Bloc-notes, puis fermez le Bloc-notes.
4. Basculez vers LON-SVR1.
5. Ouvrez l'**Observateur d'événements** et affichez les événements Succès de l'audit dans le journal de sécurité.
6. Double-cliquez sur l'une des entrées du journal dont la **Source** est **Microsoft Windows security auditing** et la **Catégorie de tâche** est **Partage de fichiers détaillé**.
7. Cliquez sur l'onglet **Détails** et notez l'accès exécuté.

Résultats : À la fin de cet exercice, vous aurez configuré l'audit avancé.

▶ 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 **22411B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez ces étapes pour **22411B-LON-SVR1** et **22411B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Certains utilisateurs chiffrent les fichiers stockés sur les partages réseau pour les protéger des autres utilisateurs de service disposant d'autorisations NTFS sur ces fichiers. Cette méthode est-elle efficace pour empêcher les utilisateurs de consulter et de modifier ces fichiers ?

Question : Pourquoi le système EFS peut-il être considéré comme une méthode de chiffrement problématique dans un environnement de serveur de fichiers réseau largement distribué ?

Question : Vous avez configuré une stratégie d'audit à l'aide de la stratégie de groupe à appliquer à tous les serveurs de fichiers de votre organisation. Après avoir activé la stratégie et confirmé l'application des paramètres de stratégie de groupe, vous constatez qu'aucun événement d'audit n'est enregistré dans les journaux d'événements. Quelle en est la raison la plus probable ?

Outils

Outil	Utilisation	Emplacement
Console de gestion des stratégies de groupe	Gérer les objets de stratégie de groupe contenant les paramètres de stratégie d'audit	Gestionnaire de serveur - Outils
Observateur d'événements	Afficher les événements de stratégie d'audit	Gestionnaire de serveur - Outils

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 12

Implémentation de la gestion des mises à jour

Table des matières :

Vue d'ensemble du module **12-1**

Leçon 1 : Vue d'ensemble de WSUS **12-2**

Leçon 2 : Déploiement des mises à jour avec WSUS **12-5**

Atelier pratique : Implémentation de la gestion des mises à jour **12-9**

Contrôle des acquis et éléments à retenir **12-14**

Vue d'ensemble du module

Windows Server® Update Services (WSUS) améliore la sécurité en appliquant des mises à jour de sécurité aux serveurs au moment opportun. Il fournit l'infrastructure permettant de télécharger, de tester et d'approuver les mises à jour de sécurité. L'application rapide de mises à jour de sécurité permet d'éviter les incidents résultant de vulnérabilités connues. Lorsque vous implémentez WSUS, vous devez garder à l'esprit la configuration matérielle et logicielle requise, les paramètres à configurer, et les mises à jour à approuver ou à supprimer selon les besoins de votre entreprise.

Objectifs

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

- décrire le rôle de WSUS ;
- déployer des mises à jour avec WSUS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble de WSUS

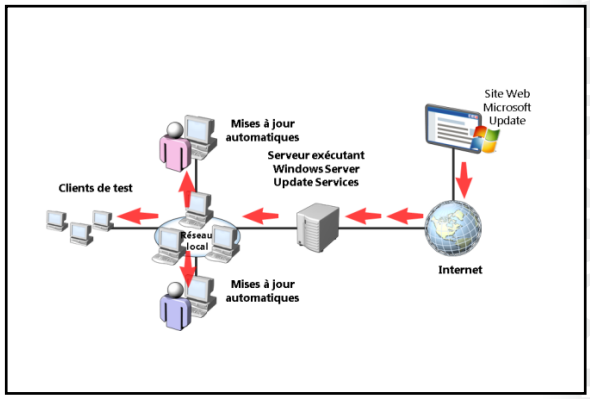
Le rôle WSUS fournit un point central de gestion des mises à jour de vos ordinateurs sous Windows®. WSUS vous permet de créer un environnement de mise à jour plus efficace dans votre entreprise et d'être mieux informé de l'état général des mises à jour des ordinateurs de votre réseau. Cette leçon vous présente WSUS et décrit les principales fonctionnalités du rôle serveur WSUS.

Objectifs de la leçon

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

- décrire les services WSUS ;
- expliquer le processus de gestion des mises à jour de WSUS ;
- identifier la configuration serveur requise pour WSUS.

Qu'est-ce que WSUS ?



WSUS est un rôle serveur compris dans le système d'exploitation Windows Server 2012, qui télécharge et distribue des mises à jour aux clients et aux serveurs Windows. WSUS peut obtenir les mises à jour qui s'appliquent au système d'exploitation et aux applications Microsoft classiques, telles que Microsoft® Office et Microsoft SQL Server®.

Dans sa configuration la plus simple, une petite entreprise peut disposer d'un seul serveur WSUS qui télécharge les mises à jour de Microsoft Update. Le serveur WSUS distribue alors ces mises à jour aux ordinateurs configurés pour obtenir des mises à jour automatiques du serveur WSUS. Vous devez approuver les mises à jour avant que les clients puissent les télécharger.

Les entreprises plus importantes peuvent créer une hiérarchie des serveurs WSUS. Dans ce scénario, un seul serveur WSUS centralisé obtient les mises à jour de Microsoft Update et d'autres serveurs WSUS obtiennent les mises à jour du serveur WSUS centralisé.

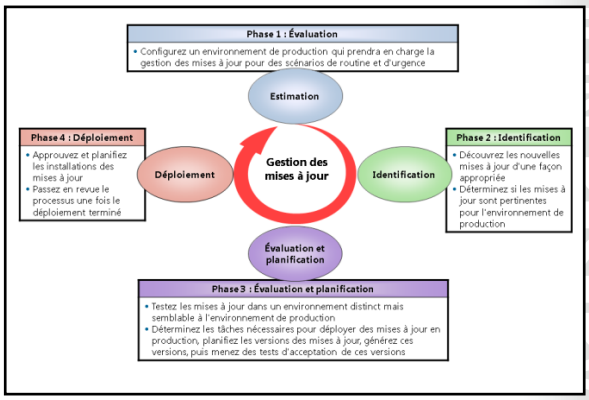
Vous pouvez organiser les ordinateurs par groupes pour simplifier l'approbation des mises à jour. Par exemple, vous pouvez configurer un groupe pilote pour être le premier à être utilisé pour tester les mises à jour.

WSUS peut générer des rapports pour faciliter le contrôle de l'installation des mises à jour. Ces derniers peuvent identifier les ordinateurs n'ayant pas appliqué les mises à jour récemment approuvées. Vous pouvez utiliser ces rapports pour déterminer pourquoi des mises à jour ne sont pas appliquées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Processus de gestion des mises à jour de WSUS

Le processus de gestion des mises à jour vous permet de gérer WSUS et les mises à jour qu'il récupère. Ce processus est un cycle continu pendant lequel vous pouvez réévaluer et adapter le déploiement de WSUS pour répondre aux besoins changeants. Les quatre phases du processus de gestion des mises à jour sont :



- l'estimation ;
- l'identification ;
- l'évaluation et la planification ;
- Déployer

Phase d'estimation

L'objectif de la phase d'estimation consiste à configurer un environnement de production prenant en charge la gestion des mises à jour pour des scénarios de routine et d'urgence. Il s'agit d'un processus constant que vous utilisez pour déterminer la topologie la plus efficace de mise à l'échelle des composants WSUS. À mesure que votre entreprise évolue, vous pouvez identifier la nécessité d'ajouter d'autres serveurs WSUS à d'autres emplacements.

Phase d'identification

La phase d'identification consiste à identifier les nouvelles mises à jour disponibles et à déterminer si elles sont appropriées pour l'entreprise. Vous pouvez soit configurer WSUS pour qu'il récupère automatiquement toutes les mises à jour, soit récupérer uniquement certains types de mises à jour. WSUS identifie également les mises à jour concernant les ordinateurs inscrits.

Phase d'évaluation et de planification

Une fois les mises à jour pertinentes identifiées, vous devez déterminer si elles fonctionnent correctement dans votre environnement. Il est toujours possible que la combinaison spécifique de logiciels de votre environnement rencontre des problèmes avec une mise à jour.

Pour évaluer les mises à jour, vous devez disposer d'un environnement de test dans lequel vous appliquez ces dernières afin de vérifier qu'elles fonctionnent correctement. Ce processus peut vous aider à identifier des dépendances permettant à une mise à jour de fonctionner correctement, et vous pouvez planifier toutes les modifications devant être apportées.

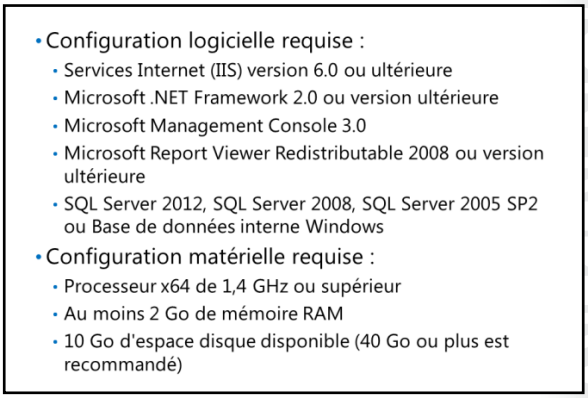
Phase de déploiement

Après avoir soigneusement testé une mise à jour et déterminé les éventuelles dépendances, vous pouvez approuver son déploiement dans le réseau de production. Dans l'idéal, vous devez approuver la mise à jour pour un groupe pilote d'ordinateurs avant de l'approuver pour l'ensemble de l'entreprise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration serveur requise pour les services WSUS

Vous pouvez utiliser le gestionnaire de serveur pour installer et configurer le rôle serveur WSUS. Cependant, pour que vous puissiez implémenter WSUS, votre serveur doit respecter une configuration matérielle et logicielle minimale.



Le logiciel requis pour WSUS 3.0 SP2 comprend les éléments suivants :

- Windows Server 2012,
  Windows Server 2008 R2,
  Windows Server 2008 Service Pack 1 (SP1) ou version ultérieure, Windows Server 2003 SP1 ou version ultérieure,
  Windows Small Business Server 2008 ou Windows Small Business Server 2003
- Services Internet (IIS) version 6.0 ou ultérieure
- Microsoft .NET Framework 2.0 ou version ultérieure
- Microsoft Management Console (MMC) 3.0
- Microsoft Report Viewer Redistributable 2008 ou version ultérieure
- SQL Server 2012, SQL Server 2008, SQL Server 2005 SP2 ou Base de données interne Windows

La configuration matérielle minimale requise pour WSUS est à peu près identique à celle des systèmes d'exploitation Windows Server. Cependant, vous devez prendre en compte l'espace disque dans le cadre de votre déploiement. Un serveur WSUS a besoin d'environ 10 gigaoctets (Go) d'espace disque et vous devez allouer au moins 30 Go d'espace disque pour les mises à jour téléchargées.

Un seul serveur WSUS peut prendre en charge des milliers de clients. Par exemple, un serveur WSUS possédant 4 Go de RAM et deux UC quadruples cœur peut prendre en charge jusqu'à 100 000 clients. Cependant, dans la plupart des cas, une entreprise possédant autant de clients dispose généralement de plusieurs serveurs WSUS pour réduire la charge sur les liaisons réseau étendu.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Déploiement des mises à jour avec WSUS

Cette leçon explique les caractéristiques du déploiement des mises à jour avec WSUS sur les ordinateurs client. Le déploiement des mises à jour sur les clients Windows Update via WSUS peut comporter de nombreux avantages. Vous pouvez configurer les mises à jour pour qu'elles soient téléchargées, approuvées et installées automatiquement, sans intervention de la part d'un administrateur. Vous pouvez également contrôler davantage le processus de mise à jour et fournir un environnement contrôlé dans lequel déployer ces dernières. Vous pouvez effectuer des tests dans un groupe isolé d'ordinateurs de test avant d'approuver une mise à jour dans l'ensemble de l'entreprise.

Objectifs de la leçon

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

- décrire comment configurer la fonction Mises à jour automatiques pour qu'elle utilise WSUS ;
- expliquer comment administrer WSUS ;
- identifier les groupes d'ordinateurs dans WSUS ;
- décrire les options d'approbation des mises à jour de WSUS.

Configuration des mises à jour automatiques

Quand vous activez la fonction Mises à jour automatiques sur un serveur, la configuration par défaut télécharge automatiquement les mises à jour depuis Microsoft Update et les installe. Après avoir implémenté WSUS, vos clients doivent être configurés pour obtenir les mises à jour automatiquement depuis le serveur WSUS.

- Vous devez configurer les ordinateurs clients pour qu'ils utilisent le serveur WSUS en tant que source pour les mises à jour
- Vous pouvez utiliser la stratégie de groupe pour configurer les clients, y compris les paramètres suivants :
  - La fréquence des mises à jour
  - Le calendrier d'installation des mises à jour
  - Le comportement de redémarrage automatique
  - Le groupe d'ordinateurs par défaut dans WSUS

L'emplacement à partir duquel la fonction Mises à jour automatiques obtient les mises à jour est contrôlé par une clé de Registre. Il est possible de configurer la clé de Registre manuellement à l'aide de l'outil Regedit, mais cette action n'est pas recommandée, sauf dans le cas où l'ordinateur ne se trouve pas dans un domaine. S'il se trouve dans un domaine, il est bien plus efficace de créer un objet de stratégie de groupe (GPO) qui configure la clé de Registre.

Pour les environnements Active Directory® Domain Services (AD DS), la fonction Mises à jour automatiques est généralement configurée dans un objet de stratégie de groupe en définissant les paramètres situés sous Configuration ordinateur. Pour accéder à ces paramètres, développez Stratégies, Modèles d'administration, Composants Windows, puis localisez le nœud Windows Update.

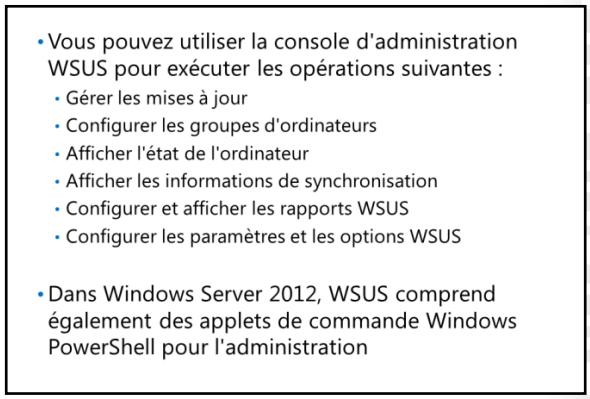
En plus de configurer la source pour les mises à jour, vous pouvez également utiliser un objet de stratégie de groupe pour configurer les paramètres suivants :

- La fréquence des mises à jour. Ce paramètre détermine à quelle fréquence les mises à jour sont détectées.
- Le calendrier d'installation des mises à jour. Ce paramètre détermine à quel moment les mises à jour sont installées. Il détermine également le moment où les mises à jour sont reprogrammées, lorsqu'elles n'ont pas pu être installées à l'heure planifiée.
- Le comportement de redémarrage automatique. Ce paramètre détermine si l'ordinateur redémarre automatiquement si une mise à jour le demande.
- Le groupe d'ordinateurs par défaut dans WSUS. Ce paramètre détermine le groupe d'ordinateurs dans lequel l'ordinateur sera enregistré lors de l'inscription initiale avec WSUS.

Administration de WSUS

La console d'administration de WSUS est un composant logiciel enfichable MMC que vous pouvez utiliser pour administrer WSUS. Vous pouvez utiliser cet outil pour :

- identifier et télécharger les mises à jour ;
- approuver le déploiement des mises à jour ;
- organiser les ordinateurs en groupes ;
- examiner l'état des mises à jour des ordinateurs ;
- générer des rapports.



La surveillance fait partie intégrante de la gestion d'un service. WSUS consigne des informations d'intégrité détaillées dans le journal des événements. En outre, vous pouvez télécharger un pack d'administration pour faciliter la surveillance dans Microsoft System Center 2012 - Operations Manager.

Contrôle des mises à jour sur les ordinateurs client

Les ordinateurs client effectuent des mises à jour en fonction d'une configuration manuelle ou, dans la plupart des environnements d'AD DS, d'une stratégie de groupe. Dans certains cas, vous souhaitez peut-être lancer le processus de mise à jour en dehors du calendrier habituel. Vous pouvez utiliser l'outil wuauclt.exe pour contrôler le comportement de mise à jour automatique sur des ordinateurs client Windows Update. La commande suivante lance la détection des mises à jour Microsoft d'après Windows Update.

```
Wuauclt.exe /detectnow
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

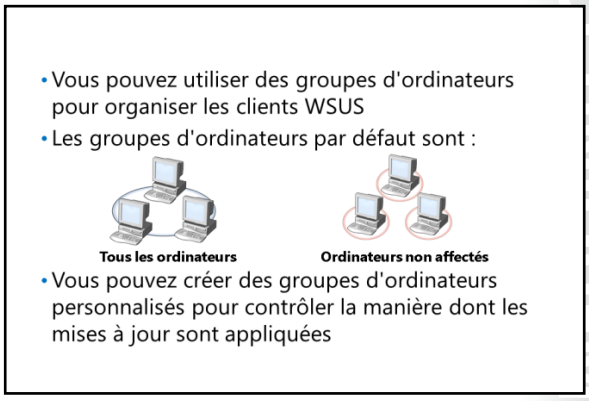
Administration avec Windows PowerShell®

Dans Windows Server 2012, WSUS comprend des applets de commande Windows PowerShell, que vous pouvez utiliser pour gérer votre serveur WSUS. Le tableau ci-après répertorie ces applets de commande.

Applet de commande	Description
Add-WsusComputer	Ajoute un ordinateur client spécifié à un groupe cible spécifié.
Approve-WsusUpdate	Approuve l'application d'une mise à jour aux clients.
Deny-WsusUpdate	Refuse le déploiement de la mise à jour.
Get-WsusClassification	Obtient la liste de toutes les classifications de WSUS actuellement disponibles dans le système.
Get-WsusComputer	Obtient l'objet Ordinateur WSUS qui représente l'ordinateur client.
Get-WsusProduct	Obtient la liste de tous les produits actuellement disponibles sur WSUS par catégorie.
Get-WsusServer	Obtient la valeur de l'objet Serveur de mise à jour WSUS.
Get-WsusUpdate	Obtient l'objet Mise à jour WSUS avec des détails concernant la mise à jour.
Invoke-WsusServerCleanup	Exécute le processus du nettoyage sur un serveur WSUS spécifié.
Set-WsusClassification	Définit si les classifications des mises à jour que WSUS synchronise sont activées ou non.
Set-WsusProduct	Définit si le produit représentant la catégorie de mises à jour à synchroniser est activé ou non.
Set-WsusServerSynchronization	Définit si le serveur WSUS effectue une synchronisation depuis Microsoft Update ou depuis un serveur en amont, en utilisant les propriétés de ce dernier.

Que sont les groupes d'ordinateurs ?

Les groupes d'ordinateurs constituent une façon d'organiser les ordinateurs pour lesquels un serveur WSUS déploie des mises à jour. Il existe deux groupes d'ordinateurs par défaut : Tous les ordinateurs et Ordinateurs non affectés. Les nouveaux ordinateurs qui contactent le serveur WSUS sont automatiquement affectés à ces deux groupes.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

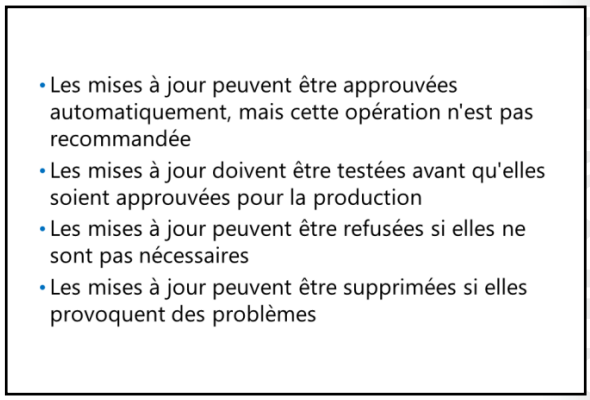
Vous pouvez créer des groupes d'ordinateurs personnalisés pour contrôler la manière dont les mises à jour sont appliquées. En général, les groupes d'ordinateurs personnalisés contiennent des ordinateurs possédant des caractéristiques semblables. Par exemple, vous pouvez créer un groupe d'ordinateurs personnalisé pour chaque service de votre entreprise. Vous pouvez également créer un groupe d'ordinateurs personnalisé pour un environnement de test où vous déployez d'abord les mises à jour pour les tester. Il est également fréquent de regrouper les serveurs séparément des ordinateurs client.

Lorsque vous affectez manuellement de nouveaux ordinateurs à un groupe d'ordinateurs personnalisé, cette opération est appelée ciblage côté serveur. Vous pouvez également utiliser le ciblage côté client pour affecter des ordinateurs à un groupe d'ordinateurs personnalisé. Pour utiliser le ciblage côté client, vous devez configurer pour l'ordinateur une clé de Registre ou un objet de stratégie de groupe qui spécifie le groupe d'ordinateurs personnalisé à rejoindre lors de l'inscription initiale avec le serveur WSUS.

Le ciblage côté serveur permet aux administrateurs de gérer manuellement l'adhésion au groupe d'ordinateurs WSUS. Cela est utile lorsque la structure d'AD DS ne prend pas en charge le côté client logique pour des groupes d'ordinateurs, ou lorsque des ordinateurs doivent être déplacés entre plusieurs groupes pour effectuer des tests ou autre. Le ciblage côté client est le plus généralement utilisé dans les grandes entreprises où l'affectation automatisée est requise et où des ordinateurs doivent être affectés à des groupes spécifiques.

Approbation des mises à jour

La configuration par défaut de WSUS n'approuve pas automatiquement les mises à jour des applications sur les ordinateurs. Bien qu'il soit possible d'approuver automatiquement les mises à jour, cette action n'est pas recommandée. Le processus recommandé pour approuver les mises à jour consiste tout d'abord à les tester dans un environnement de test, puis dans un groupe pilote, avant de passer à l'environnement de production. Vous réduisez ainsi le risque qu'une mise à jour entraîne un problème inattendu dans votre environnement de production. Vous l'effectuez en approuvant des mises à jour pour des groupes d'ordinateurs spécifiques avant de les approuver pour le groupe Tous les ordinateurs.



Certaines mises à jour ne sont pas considérées comme critiques et n'ont aucune implication en termes de sécurité. Vous pouvez décider de ne pas implémenter certaines de ces mises à jour. Pour toutes les mises à jour que vous décidez de ne pas implémenter, vous pouvez refuser la mise à jour. Une fois une mise à jour refusée, elle est supprimée de la liste des mises à jour sur le serveur WSUS dans l'affichage par défaut.

Si vous appliquez une mise à jour et découvrez qu'elle provoque à des problèmes, vous pouvez utiliser WSUS pour la supprimer. Cependant, cela est possible uniquement si cette mise à jour spécifique prend en charge la suppression. La plupart des mises à jour prennent en charge la suppression.

Lorsque vous regardez les détails d'une mise à jour, ils vous indiquent si cette dernière est remplacée par une autre mise à jour. Les mises à jour remplacées ne sont en général plus requises, car une mise à jour plus récente comprend entre autres les changements de celle-ci. Les mises à jour remplacées ne sont pas refusées par défaut, car elles sont parfois encore requises. Par exemple, une mise à jour plus ancienne peut être requise si certains serveurs n'exécutent pas le dernier Service Pack.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation de la gestion des mises à jour

Scénario

A. Datum est une société internationale d'ingénierie et de fabrication, dont le siège social se situe à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à Londres pour assister le site de Londres et d'autres succursales. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

A. Datum appliquait manuellement les mises à jour sur les serveurs d'un site distant. Elle a ainsi rencontré des difficultés à identifier les serveurs pour lesquels des mises à jour avaient ou non été appliquées. Il s'agit d'un problème de sécurité potentiel. Vous avez été invité à automatiser le processus de mise à jour en étendant le déploiement du WSUS d'A. Datum pour qu'il comprenne la succursale.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- implémenter le rôle serveur WSUS ;
- configurer des paramètres de mise à jour ;
- approuver et déployer une mise à jour à l'aide de WSUS.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-SVR1 22411B-LON-SVR4 22411B-LON-CL1
Nom d'utilisateur	**ADATUM\Administrateur**
Mot de passe	**Pa$$w0rd**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V®, cliquez sur **22411B-LON-DC1** puis, dans le volet Actions, cliquez sur **Accueil**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Ouvrez une session en utilisant les informations d'authentification suivantes :
    - Nom d'utilisateur : **ADATUM\Administrateur**
    - Mot de passe : **Pa$$w0rd**
5. Effectuez les étapes 2 à 4 pour **22411B-LON-SVR1**, **22411B-LON-SVR4** et **22411B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Implémentation du rôle serveur WSUS

Scénario

Votre entreprise possède déjà un serveur WSUS appelé LON-SVR1, qui est situé au siège social. Vous devez installer le rôle serveur WSUS sur LON-SVR4 sur le site d'une succursale. LON-SVR4 va utiliser LON-SVR1 comme source pour les téléchargements de Windows Update. L'installation sur LON-SRV4 va utiliser la base de données interne Windows pour le déploiement.

Les tâches principales de cet exercice sont les suivantes :

1. Installation du rôle serveur Windows Server Update Services (WSUS)
2. Configuration de WSUS pour qu'il se synchronise avec un serveur WSUS en amont

▶ Tâche 1 : Installation du rôle serveur Windows Server Update Services (WSUS)

1. Connectez-vous sur LON-SVR4 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Depuis le Gestionnaire de serveurs, installez le rôle **Windows Server Update Services** avec les services de rôle **WID Database** et **WSUS Services**. Configurez également l'emplacement des mises à jour sur **C:\MisesajourWSUS**.
3. Ouvrez la console Windows Server Update Services et terminez l'installation lorsque vous y êtes invité.
4. Dans l'**Assistant de configuration de Windows Server Update Services**, cliquez sur **Annuler**.
5. Fermez la console Update Services.

▶ Tâche 2 : Configuration de WSUS pour qu'il se synchronise avec un serveur WSUS en amont

1. Sur LON-SVR4, complétez l'Assistant de configuration de Windows Server Update Services, en spécifiant les paramètres suivants :
   - Serveur en amont : LON-SVR1.Adatum.com
   - Absence de serveur proxy
   - Langues par défaut
   - Planification manuelle de synchronisation
   - Début de la synchronisation initiale
2. Dans la console Windows Server Update Services, sous **Options**, définissez **Ordinateurs** sur **Utiliser les paramètres de stratégie de groupe ou de Registre sur les ordinateurs**.

Résultats : À la fin de cet exercice, vous devez avoir implémenté le rôle serveur WSUS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Configuration des paramètres de mise à jour

Scénario

Vous devez configurer les paramètres de stratégie de groupe pour déployer les paramètres automatiques de WSUS sur les ordinateurs client. Le rôle WSUS étant configuré sur LON-SVR4, vous devez vérifier que le service Recherche possède son propre groupe d'ordinateurs dans WSUS sur LON-SVR4. Vous devez également configurer les ordinateurs client de l'unité d'organisation Recherche pour qu'ils utilisent LON-SVR4 en tant que leur source pour les mises à jour.

Les tâches principales de cet exercice sont les suivantes :

1. Configuration des groupes WSUS
2. Configuration de la stratégie de groupe pour déployer les paramètres de WSUS
3. Vérification de l'application des paramètres de la Stratégie de groupe
4. Initialisation de Windows Update

▶ Tâche 1 : Configuration des groupes WSUS

1. Sur LON-SVR4, ouvrez si nécessaire la console Windows Server Update Services.
2. Créez un groupe d'ordinateurs appelé **Recherche**.

▶ Tâche 2 : Configuration de la stratégie de groupe pour déployer les paramètres de WSUS

1. Basculez vers LON-DC1.
2. Ouvrez **Gestion des stratégies de groupe**.
3. Créez un objet GPO et associez-le à l'unité d'organisation **Recherche**. Appelez-le **Recherche WSUS** et configurez les paramètres de stratégie suivants sous le nœud **Windows Update** :
   - Configuration du service Mises à jour automatiques : **Téléchargement automatique et planification des installations**
   - Emplacement du service Microsoft Update : **http://LON-SVR4.Adatum.com:8530**
   - Serveur Intranet de statistiques : **http://LON-SVR4.Adatum.com:8530**
   - Groupe de ciblage côté client : **Recherche**
4. Déplacez **LON-CL1** dans l'unité d'organisation **Recherche**.

▶ Tâche 3 : Vérification de l'application des paramètres de la Stratégie de groupe

1. Basculez vers LON-CL1.
2. Redémarrez LON-CL1.
3. Sur LON-CL1, connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Ouvrez une invite de commande à l'aide de l'option **Exécuter en tant qu'administrateur**.
5. À l'invite de commande, exécutez la commande suivante :

```
Gpresult /r
```

6. Dans la sortie de la commande, confirmez que sous **Paramètres de l'ordinateur**, **Recherche WSUS** est listé sous **Objets Stratégie de groupe appliqués**.

▶ Tâche 4 : Initialisation de Windows Update

1. Sur LON-CL1, à l'invite de commandes, tapez la commande suivante et appuyez sur ENTRÉE :

```
Wuauclt.exe /reportnow /detectnow
```

2. Basculez vers LON-SVR4.
3. Dans la console Update Services, développez **Ordinateurs**, **Tous les ordinateurs**, puis cliquez sur **Recherche**.
4. Vérifiez que LON-CL1 apparaît dans le groupe Recherche. S'il n'apparaît pas, répétez les étapes 1 à 3. L'affichage de LON-CL1 peut prendre plusieurs minutes.
5. Vérifiez que des mises à jour sont indiquées comme étant nécessaires. Si aucune mise à jour n'est indiquée, répétez les étapes 1 à 3. L'enregistrement des mises à jour peut prendre 10 à 15 minutes.

Résultats : À la fin de cet exercice, vous devez avoir configuré des paramètres de mise à jour pour les ordinateurs client.

Exercice 3 : Approbation et déploiement d'une mise à jour à l'aide de WSUS

Scénario

Une fois les paramètres de Windows Update configurés, vous pouvez à présent afficher, approuver, puis déployer les mises à jour requises. Vous avez été invité à utiliser LON-CL1 comme étude de cas pour le service Recherche. Vous allez approuver, déployer et vérifier une mise à jour sur LON-CL1 pour confirmer que l'environnement de WSUS est correctement configuré.

Les tâches principales de cet exercice sont les suivantes :

1. Approbation des mises à jour de WSUS pour le groupe d'ordinateurs Recherche
2. Déploiement des mises à jour sur LON-CL1.
3. Vérification du déploiement de la mise à jour sur LON-CL1
4. Pour préparer le module suivant

▶ Tâche 1 : Approbation des mises à jour de WSUS pour le groupe d'ordinateurs Recherche

1. Sur LON-SVR4, ouvrez la console WSUS.
2. Approuvez la mise à jour **Mise à jour de sécurité pour Microsoft Office 2010 (KB2553371), édition 32 bits** pour le groupe **Recherche**.

▶ Tâche 2 : Déploiement des mises à jour sur LON-CL1.

1. Sur LON-CL1, à l'invite de commandes, tapez la commande suivante et appuyez sur ENTRÉE :

```
Wuauclt.exe /detectnow
```

2. Ouvrez **Windows Update**, puis vérifiez la présence de mises à jour.
3. Cliquez sur **Installer** pour installer la mise à jour approuvée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Vérification du déploiement de la mise à jour sur LON-CL1

1. Sur LON-CL1, ouvrez l'observateur d'événements.
2. Accédez à **Journaux des applications et des services\Microsoft\Windows** et affichez les événements sous **WindowsUpdateClient – Opérationnel**.
3. Confirmez que les événements relatifs à la mise à jour sont enregistrés.

Résultats : À la fin de cet exercice, vous devez avoir approuvé et déployé une mise à jour à l'aide de WSUS.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial de tous les ordinateurs virtuels. Pour cela, 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 **22411B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22411B-LON-SVR1**, **22411B-LON-SVR4** et **22411B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Un collègue a affirmé que toutes les mises à jour du système d'exploitation Windows devaient être appliquées automatiquement au moment de leur sortie. Recommandez-vous un autre processus ?

Question : Votre entreprise implémente plusieurs applications qui ne sont pas des applications de Microsoft. Un collègue a proposé d'utiliser WSUS pour déployer les mises à jour des applications et du système d'exploitation. L'utilisation de WSUS peut-elle entraîner des problèmes potentiels ?

Question : Pourquoi WSUS est-il plus facile à gérer dans un domaine AD DS ?

Outils

Outil	Utilisation	Emplacement
Console d'administration WSUS	Administration de WSUS	Gestionnaire de serveur - Outils
Applets de commande WSUS Windows PowerShell	Administration de WSUS à partir de l'interface de ligne de commande	Windows PowerShell

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 13

Surveillance de Windows Server 2012

Table des matières :

Vue d'ensemble du module	**13-1**
Leçon 1 : Outils d'analyse	**13-2**
Leçon 2 : Utilisation de l'Analyseur de performances	**13-9**
Leçon 3 : Analyse des journaux d'événements	**13-18**
Atelier pratique : Surveillance de Windows Server 2012	**13-21**
Contrôle des acquis et éléments à retenir	**13-27**
Contrôle des acquis et éléments à retenir	**13-31**

Vue d'ensemble du module

Quand une défaillance du système ou un événement qui affecte les performances système se produit, vous devez pouvoir rapidement et efficacement procéder au dépannage ou à la résolution du problème. Les variables et les possibilités de l'environnement réseau moderne étant nombreuses, la capacité à déterminer la cause première repose souvent sur un ensemble de méthodes et d'outils efficaces d'analyse des performances.

Il est possible d'utiliser des outils d'analyse des performances pour identifier les composants qui nécessitent des réglages et des résolutions de problèmes supplémentaires. En identifiant ces composants, vous pouvez améliorer le rendement de vos serveurs.

Objectifs

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

- décrire les outils d'analyse pour Windows Server® 2012 ;
- utiliser l'Analyseur de performances pour afficher et analyser les statistiques de performance des programmes qui s'exécutent sur vos serveurs ;
- surveiller les journaux des événements pour afficher et interpréter les événements survenus.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Outils d'analyse

Windows Server 2012 comporte plusieurs outils permettant d'analyser le système d'exploitation et les applications sur un ordinateur. Vous pouvez utiliser ces outils pour optimiser votre système et résoudre des problèmes. Utilisez ces outils et complétez-les avec vos propres outils lorsque cela est nécessaire.

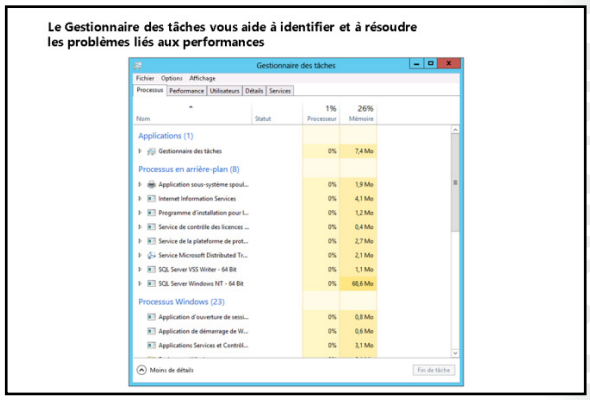
Objectifs de la leçon

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

- décrire le Gestionnaire des tâches ;
- décrire l'Analyseur de performances ;
- Ouvrez le décrire le Moniteur de ressources ;
- décrire l'Observateur d'événements.

Vue d'ensemble du Gestionnaire des tâches

Le Gestionnaire des tâches a été amélioré dans Windows Server 2012 pour fournir plus d'informations vous permettant d'identifier et de résoudre les problèmes liés aux performances. Il contient les onglets suivants :



- *Processus*. L'onglet Processus affiche la liste des programmes en cours d'exécution, subdivisés en applications et en processus Windows internes. Pour chaque processus en cours d'exécution, cet onglet affiche un résumé de l'utilisation du processeur et de la mémoire.
- *Performances*. L'onglet Performances affiche un résumé de l'utilisation du processeur et de la mémoire, ainsi que des statistiques réseau.
- *Utilisateurs*. L'onglet Utilisateurs affiche la consommation de ressources par utilisateur. Vous pouvez également développer la vue Utilisateur pour afficher des informations plus détaillées sur les processus spécifiques exécutés par un utilisateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

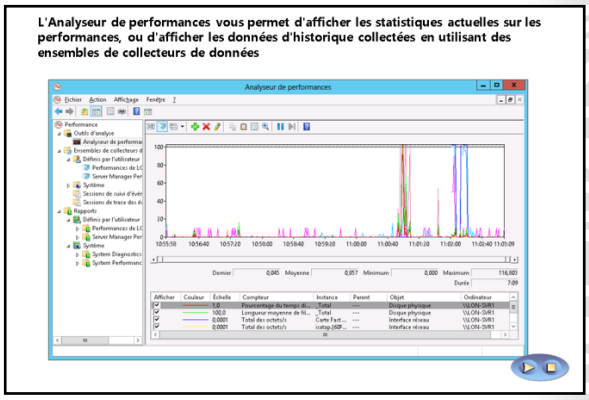
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Détails*. L'onglet Détails répertorie tous les processus en cours d'exécution sur le serveur et fournit des statistiques sur la consommation du processeur, de la mémoire et sur toute autre consommation de ressources. Vous pouvez utiliser cet onglet pour gérer les processus en cours d'exécution. Par exemple, vous pouvez arrêter un processus, arrêter un processus et tous les processus associés et modifier les valeurs de priorité des processus. En modifiant la priorité d'un processus, vous déterminez sa consommation de ressources de processeur. En augmentant la priorité, le processus peut demander plus de ressources de processeur.
- *Services*. L'onglet Services fournit une liste des services Windows en cours d'exécution, ainsi que les informations relatives, notamment si le service est en cours d'exécution et la valeur d'identité de processeur (PID) du service en cours d'exécution. Vous pouvez démarrer et arrêter des services en utilisant la liste située dans l'onglet Services.

En général, pensez à utiliser le Gestionnaire des tâches lorsqu'un problème lié aux performances se produit pour la première fois. Par exemple, vous pouvez examiner les processus en cours d'exécution pour déterminer si un programme particulier utilise des ressources de processeur excessives. Gardez toujours à l'esprit que le Gestionnaire des tâches affiche une capture instantanée de la consommation de ressources actuelle, et vous pouvez également être amené à examiner les données d'historique pour avoir une idée précise des performances et de la réponse sous la charge d'un serveur.

Vue d'ensemble de l'Analyseur de performances

L'Analyseur de performances vous permet d'afficher les statistiques actuelles sur les performances, ou d'afficher les données d'historique collectées en utilisant des ensembles de collecteurs de données.



Windows Server 2012 vous permet d'analyser les performances du système d'exploitation à l'aide des objets de performance et des compteurs dans chaque objet. Windows Server 2012 recueille les données des compteurs de différentes manières, à savoir :

- valeur de capture instantanée en temps réel ;
- total depuis le dernier démarrage de l'ordinateur ;
- moyenne sur un intervalle de temps spécifique ;
- moyenne des dernières valeurs ;
- nombre par seconde ;
- valeur maximale ;
- valeur minimale.

L'Analyseur de performances fonctionne en vous fournissant une collection d'objets et de compteurs qui enregistrent les données relatives à l'utilisation des ressources de l'ordinateur.

Il existe de nombreux compteurs que vous pouvez analyser et surveiller en fonction de vos besoins.

Principaux compteurs de processeur

Les compteurs de processeur sont une fonctionnalité du processeur de l'ordinateur qui enregistre le nombre d'événements matériels. Les principaux compteurs de processeur sont les suivants :

- Processeur > % Temps processeur. Ce compteur mesure le pourcentage de temps que le processeur utilise pour exécuter des threads actifs. Si ce pourcentage est supérieur à 85 %, le processeur est surchargé et le serveur peut nécessiter un processeur plus rapide. En d'autres termes, ce compteur affiche le pourcentage de temps qu'un thread donné a utilisé pour exécuter des instructions. Une instruction est l'unité d'exécution de base dans un processeur, et un thread est l'objet qui exécute des instructions. Le code qui gère certaines interruptions matérielles et les conditions d'interception sont inclus dans ce compte.
- Processeur > Interruptions/s. Ce compteur affiche la fréquence, en incidents par seconde, à laquelle le processeur a reçu et géré les interruptions matérielles.
- Système > Longueur de la file du processeur. Ce compteur affiche un nombre approximatif de threads géré par chaque processeur. Si cette valeur est plus de deux fois supérieure au nombre de processeurs pendant une période prolongée, le processeur du serveur n'est pas assez puissant. La longueur de la file du processeur, parfois désignée sous le nom de profondeur de la file du processeur, qui est enregistrée par ce compteur est une valeur instantanée qui est représentative uniquement d'une capture instantanée actuelle du processeur. Par conséquent, vous devez observer ce compteur pendant une période prolongée pour déterminer les tendances de données. En outre, le compteur Système > Longueur de la file du processeur enregistre la longueur totale de la file pour tous les processeurs, pas la longueur pour chaque processeur.

Principaux compteurs de mémoire

L'objet de performances Mémoire se compose de compteurs qui décrivent le comportement de la mémoire physique et virtuelle de l'ordinateur. La mémoire physique est la quantité de mémoire vive (RAM) sur l'ordinateur. La mémoire virtuelle comprend l'espace dans la mémoire physique et sur le disque. La plupart des compteurs de mémoire surveillent la pagination, qui est le déplacement de pages de code et de données entre le disque et la mémoire physique.

Le compteur Mémoire > Pages/s mesure la fréquence à laquelle les pages sont lues ou écrites sur le disque pour résoudre les défauts de page. Si une pagination excessive produit une valeur supérieure à 1 000, il peut y avoir une fuite de mémoire. En d'autres termes, le compteur Mémoire > Pages/s affiche le nombre de défauts de page par seconde. Un défaut de page se produit quand la page de mémoire demandée est introuvable dans la mémoire RAM car elle existe actuellement dans le fichier de pagination. Une augmentation de ce compteur indique qu'une pagination supplémentaire se produit, ce qui suggère un manque de mémoire physique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Principaux compteurs de disque

L'objet de performances Disque physique se compose de compteurs qui surveillent les disques durs ou fixes. Les disques contiennent les données de fichiers, de programmes et de pagination. Ils sont lus pour récupérer ces éléments, et sont écrits pour y enregistrer des modifications. Les valeurs totales des compteurs de disque physique correspondent au total de toutes les valeurs des disques logiques (ou partitions) dans lesquels elles sont divisées. Les principaux compteurs de disque sont les suivants :

- Disque physique > Pourcentage du temps disque. Ce compteur indique l'activité d'un disque particulier, et il mesure le pourcentage de temps pendant lequel le disque était occupé pendant l'intervalle d'échantillonnage. Un compteur avoisinant 100 pour cent indique que le disque est occupé presque tout le temps, et un goulot d'étranglement au niveau des performances est peut-être imminent. Vous pouvez éventuellement remplacer le système de disque actuel par un autre plus rapide.
- Disque physique > Longueur moyenne de file d'attente du disque. Ce compteur indique le nombre de demandes de disque en attente de traitement par le gestionnaire d'E/S dans Windows® 7 à un moment donné. Si cette valeur est plus de deux fois plus importante que le nombre de piles, le disque lui-même peut être engorgé. Plus la file est longue, moins le débit du disque est satisfaisant.

 **Remarque :** Le débit est la quantité totale de trafic qui passe par un point de connexion réseau donné pour chaque unité de temps. La charge de travail est la quantité de traitement effectué par l'ordinateur à un moment donné.

Principaux compteurs de réseau

La plupart des charges de travail nécessitent l'accès aux réseaux de production pour assurer la communication avec les autres applications et services, et pour communiquer avec les utilisateurs. La configuration réseau requise comprend des éléments tels que le débit et la présence de plusieurs connexions réseau.

Les charges de travail peuvent nécessiter l'accès à plusieurs réseaux différents qui doivent rester sécurisés. C'est le cas notamment des connexions pour :

- l'accès au réseau public ;
- les réseaux pour effectuer des sauvegardes et d'autres tâches de maintenance ;
- les connexions de gestion à distance dédiées ;
- l'association de cartes réseau pour les performances et le basculement ;
- les connexions à l'ordinateur hôte physique ;
- les connexions aux modules de stockage basés sur un réseau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

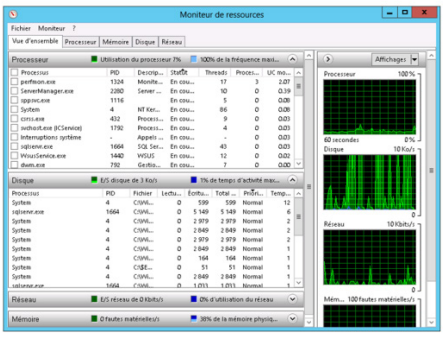
En analysant les compteurs de performance du réseau, vous pouvez évaluer les performances de votre réseau. Les principaux compteurs de réseau sont les suivants :

- Interface réseau > Bande passante actuelle. Ce compteur indique la bande passante actuelle utilisée sur l'interface réseau en bits par seconde (bits/s). La plupart des topologies de réseau ont des bandes passantes potentielles maximales exprimées en mégabits par seconde (Mbits/s). Par exemple, Ethernet peut fonctionner à des bandes passantes de 10 Mbits/s, 100 Mbits/s, 1 Gigabit par seconde (Gbits/s) et plus. Pour interpréter ce compteur, divisez la valeur donnée par 1 048 576 pour Mbits/s. Si la valeur est proche de la bande passante potentielle maximale du réseau, vous pouvez implémenter un réseau commuté ou effectuer une mise à niveau vers un réseau qui prend en charge des bandes passantes plus élevées.
- Interface réseau > Longueur de la file d'attente de sortie. Ce compteur indique la longueur actuelle de la file d'attente des paquets de sortie sur l'interface réseau sélectionnée. Une valeur croissante, ou constamment supérieure à deux, peut indiquer un goulot d'étranglement du réseau qui nécessite un examen.
- Interface réseau > Total des octets/s. Mesure la fréquence à laquelle les octets sont envoyés et reçus sur chaque carte réseau, y compris les caractères de trame. Si plus de 70 % de l'interface est utilisée, le réseau est saturé.

Vue d'ensemble du Moniteur de ressources

L'interface Moniteur de ressources dans Windows Server 2012 fournit une analyse détaillée des performances en temps réel de votre serveur.

Le Moniteur de ressources fournit une analyse détaillée des performances en temps réel de votre serveur



Vous pouvez utiliser le Moniteur de ressources pour analyser en temps réel l'utilisation et les performances du processeur, du disque, du réseau et de la mémoire. Vous pouvez ainsi identifier les conflits de ressources et les goulots d'étranglement afin de les résoudre.

En développant les éléments analysés, les administrateurs système peuvent déterminer quels processus utilisent quelles ressources. En outre, vous pouvez utiliser le Moniteur de ressources pour suivre un ou des processus en activant les cases à cocher correspondantes. Quand vous sélectionnez un processus, il reste sélectionné dans chaque volet du Moniteur de ressources, qui affiche les informations dont vous avez besoin concernant ce processus en haut de l'écran, quel que soit l'endroit où vous êtes dans l'interface.

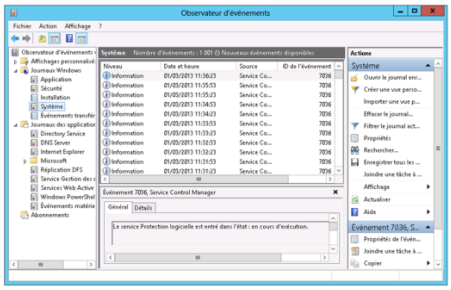
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vue d'ensemble de l'Observateur d'événements

L'Observateur d'événements Windows fournit un accès aux journaux d'événements de Windows Server 2012. Les journaux d'événements fournissent des informations concernant les événements système qui se produisent dans Windows. Ces événements comprennent les messages d'information, d'avertissement et d'erreur sur les composants Windows et les applications installées.

L'Observateur d'événements fournit des listes classées par catégorie des événements essentiels du journal Windows, et des groupements de journal pour les applications individuelles installées et des catégories de composants Windows spécifiques



L'Observateur d'événements fournit des listes classées par catégorie des événements essentiels du journal Windows, y compris les événements d'application, de sécurité, de configuration et système, ainsi que des groupements de journal pour les applications individuelles installées et des catégories de composants Windows spécifiques. Les événements individuels fournissent des informations détaillées concernant le type d'événement qui s'est produit, la date à laquelle l'événement s'est produit, la source de l'événement, ainsi que des informations techniques détaillées pour vous aider à résoudre l'événement.

En outre, l'Observateur d'événements vous permet de consolider les journaux de plusieurs ordinateurs sur un ordinateur centralisé à l'aide d'abonnements. Enfin, vous pouvez configurer l'Observateur d'événements pour exécuter une action en fonction d'un événement ou d'événements spécifiques. Cela peut inclure l'envoi d'un message électronique, le lancement d'une application, l'exécution d'un script ou d'autres actions de maintenance qui peuvent vous informer d'un problème potentiel ou tenter de le résoudre.

L'Observateur d'événements de Windows Server 2012 contient les fonctionnalités importantes suivantes :

- Inclusion de plusieurs nouveaux journaux. Vous pouvez accéder aux journaux de plusieurs composants et sous-systèmes individuels.
- Possibilité d'afficher plusieurs journaux. Vous pouvez filtrer des événements spécifiques dans plusieurs journaux, ce qui facilite l'examen et la résolution des problèmes susceptibles d'apparaître dans plusieurs journaux.
- Inclusion de vues personnalisées. Vous pouvez utiliser le filtrage pour limiter la recherche aux événements qui vous intéressent, et vous pouvez sauvegarder ces vues filtrées.
- Possibilité de configurer les tâches planifiées pour s'exécuter en réponse à des événements. Vous pouvez automatiser les réponses aux événements. L'Observateur d'événements est intégré au Planificateur de tâches.
- Possibilité de créer et de gérer les abonnements aux événements. Vous pouvez collecter des événements à partir d'ordinateurs distants, et les enregistrer localement.

Remarque : Pour collecter des événements à partir d'ordinateurs distants, vous devez créer une règle entrante dans le Pare-feu Windows pour permettre la gestion du journal des événements Windows.

L'Observateur d'événements suit les informations dans plusieurs journaux différents. Ces journaux fournissent des informations détaillées qui comprennent :

- description de l'événement ;
- numéro d'identification de l'événement ;
- composant ou sous-système qui a généré l'événement ;
- état Information, Avertissement ou Erreur ;
- date de l'occurrence ;
- nom de l'utilisateur pour le compte duquel l'événement s'est produit ;
- ordinateur sur lequel l'événement s'est produit ;
- lien vers Microsoft TechNet pour obtenir des informations supplémentaires sur l'événement.

Journaux Windows Server

L'Observateur d'événements comporte plusieurs journaux intégrés, y compris ceux contenus dans le tableau suivant.

Journal intégré	Description et utilisation
Journal des applications	Ce journal contient les erreurs, les avertissements et les événements d'information relatifs au fonctionnement d'applications telles que Microsoft Exchange Server, le service SMTP (Simple Mail Transfer Protocol) et d'autres applications.
Journal de sécurité	Ce journal enregistre les résultats de l'audit, si vous l'activez. Les événements d'audit sont décrits comme ayant réussi ou échoué, selon l'événement. Par exemple, le journal enregistre les succès ou les échecs de l'accès d'un utilisateur à un fichier.
Journal de configuration	Ce journal contient les événements relatifs à la configuration des applications.
Journal système	Les événements généraux sont enregistrés par les composants et services Windows, et sont classés en tant qu'erreur, avertissement ou information. Windows prédétermine les événements enregistrés par les composants système.
Événements transférés	Ce journal enregistre les événements collectés à partir d'ordinateurs distants. Pour collecter des événements à partir d'ordinateurs distants, vous devez créer un abonnement aux événements.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Journaux des applications et des services

Les journaux des applications et des services stockent les événements d'une application ou d'un composant plutôt que les événements qui peuvent avoir un impact à l'échelle du système. Cette catégorie de journaux comprend quatre sous-types :

- Admin
- Opérations
- Analyse
- Débogage

Les journaux d'administration présentent un intérêt pour les professionnels de l'informatique qui utilisent l'Observateur d'événements pour résoudre des problèmes. Ces journaux expliquent comment résoudre des problèmes, et ciblent principalement les utilisateurs finaux, les administrateurs et le personnel de support. Les événements des canaux d'administration indiquent un problème et une solution bien définie sur lesquels un administrateur peut agir.

Les événements du journal des opérations sont également utiles pour les professionnels de l'informatique, mais ils peuvent nécessiter une interprétation supplémentaire. Vous pouvez utiliser les événements opérationnels pour analyser et diagnostiquer un problème ou une occurrence et déclencher des outils ou des tâches en fonction du problème ou de l'occurrence.

Les journaux d'analyse et de débogage ne sont pas aussi conviviaux. Les journaux d'analyse stockent les événements qui suivent un problème, et ils enregistrent souvent un volume élevé d'événements. Les développeurs utilisent les journaux de débogage quand ils déboguent des applications. Par défaut, les journaux d'analyse et de débogage sont masqués et désactivés.

Par défaut, les fichiers journaux Windows ont une taille de 1 028 kilo-octets (Ko), et les événements sont remplacés autant que nécessaire. Si vous souhaitez effacer un journal manuellement, vous devez être connecté au serveur en tant qu'administrateur local. Si vous souhaitez configurer de manière centralisée les paramètres des journaux d'événements, vous pouvez utiliser la stratégie de groupe. Ouvrez l'**Éditeur de gestion des stratégies de groupe** pour votre objet de stratégie de groupe sélectionné, puis naviguez jusqu'à **Configuration ordinateur\Stratégies\Modèles d'administration\Composants Windows\ Service Journal des événements**.

Pour chaque journal, vous pouvez définir :

- l'emplacement du fichier journal ;
- la taille maximale du fichier journal ;
- les options de sauvegarde automatique ;
- les autorisations sur les journaux ;
- le comportement qui se produit quand le journal est plein.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Utilisation de l'Analyseur de performances

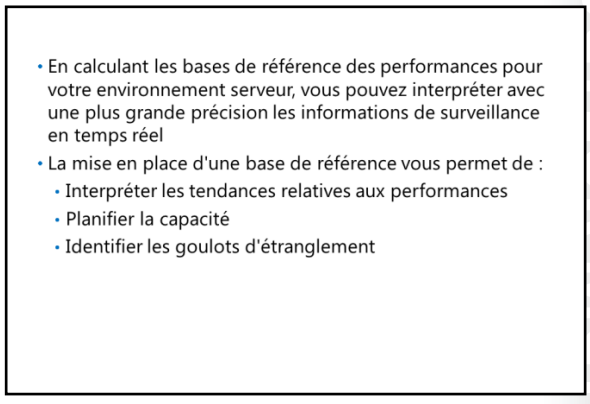
Vous pouvez utiliser l'Analyseur de performances pour collecter, analyser et interpréter les données liées aux performances des serveurs de votre organisation. Cela vous permet de prendre des décisions avisées relatives à la planification de la capacité. Cependant, pour prendre des décisions avisées, il est important que vous sachiez comment établir une base de référence des performances, utiliser des ensembles de collecteurs de données et utiliser des rapports pour vous aider à comparer les données de performances à votre base de référence.

Objectifs de la leçon

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

- décrire une base de référence ;
- décrire des ensembles de collecteurs de données ;
- expliquer comment capturer les données de compteur avec un ensemble de collecteurs de données ;
- expliquer comment configurer une alerte ;
- expliquer comment afficher les rapports de l'Analyseur de performances ;
- identifier les principaux paramètres que vous devez suivre lors de la surveillance des services d'infrastructure réseau ;
- identifier les éléments à prendre en considération pour la surveillance d'ordinateurs virtuels.

Base de référence, tendances et planification de la capacité



En calculant les bases de référence des performances pour votre environnement serveur, vous pouvez interpréter avec une plus grande précision les informations de surveillance en temps réel. Une base de référence des performances de votre serveur indique l'apparence de vos statistiques d'analyse des performances pendant une utilisation normale, et vous pouvez établir une base de référence en analysant les statistiques de performances sur une période spécifique. Quand un problème ou un symptôme se produit en temps réel, vous pouvez comparer vos statistiques de référence à vos statistiques en temps réel et identifier les anomalies.

Analyse des tendances

Vous devez examiner attentivement la valeur des données de performance pour vérifier qu'elles reflètent votre environnement serveur réel.

En outre, vous devez envisager une analyse des performances, ainsi que des plans de croissance et de mise à niveau commerciaux ou technologiques. Il est possible de réduire le nombre de serveurs en service une fois que vous avez mesuré les performances et évalué l'environnement requis.

En analysant les tendances de performance, vous pouvez prédire quand la capacité existante sera épuisée. Examinez l'analyse de l'historique par rapport aux besoins de votre entreprise et déterminez à partir de vos conclusions quand la capacité des serveurs devra être augmentée. Certains pics sont associés aux activités uniques telles que les commandes importantes. D'autres pics se produisent régulièrement, comme le paiement mensuel des salaires. Ces pics peuvent nécessiter une capacité plus importante pour répondre à l'augmentation du nombre d'employés.

La prévision des besoins en termes de capacité des serveurs est obligatoire pour toutes les entreprises. Dans le cadre de la planification des besoins, l'augmentation de la capacité des serveurs est souvent nécessaire pour répondre aux objectifs de l'entreprise. En alignant votre stratégie informatique sur la stratégie de votre entreprise, vous pouvez atteindre les objectifs fixés.

En outre, vous devez également envisager de virtualiser votre environnement pour réduire le nombre de serveurs physiques requis. Vous pouvez consolider les serveurs en implémentant le rôle Hyper-V® dans l'environnement Windows Server 2012.

Planification de la capacité

La planification de la capacité est centrée sur l'évaluation de la charge de travail du serveur, du nombre d'utilisateurs qu'il peut prendre en charge et des méthodes d'évolutivité du système pour qu'il puisse répondre ultérieurement à une charge de travail plus importante et à un plus grand nombre d'utilisateurs.

L'ajout de services et d'applications de serveur ont un impact sur les performances de votre infrastructure informatique. Ces services peuvent recevoir le matériel dédié bien qu'ils utilisent souvent le même réseau local (LAN) et la même infrastructure de réseau sans fil (WAN). La planification des besoins en termes de capacité doit inclure tous les composants matériels et doit tenir compte de l'impact des nouveaux serveurs, services et applications sur l'infrastructure existante. Les facteurs tels que l'alimentation, le refroidissement et la capacité du rack sont souvent oubliés pendant les premières phases de planification de l'augmentation de la capacité. Vous devez réfléchir à la manière dont vous allez adapter vos serveurs à une augmentation de la charge de travail.

Les tâches telles que la mise à niveau vers Windows Server 2008 R2 et la mise à jour des systèmes d'exploitation peuvent avoir un impact sur vos serveurs et votre réseau. Une mise à jour peut parfois produire un problème avec une application. Une analyse précise des performances avant et après l'application des mises à jour peut identifier les problèmes.

L'augmentation de l'activité d'une entreprise implique un plus grand nombre d'utilisateurs à prendre en charge. Vous devez tenir compte des besoins de l'entreprise lorsque vous achetez du matériel. Vous devrez ainsi augmenter le nombre de serveurs ou la capacité du matériel existant lorsque de nouveaux besoins l'exigent.

Les besoins en termes de capacité sont les suivants :

- plus de serveurs ;
- matériel supplémentaire ;
- réduction des charges des applications ;
- réduction du nombre d'utilisateurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Description des goulots d'étranglement

Un goulot d'étranglement au niveau des performances se produit quand un ordinateur ne peut pas gérer les demandes actuelles pour une ressource spécifique. La ressource peut être un composant clé, tel qu'un disque, une mémoire, un processeur ou un réseau. La pénurie d'un composant dans un package d'applications peut provoquer le goulot d'étranglement.

En utilisant régulièrement les outils d'analyse des performances et en comparant les résultats à votre base de référence et aux données d'historique, vous pouvez identifier les goulots d'étranglement au niveau des performances avant qu'ils affectent les utilisateurs.

Une fois que vous avez identifié un goulot d'étranglement, vous devez décider comment le supprimer. Les options de suppression d'un goulot d'étranglement sont les suivantes :

- exécution d'un nombre réduit d'applications ;
- ajout de ressources à l'ordinateur.

Un ordinateur confronté à une grave pénurie de ressources peut cesser de traiter les demandes des utilisateurs, ce qui nécessite une attention immédiate. Cependant, si votre ordinateur rencontre un goulot d'étranglement, mais continue de fonctionner dans des limites acceptables, vous pouvez décider de différer les modifications jusqu'à ce que vous résolviez la situation ou que vous ayez la possibilité de prendre des mesures correctives.

Analyse des composants matériels clés

En comprenant comment votre système d'exploitation utilise les quatre composants matériels clés (processeur, disque, mémoire et réseau) et comment ils interagissent entre eux, vous commencez à comprendre comment optimiser les performances du serveur.

Processeur

La vitesse du processeur est un facteur important pour déterminer la capacité globale du processeur de votre serveur. Elle est déterminée par le nombre d'opérations exécutées dans une période mesurée. Les serveurs équipés de plusieurs processeurs ou de processeurs à plusieurs cœurs, exécutent généralement les tâches qui sollicitent beaucoup le processeur avec une plus grande efficacité, et sont souvent plus rapides que les ordinateurs équipés d'un processeur unique ou de processeurs à cœur unique.

L'architecture du processeur est également importante. Les processeurs 64 bits peuvent accéder à davantage de mémoire et ont un impact significatif sur les performances. Cependant, il est important de noter que Windows Server 2012 et Windows Server 2008 R2 sont disponibles en versions 64 bits uniquement.

Disque

Les disques durs stockent les programmes et les données. Par conséquent, le débit des disques affecte la vitesse de la station de travail ou du serveur, en particulier quand la station de travail ou le serveur exécute des tâches qui sollicitent beaucoup les disques. La plupart des disques durs ont des composants mobiles, et le placement des têtes de lecture et d'écriture sur la partie appropriée du disque pour récupérer les informations demandées peut prendre du temps.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

En sélectionnant des disques plus rapides et en utilisant des collections de disques pour optimiser les temps d'accès, vous pouvez limiter le risque que le sous-système de disque crée un goulot d'étranglement au niveau des performances.

Vous devez également garder à l'esprit que les informations sur le disque sont déplacées dans la mémoire avant qu'elles soient utilisées. S'il y a un excédent de mémoire, le système d'exploitation Windows Server crée un cache de fichier pour les éléments récemment écrits ou lus à partir des disques. L'installation d'une mémoire supplémentaire dans un serveur peut souvent améliorer les performances du sous-système de disque, car l'accès au cache est plus rapide que le déplacement des informations dans la mémoire.

Mémoire

Les programmes et les données sont chargés à partir du disque dans la mémoire avant que le programme manipule les données. Dans les serveurs qui exécutent plusieurs programmes ou lorsque les ensembles de données sont très volumineux, l'augmentation de la quantité de mémoire installée peut aider à améliorer les performances du serveur.

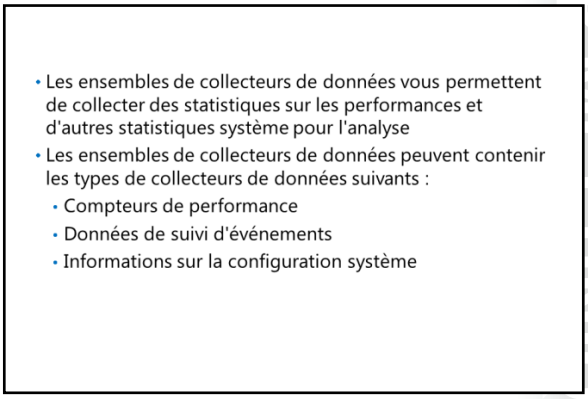
Windows Server utilise un modèle de mémoire dans lequel les demandes de mémoire excessives ne sont pas refusées, mais traitées par un processus appelé pagination. Pendant la pagination, les données et les programmes en mémoire qui ne sont pas en cours d'utilisation par les processus sont déplacés dans une zone du disque dur, appelée *fichier de pagination*. Cela libère de la mémoire physique pour répondre aux demandes excessives, mais comme un disque dur est comparativement lent, il a un impact négatif sur les performances de la station de travail. En ajoutant de la mémoire et en utilisant une architecture de processeur 64 bits qui prend en charge une mémoire de plus grande taille, vous pouvez réduire la nécessité d'une pagination.

Réseau

Il est facile de sous-estimer l'impact d'un réseau aux performances médiocres, car il n'est pas aussi facile à déterminer ou à mesurer que les trois autres composants de la station de travail. Cependant, le réseau est un composant crucial pour l'analyse des performances, car les périphériques réseau stockent un grand nombre de programmes, de données de traitement et d'applications.

Que sont les ensembles de collecteurs de données ?

Un ensemble de collecteurs de données est la base de l'analyse et de la création de rapports sur les performances de Windows Server dans l'Analyseur de performances.



Vous pouvez utiliser des ensembles de collecteurs de données pour collecter des informations sur les performances et d'autres statistiques système, sur lesquelles vous pouvez effectuer une analyse avec d'autres outils de l'Analyseur de performances ou des outils tiers.

Bien qu'il soit utile d'analyser l'activité actuelle des performances d'un serveur, il peut s'avérer plus utile de collecter des données de performances sur une période définie, puis de les analyser et de les comparer aux données que vous avez collectées précédemment. Vous pouvez utiliser cette comparaison de données pour déterminer l'utilisation des ressources en vue de planifier leur augmentation et d'identifier des problèmes de performances potentiels.

Les ensembles de collecteurs de données peuvent contenir les types de collecteurs de données suivants :

- *Compteurs de performance*. Ce collecteur de données fournit les données de performances du serveur.
- *Données de suivi d'événements*. Ce collecteur de données fournit des informations sur les activités et les événements du système, qui sont souvent utiles pour la résolution des problèmes.
- *Informations sur la configuration système*. Ce collecteur de données vous permet d'enregistrer l'état actuel des clés de Registre, ainsi que les modifications apportées à ces clés.

Vous pouvez créer un ensemble de collecteurs de données à partir d'un modèle, d'un ensemble de collecteurs de données existant dans un affichage Analyseur de performances ou en sélectionnant des collecteurs de données individuels et en définissant chaque option dans les propriétés de l'ensemble de collecteurs de données.

Démonstration : Capture de données de compteur avec un ensemble de collecteurs de données

Cette démonstration montre comment :

- créer un ensemble de collecteurs de données ;
- créer une charge sur le serveur ;
- analyser les données obtenues dans un rapport.

Procédure de démonstration

Créer un ensemble de collecteurs de données

1. Basculez vers LON-SVR1, puis connectez-vous avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Ouvrez l'**Analyseur de performances**.
3. Créez un ensemble de collecteurs de données **Défini par l'utilisateur** avec les compteurs clés suivants :
    - Processeur > % Temps processeur
    - Mémoire > Pages/s
    - Disque physique > Pourcentage du temps disque
    - Disque physique > Longueur moyenne de file d'attente du disque
    - Système > Longueur de la file du processeur
    - Interface réseau > Total des octets/s
4. Démarrez l'ensemble de collecteurs de données.

Créer une charge de disque sur le serveur

1. Ouvrez une invite de commandes, puis utilisez la commande **fsutil** pour créer un fichier volumineux.
2. Copiez le fichier sur le serveur LON-DC1 pour générer la charge du réseau.
3. Créez une copie du fichier volumineux sur le disque dur local en le copiant à partir de LON-DC1.
4. Supprimez tous les nouveaux fichiers créés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Analyser les données obtenues dans un rapport

1. Basculez vers l'Analyseur de performances, puis arrêtez l'ensemble de collecteurs de données.
2. Sélectionnez l'outil Analyseur de performances,, puis sélectionnez **Affiche les données du journal**.
3. Ajoutez les données que vous avez collectées dans l'ensemble de collecteurs de données au graphique.
4. Basculez vers la vue **Rapport**.

Démonstration : Configuration d'une alerte

Les compteurs d'alerte vous permettent de créer un ensemble de collecteurs de données personnalisé qui contient les compteurs de performance pour lesquels vous pouvez configurer des actions qui se produisent selon que les compteurs mesurés sont supérieurs ou inférieurs aux limites que vous définissez. Une fois que vous avez créé l'ensemble de collecteurs de données, vous devez configurer les actions que le système exécutera quand les critères d'alerte seront remplis.

Les compteurs d'alerte sont utiles dans les situations où un problème de performances apparaît périodiquement, et vous pouvez utiliser les actions pour exécuter des programmes, générer des événements ou une combinaison de ces éléments.

Cette démonstration montre comment :

- créer un ensemble de collecteurs de données avec un compteur d'alerte ;
- générer une charge de serveur qui dépasse le seuil configuré ;
- examiner le journal d'événements pour l'événement obtenu.

Procédure de démonstration

Créer un ensemble de collecteurs de données avec un compteur d'alerte

1. Créez un ensemble de collecteurs de données **Défini par l'utilisateur**.
2. Utilisez l'option **Alerte de compteur de performance**, puis ajoutez uniquement le compteur **Processeur > % Temps processeur**.
3. Définissez le seuil de telle sorte qu'il soit supérieur à **10** pour cent et qu'il génère une entrée dans le journal d'événements lorsque cette condition est remplie.
4. Démarrez l'ensemble de collecteurs de données.

Générer une charge de serveur qui dépasse le seuil configuré

1. Ouvrez une invite de commandes, puis exécutez un outil pour générer une charge sur le serveur.
2. Quand l'outil a été exécuté pendant une minute, arrêtez-le.

Examiner le journal d'événements pour l'événement obtenu

- Ouvrez l'Observateur d'événements et examinez le journal **Diagnosis-PLA** pour les alertes de performances.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Affichage de rapports dans l'Analyseur de performances

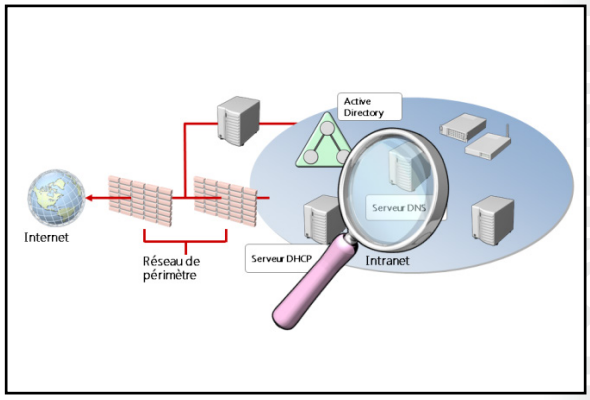
Cette démonstration explique comment afficher un rapport de performances.

Procédure de démonstration

Afficher un rapport de performances

1. Dans le volet de navigation, développez **Rapports/Définis par l'utilisateur/Performances de LON-SVR1**.
2. Développez le dossier sous **Performances de LON-SVR1**. Le précédent processus de collecte de l'ensemble de collecteurs de données a généré ce rapport. Vous pouvez passer de l'affichage Graphique à un autre affichage pris en charge.
3. Fermez toutes les fenêtres.

Surveillance des services d'infrastructure réseau



Puisque les services d'infrastructure réseau constituent une base essentielle de beaucoup d'autres services basés sur un serveur, il est important qu'ils soient configurés correctement et s'exécutent de façon optimale.

Votre organisation peut tirer parti de plusieurs façons de la collecte de données liées aux performances sur vos services d'infrastructure réseau, notamment :

- Elle aide à optimiser les performances du serveur d'infrastructure réseau. En fournissant des bases de performances et des données de tendance, vous pouvez aider votre organisation à optimiser les performances du serveur d'infrastructure réseau.
- Elle permet de résoudre les problèmes de serveurs. Là où les performances du serveur ont décru, au fil du temps ou au cours des pointes d'activité, vous pouvez aider à identifier des causes possibles et prendre les mesures nécessaires. Ainsi, il est possible de rétablir le service dans les limites de votre contrat de niveau de service (SLA).
- Elle vous permet d'utiliser l'Analyseur de performances pour collecter et analyser les données appropriées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Analyse du service DNS

Le système DNS (Domain Name System) fournit des services de résolution de noms sur votre réseau. Vous pouvez surveiller le rôle serveur DNS de Windows Server 2012 pour déterminer les aspects suivants de votre infrastructure DNS :

- des statistiques générales sur le serveur DNS, y compris le total des requêtes et des réponses qui sont traitées par le serveur DNS ;
- les compteurs des protocoles UDP (User Datagram Protocol) ou TCP (Transmission Control Protocol), pour mesurer les requêtes DNS et les réponses qui sont traitées par le serveur DNS, respectivement, à l'aide de l'un ou l'autre de ces protocoles de transport ;
- les compteurs de mise à jour dynamiques et sécurisés, pour mesurer les activités d'inscription et de mise à jour qui sont générées par les clients dynamiques ;
- le compteur d'utilisation de la mémoire, pour mesurer les modèles d'utilisation et d'allocation de mémoire du système qui sont créés en faisant fonctionner le serveur en tant que serveur DNS ;
- les compteurs de recherche récursive, pour mesurer des requêtes et des réponses quand le service Serveur DNS utilise la récursivité pour rechercher et résoudre entièrement des noms DNS à la demande des clients ;
- les compteurs de transfert de zone, y compris les compteurs spécifiques pour mesurer ce qui suit : tout transfert de zone (AXFR), transfert incrémentiel de zone (IXFR) et toute activité de notification de mise à jour.

Analyse du service DHCP

Le service de protocole DHCP (Dynamic Host Configuration Protocol) fournit des services dynamiques de configuration IP sur votre réseau. Vous pouvez surveiller le rôle serveur DHCP de Windows Server 2012 pour déterminer les aspects suivants de votre serveur DHCP :

- La longueur moyenne de file d'attente indique la longueur actuelle de la file d'attente interne des messages du serveur DHCP. Cette valeur représente le nombre de messages non traités que reçoit le serveur. Une valeur élevée pourrait indiquer un trafic serveur élevé.
- Le compteur de millisecondes par paquet (moy.) indique le temps moyen en millisecondes nécessaire au serveur DHCP pour traiter chaque paquet qu'il reçoit. Cette valeur varie en fonction du serveur et de son sous-système d'E/S. La présence d'un pic pourrait indiquer un problème, soit avec le sous-système d'E/S devenant plus lent, soit en raison d'une surcharge de traitement intrinsèque sur le serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en considération pour la surveillance d'ordinateurs virtuels

La virtualisation de serveur est un élément du système d'exploitation Windows Server depuis la version de Windows Server 2008 et l'introduction du rôle Hyper-V. De nombreuses organisations ont migré une partie ou l'ensemble de leurs charges de travail de serveur sur des ordinateurs virtuels qui s'exécutent sur la plateforme Hyper-V. D'un point de vue de la surveillance, il est important de garder à l'esprit que les serveurs qui s'exécutent en tant qu'ordinateurs virtuels invités utilisent des ressources de la même manière que les serveurs hôtes physiques.

Éléments à prendre en considération pour la surveillance d'ordinateurs virtuels :

- Les ordinateurs virtuels doivent disposer de ressources suffisantes pour leur charge de travail
- Si plusieurs ordinateurs virtuels s'exécutent sur un hôte, vérifiez que l'hôte dispose de ressources suffisantes
- Les ressources sont partagées, par conséquent, les performances d'un ordinateur virtuel peuvent affecter celles des autres ordinateurs virtuels
- N'oubliez pas de surveiller l'utilisation des ressources sur l'hôte et les invités

La virtualisation de serveur Hyper-V vous permet de créer des ordinateurs virtuels distincts et de les exécuter simultanément en utilisant les ressources du système d'exploitation d'un serveur unique. Ces ordinateurs virtuels sont appelés *invités*, alors que l'ordinateur exécutant Hyper-V est l'*hôte*.

Les ordinateurs virtuels invités fonctionnent comme des ordinateurs normaux. Les ordinateurs virtuels invités qui sont hébergés sur le même hyperviseur restent indépendants les uns des autres. Vous pouvez exécuter plusieurs ordinateurs virtuels qui utilisent différents systèmes d'exploitation sur un serveur hôte de manière simultanée, à condition que le serveur hôte dispose de suffisamment de ressources.

Quand vous créez un ordinateur virtuel, vous configurez les caractéristiques qui définissent les ressources disponibles pour cet invité. Ces ressources comprennent la mémoire, les processeurs, la configuration du disque et la technologie de stockage et la configuration de la carte réseau. Ces ordinateurs virtuels fonctionnent dans les limites des ressources que vous leur allouez, et peuvent rencontrer les mêmes goulots d'étranglement des performances que les serveurs hôtes. Par conséquent, il est important que vous surveilliez les ordinateurs virtuels de la même manière, et avec les mêmes outils, que vous surveilliez vos serveurs hôtes.

Remarque : Outre la surveillance des ordinateurs virtuels invités, gardez toujours à l'esprit que vous devez surveiller l'hôte qui les exécute.

Microsoft fournit un outil, Contrôle des ressources Hyper-V, qui vous permet de surveiller l'utilisation de ressources sur vos ordinateurs virtuels.

Le contrôle des ressources vous permet de suivre l'utilisation des ressources des ordinateurs virtuels hébergés sur des ordinateurs Windows Server 2012 où le rôle Hyper-V est installé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Grâce au contrôle des ressources, vous pouvez mesurer les paramètres suivants sur des ordinateurs virtuels Hyper-V individuels :

- utilisation GPU (Graphics Processing Unit) moyenne ;
- utilisation moyenne de la mémoire physique, notamment :
  - utilisation mémoire minimum ;
  - utilisation mémoire maximum.
- allocation d'espace disque maximum ;
- trafic réseau entrant pour une carte réseau ;
- trafic réseau sortant pour une carte réseau.

En mesurant la quantité de ressources utilisée par chaque ordinateur virtuel, une organisation peut facturer des services ou des clients en fonction de l'utilisation de leurs ordinateurs virtuels hébergés, au lieu d'appliquer un forfait fixe par ordinateur virtuel. Une organisation comportant uniquement des clients internes peut également utiliser ces mesures pour dégager des modèles d'utilisation et prévoir de futures extensions.

Vous effectuez des tâches de contrôle des ressources à l'aide des applets de commande Windows PowerShell® du module Hyper-V Windows PowerShell. Il n'existe pas d'outil d'interface graphique utilisateur qui vous permet d'effectuer cette tâche. Vous pouvez utiliser les applets de commande suivants pour effectuer des tâches de contrôle des ressources :

- **Enable-VMResourceMetering**. Démarre la collecte de données sur chaque ordinateur virtuel.
- **Disable-VMResourceMetering**. Désactive le contrôle des ressources sur chaque ordinateur virtuel.
- **Reset-VMResourceMetering**. Réinitialise les compteurs de contrôle des ressources sur les ordinateurs virtuels.
- **Measure-VM**. Affiche des statistiques de contrôle des ressources pour un ordinateur virtuel spécifique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Analyse des journaux d'événements

L'Observateur d'événements fournit un emplacement pratique et accessible pour vous permettre d'afficher les événements qui se produisent et que Windows Server enregistre dans un de plusieurs fichiers journaux selon le type d'événement qui se produit. Pour aider vos utilisateurs, vous devez savoir comment accéder rapidement et facilement aux informations sur les événements, et comment interpréter les données du journal des événements.

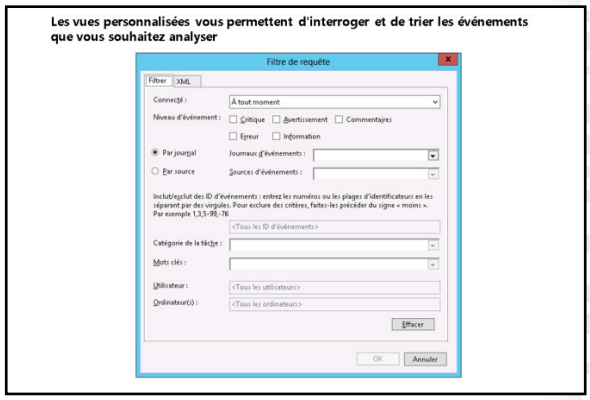
Objectifs de la leçon

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

- décrire une vue personnalisée ;
- expliquer comment créer une vue personnalisée ;
- décrire les abonnements aux événements ;
- expliquer comment configurer un abonnement aux événements.

Qu'est-ce qu'une vue personnalisée ?

Les journaux d'événements contiennent des quantités importantes de données, et il peut être difficile de limiter l'ensemble des événements aux événements qui vous intéressent. Dans les versions antérieures de Windows, vous pouviez appliquer des filtres aux journaux, mais vous ne pouviez pas enregistrer ces filtres. Dans Windows Server 2008 et Windows Server 2012, les vues personnalisées vous permettent d'interroger et de trier uniquement les événements que vous souhaitez analyser. Vous pouvez également enregistrer, exporter, importer et partager ces vues personnalisées.



L'Observateur d'événements vous permet de filtrer des événements spécifiques dans plusieurs journaux, et d'afficher tous les événements qui peuvent être liés au problème que vous examinez. Pour spécifier un filtre qui couvre plusieurs journaux, vous devez créer une vue personnalisée.

Créez des vues personnalisées dans le volet Actions de l'Observateur d'événements. Vous pouvez filtrer les vues personnalisées en fonction de plusieurs critères, notamment :

- heure d'enregistrement de l'événement ;
- niveau d'événement à afficher, tel que des erreurs ou des avertissements ;
- journaux à partir desquels inclure les événements ;
- identificateurs d'événement spécifiques à inclure ou exclure ;
- contexte utilisateur de l'événement ;
- ordinateur sur lequel l'événement s'est produit.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Création d'une vue personnalisée

Cette démonstration montre comment :

- afficher les vues personnalisées de rôles serveur ;
- créer une vue personnalisée.

Procédure de démonstration

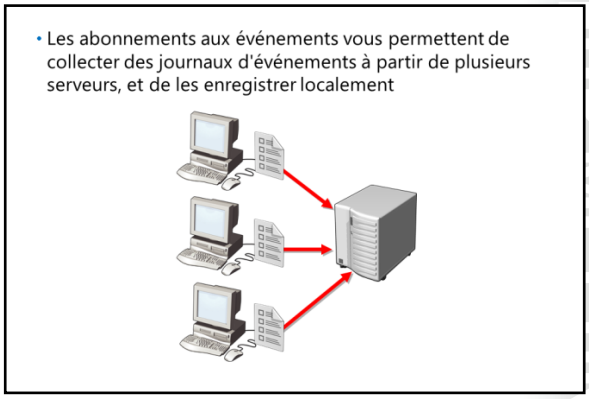
Afficher les vues personnalisées de rôles serveur

- Dans l'Observateur d'événements, examinez les vues personnalisées **Rôles du serveur** prédéfinies.

Créer une vue personnalisée

1. Créez une vue personnalisée pour sélectionner les types d'événement suivants :
   - **Critique**
   - **Avertissement**
   - **Erreur**
2. Sélectionnez les journaux suivants :
   - **Système**
   - **Application**
3. Nommez la vue personnalisée en tant que **Vue personnalisée Adatum.**
4. Affichez les événements filtrés obtenus dans le volet d'informations.

Qu'est-ce qu'un abonnement aux événements ?



L'Observateur d'événements vous permet de consulter des événements sur un ordinateur distant unique. Cependant, vous devez parfois examiner un ensemble d'événements stockés dans plusieurs journaux répartis sur plusieurs ordinateurs pour pouvoir résoudre un problème. À cet effet, l'Observateur d'événements offre la possibilité de collecter des copies d'événements à partir de plusieurs ordinateurs distants et de les stocker localement. Pour spécifier les événements à collecter, créez un abonnement aux événements. Une fois l'abonnement activé et les événements collectés, il est possible de consulter et de manipuler ces événements transférés comme tout autre événement stocké localement.

Pour utiliser la fonctionnalité de collecte d'événements, vous devez configurer les ordinateurs de transfert et de collecte. La fonctionnalité de collecte d'événements repose sur les services Gestion à distance de Windows (WinRM) et Collecteur d'événements Windows (Wecsvc). Ces deux services doivent être exécutés sur les ordinateurs qui participent au transfert et à la collecte des événements.

Activation d'abonnements

Pour activer les abonnements, effectuez les tâches suivantes :

1. Sur chaque ordinateur source, exécutez la commande suivante à l'invite de commandes avec élévation de privilèges pour activer WinRM :

```
winrm quickconfig
```

2. Sur l'ordinateur de collecte, tapez la commande suivante à l'invite de commandes avec élévation de privilèges pour activer Wecsvc :

```
wecutil qc
```

3. Ajoutez le compte d'ordinateur de l'ordinateur de collecte au groupe local Administrateurs sur chaque ordinateur source.

Démonstration : Configuration d'un abonnement aux événements

Cette démonstration montre comment :

- configurer l'ordinateur source ;
- configurer l'ordinateur collecteur ;
- créer et afficher le journal abonné.

Procédure de démonstration

Configurer l'ordinateur source

1. Basculez vers LON-DC1 et, si nécessaire, connectez-vous avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Exécutez la commande **winrm quickconfig** à l'invite de commandes.



Remarque : le service est déjà en cours d'exécution.

3. Ouvrez **Utilisateurs et ordinateurs Active Directory** et ajoutez l'ordinateur **LON-SVR1** en tant que membre du groupe local de domaine **Administrateurs**.

Configurer l'ordinateur collecteur

1. Basculez vers LON-SVR1, puis ouvrez une invite de commandes.
2. Exécutez la commande **wecutil qc**.

Créer et afficher le journal abonné

1. Basculez vers l'Observateur d'événements.
2. Créez un abonnement pour collecter des événements à partir de LON-DC1 :.
   - initialisation par le collecteur ;
   - ordinateur source LON-DC1 ;
   - tous les types d'événements ;
   - les 30 derniers jours.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Surveillance de Windows Server 2012

Scénario

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social de Londres et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012.

Comme l'entreprise a déployé de nouveaux serveurs, il est important d'établir une base de référence des performances avec une charge normale pour ces nouveaux serveurs. Vous êtes chargé de travailler sur ce projet. En outre, pour faciliter le processus de surveillance et de résolution de problèmes, vous décidez d'effectuer une surveillance centralisée des journaux des événements.

Objectifs

À la fin de cet atelier pratique, vous serez à même d'effectuer les tâches suivantes :

- établir une base de référence des performances ;
- identifier la source des problèmes de performances ;
- afficher et configurer des journaux d'événements centralisés.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-SVR1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez procéder aux étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Accueil**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22411B-LON-DC1** et, dans le volet Actions, cliquez sur **Accueil**.
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 **22411B-LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Mise en place d'une base de référence des performances

Scénario

Dans cet exercice, vous utiliserez l'Analyseur de performances sur le serveur et créerez une base de référence à l'aide de compteurs de performance classiques.

Les tâches principales de cet exercice sont les suivantes :

1. Créer et démarrer un ensemble de collecteurs de données
2. Créer une charge de travail classique sur le serveur
3. Analyser les données collectées

▶ Tâche 1 : Créer et démarrer un ensemble de collecteurs de données

1. Basculez vers l'ordinateur LON-SVR1.
2. Ouvrez l'**Analyseur de performances**.
3. Créez un ensemble de collecteurs de données **Défini par l'utilisateur** en utilisant les informations suivantes pour terminer le processus :
   - Nom : **Performances de LON-SVR1**
   - Créer : **Créer manuellement (avancé)**
   - Types de données : **Compteur de performance**
   - Sélectionnez les compteurs suivants :
     - Mémoire, Pages/s
     - Interface réseau, Total des octets/s
     - Disque physique, Pourcentage du temps disque
     - Disque physique, Longueur moyenne de file d'attente du disque
     - Processeur, % Temps processeur
     - Système, Longueur de la file du processeur
   - Intervalle d'échantillonnage : **1** seconde
   - Emplacement de stockage des données : valeur par défaut
4. Enregistrez et fermez l'ensemble de collecteurs de données.
5. Dans l'Analyseur de performances, dans le volet de résultats, cliquez avec le bouton droit sur **Performances de LON-SVR1**, puis cliquez sur **Accueil**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer une charge de travail classique sur le serveur

1. Ouvrez une invite de commandes, puis exécutez les commandes ci-dessous en appuyant sur Entrée après chaque commande :

```
Fsutil file createnew bigfile 104857600
Copy bigfile \\LON-dc1\c$
Copy \\LON-dc1\c$\bigfile bigfile2
Del bigfile*.*
Del \\LON-dc1\c$\bigfile*.*
```

2. Ne fermez pas la fenêtre d'invite de commandes.

▶ Tâche 3 : Analyser les données collectées

1. Basculez vers l'Analyseur de performances.
2. Arrêtez l'ensemble de collecteurs de données **Performances de LON-SVR1**.
3. Basculez vers le nœud **Analyseur de performances**.
4. Affichez les données enregistrées, puis ajoutez les compteurs suivants :
   - Mémoire, Pages/s
   - Interface réseau, Total des octets/s
   - Disque physique, Pourcentage du temps disque
   - Disque physique, Longueur moyenne de file d'attente du disque
   - Processeur, % Temps processeur
   - Système, Longueur de la file du processeur
5. Dans la barre d'outils, cliquez sur la flèche vers le bas, puis sur **Rapport**.
6. Enregistrez les valeurs répertoriées dans le rapport pour une analyse ultérieure. Les valeurs enregistrées comprennent :
   - Mémoire, Pages/s
   - Interface réseau, Total des octets/s
   - Disque physique, Pourcentage du temps disque
   - Disque physique, Longueur moyenne de file d'attente du disque
   - Processeur, % Temps processeur
   - Système, Longueur de la file du processeur

Résultats : À la fin de cet exercice, vous devez avoir établi une base de référence pour la comparaison des performances.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Identification de la source des problèmes de performance

Scénario

Dans cet exercice, vous simulerez une charge pour représenter le système dans des conditions d'utilisation réelles, collecterez les données de performances avec votre ensemble de collecteurs de données et déterminerez la cause potentielle du problème de performances.

Les tâches principales de cet exercice sont les suivantes :

1. Créer une charge de travail supplémentaire sur le serveur
2. Capturer les données de performances avec un ensemble de collecteurs de données
3. Supprimer la charge de travail et examiner les données de performances

▶ Tâche 1 : Créer une charge de travail supplémentaire sur le serveur

1. Sur LON-SVR1, basculez vers l'invite de commandes.
2. Accédez au dossier **C:\FichiersAtelier**.
3. Sur LON-SVR1, exécutez **StressTool.exe 95**.

▶ Tâche 2 : Capturer les données de performances avec un ensemble de collecteurs de données

1. Basculez vers l'Analyseur de performances.
2. Dans l'Analyseur de performances, cliquez sur **Définis par l'utilisateur**, et dans le volet de résultats, cliquez avec le bouton droit sur **Performances de LON-SVR1**.
3. Patientez une minute pour permettre la capture des données.

▶ Tâche 3 : Supprimer la charge de travail et examiner les données de performances

1. À l'invite de commandes, appuyez sur Ctrl+C. Laissez l'invite de commandes en cours d'exécution.
2. Basculez vers l'**Analyseur de performances**.
3. Arrêtez l'ensemble de collecteurs de données.
4. Dans l'Analyseur de performances, dans le volet de navigation, cliquez sur **Analyseur de performances**.
5. Dans la barre d'outils, cliquez sur **Affiche les données du journal**.
6. Dans la boîte de dialogue **Propriétés de : Analyseur de performances**, sous l'onglet **Source**, cliquez sur **Fichiers journaux**, puis sur **Supprimer**.
7. Cliquez sur **Ajouter**.
8. Dans la boîte de dialogue **Sélectionner le fichier journal**, cliquez sur **Dossier parent**.
9. Double-cliquez sur le dossier **LON-SVR1_date-000002**, puis sur **DataCollector01.blg**.
10. Cliquez sur l'onglet **Données**, puis sur **OK**.

 **Remarque :** Si vous recevez un message d'erreur à ce stade ou si les valeurs de votre rapport sont nulles, répétez les étapes 4 à 9.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Valeurs enregistrées :
    - Mémoire, Pages/s
    - Interface réseau, Total des octets/s
    - Disque physique, Pourcentage du temps disque
    - Disque physique, Longueur moyenne de file d'attente du disque
    - Processeur, % Temps processeur
    - Système, Longueur de la file du processeur

    Question : Par rapport à votre précédent rapport, quelles valeurs ont changé ?

    Question : Quelle solution conseillez-vous ?

Résultats : À la fin de cet exercice, vous devez avoir utilisé les outils de performances pour identifier un goulot d'étranglement potentiel au niveau des performances.

Exercice 3 : Affichage et configuration des journaux d'événements centralisés

Scénario

Dans cet exercice, vous utiliserez LON-DC1 pour collecter des journaux d'événements à partir de LON-SVR1. Plus précisément, vous utiliserez ce processus pour collecter les alertes liées aux performances à partir de vos serveurs réseau.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les éléments préalables aux abonnements
2. Créer un abonnement
3. Configurer une alerte de compteur de performance
4. Ajouter une charge de travail supplémentaire sur le serveur
5. Vérifier les résultats
6. Pour préparer le module suivant

▶ Tâche 1 : Configurer les éléments préalables aux abonnements

1. Basculez vers LON-SVR1.
2. À l'invite de commandes, exécutez **winrm quickconfig** pour activer les modifications d'administration qui sont requises sur un ordinateur source.
3. Ajoutez l'ordinateur **LON-DC1** au groupe **Administrateurs** local.
4. Basculez vers LON-DC1.
5. À l'invite de commandes, exécutez la commande **wecutil qc** pour activer les modifications d'administration qui sont requises sur un ordinateur collecteur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer un abonnement

1. Ouvrez l'**Observateur d'événements**.
2. Créez un nouvel abonnement disposant des propriétés suivantes :
   - Ordinateurs : **LON-SVR1**
   - Nom : **Événements de LON-SVR1**
   - Initialisation par **le collecteur**
   - Événements : **Critique**, **Avertissement**, **Information**, **Commentaires** et **Erreur**
   - Connecté : **Les 7 derniers jours**
   - Journaux : **Applications et services > Microsoft > Windows > Diagnosis-PLA > Opérationnel**

▶ Tâche 3 : Configurer une alerte de compteur de performance

1. Basculez vers LON-SVR1.
2. Ouvrez l'Analyseur de performances.
3. Créez un ensemble de collecteurs de données **Définis par l'utilisateur** en utilisant les informations suivantes pour terminer le processus :
   - Nom : **Alerte de LON-SVR1**
   - Créer : **Créer manuellement (avancé)**
   - Types de données : **Alerte de compteur de performance**
   - Sélectionnez les compteurs suivants : **Processeur, % Temps processeur** supérieur à **10** %
   - Intervalle d'échantillonnage : **1** seconde
   - Emplacement de stockage des données : valeur par défaut
   - Action de l'alerte : **Ajouter une entrée dans le journal des événements des applications**
4. Démarrez l'ensemble de collecteurs de données **Alerte de LON-SVR1**.

▶ Tâche 4 : Ajouter une charge de travail supplémentaire sur le serveur

1. Revenez à l'invite de commandes.
2. Accédez à C:\FichiersAtelier, puis exécutez **StressTool.exe 95**.
3. Patientez une minute pour permettre la capture des données et, à l'invite de commandes, appuyez sur Ctrl+C, puis fermez la fenêtre d'invite de commandes.

▶ Tâche 5 : Vérifier les résultats

- Basculez vers LON-DC1, puis ouvrez **Événements transférés**.

  Question : Dans l'Analyseur de performances, le journal d'applications abonné contient-il des alertes liées aux performances ? Conseil : Leur identificateur est 2031.

Résultats : À la fin de cet exercice, vous aurez centralisé les journaux d'événements et examiné ces journaux pour les événements liés aux performances.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial de tous les ordinateurs virtuels. Pour cela, 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 **22411B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22411B-LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quels compteurs importants devez-vous analyser dans l'Analyseur de performances ?

Question : Pourquoi est-il important d'analyser régulièrement les performances du serveur ?

Question : Pourquoi devez-vous utiliser des alertes de performances ?

Outils

Outil	Utilisation	Emplacement
Fsutil.exe	Configuration et gestion du système de fichiers	Ligne de commande
Analyseur de performances	Surveillance et analyse des données de performances en temps réel et enregistrées	Menu Accueil
Logman.exe	Gestion et planification des collections de compteurs de performance et de journaux de suivi d'événements	Ligne de commande
Moniteur de ressources	Analyse en temps réel de l'utilisation et des performances du processeur, du disque, du réseau et de la mémoire	Menu Accueil
Observateur d'événements	Affichage et gestion des journaux d'événements	Menu Accueil
Gestionnaire des tâches	Identification et résolution des problèmes liés aux performances	Menu Accueil

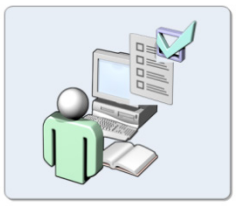
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

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

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 1: Déploiement et maintenance des images de serveur

Atelier pratique : Utilisation des services de déploiement Windows pour déployer Windows Server 2012

Exercice 1 : Installation et configuration des services de déploiement Windows

▶ Tâche 1 : Lisez la documentation fournie avec le produit.

- Lisez la documentation fournie dans le scénario d'exercice pour connaître les détails du déploiement.

▶ Tâche 2 : Installez le rôle des services de déploiement Windows

1. Basculez vers l'ordinateur **LON-SVR1**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, 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. Sur la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services de déploiement Windows**.
7. Dans la fenêtre Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Ajouter des fonctionnalités**.
8. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
9. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
10. Sur la page **WDS**, vérifiez les informations affichées puis cliquez sur **Suivant**.
11. Sur la page **Sélectionner des services de rôle**, cliquez sur **Suivant**.
12. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
13. Sur la page **Progression de l'installation**, cliquez sur **Fermer**.

▶ Tâche 3 : Configurer les services de déploiement Windows

1. Dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Services de déploiement Windows**.
2. Dans la console Services de déploiement Windows, développez **Serveurs**.
3. Cliquez avec le bouton droit sur **LON-SVR1.Adatum.com**, puis cliquez sur **Configurer le serveur**. Cliquez sur **Suivant**.
4. Sur la page **Options d'installation**, cliquez sur **Suivant**.
5. Sur la page **Emplacement du dossier d'installation à distance**, cliquez sur **Suivant**.
6. Dans la boîte de dialogue **Avertissement du volume système**, cliquez sur **Oui**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Sur la page **Paramètres initiaux du serveur PXE**, cliquez sur **Répondre à tous les ordinateurs clients (connus et inconnus)**, puis sur **Suivant**.
8. Sur la page **Opération terminée**, désactivez la case à cocher **Ajouter les images au serveur maintenant**, puis cliquez sur **Terminer**.

Résultats : Après avoir terminé cet exercice, vous aurez installé et configuré les services de déploiement Windows.

Exercice 2 : Création d'images du système d'exploitation avec les services de déploiement Windows

▶ Tâche 1 : Insérer le support d'installation de Windows Server 2012 dans LON-SVR1

1. Sur l'ordinateur hôte, ouvrez le Gestionnaire Hyper-V.
2. Dans le gestionnaire Hyper-V, faites un clic droit sur l'ordinateur virtuel **22411B-LON-SVR1**, puis cliquez sur **Paramètres**.
3. Dans la fenêtre Paramètres, sous **Controlêur IDE 1**, cliquez sur **Lecteur de DVD**.
4. Dans la fenêtre Paramètres, sous **Support**, sélectionnez **Fichier image**, puis cliquez sur **Parcourir**.
5. Dans la fenêtre Ouvrir, double-cliquez sur **Disque local (C:)**, double-cliquez sur **Programmes**, double-cliquez sur **Microsoft Learning**, double-cliquez sur **22411**, double-cliquez sur **Drives** puis double-cliquez sur **WIndows2012_RTM_FR.iso**.
6. Cliquez sur **OK** pour fermer la fenêtre des paramètres pour 22411B-LON-SVR1.

▶ Tâche 2 : Ajouter une image de démarrage

1. Basculez vers LON-SVR1.
2. Dans l'arborescence de la console **Services de déploiement Windows**, développez **LON-SVR1.Adatum.com**.
3. Cliquez avec le bouton droit sur **Images de démarrage**, puis cliquez sur **Ajouter une image de démarrage**.
4. Dans l'Assistant Ajout d'images, sur la page **Fichier image**, cliquez sur **Parcourir**.
5. Dans la boîte de dialogue **Sélectionner un fichier image Windows**, dans le volet de navigation, cliquez sur **Ordinateur**, double-cliquez sur **Lecteur de DVD (D:)**, double-cliquez sur **sources**, puis double-cliquez sur **boot.wim**.
6. Sur la page **Fichier image**, cliquez sur **Suivant**.
7. Sur la page **Métadonnées d'image**, cliquez sur **Suivant**.
8. Sur la page **Résumé**, cliquez sur **Suivant**.
9. Sur la page **Progression de la tâche**, cliquez sur **Terminer**.

▶ Tâche 3 : Ajouter une image d'installation

1. Dans la console Services de déploiement Windows, cliquez avec le bouton droit sur **Images d'installation**, puis cliquez sur **Ajouter un groupe d'images**.
2. Dans la boîte de dialogue **Ajouter un groupe d'images,** dans le champ **Entrez un nom pour le groupe d'images**, saisissez **Windows Server 2012**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la console Services de déploiement Windows, cliquez avec le bouton droit sur **Windows Server 2012**, puis cliquez sur **Ajouter une image d'installation**.
4. Dans l'Assistant Ajout d'images, sur la page **Fichier image**, cliquez sur **Parcourir**.
5. Dans la zone de texte **Nom du fichier**, saisissez **D:\sources\install.wim**, puis cliquez sur **Ouvrir**.
6. Sur la page **Fichier image**, cliquez sur **Suivant**.
7. Sur la page **Images disponibles**, désactivez toutes les cases à cocher excepté **Windows Server 2012 SERVERSTANDARDCORE**, puis cliquez sur **Suivant**.
8. Sur la page **Résumé**, cliquez sur **Suivant**.
9. Sur la page **Progression de la tâche**, cliquez sur **Terminer**.
10. Réduisez la fenêtre Services de déploiement Windows.

Résultats : Après avoir terminé cet exercice, vous allez créer une image du système d'exploitation avec les services de déploiement Windows.

Exercice 3 : Configuration d'un format de nom personnalisé des ordinateurs

▶ Tâche 1 : Configurer l'attribution automatique de noms

1. Dans l'arborescence de la console Services de déploiement Windows, cliquez avec le bouton droit sur **LON-SVR1.Adatum.com**, puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **AD DS**.
3. Dans la zone de texte **Format**, saisissez **BRANCH-SVR-%02#**.
4. Sous **Emplacement du compte d'ordinateur**, cliquez sur **L'emplacement suivant**, puis sur **Parcourir**.
5. Dans la boîte de dialogue **Rechercher un dossier Active Directory**, développez **Adatum**, cliquez sur **Research**, puis cliquez sur **OK**.
6. Dans la boîte de dialogue **Propriétés de : LON-SVR1**, cliquez sur **OK**.

▶ Tâche 2 : Configurer l'approbation d'administrateur

1. Dans l'arborescence de la console Services de déploiement Windows, cliquez avec le bouton droit sur **LON-SVR1.Adatum.com**, puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **Réponse PXE**.
3. Activez la case à cocher **Exiger l'approbation administrateur pour les ordinateurs inconnus**. Modifiez le **Délai de réponse PXE** sur **3 secondes**, puis cliquez sur **OK**.
4. Dans la barre des tâches, cliquez sur le raccourci **Windows PowerShell®**.
5. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
WDSUTIL /Set-Server /AutoAddPolicy /Message: "L'administrateur d'Adatum autorise
cette demande. Veuillez patienter."
```

6. Fermez la fenêtre d'invite de commandes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer les autorisations des services de domaine Active Directory (AD DS)

1. Basculez vers l'ordinateur LON-DC1.
2. Dans Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
3. Dans Utilisateurs et ordinateurs Active Directory, développez **Adatum.com**, cliquez avec le bouton droit sur **Research**, puis cliquez sur **Délégation de contrôle**.
4. Dans l'Assistant Délégation de contrôle, cliquez sur **Suivant**.
5. Sur la page **Utilisateurs ou groupes**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Sélectionnez des utilisateurs**, **des ordinateurs ou des groupes**, cliquez sur **Types d'objets**.
7. Dans la boîte de dialogue **Types d'objets**, activez la case à cocher **des Ordinateurs**, puis cliquez sur **OK**.
8. Dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs ou des groupes**, dans la zone de texte **Entrez les noms des objets à sélectionner**, saisissez **LON-SVR1**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
9. Sur la page **Utilisateurs ou groupes**, cliquez sur **Suivant**.
10. Sur la page **Tâches à déléguer**, cliquez sur **Créer une tâche personnalisée à déléguer**, puis sur **Suivant**.
11. Sur la page **Type d'objet Active Directory**, cliquez sur **Seulement des objets suivants dans le dossier**, activez les cases à cocher **Objets Ordinateur** et **Créer les objets sélectionnés dans ce dossier**, puis cliquez sur **Suivant**.
12. Sur la page **Autorisations**, dans Autorisations, activez la case à cocher **Contrôle total**, puis cliquez sur **Suivant**.
13. Sur la page **Fin de l'Assistant Délégation de contrôle**, cliquez sur **Terminer**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré le format de nom personnalisé des ordinateurs.

Exercice 4 : Déploiement d'images avec les services de déploiement Windows

▶ Tâche 1 : Configurer un serveur des services de déploiement Windows pour la transmission par multidiffusion

1. Basculez vers l'ordinateur LON-SVR1.
2. Dans l'arborescence de la console Services de déploiement Windows, cliquez avec le bouton droit sur **Transmission par multidiffusion**, puis sur **Créer une transmission par multidiffusion**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans l'Assistant Création d'une transmission par multidiffusion, sur la page **Nom de la transmission**, dans le champ **Tapez un nom pour la transmission**, saisissez **Windows Server 2012 Branch Servers**, puis cliquez sur **Suivant**.
4. Sur la page **Sélection de l'image**, dans la liste **Sélectionner le groupe d'images contenant l'image,** cliquez sur **Windows Server 2012**.
5. Dans la liste **Nom**, cliquez sur **Windows Server 2012 SERVERSTANDARDCORE**, puis cliquez sur **Suivant**.
6. Sur la page **Type de multidiffusion**, vérifiez que l'option **Diffusion automatique** est sélectionnée, puis cliquez sur **Suivant**.
7. Cliquez sur **Terminer**.

▶ Tâche 2 : Configurer le client pour le démarrage PXE (Pre-Boot Execution Environment)

1. Sur l'ordinateur hôte, basculez vers le gestionnaire Hyper-V®.
2. Dans la liste Ordinateurs virtuels, faites un clic droit sur **22411B-LON-SVR3**, puis cliquez sur **Paramètres**.
3. Dans la boîte de dialogue **Paramètres pour 22411B-LON-SVR3**, cliquez sur **BIOS**.
4. Dans le volet des résultats, cliquez sur **Carte réseau héritée**.
5. Utilisez les flèches pour déplacer la **Carte réseau héritée** en haut de la liste, puis cliquez sur **OK**.
6. Dans le Gestionnaire Hyper-V, cliquez sur **22411B-LON-SVR3**, puis sur **Accueil** dans le volet Actions.
7. Dans le volet Actions, cliquez sur **Se connecter**.
8. Quand l'ordinateur redémarre, vérifiez le message du protocole DHCP (Dynamic Host Configuration Protocol) PXE. Lorsque vous y êtes invité, appuyez sur **F12** pour le démarrage réseau.

   Question : Voyez-vous le message d'approbation administrateur ?

   Réponse : Oui.
9. Basculez vers l'ordinateur LON-SVR1.
10. Dans la console Services de déploiement Windows, cliquez sur **Périphériques en attente**.
11. Cliquez avec le bouton droit sur la **demande en attente**, puis cliquez sur **Approuver**.
12. Dans la boîte de dialogue **Périphérique en attente**, cliquez sur **OK**.
13. Basculez vers l'ordinateur LON-SVR3.

    Question : Quelle est l'image par défaut ?

    Réponse : Installation de Microsoft® Windows (x64)

    Question : L'installation démarre-t-elle ?

    Réponse : Oui
14. Vous n'êtes pas obligé de continuer l'installation.

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

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Faites un clic droit sur **22411B-LON-DC1** dans la liste **Ordinateurs virtuels**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez ces étapes pour **22411B-LON-SVR3** et **22411B-LON-SVR1**.

Résultats : Après avoir terminé cet exercice, vous aurez déployé une image avec les services de déploiement Windows.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 2: Configuration et résolution des problèmes du système DNS

Atelier pratique : Configuration et résolution des problèmes du système DNS

Exercice 1 : Configuration des enregistrements de ressource DNS

▶ Tâche 1 : Ajouter l'enregistrement MX requis

1. Basculez vers LON-DC1, puis connectez-vous avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
3. Dans le Gestionnaire DNS, développez successivement **LON-DC1** et **Zones de recherche directes**, puis cliquez sur **Adatum.com**.
4. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
5. Dans la boîte de dialogue **Nouvel hôte**, dans la zone **Nom**, saisissez **Mail1**.
6. Dans la zone **Adresse IP**, saisissez **172.16.0.250**, puis cliquez sur **Ajouter un hôte**.
7. Dans la boîte de dialogue **DNS**, cliquez sur **OK**.
8. Dans la boîte de dialogue **Nouvel hôte**, cliquez sur **Terminé**.
9. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouveau serveur de messagerie (MX)**.
10. Dans la boîte de dialogue **Nouvel enregistrement de ressource**, dans la zone **Nom de domaine pleinement qualifié (FQDN) pour le serveur de messagerie**, saisissez **Mail1.Adatum.com** et cliquez sur **OK**.

▶ Tâche 2 : Ajouter les enregistrements de serveur Lync requis

1. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
2. Dans la boîte de dialogue **Nouvel hôte**, dans la zone **Nom**, saisissez **Lync-svr1**.
3. Dans la zone **Adresse IP**, saisissez **172.16.0.251**, puis cliquez sur **Ajouter un hôte**.
4. Dans la boîte de dialogue **DNS**, cliquez sur **OK**.
5. Dans la boîte de dialogue **Nouvel hôte**, cliquez sur **Terminé**.
6. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouveaux enregistrements**.
7. Dans la boîte de dialogue **Type d'enregistrement de ressource**, dans la liste **Choisissez un type d'enregistrement de ressource**, cliquez sur **Emplacement du service (SRV)**, puis sur **Créer un enregistrement**.
8. Dans la boîte de dialogue **Nouvel enregistrement de ressource**, dans la zone **Service**, saisissez **_sipinternaltls**.
9. Dans la zone **Protocole**, saisissez **_tcp**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Dans la zone **Numéro du port**, saisissez **5061**.
11. Dans la zone **Hôte offrant ce service**, saisissez **Lync-svr1.adatum.com**.
12. Cliquez sur **OK**, puis sur **Terminé**.

▶ Tâche 3 : Créer la zone de recherche inversée

1. Dans le Gestionnaire DNS, dans le volet de navigation, cliquez sur **Zones de recherche inversée**.
2. Cliquez avec le bouton droit sur **Zones de recherche inversée**, puis cliquez sur **Nouvelle zone**.
3. Dans l'Assistant Nouvelle zone, cliquez sur **Suivant**.
4. Sur la page **Type de zone**, cliquez sur **Zone principale**, puis cliquez sur **Suivant**.
5. Sur la page **Étendue de la zone de réplication de Active Directory**, cliquez sur **Suivant**.
6. Sur la page **Nom de la zone de recherche inversée**, cliquez sur **Zone de recherche inversée IPv4**, puis cliquez sur **Suivant**.
7. Sur la deuxième page **Nom de la zone de recherche inversée**, dans la zone **ID réseau :** saisissez **172.16.0**, puis cliquez sur **Suivant**.
8. Sur la page **Mise à niveau dynamique**, cliquez sur **Suivant**.
9. Sur la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.

Résultats : À la fin de cet exercice, vous aurez configuré les enregistrements de service de messagerie requis et la zone de recherche inversée.

Exercice 2 : Configuration de la redirection conditionnelle DNS

▶ Tâche 1 : Ajouter l'enregistrement de redirection conditionnelle pour contoso.com

1. Dans DNS, dans le volet de navigation, cliquez sur **Redirecteurs conditionnels**.
2. Cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez sur **Nouveau redirecteur conditionnel**.
3. Dans la boîte de dialogue **Nouveau redirecteur conditionnel**, dans la zone **Domaine DNS**, saisissez **contoso.com**.
4. Cliquez sur la zone **<Cliquez ici pour ajouter une adresse IP ou un nom DNS>**. Saisissez **131.107.1.2**, puis appuyez sur Entrée. La validation échouera puisque le serveur ne peut pas être contacté.
5. Activez la case à cocher **Stocker ce redirecteur conditionnel dans Active Directory, et le répliquer comme suit**.
6. Cliquez sur **OK**.

Résultats : À la fin de cet exercice, vous aurez configuré avec succès la redirection conditionnelle.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Installer et configurer des zones DNS

▶ Tâche 1 : Installer le rôle de serveur DNS sur LON-SVR1

1. Basculez vers LON-SVR1, puis connectez-vous avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Si nécessaire, cliquez sur **Gestionnaire de serveur** dans la barre des tâches.
3. Dans le Gestionnaire de serveur, dans le volet de navigation, cliquez sur **Tableau de bord**, puis dans le volet d'informations, cliquez sur **Ajouter des rôles et des fonctionnalités**.
4. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner des rôles de serveurs**, dans la liste **Rôles**, activez la case à cocher **Serveur DNS**.
8. Dans la boîte de dialogue **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**.
9. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
10. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
11. Sur la page **Serveur DNS**, cliquez sur **Suivant**.
12. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
13. Une fois que le rôle est installé, cliquez sur **Fermer**.

▶ Tâche 2 : Créer les zones secondaires requises sur LON-SVR1

1. Suspendez votre pointeur de la souris dans le coin inférieur gauche de l'affichage, puis cliquez sur **Accueil**.
2. Dans Accueil, saisissez **cmd.exe**, puis appuyez sur Entrée.
3. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Dnscmd.exe /zoneadd Adatum.com /secondary 172.16.0.10
```

4. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
5. À partir de Accueil, cliquez sur **DNS**.
6. Dans le Gestionnaire DNS, dans le volet de navigation, développez **LON-SVR1**, puis cliquez sur **Zones de recherche directes**. Remarquez la nouvelle zone.

▶ Tâche 3 : Activer et configurer les transferts de zone

1. Basculez vers LON-DC1.
2. Suspendez votre pointeur de la souris dans le coin inférieur gauche de l'affichage, puis cliquez sur **Accueil**.
3. Dans Accueil, saisissez **cmd.exe**, puis appuyez sur Entrée.

4. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Dnscmd.exe /zoneresetsecondaries Adatum.com /notifylist 172.16.0.21
```

5. Dans le Gestionnaire DNS, dans le volet de navigation, cliquez sur **Adatum.com**, puis dans la barre d'outils, cliquez sur **Actualiser**.
6. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Propriétés**.
7. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur l'onglet **Transferts de zone**.
8. Cliquez sur **Notifier** et vérifiez que le serveur **172.16.0.21** est listé.
9. Cliquez sur **Annuler**.
10. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : Adatum.com**.

▶ Tâche 4 : Configurer la durée de vie, le vieillissement et le nettoyage

1. Sur LON-DC1, cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur l'onglet **Source de noms (SOA)**.
3. Dans la zone **Durée de vie minimale (par défaut)**, saisissez **2**, puis cliquez sur **OK**.
4. Cliquez avec le bouton droit sur **LON-DC1**, puis cliquez sur **Définir le vieillissement/nettoyage pour toutes les zones...**.
5. Dans la boîte de dialogue **Vieillissement de serveur/Propriétés de nettoyage**, activez la case à cocher **Nettoyer les enregistrements de ressources obsolètes**, puis cliquez sur **OK**.
6. Dans la boîte de dialogue **Vieillissement de serveur/Confirmation de nettoyage**, activez la case à cocher **Appliquer ces paramètres aux zones existantes intégrées à Active Directory**, puis cliquez sur **OK**.

▶ Tâche 5 : Configurer les clients pour qu'ils utilisent le nouveau nom de serveur

1. Basculez vers LON-CL1.
2. Connectez-vous à l'ordinateur virtuel LON-CL1 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
3. Sur l'écran d'accueil, saisissez **Panneau**, puis cliquez sur **Panneau de configuration**.
4. Dans le Panneau de configuration, cliquez sur **Réseau et Internet**.
5. Dans Réseau et Internet, cliquez sur **Centre Réseau et partage.**
6. Dans le Centre Réseau et partage, à droite du Réseau avec domaine Adatum.com, cliquez sur **Connexion au réseau local**.
7. Dans la boîte de dialogue **État de Connexion au réseau local**, cliquez sur **Propriétés**.
8. Cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur **Propriétés**.
9. Dans la boîte de dialogue **Propriétés de : Protocole Internet version 4 (TCP/IPv4)**, dans la zone **Serveur DNS préféré**, saisissez **172.16.0.21**, puis cliquez sur **OK**.
10. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, cliquez sur **Fermer**.
11. Dans la boîte de dialogue **État de Connexion au réseau local**, cliquez sur **Fermer**.

Résultats : À la fin de cet exercice, vous aurez installé et configuré avec succès DNS sur LON-SVR1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 4 : Dépannage du système DNS

▶ Tâche 1 : Tester les requêtes simples et récursives

1. Basculez vers LON-DC1.
2. Sur LON-DC1, basculez vers le Gestionnaire DNS.
3. Dans le volet de navigation, cliquez avec le bouton droit sur **LON-DC1**, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Analyse**.
5. Sous l'onglet **Analyse**, activez la case à cocher **Une requête simple sur un serveur DNS**, puis cliquez sur **Tester**.
6. Sous l'onglet **Analyse**, activez la case à cocher **Une requête récursive aux autres serveurs DNS**, puis cliquez sur **Tester**. Notez que le test Récursive échoue pour LON-DC1, ce qui est normal étant donné qu'aucun redirecteur n'est configuré pour ce serveur DNS.
7. Suspendez votre pointeur de la souris dans le coin inférieur gauche de l'affichage, puis cliquez sur **Accueil**.
8. Dans Accueil, saisissez **cmd**, puis appuyez sur Entrée.
9. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
sc stop dns
```

10. Rebasculez vers le Gestionnaire DNS.
11. Dans le Gestionnaire DNS, dans la boîte de dialogue **Propriétés de : LON-DC1**, sous l'onglet **Analyse**, cliquez sur **Tester**. À présent, les tests simples et récursifs échouent parce qu'aucun serveur DNS n'est disponible.
12. Revenez à l'invite de commandes.
13. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
sc start dns
```

14. Rebasculez vers le Gestionnaire DNS.
15. Sous l'onglet **Analyse**, cliquez sur **Tester** . Le test Simple s'effectue correctement.
16. Fermez la boîte de dialogue **Propriétés de LON-DC1**.

▶ Tâche 2 : Vérifier les enregistrements de ressource de source de noms (SOA) avec Windows PowerShell®

1. Sur LON-DC1, dans la barre des tâches, cliquez sur **Windows PowerShell**.
2. À l'invite Windows PowerShell®, tapez la commande suivante, puis appuyez sur Entrée :

```
resolve-dnsname –name Adatum.com –type SOA
```

3. Fermez l'invite Windows PowerShell.

Résultats : À la fin de cet exercice, vous aurez testé et vérifié le système DNS avec succès.

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 cela, 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 **22411B-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 **22411B-LON-SVR1** et **22411B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 3: Gestion des services de domaine Active Directory

Atelier pratique : Gestion d'AD DS

Exercice 1 : Installation et configuration d'un contrôleur de domaine en lecture seule (RODC)

▶ Tâche 1 : Vérifier la configuration requise pour installer un RODC

1. Sur LON-DC1, dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans **Utilisateurs et ordinateurs Active Directory**, dans le volet de navigation, cliquez avec le bouton droit sur le domaine **Adatum.com**, puis cliquez sur **Augmenter le niveau fonctionnel du domaine**.
3. Dans la fenêtre Augmenter le niveau fonctionnel du domaine, confirmez que **Niveau fonctionnel du domaine actuel** est configuré sur **Windows Server 2008 R2**. Le niveau minimum pour la prise en charge de contrôleur de domaine en lecture seule est Windows Server 2003. Cliquez sur **Annuler**.
4. Basculez vers **LON-SVR1**.
5. Sur **LON-SVR1**, dans **Gestionnaire de serveur**, cliquez sur **Serveur local**, puis cliquez sur **LON-SVR1** situé à côté de **Nom de l'ordinateur**.
6. Dans la fenêtre Propriétés système,, cliquez sur **Modifier**.
7. Dans la fenêtre Modification du nom ou du domaine de l'ordinateur, cliquez sur la case d'option **Groupe de travail**, saisissez **TEMPORAIRE** dans le champ **Groupe de travail**, puis cliquez sur **OK**.
8. Dans la fenêtre Modification du nom ou du domaine de l'ordinateur, cliquez sur **OK**.
9. Cliquez deux fois sur **OK** pour confirmer le changement de nom et le redémarrage du serveur en attente.
10. Dans la fenêtre Propriétés système, cliquez sur **Fermer**.
11. Dans la fenêtre Microsoft Windows, cliquez sur **Redémarrer maintenant**.
12. Basculez vers **LON-DC1**.
13. Sur **LON-DC1**, dans **Utilisateurs et ordinateurs Active Directory**, dans le volet de navigation, développez **Adatum.com**, puis cliquez sur **Computers**.
14. Cliquez avec le bouton droit sur **LON-SVR1**, puis cliquez sur **Supprimer**.
15. Cliquez deux fois sur **Oui**.
16. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur **Domain Controllers**, puis cliquez sur **Créer au préalable un compte de contrôleur de domaine en lecture seule**.
17. Dans la fenêtre Assistant Installation des services de domaine Active Directory**,** cliquez sur **Suivant**.
18. Cliquez sur **Suivant** pour accepter les informations d'identification actuelles.
19. Dans le champ **Nom de l'ordinateur**, saisissez **LON-SVR1**, puis cliquez sur **Suivant**.
20. Sur la page **Sélectionnez un site**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

21. Sur la page **Options supplémentaires pour le contrôleur de domaine**, cliquez sur **Suivant**.
22. Sur la page **Délégation de l'installation et de l'administration du RODC**, saisissez **ADATUM\IT** dans le champ **Groupe ou utilisateur,** puis cliquez sur **Suivant**.
23. Sur la page **Résumé**, cliquez sur **Suivant**.
24. Cliquez sur **Terminer** pour fermer l'Assistant.
25. Fermez la fenêtre Utilisateurs et ordinateurs Active Directory.

▶ Tâche 2 : Installer un serveur RODC

1. Ouvrez une session sur LON-SVR1 en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd.**
2. Sur LON-SVR1, dans **Gestionnaire de serveur**, cliquez sur **Gérer**, puis cliquez sur **Ajouter des rôles et fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
4. Vérifiez que **Installation basée sur un rôle ou une fonctionnalité** est sélectionné, puis cliquez sur **Suivant**.
5. Sélectionnez LON-SVR1, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs** activez la case à cocher pour sélectionner **Services AD DS**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
7. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Cliquez sur **Suivant**, puis cliquez sur **Installer** pour continuer l'installation.
9. Une fois l'installation terminée, cliquez sur **Fermer**.
10. Dans **Gestionnaire de serveur**, cliquez sur l'icône **Notifications**, puis cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.
11. Dans la fenêtre Configuration de déploiement, à côté de **Domaine**, cliquez sur **Sélectionner**.
12. Dans la fenêtre Sécurité de Windows, saisissez **ADATUM\April** pour **Nom d'utilisateur** et **Pa$$w0rd** comme mot de passe, puis cliquez sur **OK**.
13. Dans la fenêtre Sélectionner un domaine dans la forêt, cliquez sur **Adatum.com**, puis cliquez sur **OK**.
14. Dans la fenêtre Configuration de déploiement, cliquez sur **Suivant**.
15. Sur l'écran **Options du contrôleur de domaine**, situé en dessous de **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)**, saisissez **Pa$$w0rd** dans les champs **Mot de passe** et **Confirmer le mot de passe,** puis cliquez sur **Suivant**.
16. Sur la page **Options supplémentaires**, à côté de **Répliquer depuis**, cliquez sur la zone déroulante, cliquez sur **LON-DC1.Adatum.com**, puis cliquez sur **Suivant**.
17. Sur la page **Chemins d'accès**, cliquez sur **Suivant**.
18. Sur la page **Examiner les options**, cliquez sur **Suivant**.
19. Sur la page **Vérification de la configuration requise**, cliquez sur **Installer**.
20. Après la fin de l'Assistant de services de domaine Active Directory, LON-SVR1 redémarrera.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer une stratégie de réplication du mot de passe

Configurer des groupes de réplication du mot de passe

1. Sur LON-DC1, dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans la fenêtre Utilisateurs et ordinateurs Active Directory, cliquez sur le conteneur **Users**, double-cliquez sur **Groupe de réplication dont le mot de passe RODC est autorisé**, cliquez sur l'onglet **Membres**, puis vérifiez que rien n'est listé.
3. Cliquez sur **OK**.
4. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez sur l'unité d'organisation **Domain Controllers**, cliquez avec le bouton droit sur **LON-SVR1**, puis cliquez sur **Propriétés**.
5. Cliquez sur l'onglet **Stratégie de réplication de mot de passe** et confirmez que le **Groupe de réplication dont le mot de passe RODC est autorisé** et le **Groupe de réplication dont le mot de passe RODC est refusé** sont listés.
6. Cliquez sur **OK**.

Créer un groupe pour gérer la réplication de mot de passe sur le contrôleur de domaine en lecture seule de bureau distant

1. Sur LON-DC1, dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur l'unité d'organisation **Research**, cliquez sur **Nouveau**, puis cliquez sur **Groupe**.
2. Dans la fenêtre Nouvel objet - Groupe**,** saisissez **Utilisateurs de bureau distant** dans le champ **Nom de groupe**, confirmez que **Globale** et **Sécurité** sont sélectionnés, puis cliquez sur **OK**.
3. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez sur l'unité d'organisation **Research**, puis double-cliquez sur le groupe **debureau**.
4. Dans la fenêtre Propriétés des utilisateurs de bureau distant, cliquez sur l'onglet **Membres**.
5. Cliquez sur **Ajouter**, saisissez **Aziz** ; **Colin ; Lukas ; Louise** puis cliquez sur **Vérifier les noms.**
6. Cliquez sur **Types d'objets**, sélectionnez **des Ordinateurs**, puis cliquez sur **OK**.
7. Dans le champ **Entrez les noms des objets à sélectionner**, saisissez **LON-CL1**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
8. Cliquez sur **OK** pour fermer la fenêtre Propriétés des utilisateurs de bureau distant.

Configurer une stratégie de réplication de mot de passe pour le contrôleur de domaine en lecture seule de bureau distant

1. Sur LON-DC1, dans **Utilisateurs et ordinateurs Active Directory**, cliquez sur l'unité d'organisation **Domain Controllers**, cliquez avec le bouton droit sur **LON-SVR1**, puis cliquez sur **Propriétés**.
2. Dans la fenêtre Propriétés LON-SVR1**,** cliquez sur l'onglet **Stratégie de réplication de mot de passe,** puis cliquez sur **Ajouter**.
3. Dans la fenêtre Ajouter des groupes, utilisateurs et ordinateurs**,** cliquez sur la case d'option pour sélectionner **Autoriser la réplication des mots de passe du compte sur ce contrôleur de domaine en lecture seule (RODC)**, puis cliquez sur **OK**.
4. Dans la fenêtre de recherche, dans le champ **Entrez les noms des objets à sélectionner**, saisissez **Utilisateurs de bureau distant**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
5. Dans la fenêtre Propriétés LON-SVR1**,** cliquez sur **Appliquer**, et ne fermez pas la fenêtre.

Évaluer la stratégie de réplication de mot de passe résultante

1. Sur LON-DC1, dans la fenêtre Propriétés LON-SVR1, sur l'onglet **Stratégie de réplication de mot de passe,** cliquez sur **Avancé**.
2. Cliquez sur l'onglet **Stratégie résultante**, cliquez sur **Ajouter**, saisissez **Aziz**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
3. Confirmez que le paramètre résultant pour Aziz est **Autoriser**.
4. Cliquez sur **Fermer**, puis cliquez sur **OK** pour fermer la boîte de dialogue Propriétés LON-SVR1.

Surveiller la mise en cache des informations d'identification

1. Basculez vers LON-SVR1.
2. Essayez de vous connecter avec l'identifiant **ADATUM\Aziz** avec le mot de passe **Pa$$w0rd**. L'ouverture de session échouera, parce qu'Aziz n'a pas l'autorisation de se connecter à LON-SVR1. Cependant, les informations d'identification pour le compte d'Aziz ont été traitées et mises en cache sur LON-SVR1.
3. Basculez vers LON-DC1.
4. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez sur l'unité d'organisation **DomainControllers**, double-cliquez sur **LON-SVR1**, puis cliquez sur l'onglet **Stratégie de réplication de mot de passe**.
5. Sur l'onglet **Stratégie de réplication de mot de passe,** cliquez sur **Avancé**. Remarquez que le mot de passe du compte d'Aziz a été enregistré sur LON-SVR1.
6. Cliquez sur **Fermer**, puis sur **OK**.

Préremplir la mise en cache des informations d'identification

1. Sur LON-DC1, dans **Utilisateurs et ordinateurs Active Directory**, cliquez sur l'unité d'organisation **Domain Controllers**, double-cliquez sur **LON-SVR1**, puis cliquez sur l'onglet **Stratégie de réplication de mot de passe**.
2. Sur l'onglet **Stratégie de réplication de mot de passe**, cliquez sur **Avancé**, puis cliquez sur **Préremplir les mots de passe**.
3. Saisissez **Louise; LON-CL1**, cliquez sur **Vérifier les noms**, cliquez sur **OK**, puis cliquez sur **Oui**.
4. Cliquez sur **OK** et confirmez que Louise et LON-CL1 ont chacun été ajoutés à la liste de comptes avec des informations d'identification mises en cache.
5. Fermez toutes les fenêtres ouvertes sur LON-DC1.

Résultats : Après avoir terminé cet exercice, vous aurez installé et configuré un RODC.

Exercice 2 : Configuration des instantanés d'AD DS

▶ Tâche 1 : Créer un instantané d'AD DS

1. Sur LON-DC1, déplacez votre souris sur le coin inférieur gauche, puis cliquez sur l'icône **Accueil**.
2. Dans l'écran Accueil, saisissez **cmd**, puis appuyez sur Entrée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
ntdsutil
```

4. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
snapshot
```

5. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
activate instance ntds
```

6. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
create
```

   Notez le numéro de GUID que la commande renvoie ou copiez-le sur le presse-papiers.

7. Après que l'instantané est créé, à l'invite de commandes, saisissez ce qui suit, puis appuyez sur Entrée :

```
quit
```

8. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
quit
```

▶ Tâche 2 : Modifier AD DS

1. Sur LON-DC1, ouvrez le **Gestionnaire de serveur,** cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans **Utilisateurs et ordinateurs Active Directory**, double-cliquez sur l'unité d'organisation **Marketing**, cliquez avec le bouton droit sur **Adam Barr**, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression.

▶ Tâche 3 : Monter un instantané d'Active Directory et créer une nouvelle instance

1. Sur LON-DC1, déplacez votre souris sur le coin inférieur gauche, puis cliquez sur l'icône **Accueil**.
2. Sur l'écran Accueil, saisissez **cmd**, cliquez avec le bouton droit sur **Invite de commandes**, puis cliquez sur **Exécuter comme administrateur**.
3. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
ntdsutil
```

4. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
snapshot
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
activate instance ntds
```

6. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
list all
```

7. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
mount <GUID>
```

Où <*GUID*> représente l'identificateur unique global renvoyé par la commande de création dans la tâche 1.

8. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
quit
```

9. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
quit
```

10. À l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
dsamain /dbpath C:\$SNAP_datetime_volumec$\windows\ntds\ntds.dit /ldapport 50000
```

Notez que *datetime* sera une valeur unique. Il ne doit y avoir qu'un dossier sur votre lecteur C:\ avec un nom qui commence par $snap.

Un message indique que le démarrage des Services de domaine Active Directory est terminé. Laissez Dsamain.exe fonctionner et ne fermez pas l'invite de commandes.

▶ Tâche 4 : Explorer un instantané avec des utilisateurs et des ordinateurs Active Directory

1. Basculez vers **Utilisateurs et ordinateurs Active Directory**. Cliquez avec le bouton droit sur le composant logiciel enfichable, puis sur **Changer de contrôleur de domaine...**.
2. Cliquez sur **<Tapez ici un nom de serveur d'annuaire:[port]>**, saisissez **LON-DC1:50000**, puis appuyez sur Entrée. Cliquez sur **OK**.
3. Dans le volet de navigation, double-cliquez sur **Adatum.com**.
4. Dans le volet de navigation, double-cliquez sur l'unité d'organisation **Marketing**.
5. Localisez l'objet de compte d'utilisateur **Adam Barr**. Notez que l'objet Adam Barr est affiché parce que l'instantané a été pris avant de le supprimer.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Démonter un instantané d'Active Directory

1. Dans l'invite de commandes, appuyez sur Ctrl+C. pour arrêter DSAMain.exe.
2. Saisissez les commandes suivantes :

```
ntdsutil
snapshot
activate instance ntds
list all
unmount guid
list all
quit
Quit
```

Où *guid* représente l'identificateur unique global de l'instantané.

Résultats : Après avoir terminé cet exercice, vous aurez configuré des instantanés d'AD DS.

Exercice 3 : Configuration de la Corbeille Active Directory

▶ Tâche 1 : Activer la corbeille Active Directory

1. Sur LON-DC1, dans Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Cliquez sur **Adatum (local).**
3. Dans le volet **Tâches**, cliquez sur **Activer la corbeille**, cliquez sur **OK** sur la zone de message d'avertissement, puis cliquez sur **OK** sur le message d'actualisation du **Centre d'administration Active Directory**.
4. Appuyez sur F5 pour actualiser le **Centre d'administration Active Directory**.

▶ Tâche 2 : Créer et supprimer des utilisateurs test

1. Dans le **Centre d'administration Active Directory**, double-cliquez sur l'unité d'organisation **Research**.
2. Dans le volet **Tâches**, cliquez sur **Nouveau**, puis cliquez sur **Utilisateur**.
3. Entrez les informations suivantes dans **Compte**, puis cliquez sur **OK** :
   - Nom complet : **Test1**
   - Ouverture de session UPN de l'utilisateur : **Test1**
   - Mot de passe : **Pa$$w0rd**
   - Confirmation : **Pa$$w0rd**
4. Répétez les étapes précédentes pour créer un deuxième utilisateur, **Test2**.
5. Sélectionnez les deux **Test1** et **Test2**. Cliquez avec le bouton droit sur la sélection, puis cliquez sur **Supprimer**.
6. Cliquez sur **Oui** à l'invite de confirmation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Restaurer les utilisateurs supprimés

1. Dans **Centre d'administration Active Directory**, cliquez sur **Adatum (local)**, puis double-cliquez sur **Deleted Objects**.
2. Cliquez avec le bouton droit sur **Test1**, puis cliquez sur **Restaurer**.
3. Cliquez avec le bouton droit sur **Test2**, puis cliquez sur **Restaurer sur**.
4. Dans la fenêtre Restaurer vers, cliquez sur l'unité d'organisation **IT**, puis cliquez sur **OK**.
5. Confirmez que Test1 est maintenant situé dans l'unité d'organisation Research et que Test2 est dans l'unité d'organisation IT.

▶ Tâche 4 : Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez les ordinateurs virtuels à leur état initial en complétant les étapes suivantes :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22411B-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 **22411B-LON-SVR1**.

Résultats : À la fin de cet exercice, vous devez avoir configuré la corbeille Active Directory.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4: Gestion des comptes d'utilisateurs et de service

Atelier pratique : Gestion des comptes d'utilisateurs et de service

Exercice 1 : Configuration des paramètres de stratégie de mot de passe et de verrouillage de compte

▶ Tâche 1 : Configurez une stratégie de mot de passe basée sur le domaine

1. Sur LON-DC1, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans **Gestion des stratégies de groupe**, développez **Forêt : Adatum.com**. développez **Domaines**, développez **Adatum.com**, développez **Objets de stratégie de groupe**, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
3. Dans l'Éditeur de gestion des stratégies de groupe, dans le volet de navigation, naviguez jusqu'à **Configuration ordinateur**, développez **Stratégies**, développez **Paramètres Windows**, développez **Paramètres de sécurité**, développez **Stratégies de comptes** et cliquez sur **Stratégie de mot de passe**.
4. Double-cliquez sur **Conserver l'historique des mots de passe**.
5. Dans la fenêtre de propriétés Conserver l'historique des mots de passe, saisissez **20** dans le champ **Conserver l'historique du mot de passe pendant**, puis cliquez sur **OK**.
6. Double-cliquez sur **Durée de vie maximale du mot de passe**.
7. Dans la fenêtre de propriétés Durée de vie maximale du mot de passe, saisissez **45** dans le champ **Le mot de passe expirera dans**, puis cliquez sur **OK**.
8. Double-cliquez sur **Durée de vie minimale du mot de passe**.
9. Dans la fenêtre de propriétés Durée de vie minimale du mot de passe, assurez-vous que le champ **Le mot de passe peut être modifié après** est défini sur **1**, puis cliquez sur **OK**.
10. Double-cliquez sur **Longueur minimale du mot de passe**.
11. Dans la fenêtre de propriétés Longueur minimale du mot de passe, saisissez **10** dans le champ **Le mot de passe doit faire au minimum**, puis cliquez sur **OK**.
12. Double-cliquez sur **Le mot de passe doit respecter des exigences de complexité**.
13. Dans la boîte de dialogue Le mot de passe doit respecter les exigences de complexité - Propriétés, cliquez sur **Activé**, puis sur **OK**.
14. Ne fermez pas la console Éditeur de gestion des stratégies de groupe.

▶ Tâche 2 : Configurez une stratégie de verrouillage du compte

1. Dans l'éditeur de gestion des stratégies de groupe, dans le volet de navigation, cliquez sur **Stratégie de verrouillage du compte**.
2. Double-cliquez sur **Durée de verrouillage des comptes**.

3. Dans la fenêtre Propriétés de durée de verrouillage de compte, cliquez sur **Définir ce paramètre de stratégie**, saisissez **30** dans le champ **minutes** , puis cliquez sur **OK**.
4. Dans la fenêtre Modifications suggérées pour les valeurs, notez les valeurs suggérées, y compris la configuration automatique de **Seuil de verrouillage de compte**, puis cliquez sur **OK**.
5. Double-cliquez sur **Réinitialiser le compteur de verrouillages du compte après**.
6. Dans la fenêtre Réinitialiser le compteur de verrouillages du compte après - Propriétés, saisissez **15** dans le champ **Réinitialiser le compteur de verrouillages du compte après**, puis cliquez sur **OK**.
7. Fermez l'Éditeur de gestion des stratégies de groupe.
8. Fermez Gestion de stratégies de groupe.

▶ Tâche 3 : Configurez et appliquez une stratégie de mot de passe affinée

1. Sur LON-DC1, dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Adatum (local)**.
3. Dans le volet d'informations, double-cliquez sur l'unité d'organisation **Managers**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur le groupe **Managers**, puis cliquez sur **Propriétés**.

Remarque : vérifiez que vous ouvrez la page Propriétés du groupe Managers et non l'unité d'organisation Managers. Dans la fenêtre Managers, sous **Étendue du groupe**, cliquez sur **Global**, puis cliquez sur **OK**.

5. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Adatum (local)**.
6. Dans le volet d'informations, double-cliquez sur le conteneur **System**.
7. Dans le volet d'informations, cliquez avec le bouton droit sur **Password Settings Container**, cliquez sur **Nouveau**, puis cliquez sur **Paramètres de mot de passe**.
8. Dans la fenêtre Paramètres de création mot de passe, complétez les étapes suivantes :
   a. Saisissez **ManagersPSO** dans le champ **Nom**.
   b. Saisissez **10** dans le champ **Priorité**.
   c. Saisissez **15** dans le champ **Longueur minimale du mot de passe (caractères)**.
   d. Saisissez **20** dans le champ **Nombre de mots de passe mémorisés** .
   e. Saisissez **30** dans le champ **Appliquer l'âge maximal de mot de passe**.
   f. Cliquez sur **Appliquer la stratégie de verrouillage des comptes**.
   g. Saisissez **3** dans le champ **Nombre de tentatives de connexion échouées autorisées**.
   h. Saisissez **30** dans le champ **Réinitialiser le nombre de tentatives de connexion échouées après**.
   i. Cliquez sur l'option **Jusqu'à ce qu'un administrateur déverrouille manuellement le compte**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Dans la section **S'applique directement à**, cliquez sur **Ajouter**.
10. Dans le champ **Entrez les noms des objets à sélectionner**, saisissez **ADATUM\Managers**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
11. Dans la fenêtre Paramètres de création mot de passe, cliquez sur **OK**.
12. Fermez le Centre d'administration Active Directory.

Résultats : Après avoir complété cet exercice, vous aurez configuré des paramètres de stratégie de mot de passe et de verrouillage de compte.

Exercice 2 : Création et association d'un compte de service géré

▶ Tâche 1 : Créer et associer un compte de service géré

1. Sur LON-DC1, dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis cliquez sur **Module Active Directory pour Windows PowerShell**.
2. Saisissez ce qui suit dans la fenêtre de la commande Windows PowerShell® puis appuyez sur Entrée :

```
Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))
```

3. Saisissez ce qui suit dans la fenêtre de commande Windows PowerShell, puis appuyez sur Entrée :

```
New-ADServiceAccount –Name Webservice –DNSHostName LON-DC1 –
PrincipalsAllowedToRetrieveManagedPassword LON-DC1$
```

4. Saisissez ce qui suit dans la fenêtre de commande Windows PowerShell, puis appuyez sur Entrée :

```
Add-ADComputerServiceAccount –identity LON-DC1 –ServiceAccount Webservice
```

5. Saisissez ce qui suit dans la fenêtre de commande Windows PowerShell, puis appuyez sur Entrée :

```
Get-ADServiceAccount -Filter *
```

6. Notez la sortie de la commande, en vérifiant que le compte nouvellement créé est bien répertorié.
7. Réduisez la fenêtre de la commande Windows PowerShell.

▶ Tâche 2 : Installer un compte de service géré sur LON-DC1

1. Sur LON-DC1, saisissez ce qui suit dans la fenêtre de commande Windows PowerShell, puis appuyez sur Entrée :

```
Install-ADServiceAccount –Identity Webservice
```

2. Dans le Gestionnaire de serveur, cliquez sur le menu **Outils** , puis cliquez sur **Gestionnaire des services Internet (IIS)**.
3. Dans la console Gestionnaire Internet Information Services (IIS), développez **LON-DC1 (ADATUM\Administrateur)**, puis cliquez sur **Pools d'applications**. Si la fenêtre Gestionnaire des services Internet (IIS) s'affiche, cliquez sur **Non**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur **DefaultAppPool**, puis cliquez sur **Paramètres avancés**.
5. Dans la boîte de dialogue **Paramètres avancés**, cliquez sur **Identité** puis cliquez sur les **ellipses**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans la boîte de dialogue **Identité du pool d'applications**, cliquez sur **Compte personnalisé** puis cliquez sur **Définir**.
7. Dans la boîte de dialogue **Définir les informations d'identification**, saisissez **ADATUM\Webservice$** dans le champ Nom d'utilisateur : et cliquez trois fois de suite sur **OK**.
8. Dans le volet Actions, cliquez sur **Arrêter** pour arrêter le pool d'applications.
9. Cliquez sur **Accueil** pour démarrer le pool d'applications.
10. Fermez le Gestionnaire des services Internet (IIS).

▶ Pour préparer le module suivant

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22411B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.

Résultats : Après avoir complété cet exercice, vous aurez créé et associé un compte de service géré.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 5: Implémentation d'une infrastructure de stratégie de groupe

Atelier pratique : Implémentation d'une infrastructure de stratégie de groupe

Exercice 1 : Création et configuration d'objets de stratégie de groupe

▶ Tâche 1 : Créer et modifier un objet de stratégie de groupe

1. Sur LON-DC1, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans l'arborescence de console, développez **Forêt : Adatum.com**, **Domaines**, et **Adatum.com**, puis cliquez sur le conteneur **Objets de stratégie de groupe**.
3. Dans l'arborescence de la console, cliquez avec le bouton droit sur le conteneur **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
4. Dans la zone **Nom**, saisissez **Normes ADATUM** puis cliquez sur **OK**.
5. Dans le volet d'informations de la console Gestion des stratégies de groupe, cliquez avec le bouton droit sur l'objet de stratégie de groupe **Normes ADATUM**, puis cliquez sur **Modifier**.
6. Dans l'arborescence de la console, développez (si nécessaire) **Configuration utilisateur**, **Stratégies**, et **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordenateur local**, cliquez sur **Système**.
7. Double-cliquez sur le paramètre de stratégie **Ne pas exécuter les applications Windows spécifiées**.
8. Dans la fenêtre Ne pas exécuter les applications Windows spécifiées, cliquez sur **Activé**.
9. Cliquez sur **Afficher**.
10. Dans la boîte de dialogue **Afficher le contenu**, dans la liste **Valeur**, saisissez **notepad.exe**, puis cliquez sur **OK**.
11. Dans la boîte de dialogue **Ne pas exécuter les applications Windows spécifiées**, cliquez sur **OK**.
12. Dans l'arborescence de la console, développez **Configuration utilisateur**, **Stratégies**, **Modèles d'administration** et **Panneau de configuration**, puis cliquez sur **Personnalisation**.
13. Dans le volet d'informations, cliquez sur le paramètre de stratégie **Dépassement du délai d'expiration de l'écran de veille**.
14. Double-cliquez sur le paramètre de stratégie **Dépassement du délai d'expiration de l'écran de veille**.
15. Cliquez sur **Activé**.
16. Dans la zone **Secondes**, saisissez **600**, puis cliquez sur **OK**.
17. Double-cliquez sur le paramètre de stratégie **Un mot de passe protège l'écran de veille**.
18. Cliquez sur **Activé**, puis sur **OK**.
19. Fermez l'Éditeur de gestion des stratégies de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Lier l'objet de stratégie de groupe

1. Dans la fenêtre Gestion des stratégies de groupe, cliquez avec le bouton droit sur le domaine **Adatum.com**, puis cliquez sur **Lier un objet de stratégie de groupe existant**.
2. Dans la boîte de dialogue **Objets de stratégie de groupe**, cliquez sur **Normes ADATUM**, puis cliquez sur **OK**.

▶ Tâche 3 : Afficher les effets des paramètres de l'objet de stratégie de groupe.

1. Basculez vers **LON-CL1**, puis ouvrez une session avec le nom d'utilisateur **ADATUM\Pat** et le mot de passe **Pa$$w0rd**.
2. Sur l'écran Accueil, cliquez sur la mosaïque du **Bureau**.
3. Cliquez avec le bouton droit sur le **Bureau**, puis cliquez sur **Personnaliser**.
4. Cliquez sur **Écran de veille**. Vous constatez que le contrôle **Délai** est désactivé ; vous ne pouvez pas modifier le délai d'activation. Vous constatez que l'option **À la reprise, demander l'ouverture de session** est sélectionnée et désactivée, et que vous ne pouvez pas désactiver la protection par mot de passe.
5. Cliquez sur **OK** pour fermer la boîte de dialogue **Paramètres de l'écran de veille**.
6. Placez le pointeur de votre souris dans le coin inférieur droit de l'écran, puis cliquez sur **Accueil**.
7. Cliquez avec le bouton droit sur l'écran d'accueil, puis cliquez sur **Toutes les applications**.
8. Dans la liste **Applications**, cliquez sur **Bloc-notes**. Le Bloc-notes ne s'ouvre pas.

Résultats : À la fin de cet exercice, vous devez avoir correctement créé, modifié et lié les objets de stratégie de groupe requis.

Exercice 2 : Gestion de l'étendue des objets de stratégie de groupe

▶ Tâche 1 : Créer et lier les objets de stratégie de groupe requis.

1. Sur LON-DC1, basculez vers **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console, développez le domaine **Adatum.com**, puis cliquez sur l'unité d'organisation **Research**.
3. Cliquez avec le bouton droit sur l'unité d'organisation **Research**, pointez sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
4. Saisissez **Ingénieurs**, puis cliquez sur **OK**.
5. Fermez la fenêtre Utilisateurs et ordinateurs Active Directory®.
6. Basculez vers la console Gestion de stratégie de groupe.
7. Dans l'arborescence de console, développez **Forêt : Adatum.com**, **Domaines**, **Adatum.com**, **Research**, puis cliquez sur l'unité d'organisation **Ingénieurs.**
8. Cliquez avec le bouton droit sur l'unité d'organisation **Ingénieurs**, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Saisissez **Remplacement d'application d'ingénierie**, puis cliquez sur **OK**.
10. Cliquez avec le bouton droit sur l'objet de stratégie de groupe **Remplacement d'application d'ingénierie**, puis cliquez sur **Modifier**.
11. Dans l'arborescence de la console, développez **Configuration Utilisateur**, **Stratégies**, **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordenateur local** et **Panneau de configuration**, puis cliquez sur **Personnalisation**.
12. Double-cliquez sur le paramètre de stratégie **Dépassement du délai d'expiration de l'écran de veille**.
13. Cliquez sur **Désactivé**, puis sur **OK**.
14. Fermez l'Éditeur de gestion des stratégies de groupe.

▶ Tâche 2 : Vérifier l'ordre de priorité

1. Dans l'arborescence de la console Gestion des stratégies de groupe, cliquez sur l'unité d'organisation **Ingénieurs**.
2. Cliquez sur l'onglet **Héritage de stratégie de groupe**. Vous constatez que l'objet de stratégie de groupe Remplacement d'application d'ingénierie a une priorité supérieure à celle de l'objet de stratégie de groupe Normes ADATUM. Le paramètre de stratégie de délai d'expiration de l'écran de veille que vous venez de configurer dans l'objet de stratégie de groupe Remplacement d'application d'ingénierie est appliqué après le paramètre de l'objet de stratégie de groupe Normes ADATUM. Par conséquent, le nouveau paramètre remplacera le paramètre de normes et *l'emportera*. Le délai d'expiration de l'écran de veille sera désactivé pour les utilisateurs couverts par l'étendue de l'objet de stratégie de groupe Remplacement d'application d'ingénierie.

▶ Tâche 3 : Configurer l'étendue d'un objet de stratégie de groupe avec le filtrage de sécurité

1. Sur LON-DC1, à partir du **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console, s'il y a lieu, développez le domaine **Adatum.com** et l'unité d'organisation **Research**, puis cliquez sur l'unité d'organisation **Ingénieurs**.
3. Cliquez avec le bouton droit sur l'unité d'organisation **Ingénieurs**, pointez sur **Nouveau**, puis cliquez sur **Groupe**.
4. Saisissez **Application GPO_Engineering Override_Apply**, puis cliquez sur Entrée.
5. Basculez vers la console **Gestion de stratégie de groupe**.
6. Dans l'arborescence de la console, s'il y a lieu, développez l'unité d'organisation **Ingénieurs**, puis double-cliquez sur le lien de l'objet de stratégie de groupe **Remplacement d'application d'ingénierie** sous l'unité d'organisation **Ingénieurs**. Le message suivant s'affiche :
7. Lisez le message, activez la case à cocher **Ne plus afficher ce message**, puis cliquez sur **OK**. Vous constatez que, dans la section Filtrage de sécurité, l'objet de stratégie de groupe s'applique par défaut à tous les utilisateurs authentifiés.
8. Dans la section de Filtrage de sécurité, cliquez sur **Utilisateurs authentifiés**.
9. Cliquez sur le bouton **Supprimer**. Une invite de confirmation s'affiche.
10. Cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans le volet d'informations, cliquez sur le bouton **Ajouter**.
12. Dans la boîte de dialogue **Sélectionnez un utilisateur, un ordinateur ou un groupe**, dans la zone **Entrez le nom de l'objet à sélectionner (exemples) :** saisissez **Application GPO_Engineering Override_Apply**, puis appuyez sur Entrée.
13. Basculez vers **Utilisateurs et ordinateurs Active Directory**.
14. Dans l'arborescence de la console, développez le domaine **Adatum.com**, puis cliquez sur le dossier **Users**.
15. Cliquez avec le bouton droit sur **User**, pointez sur **Nouveau**, puis cliquez sur **Groupe**.
16. Saisissez **GPO_ADATUM Standards_Exempt**, puis appuyez sur Entrée.
17. Basculez vers la console **Gestion de stratégie de groupe**.
18. Dans l'arborescence de la console, cliquez sur l'objet de domaine **Adatum.com**, puis double-cliquez sur l'objet de stratégie de groupe **Normes ADATUM**. Dans la section Filtrage de sécurité, vous constatez que l'objet de stratégie de groupe s'applique par défaut à tous les utilisateurs authentifiés.
19. Cliquez sur l'onglet **Délégation**.
20. Cliquez sur le bouton **Avancé**. La boîte de dialogue **Paramètres de sécurité pour Normes ADATUM** s'affiche.
21. Cliquez sur le bouton **Ajouter**. La boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou groupes** s'affiche.
22. Dans la zone **Entrez les noms des objets à sélectionner (exemples) :**, saisissez **GPO_ADATUM Standards_Exempt**, puis appuyez sur Entrée.
23. Activez la case à cocher **Refuser**, en regard de **Appliquer la stratégie de groupe**.
24. Cliquez sur **OK**. Un message d'avertissement s'affiche afin de vous rappeler que les refus d'accès remplacent les autorisations d'accès. Cliquez sur **Oui**. Vous constatez que dans l'onglet **Délégation**, l'autorisation s'affiche comme **Personnalisé**.

▶ Tâche 4 : Configurer le traitement par boucle de rappel

1. Sur LON-DC1, basculez vers **Utilisateurs et ordinateurs Active Directory**.
2. Dans la console, cliquez sur **Adatum.com**.
3. Cliquez avec le bouton droit sur **Adatum.com**, pointez sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
4. Dans la boîte de dialogue **Nouvel objet - Unité d'organisation**, saisissez **Bornes**, puis cliquez sur **OK**.
5. Cliquez avec le bouton droit sur **Bornes**, pointez sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
6. Dans la boîte de dialogue **Nouvel objet – Unité d'organisation**, saisissez **Salles de conférence**, puis cliquez sur **OK**.
7. Basculez vers la console Gestion de stratégie de groupe. Actualisez la console s'il y a lieu.
8. Dans l'arborescence, développez l'unité d'organisation **Bornes**, puis cliquez sur l'unité d'organisation **Salles de conférence**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Cliquez avec le bouton droit sur l'unité d'organisation **Salles de conférence**, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**.
10. Dans la boîte de dialogue **Nouvel objet GPO**, dans la zone de texte **Nom**, saisissez **Stratégies de salle de conférence**, puis appuyez sur Entrée.
11. Dans l'arborescence de la console, développez **Salles de conférence**, puis cliquez sur l'objet de stratégie de groupe **Stratégies de salle de conférence**.
12. Cliquez sur l'onglet **Étendue**. Confirmez que l'étendue de l'objet de stratégie de groupe s'applique à Utilisateurs authentifiés.
13. Dans l'arborescence de la console, cliquez avec le bouton droit sur l'objet de stratégie de groupe **Stratégies de salle de conférence**, puis cliquez sur **Modifier**.
14. Dans l'arborescence de la console Éditeur de gestion des stratégies de groupe, développez **Configuration Utilisateur**, **Stratégies**, **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordenateur local** et **Panneau de configuration**, puis cliquez sur **Personnalisation**.
15. Double-cliquez sur le paramètre de stratégie **Dépassement du délai d'expiration de l'écran de veille**.
16. Cliquez sur **Activé**.
17. Dans la zone **Secondes**, saisissez **2700**, puis cliquez sur **OK**.
18. Dans l'arborescence de la console, développez **Configuration ordinateur**, **Stratégies**, **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordenateur local** et **Système**, puis cliquez sur **Stratégie de groupe**.
19. Double-cliquez sur le paramètre de stratégie **Configurer le mode de traitement par boucle de la stratégie de groupe utilisateur**.
20. Cliquez sur **Activé**.
21. Dans la liste déroulante **Mode**, sélectionnez **Fusionner**, puis cliquez sur **OK**.
22. Fermez l'Éditeur de gestion des stratégies de groupe.

Résultats : À la fin de cet exercice, vous devez avoir correctement configuré l'étendue requise des objets de stratégie de groupe.

Exercice 3 : Vérification de l'application des objets de stratégie de groupe

▶ Tâche 1 : Exécuter l'analyse du jeu de stratégie résultant (RSoP)

1. Basculez vers LON-CL1.
2. Vérifiez que vous êtes connecté en tant que ADATUM\Pat. S'il y a lieu, indiquez le mot de passe **Pa$$w0rd**.
3. Placez le pointeur de votre souris dans le coin inférieur droit de l'écran, puis cliquez sur **Accueil**.
4. Cliquez avec le bouton droit sur l'écran d'accueil, puis cliquez sur **Toutes les applications**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR – MCT UNIQUEMENT

5. Dans la liste **Applications**, cliquez avec le bouton droit sur **Invite de commandes**, puis cliquez sur **Exécuter comme administrateur**.
6. Dans la boîte de dialogue **Contrôle de compte d'utilisateur**, dans la zone **Nom d'utilisateur**, saisissez **Administrateur**. Dans la zone **Mot de passe**, saisissez **Pa$$w0rd**. Cliquez sur **Oui**.
7. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpupdate.exe /force
```

8. Attendez la fin de la commande. Notez l'heure système actuelle, que vous devrez connaître pour une tâche ultérieure dans cet atelier pratique. Pour enregistrer l'heure système, saisissez la commande suivante, puis appuyez deux fois sur Entrée :

```
Time
```

9. Redémarrez LON-CL1.
10. Attendez que LON-CL1 redémarre avant de passer à la tâche suivante. N'ouvrez pas de session sur LON-CL1.
11. Basculez vers LON-DC1.
12. Basculez vers la console **Gestion de stratégie de groupe**.
13. Dans l'arborescence de la console, développez **Forêt. Adatum.com**, puis cliquez sur **Résultats de stratégie de groupe**.
14. Cliquez avec le bouton droit sur **Résultats de stratégie de groupe** et sélectionnez **Assistant Résultats de stratégie de groupe**.
15. Sur la page **Assistant Résultats de stratégie de groupe**, cliquez sur **Suivant**.
16. Sur la page **Sélection des ordinateurs**, cliquez sur **Un autre ordinateur**, saisissez **LON-CL1**, puis cliquez sur **Suivant**.
17. Sur la page **Sélection de l'utilisateur,** vérifiez que **Afficher les paramètres de stratégie de**, et **Sélectionner un utilisateur spécifique** sont sélectionnés, sélectionnez **ADATUM\Pat**, puis cliquez sur **Suivant**.
18. Sur la page **Aperçu des sélections**, passez en revue vos ajouts, puis cliquez sur **Suivant**.
19. Cliquez sur **Terminer**. Le rapport RSoP s'affiche dans le volet d'informations de la console.
20. Examinez les résultats de stratégie de groupe. Pour la configuration utilisateur et ordinateur, identifiez l'heure de la dernière actualisation de stratégie et la liste des objets Stratégie de groupe autorisés et refusés. Identifiez les composants qui ont été utilisés pour traiter les paramètres de stratégie.
21. Cliquez sur l'onglet **Détails**. Examinez les paramètres appliqués pendant l'application de stratégie utilisateur et ordinateur, puis identifiez l'objet de stratégie de groupe à partir duquel les paramètres ont été obtenus.
22. Cliquez sur l'onglet **Événements de stratégie**, puis localisez l'événement qui journalise l'actualisation de stratégie que vous avez déclenchée à l'aide de la commande GPUpdate dans la tâche 1.
23. Cliquez sur l'onglet **Résumé**, cliquez avec le bouton droit sur la page, puis sélectionnez **Enregistrer le rapport**.
24. Dans le volet de navigation, cliquez sur **Bureau**, puis cliquez sur **Enregistrer**.
25. Ouvrez le rapport RSoP à partir du bureau. Examinez le rapport RSoP, puis fermez-le.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Analysez RSoP avec GPResults

1. Ouvrez une session sur LON-CL1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Cliquez avec le bouton droit sur l'écran d'accueil, puis cliquez sur **Toutes les applications**.
3. Dans la liste **Applications**, cliquez sur **Invite de commandes**.
4. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpresult /r
```

   Les résultats récapitulatifs de RSoP sont affichés. Les informations sont très similaires à celles contenues dans l'onglet **Résumé** du rapport RSoP généré par l'Assistant Résultats de stratégie de groupe.

5. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpresult /v
```

   Vous constatez que beaucoup des paramètres de stratégie de groupe appliqués par le client sont répertoriés dans ce rapport.

6. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpresult /z
```

   Le rapport RSoP le plus détaillé est généré.

7. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpresult /h:"%userprofile%\Desktop\RSOP.html"
```

   Un rapport RSoP est enregistré comme fichier HTML sur votre bureau.

8. Ouvrez le rapport RSoP enregistré à partir de votre bureau.
9. Comparez le rapport, ses informations, et sa mise en forme avec le rapport RSoP que vous avez enregistré dans la tâche précédente.

▶ Tâche 3 : Évaluez les résultats de l'objet de stratégie de groupe à l'aide de l'Assistant Modélisation de stratégie de groupe.

1. Basculez vers LON-DC1.
2. Dans l'arborescence de la console Gestion des stratégies de groupe, développez **Forêt : Adatum.com**, puis cliquez sur **Modélisation de stratégie de groupe**.
3. Cliquez avec le bouton droit sur **Modélisation de stratégie de groupe**, puis cliquez sur **Assistant Modélisation de stratégie de groupe**. L'Assistant Modélisation de stratégie de groupe s'affiche.
4. Cliquez sur **Suivant**.
5. Sur la page **Sélection du contrôleur de domaine**, cliquez sur **Suivant**.
6. Sur la page **Sélection d'ordinateurs et d'utilisateurs**, dans la section **Informations sur l'utilisateur**, cliquez sur le bouton **Utilisateur**, puis cliquez sur **Parcourir**. La boîte de dialogue **Sélectionnez un utilisateur** s'affiche.

7. Saisissez **Mike**, puis appuyez sur Entrée.
8. Dans la section **Informations sur l'ordinateur**, cliquez sur le bouton **Ordinateur,** puis cliquez sur **Parcourir**. La boîte de dialogue **Sélectionnez un ordinateur** s'affiche.
9. Saisissez **LON-CL1**, puis appuyez sur Entrée.
10. Cliquez sur **Suivant**.
11. Sur la page **Options de simulation avancées**, activez la case à cocher **Traitement en boucle**, puis cliquez sur **Fusionner**. Bien que l'objet de stratégie de groupe Salle de conférence spécifie le traitement par boucle de rappel, vous devez indiquer à l'Assistant Modélisation de stratégie de groupe qu'il doit prendre en compte le traitement par boucle de rappel dans sa simulation.
12. Cliquez sur **Suivant**.
13. Sur la page **Autres chemins d'accès Active Directory,** cliquez sur le bouton **Parcourir** en regard de l'emplacement de l'ordinateur. La boîte de dialogue **Choisir un conteneur d'ordinateur** s'affiche.
14. Développez **Adatum** et **Bornes**, puis cliquez sur **Salles de conférence**. Vous simulez l'effet de LON-CL1 comme ordinateur de salle de conférence.
15. Cliquez sur **OK**.
16. Cliquez sur **Suivant**.
17. Sur la page **Groupes de sécurité utilisateur**, cliquez sur **Suivant**.
18. Sur la page **Groupe de sécurité ordinateur**, cliquez sur **Suivant**.
19. Sur la page **Filtres WMI pour Utilisateurs**, cliquez sur **Suivant**.
20. Sur la page **Filtres WMI pour Ordinateurs**, cliquez sur **Suivant**.
21. Passez en revue vos paramètres sur la page **Aperçu des sélections**, puis cliquez sur **Suivant**.
22. Cliquez sur **Terminer**.
23. Sur l'onglet **Détails**, faites défiler et développez, s'il y a lieu, **Détails de l'utilisateur**, **Objets de stratégie de groupe** et **Objets GPO appliqués**.
24. Vérifiez si l'objet de stratégie de groupe Stratégies de salle de conférence s'applique à Mike en tant que stratégie utilisateur lorsqu'il ouvre une session sur LON-CL1, si LON-CL1 se trouve dans l'unité d'organisation Salles de conférence.
25. Faites défiler et développez s'il y a lieu, **Détails de l'utilisateur, Stratégies, Modèles d'administration** et **Panneau de configuration/Personnalisation**.
26. Confirmez que le délai d'activation de l'écran de veille est de 2700 secondes (45 minutes), le paramètre configuré par l'objet de stratégie de groupe Stratégies de salle de conférence qui remplace la valeur par défaut de 10 minute configurée par l'objet de stratégie de groupe Normes ADATUM.

▶ Tâche 4 : Examinez les événements de stratégie et déterminez l'état d'infrastructure de l'objet de stratégie de groupe.

1. Basculez vers LON-CL1.
2. Placez le pointeur de votre souris dans le coin inférieur droit de l'écran, puis cliquez sur **Paramètres**. Cliquez sur **Panneau de configuration**.
3. Cliquez sur **Système et sécurité**.
4. Cliquez sur **Outils d'administration**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Double-cliquez sur **Observateur d'événements**.
6. Dans l'arborescence de la console, développez **Journaux Windows**, puis cliquez sur le journal **Système**.
7. Triez le journal système par **Source**.
8. Localisez les événements possédant la stratégie de groupe comme source. Vous pouvez même cliquer sur le lien Filtrer le journal actuel dans le volet Actions, puis sélectionner Stratégie de groupe dans la liste déroulante Sources de l'événement.
9. Examinez les informations associées aux événements de stratégie de groupe.
10. Dans l'arborescence de la console, cliquez sur le journal **Application**.
11. Triez le journal des applications selon la colonne **Source**.
12. Examinez les événements et identifiez les événements de stratégie de groupe qui ont été écrits dans ce journal. Quels sont les événements liés à l'application de stratégie de groupe et ceux liés aux activités effectuées pour gérer la stratégie de groupe ? Notez que, selon la durée d'exécution de l'ordinateur virtuel, il peut n'y avoir aucun événement de stratégie de groupe dans le journal des applications.
13. Dans l'arborescence de la console, développez **Journaux des applications et des services**, **Microsoft**, **Windows**, et **GroupPolicy**, puis cliquez sur **Opérationnel**.
14. Localisez le premier événement associé à l'actualisation de la stratégie de groupe que vous avez initialisée dans l'exercice 1 à l'aide de la commande **GPUpdate**. Examinez cet événement et les événements qui l'ont suivi.

Résultats : À la fin de cet exercice, vous devez avoir utilisé avec succès les outils RSoP pour vérifier l'application correcte de vos objets de stratégie de groupe.

Exercice 4 : Gestion des objets de stratégie de groupe

▶ Tâche 1 : Exécuter une sauvegarde des objets de stratégie de groupe.

1. Basculez vers LON-DC1.
2. Basculez vers la console **Gestion de stratégie de groupe** puis cliquez sur le nœud **Objets de stratégie de groupe**.
3. Dans le volet d'informations, cliquez avec le bouton droit sur **Normes ADATUM**, puis cliquez sur **Sauvegarder**.
4. Dans la boîte de dialogue **Sauvegarde de l'objet GPO**, dans la zone **Emplacement**, saisissez **C:**.
5. Cliquez sur **Sauvegarder**.
6. Dans la boîte de dialogue **Sauvegarder**, cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Exécuter une restauration d'objets de stratégie de groupe.

1. Dans le volet d'informations de la console Gestion des stratégies de groupe, cliquez avec le bouton droit sur **Normes ADATUM**, puis cliquez sur **Restaurer à partir d'une sauvegarde**.
2. Dans la boîte de dialogue **Assistant Restauration d'objet de stratégie de groupe**, cliquez sur **Suivant**.
3. Sur la page **Emplacement de sauvegarde**, cliquez sur **Suivant**.
4. Sur la page **Objet de stratégie de groupe source**, cliquez sur **Suivant**.
5. Sur la page **Fin de l'Assistant Restauration d'objet de stratégie de groupe**, cliquez sur **Terminer**.
6. Dans la boîte de dialogue **Restaurer**, cliquez sur **OK**.
7. Fermez toutes les fenêtres.

▶ Pour préparer le module suivant

Une fois l'atelier terminé, rétablissez tous les ordinateurs virtuels à leurs états initiaux.

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V®.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22411B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22411B-LON-CL1**.

Résultats : Implémentation d'une infrastructure de stratégie de groupe À la fin de cet exercice, vous devez avoir effectué avec succès des tâches de gestion courantes sur vos objets de stratégie de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 6: Gestion des bureaux des utilisateurs avec la stratégie de groupe

Atelier pratique : Gestion des bureaux des utilisateurs avec la stratégie de groupe

Exercice 1 : Implémentation des paramètres à l'aide des préférences de stratégie de groupe

▶ Tâche 1 : Créer le script d'ouverture de session requis

1. Ouvrez une session sur LON-DC1 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 le volet de navigation, cliquez sur **Ordinateur**.
4. Dans le volet d'informations, double-cliquez sur **Disque local (C:)** puis, sous l'onglet **Accueil**, cliquez sur **Nouveau dossier**.
5. Nommez le nouveau dossier **Branch1**.
6. Cliquez avec le bouton droit sur le dossier **Branch1**, sélectionnez **Partager avec**, puis cliquez sur **Des personnes spécifiques**.
7. Dans la boîte de dialogue **Partage de fichiers**, cliquez sur la flèche de déroulement et sélectionnez **Tout le monde**, puis cliquez sur **Ajouter**.
8. Pour le groupe **Tout le monde**, cliquez sur la flèche de déroulement **Niveau d'autorisation**, puis sélectionnez **Lecture/écriture**.
9. Cliquez sur **Partager**, puis sur **Terminé**.
10. Fermez la fenêtre Disque local (C:).
11. Suspendez votre pointeur de souris dans le coin inférieur droit de l'écran, puis cliquez sur **Accueil**.
12. Saisissez **Bloc-notes**, puis appuyez sur Entrée.
13. Dans le Bloc-notes, saisissez **Net use S: \\LON-DC1\Branch1**.
14. Cliquez sur le menu **Fichier**, puis sur **Enregistrer**.
15. Dans la boîte de dialogue **Enregistrer sous**, dans la zone **Nom du fichier,** saisissez **BranchScript.bat**.
16. Dans la liste **Type,** sélectionnez **Tous les fichiers**.
17. Dans le volet de navigation, cliquez sur **Bureau**, puis cliquez sur **Enregistrer**.
18. Fermez le Bloc-notes.
19. Sur le Bureau, cliquez avec le bouton droit sur le fichier **BranchScript.bat**, puis cliquez sur **Copier**. Vous collerez le fichier dans le dossier approprié plus tard dans l'atelier pratique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer un nouvel objet de stratégie de groupe et le lier à l'unité d'organisation Filiale 1

1. Sur la machine LON-DC1, suspendez le pointeur de votre souris dans le coin inférieur droit de l'écran, puis cliquez sur **Accueil**.
2. Cliquez sur **Outils d'administration**.
3. Dans Outils d'administration, double-cliquez sur **Utilisateurs et ordinateurs Active Directory**.
4. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez sur **Adatum.com**.
5. Cliquez avec le bouton droit sur **Adatum.com**, pointez la souris sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
6. Dans la boîte de dialogue **Nouvel objet – Unité d'organisation**, dans la zone **Nom**, saisissez **Filiale 1**, puis cliquez sur **OK**.
7. Dans le volet de navigation, cliquez sur **IT**.
8. Dans le volet d'informations, cliquez avec le bouton droit sur **Holly Dickson**, puis cliquez sur **Déplacer**.
9. Dans la boîte de dialogue **Déplacer**, cliquez sur **Filiale 1**, puis cliquez sur **OK**.
10. Dans le volet de navigation, cliquez sur **Computers**.
11. Dans le volet d'informations, cliquez avec le bouton droit sur **LON-CL1**, puis cliquez sur **Déplacer**.
12. Dans la boîte de dialogue **Déplacer**, cliquez sur **Filiale 1**, puis cliquez sur **OK**.
13. Suspendez votre pointeur de souris dans le coin inférieur droit de l'écran, puis cliquez sur **Accueil**.
14. Cliquez sur **Outils d'administration**, puis double-cliquez sur **Gestion des stratégies de groupe**.
15. Développez la **Forêt : Adatum.com**, développez **Domaines**, puis développez **Adatum.com**.
16. Cliquez avec le bouton droit sur **Filiale 1**, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**.
17. Dans la boîte de dialogue **Nouvel objet GPO**, dans la zone **Nom**, saisissez **Branch1**, puis cliquez sur **OK**.
18. Dans le volet de navigation, cliquez sur **Objets de stratégie de groupe**.
19. Cliquez avec le bouton droit sur l'objet de stratégie de groupe **Branch1**, puis cliquez sur **Modifier**.
20. Dans l'éditeur de gestion des stratégies de groupe, développez **Configuration utilisateur**, **Stratégies**, **Paramètres Windows**, puis cliquez sur **Scripts (ouverture/fermeture de session)**.
21. Dans le volet d'informations, double-cliquez sur **Ouverture de session**.
22. Dans la boîte de dialogue **Propriétés de : Ouverture de session**, cliquez sur **Afficher les fichiers**.
23. Dans le volet d'informations, cliquez avec le bouton droit dans une zone vide puis sur **Coller**.
24. Fermez la fenêtre Logon.
25. Dans la boîte de dialogue **Propriétés de : Ouverture de session**, cliquez sur **Ajouter**.
26. Dans la boîte de dialogue **Ajout d'un script**, cliquez sur **Parcourir**.
27. Cliquez sur le script **BranchScript.bat**,puis cliquez sur **Ouvrir**.
28. Cliquez à deux reprises sur **OK** pour fermer toutes les boîtes de dialogue.
29. Fermez l'Éditeur de gestion des stratégies de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Modifier la stratégie de domaine par défaut avec les préférences de stratégie de groupe requises

1. Dans la console de gestion des stratégies de groupe, cliquez sur le dossier **Objets de stratégie de groupe** puis, dans le volet d'informations, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
2. Développez **Configuration utilisateur**, **Préférences**, **Paramètres Windows**, cliquez avec le bouton droit sur **Raccourcis**, pointez la souris sur **Nouveau**, puis cliquez sur **Raccourci**.
3. Dans la boîte de dialogue **Nouvelles propriétés de Raccourci**, dans la liste **Actions**, cliquez sur **Créer**.
4. Dans la zone **Nom**, saisissez **Bloc-notes**.
5. Dans la zone **Emplacement**, cliquez sur la flèche, puis sélectionnez **Bureau**.
6. Dans la zone **Chemin d'accès cible**, saisissez **C:\Windows\Notepad.exe**.
7. Sur l'onglet **Commun**, activez la case à cocher **Ciblage au niveau de l'élément**, puis cliquez sur **Ciblage**.
8. Dans la boîte de dialogue **Éditeur cible**, cliquez sur **Nouvel élément**, puis cliquez sur **Groupe de sécurité**.
9. Dans la partie inférieure de la boîte de dialogue, cliquez sur le bouton de sélection.
10. Dans la boîte de dialogue **Sélectionner un groupe**, dans la zone de texte **Entrez le nom de l'objet à sélectionner (exemples)**, saisissez **IT**, puis cliquez sur **OK**.
11. Cliquez sur **OK** à deux reprises.
12. Fermez toutes les fenêtres.

▶ Tâche 4 : Tester les préférences

1. Basculez vers LON-CL1.
2. Suspendez le pointeur de votre souris dans le coin inférieur droit de l'écran puis cliquez sur **Paramètres**.
3. Cliquez sur **Marche/Arrêt**, puis sur **Redémarrer**.
4. Lorsque l'ordinateur est redémarré, ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
5. Dans l'écran Accueil, saisissez **cmd.exe**, puis appuyez sur Entrée.
6. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

7. Déconnectez-vous de LON-CL1.
8. Connectez-vous en tant que **ADATUM\Holly** avec le mot de passe **Pa$$word**.
9. Cliquez sur **Bureau** et, sur la barre des tâches, cliquez sur **Explorateur de fichiers**.
10. Examinez le volet de navigation, puis vérifiez que vous possédez un lecteur mappé à \\lon-dc1\Branch1.
11. Vérifier que le raccourci vers le Bloc-notes a été ajouté sur le Bureau de Holly.

12. Si le raccourci n'apparaît pas, répétez les étapes 4 à 8.
13. Se déconnecter de la machine LON-CL1.

Résultats : À la fin de cet exercice, vous devriez avoir créé les scripts et les paramètres de préférence requis avec succès, et les avoir alors attribués à l'aide des objets de stratégie de groupe.

Exercice 2 : Configuration de la redirection de dossiers

▶ Tâche 1 : Créer un répertoire partagé pour stocker les dossiers redirigés

1. Dans la barre des tâches de LON-DC1, cliquez sur **Explorateur de fichiers**.
2. Dans le volet de navigation, cliquez sur **Ordinateur**.
3. Dans le volet d'informations, double-cliquez sur **Disque local (C:)** puis, sous l'onglet **Accueil**, cliquez sur **Nouveau dossier**.
4. Nommez le nouveau dossier **Branch1Redirect**.
5. Cliquez avec le bouton droit sur le dossier **Branch1Redirect**, sélectionnez **Partager avec**, puis cliquez sur **Des personnes spécifiques**.
6. Dans la boîte de dialogue **Partage de fichiers**, cliquez sur la flèche de déroulement et sélectionnez **Tout le monde**, puis cliquez sur **Ajouter**.
7. Pour le groupe **Tout le monde**, cliquez sur la flèche de déroulement **Niveau d'autorisation**, puis cliquez sur **Lecture/écriture**.
8. Cliquez sur **Partager**, puis sur **Terminé**.
9. Fermez la fenêtre Disque local (C:).

▶ Tâche 2 : Créer un nouvel objet de stratégie de groupe et le lier à l'unité d'organisation de la filiale

1. Sur LON-DC1, dans le gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans Gestion des stratégies de groupe, développez **Forêt : Adatum.com**, développez **Domaines**, puis développez **Adatum.com**.
3. Cliquez avec le bouton droit sur **Filiale 1**, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**. Cliquez sur **OK**.
4. Dans la boîte de dialogue **Nouvel objet GPO**, dans la zone **Nom**, saisissez **Redirection de dossiers**, puis cliquez sur **OK**.

▶ Tâche 3 : Modifier les paramètres de redirection de dossiers dans la stratégie

1. Développez **Filiale 1**, cliquez avec le bouton droit sur **Redirection de dossiers**, puis cliquez sur **Modifier**.
2. Dans l'éditeur de gestion des stratégies de groupe, développez **Configuration utilisateur**, **Stratégies**, **Paramètres Windows**, puis **Redirection de dossiers**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Cliquez avec le bouton droit sur **Documents**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de : Documents**, sélectionnez l'onglet **Cible** et, à côté de **Paramètre**, cliquez sur la flèche de déroulement pour sélectionner **De base - Rediriger les dossiers de tout le monde vers le même emplacement**.
5. Vérifiez que la case **Emplacement du dossier cible** est définie sur **Créer un dossier pour chaque utilisateur sous le chemin d'accès racine**.
6. Dans la zone **Chemin d'accès de la racine**, saisissez **\\LON-DC1\Branch1Redirect**, puis cliquez sur **OK**.
7. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
8. Fermez toutes les fenêtres ouvertes sur LON-DC1.

▶ Tâche 4 : Tester le paramètre de redirection de dossiers

1. Basculez vers LON-CL1.
2. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans l'écran Accueil, saisissez **cmd.exe**, puis appuyez sur Entrée.
4. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

5. Déconnectez-vous, puis reconnectez-vous en tant que **ADATUM\Holly** avec le mot de passe **Pa$$word**.
6. À partir du menu **Accueil**, cliquez sur **Bureau**.
7. Cliquez avec le bouton droit sur le Bureau, puis cliquez sur **Personnaliser**.
8. Dans le volet de navigation, cliquez sur **Changer les icônes du bureau**.
9. Dans les **Paramètres des icônes du bureau**, activez la case à cocher **Fichiers de l'utilisateur** puis cliquez sur **OK**.
10. Sur le bureau, double-cliquez sur **Holly Dickson**.
11. Cliquez avec le bouton droit sur **Mes documents**, puis cliquez sur **Propriétés**.
12. Dans la boîte de dialogue **Propriétés de : Mes documents**, remarquez que l'emplacement du dossier est désormais le partage réseau dans un sous-dossier nommé comme l'utilisateur.
13. Si la redirection de dossiers n'est pas claire, déconnectez-vous, et connectez-vous en tant que **ADATUM\Holly** avec le mot de passe **Pa$$word**. Répétez les étapes 10 à 12.
14. Déconnectez-vous de LON-CL1.

Résultats : À la fin de cet exercice, vous devriez avoir configuré avec succès la redirection de dossiers vers un dossier partagé sur le serveur LON-DC1.

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 cela, procédez comme suit :

15. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
16. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22411B-LON-DC1**, puis cliquez sur **Rétablir**.
17. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
18. Répétez les étapes 2 et 3 pour **22411B-LON-CL1**.

Résultats : À la fin de cet exercice, vous devriez avoir configuré avec succès la redirection de dossiers vers un dossier partagé sur le serveur LON-DC1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 7: Configuration et résolution des problèmes d'accès à distance

Atelier pratique A : Configuration de l'accès à distance

Exercice 1 : Configurer un serveur de réseau privé virtuel

▶ Tâche 1 : Configurer les certificats serveur et client

1. Basculez vers LON-DC1.

   Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Autorité de certification**.

3. Dans la console de gestion certsrv, développez **Adatum-LON-DC1-CA**, cliquez avec le bouton droit sur **Modèles de certificats**, puis cliquez sur **Gérer**.

4. Dans le volet d'informations de la Console des modèles de certificat, cliquez avec le bouton droit sur **Ordinateur**, puis cliquez sur **Propriétés**.

5. Dans la boîte de dialogue **Propriétés de : Ordinateur**, cliquez sur l'onglet **Sécurité**, puis sur **Utilisateurs authentifiés**.

6. Dans **Autorisations pour Utilisateurs authentifiés**, activez la case à cocher **Autoriser** pour l'autorisation **Inscrire**, puis cliquez sur **OK**.

7. Fermez la Console des modèles de certificat.

8. Dans **certsrv – [Autorité de certification (local)]**, cliquez avec le bouton droit sur **Adatum-LON-DC1-CA**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Arrêter le service**.

9. Cliquez avec le bouton droit sur **Adatum-LON-DC1-CA**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Accueil le service.**

10. Fermez la console de gestion certsrv.

11. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de stratégie de groupe**.

12. Dans le volet de liste Gestion des stratégies de groupe, développez **Forêt : Adatum.com**, développez **Domaines**, puis développez **Adatum.com**.

13. Dans le volet de liste, sous Adatum.com, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.

14. Dans l'Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, développez successivement **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, puis **Stratégies de clé publique**.

15. Dans le volet de navigation, cliquez avec le bouton droit sur **Paramètres de demande automatique de certificat**, pointez le curseur sur **Nouveau**, puis cliquez sur **Demande automatique de certificat**.

16. Dans l'**Assistant Création de demandes automatiques de certificats**, cliquez sur **Suivant**.

17. Sur la page **Modèle de certificat**, acceptez le paramètre par défaut d'**Ordinateur**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Sur la page **Fin de l'Assistant Création de demandes automatiques de certificats**, cliquez sur **Terminer**.
19. Fermez l'Éditeur de gestion des stratégies de groupe.
20. Fermez **Gestion de stratégie de groupe**.
21. Basculez vers l'ordinateur LON-RTR, puis ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
22. Suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur Accueil.
23. Saisissez **mmc.exe**, puis appuyez sur Entrée.
24. Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
25. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez successivement sur **Certificats**, **Ajouter**, **Un compte d'ordinateur**, **Suivant**, puis sur **Terminer**.
26. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **OK**.
27. Dans l'arborescence de la console, développez **Certificats**, cliquez avec le bouton droit sur **Personnel**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Demander un Nouveau certificat**.
28. Dans la boîte de dialogue **Inscription de certificats**, cliquez sur **Suivant**.
29. Sur la page **Sélectionner la stratégie d'inscription de certificat**, cliquez sur **Stratégie d'inscription à Active Directory**, puis sur **Suivant**.
30. Activez la case à cocher **Ordinateur**, puis cliquez sur **Inscription**.
31. Vérifiez que l'état d'installation du certificat indique Réussite, puis cliquez sur **Terminer**.
32. Fermez la fenêtre Console1.
33. Lorsque vous êtes invité à enregistrer les paramètres de la console, cliquez sur **Non**.
34. Basculez vers LON-CL2, puis ouvrez une session avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.
35. Dans Accueil, tapez **cmd.exe**, puis appuyez sur Entrée.
36. À l'invite de commandes, saisissez **gpupdate /force**, puis appuyez sur Entrée.
37. Fermez la fenêtre d'invite de commandes.
38. Suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
39. Dans Accueil, saisissez **mmc**, puis appuyez sur Entrée.
40. Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
41. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez successivement sur **Certificats**, **Ajouter**, **Un compte d'ordinateur**, **Suivant**, puis sur **Terminer**.
42. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **OK**.
43. Dans l'arborescence de la console, développez successivement **Certificats** et **Personnel**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

44. Vérifiez qu'un certificat émis par Adatum-LON-DC1-CA existe pour LON-CL2.
45. Fermez la fenêtre Console1.
46. Lorsque vous êtes invité à enregistrer les paramètres de la console, cliquez sur **Non**.

▶ Tâche 2 : Configurer le rôle Accès à distance

1. Basculez vers LON-RTR.
2. Si nécessaire, cliquez sur **Gestionnaire de serveur** dans la barre des tâches.
3. Dans le volet Détails, cliquez sur **Ajouter des rôles et des fonctionnalités**.
4. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le type d'installation**, vérifiez que **Installation basée sur un rôle ou une fonctionnalité** est sélectionné, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services de stratégie et d'accès réseau**.
8. Cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant** à deux reprises.
9. Sur la page **Services de stratégie et d'accès réseau**, cliquez sur **Suivant**.
10. Sur la page **Sélectionner des services de rôle**, vérifiez que la case à cocher **Serveur NPS (Network Policy Server)** est activée, puis cliquez sur **Suivant**.
11. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
12. Vérifiez que l'installation a réussi, puis cliquez sur **Fermer**.
13. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Serveur NPS (Network Policy Server)**.
14. Dans le volet de navigation du Gestionnaire de stratégies réseau, cliquez avec le bouton droit sur **NPS (local)**, puis cliquez sur **Inscrire un serveur dans Active Directory**.
15. Dans la zone de message **Serveur NPS (Network Policy Server)**, cliquez sur **OK**.
16. Dans la boîte de dialogue **Serveur NPS (Network Policy Server)** suivante, cliquez sur **OK**.
17. Laissez la fenêtre de la console Serveur NPS (Network Policy Server) ouverte.
18. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Routage et accès distant**. Dans l'**Assistant Activation de DirectAccess**, cliquez sur **Annuler**, puis sur **OK**.
19. Dans la console Routage et accès distant, cliquez avec le bouton droit sur **LON-RTR (local)**, puis cliquez sur **Désactiver le routage et l'accès à distance**.
20. Dans la boîte de dialogue, cliquez sur **Oui**.
21. Dans la console Routage et accès distant, cliquez avec le bouton droit sur **LON-RTR (local)**, puis cliquez sur **Configurer et activer le routage et l'accès à distance**.
22. Cliquez sur **Suivant**, sélectionnez **Accès à distance (connexion à distance ou VPN)**, puis cliquez sur **Suivant**.
23. Activez la case à cocher **VPN**, puis cliquez sur **Suivant**.
24. Cliquez sur l'interface réseau **Connexion au réseau local 2**. Désactivez la case à cocher **Sécuriser l'interface sélectionnée en configurant des filtres de paquet statiques**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

25. Sur la page **Attribution d'adresses IP**, cliquez sur **À partir d'une plage d'adresses spécifiée**, puis cliquez sur **Suivant**.
26. Sur la page **Assignation de plages d'adresses**, cliquez sur **Nouveau**. Dans la zone de texte Adresse IP de début, saisissez **172.16.0.100**, dans la zone de texte Adresse IP de fin, saisissez **172.16.0.110**, puis cliquez sur **OK**.
27. Vérifiez que 11 adresses IP ont été attribuées aux clients distants, puis cliquez sur **Suivant**.
28. Sur la page **Gestion de serveurs d'accès à distance multiples**, cliquez sur **Suivant**.
29. Cliquez sur **Terminer**.
30. Dans la boîte de dialogue **Routage et accès distant**, cliquez sur **OK**.
31. Si vous y êtes invité, cliquez de nouveau sur **OK**.

▶ Tâche 3 : Créer une stratégie réseau pour les clients d'un réseau privé virtuel (VPN)

1. Dans LON-RTR, basculez vers **Serveur NPS (Network Policy Server)**.
2. Dans Serveur NPS (Network Policy Server), développez **Stratégies**, puis cliquez sur **Stratégies réseau**.
3. Dans le volet d'informations, cliquez avec le bouton droit sur la première stratégie de la liste, puis cliquez sur **Désactiver**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur la dernière stratégie de la liste, puis cliquez sur **Désactiver**.
5. Dans le volet de navigation, cliquez avec le bouton droit sur **Stratégies réseau**, puis cliquez sur **Nouveau**.
6. Dans l'Assistant Nouvelle stratégie réseau, dans la zone de texte **Nom de la stratégie**, saisissez **Stratégie VPN pilote informatique**.
7. Dans la liste **Type de serveur d'accès réseau**, cliquez sur **Serveur d'accès à distance (VPN-Dial up)**, puis sur **Suivant**.
8. Sur la page **Spécifier les conditions**, cliquez sur **Ajouter**.
9. Dans la boîte de dialogue **Sélectionner une condition**, cliquez sur **Groupes Windows**, puis cliquez sur **Ajouter**.
10. Dans la boîte de dialogue **Groupes Windows**, cliquez sur **Ajouter des groupes**.
11. Dans la boîte de dialogue **Sélectionnez un groupe**, dans la zone de texte **Entrez le nom de l'objet à sélectionner (exemples)**, saisissez **IT**, puis cliquez sur **OK**.
12. Cliquez de nouveau sur **OK**, cliquez sur **Suivant**, et sur la page **Spécifier l'autorisation d'accès**, cliquez sur **Accès accordé**, puis sur **Suivant**.
13. Sur la page **Configurer les méthodes d'authentification**, désactivez la case à cocher **Authentification chiffrée Microsoft (MS-CHAP)**, puis cliquez sur **Suivant**.
14. Sur la page **Configurer des contraintes**, cliquez sur **Restrictions relatives aux jours et aux heures**.
15. Activez la case à cocher **Autoriser l'accès les jours suivants et à ces horaires uniquement**, puis cliquez sur **Modifier**.
16. Dans la boîte de dialogue **Restrictions relatives aux jours et aux heures**, cliquez sur **Dimanche**, puis cliquez sur **Refusés**.
17. Cliquez sur **Samedi**, sur **Refusés**, puis sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Cliquez sur **Suivant**.
19. Sur la page **Configurer les paramètres**, cliquez sur **Suivant**.
20. Sur la page **Fin de la configuration de la nouvelle stratégie réseau**, cliquez sur **Terminer**.

Résultats : À la fin de cet exercice, vous devriez avoir déployé un serveur VPN et configuré l'accès pour les membres du groupe de sécurité global informatique.

Exercice 2 : Configuration de clients VPN

▶ Tâche 1 : Configurer et distribuer un profil Kit d'administration du Gestionnaire des connexions

1. Basculez vers LON-CL2.
2. Suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
3. Dans l'écran d'accueil, tapez **Panneau**, puis dans la liste **Applications**, cliquez sur **Panneau de configuration**.
4. Cliquez sur **Programmes**, puis cliquez sur **Activer ou désactiver des fonctionnalités Windows**.
5. Dans Fonctionnalités de Windows, activez la case à cocher **Kit d'administration du Gestionnaire des connexions Microsoft (CMAK) RAS**, puis cliquez sur **OK**.
6. Cliquez sur **Fermer**.
7. Dans le Panneau de configuration, cliquez sur **Page d'accueil du Panneau de configuration**.
8. Dans la liste **Afficher par**, cliquez sur **Grandes icônes**.
9. Cliquez sur **Outils d'administration**, puis double-cliquez sur **Kit d'administration du Gestionnaire des connexions**.
10. Dans l'Assistant Kit d'administration du Gestionnaire des connexions, cliquez sur **Suivant**.
11. Sur la page **Sélectionner le système d'exploitation cible**, vérifiez que **Windows Vista ou version ultérieure** est sélectionné, puis sur **Suivant**.
12. Sur la page **Créer ou modifier un profil Gestionnaire des connexions**, vérifiez que **Nouveau profil** est sélectionné, puis sur **Suivant**.
13. Sur la page **Spécifier les noms de service et de fichier**, dans la zone de texte **Nom du service**, saisissez **VPN pilote Adatum**, dans la zone de texte **Nom du fichier**, saisissez **Adatum**, puis cliquez sur **Suivant**.
14. Sur la page **Spécifier un nom de domaine**, cliquez sur **Ne pas ajouter de nom de domaine Kerberos au nom d'utilisateur**, puis sur **Suivant**.
15. Sur la page **Fusionner des informations à partir d'autres profils**, cliquez sur **Suivant**.
16. Sur la page **Ajouter une prise en charge des connexions VPN**, activez la case à cocher **Annuaire de ce profil**.
17. Dans la zone de texte **Nom de serveur VPN ou adresse IP**, saisissez **10.10.0.1**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Sur la page **Créer ou modifier une entrée VPN**, cliquez sur **Modifier**.
19. Dans la boîte de dialogue **Modifier l'entrée VPN**, cliquez sur l'onglet **Sécurité**.
20. Dans la liste **Stratégie VPN**, cliquez sur **Utiliser uniquement le protocole L2TP (Protocole Layer two Tunneling Protocol)**, puis cliquez sur **OK**.
21. Cliquez sur **Suivant**.
22. Sur la page **Ajouter un annuaire téléphonique personnalisé**, désactivez la case à cocher **Téléchargement automatique des mises à jour de l'annuaire téléphonique**, puis cliquez sur **Suivant**.
23. Sur la page **Configurer des entrées d'accès à distance**, cliquez sur **Suivant**.
24. Sur la page **Spécifier des mises à jour de table de routage**, cliquez sur **Suivant**.
25. Sur la page **Configurer les paramètres proxy pour Internet Explorer**, cliquez sur **Suivant**.
26. Sur la page **Ajouter des actions personnalisées**, cliquez sur **Suivant**.
27. Sur la page **Afficher une image bitmap de connexion personnalisée**, cliquez sur **Suivant**.
28. Sur la page **Afficher une image bitmap d'annuaire téléphonique personnalisée**, cliquez sur **Suivant**.
29. Sur la page **Afficher des icônes personnalisées**, cliquez sur **Suivant**.
30. Sur la page **Inclure un fichier d'aide personnalisé**, cliquez sur **Suivant**.
31. Sur la page **Afficher des informations de support technique personnalisées**, cliquez sur **Suivant**.
32. Sur la page **Afficher un contrat de licence personnalisé**, cliquez sur **Suivant**.
33. Sur la page **Installer des fichiers supplémentaires avec le profil Gestionnaire des connexions**, cliquez sur **Suivant**.
34. Sur la page **Générer le profil Gestionnaire des connexions et son programme**, cliquez sur **Suivant**.
35. Sur la page **Votre profil Gestionnaire des connexions est terminé et prêt à être distribué**, cliquez sur **Terminer**.
36. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
37. Dans la zone d'adresse de l'Explorateur de fichiers, saisissez **C:\Programmes\CMAK\Profils\Windows Vista and above\Adatum**, puis appuyez sur Entrée.
38. Double-cliquez sur **Adatum.exe**.
39. Dans la boîte de dialogue **VPN pilote Adatum**, cliquez sur **Oui**.
40. Dans la deuxième boîte de dialogue **VPN pilote Adatum**, cliquez sur **Tous les utilisateurs**, puis sur **OK**.
41. Dans la boîte de dialogue **VPN pilote Adatum**, cliquez sur **Annuler**.

▶ Tâche 2 : Vérifier l'accès au client

1. Déconnectez-vous de LON-CL2.
2. Ouvrez une session en tant qu'**ADATUM\April** avec le mot de passe **Pa$$w0rd**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans l'écran d'accueil, tapez **Panneau**, puis dans la liste **Applications**, cliquez sur **Panneau de configuration**.
4. Dans le Panneau de configuration, cliquez sur **Réseau et Internet**.
5. Dans la fenêtre Réseau et Internet, cliquez sur **Centre Réseau et partage**.
6. Dans Centre Réseau et partage, cliquez sur **Modifier les paramètres de la carte**.
7. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur la connexion **VPN pilote Adatum**, puis cliquez sur **Connecter/Déconnecter**.
8. Dans la liste Réseaux de droite, cliquez sur **VPN pilote Adatum**, puis sur **Connexion**.
9. Dans **VPN pilote Adatum**, dans la zone de texte **Nom d'utilisateur**, saisissez **ADATUM\April**.
10. Dans la zone de texte **Mot de passe**, saisissez **Pa$$w0rd**.
11. Activez la case à cocher **Enregistrer le mot de passe**, puis cliquez sur **Connexion**.
12. Attendez que la connexion VPN soit établie.
13. Fermez toutes les fenêtres.

▶ Pour préparer l'atelier suivant

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V®.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22411B-LON-CL2**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22411B-LON-RTR** et **22411B-LON-DC1**.

Résultats : À la fin de cet exercice, vous aurez distribué avec succès un profil CMAK et testé l'accès VPN.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique B : Configuration de DirectAccess

Exercice 1 : Configuration de l'infrastructure DirectAccess

▶ Tâche 1 : Configurer les services de domaine Active Directory (AD DS) et du système DNS (Domain Name System)

1. Créez un groupe de sécurité pour les ordinateurs clients Windows® DirectAccess en procédant comme suit :
   a. Basculez vers LON-DC1.
   b. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
   c. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
   d. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Adatum.com**, cliquez sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
   e. Dans la fenêtre Nouvel objet - Unité d'organisation, dans la zone de texte **Nom**, saisissez **DA_Clients OU**, puis cliquez sur **OK**.
   f. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **DA_Clients OU**, cliquez sur **Nouveau**, puis cliquez sur **Groupe**.
   g. Dans la boîte de dialogue **Nouvel objet - Groupe**, sous **Nom du groupe**, saisissez **DA_Clients**.
   h. Sous **Étendue du groupe**, vérifiez que **Globale** est sélectionné, sous **Type de groupe**, vérifiez que **Sécurité** est sélectionné, puis cliquez sur **OK**.
   i. Dans le volet d'informations, double-cliquez sur **DA_Clients**.
   j. Dans la boîte de dialogue **Propriétés de : DA_Clients**, cliquez sur l'onglet **Membres**, puis cliquez sur **Ajouter**.
   k. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des contacts, des ordinateurs, des comptes de service ou groupes**, cliquez sur **Types d'objets**, activez la case à cocher **des ordinateurs**, puis cliquez sur **OK**.
   l. Sous **Entrez les noms des objets à sélectionner (exemples)**, saisissez **LON-CL1**, puis cliquez sur **OK**.
   m. Vérifiez que LON-CL1 s'affiche correctement sous **Membres**, puis cliquez sur **OK**.
   n. Fermez la console Utilisateurs et ordinateurs Active Directory.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

2. Configurez les règles de pare-feu pour le trafic ICMPv6 en exécutant les étapes suivantes :

Remarque : Il est important de configurer des règles de pare-feu pour le trafic ICMPv6 afin de permettre l'essai suivant de DirectAccess dans l'environnement de test.

a. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de stratégie de groupe**.

b. Dans la Console de gestion des stratégies de groupe, développez **Forêt : Adatum.com**, développez **Domaines**, puis développez **Adatum.com**.

c. Sous Adatum.com, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.

d. Dans l'Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur** et développez successivement **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, **Pare-feu Windows avec fonctions avancées de sécurité**, puis cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité**.

e. Dans Pare-feu Windows avec fonctions avancées de sécurité, cliquez sur **Règles de trafic entrant**, cliquez avec le bouton droit sur **Règles de trafic entrant**, puis cliquez sur **Nouvelle règle**.

f. Sur la page **Type de règle**, cliquez sur **Personnalisée**, puis cliquez sur **Suivant**.

g. Sur la page **Programme**, cliquez sur **Suivant**.

h. Sur la page **Protocole et ports**, sous **Type de protocole**, cliquez sur **ICMPv6**, puis cliquez sur **Perso.**.

i. Dans la boîte de dialogue **Personnaliser les paramètres ICMP**, cliquez sur **Certains types ICMP**, cliquez sur **Requête d'écho**, puis cliquez sur **OK**.

j. Cliquez sur **Suivant**.

k. Sur la page **Étendue**, cliquez sur **Suivant**.

l. Sur la page **Action**, cliquez sur **Suivant**.

m. Sur la page **Profil**, cliquez sur **Suivant**.

n. Sur la page **Nom**, dans la zone de texte **Nom**, saisissez **Demandes Echo ICMPv6 entrantes**, puis cliquez sur **Terminer**.

o. Dans l'arborescence de la console, cliquez sur **Règles de trafic sortant**, cliquez avec le bouton droit sur **Règles de trafic sortant**, puis cliquez sur **Nouvelle règle**.

p. Sur la page **Type de règle**, cliquez sur **Personnalisée**, puis cliquez sur **Suivant**.

q. Sur la page **Programme**, cliquez sur **Suivant**.

r. Sur la page **Protocole et ports**, sous **Type de protocole**, cliquez sur **ICMPv6**,, puis cliquez sur **Perso.**.

s. Dans la boîte de dialogue **Personnaliser les paramètres ICMP**, cliquez sur **Certains types ICMP**, cliquez sur **Requête d'écho**, puis cliquez sur **OK**.

t. Cliquez sur **Suivant**.

u. Sur la page **Étendue**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

v. Sur la page **Action**, cliquez sur **Autoriser la connexion**, puis cliquez sur **Suivant**.

w. Sur la page **Profil**, cliquez sur **Suivant**.

x. Sur la page **Nom**, dans la zone de texte **Nom**, saisissez **Demandes Echo ICMPv6 sortantes**, puis cliquez sur **Terminer**.

y. Fermez l'Éditeur et la Console de gestion des stratégies de groupe.

3. Créez les enregistrements DNS requis en procédant comme suit :

a. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.

b. Dans la console du Gestionnaire DNS, développez **LON-DC1**, puis **Zones de recherche directes**, puis cliquez sur **Adatum.com**.

c. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.

d. Dans la zone de texte **Nom**, tapez **nls**. Dans la zone de texte **Adresse IP**, tapez **172.16.0.21**, cliquez sur **Ajouter un hôte**, puis cliquez sur **OK**.

e. Dans la boîte de dialogue **Nouvel hôte**, dans la zone de texte **Nom**, tapez **CRL**. Dans la zone de texte **Adresse IP**, saisissez **172.16.0.1**, puis cliquez sur **Ajouter un hôte**.

f. Dans la boîte de dialogue **DNS** vous informant que l'enregistrement a été créé, cliquez sur **OK**.

g. Dans la boîte de dialogue **Nouvel hôte**, cliquez sur **Terminé**.

h. Fermez la console du Gestionnaire DNS.

4. Supprimez le nom ISATAP de la liste rouge de requêtes globale DNS en procédant comme suit :

a. Déplacez le pointeur de la souris vers le coin inférieur droit, sélectionnez **Rechercher** dans le menu droit, puis saisissez **cmd.exe**. Appuyez sur Entrée.

b. Dans la fenêtre d'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
dnscmd /config /globalqueryblocklist wpad
```

c. Vérifiez que le message **La commande a été correctement exécutée** s'affiche.

d. Fermez la fenêtre d'invite de commandes.

5. Pour configurer le suffixe DNS sur LON-RTR en exécutant les étapes suivantes :

a. Basculez vers LON-RTR.

b. Déplacez le pointeur de la souris sur le coin inférieur droit de l'écran, cliquez sur **Paramètres**, cliquez sur **Panneau de configuration**, puis cliquez sur **Afficher l'état et la gestion du réseau**.

c. Dans la fenêtre Centre Réseau et partage, cliquez sur **Modifier les paramètres de la carte**.

d. Dans la fenêtre Connexion au réseau, cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Propriétés**.

e. Dans la fenêtre Propriétés de Connexion au réseau local, double-cliquez sur **Protocole Internet version 4 (TCP/IPv4)**.

f. Dans la boîte de dialogue **Proriétés de : Protocole Internet version 4 (TCP/IPv4)**, cliquez sur **Avancé**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

g. Dans l'onglet **DNS**, dans la zone de texte **Suffixe DNS pour cette connexion**, saisissez **Adatum.com**, puis cliquez sur **OK**.

h. Dans la boîte de dialogue **Proriétés de : Protocole Internet version 4 (TCP/IPv4)**, cliquez sur **OK**.

i. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, cliquez sur **OK**.

6. Configurez les propriétés de la connexion au réseau local 2 sur LON-RTR :

a. Dans la fenêtre Connexion au réseau, cliquez avec le bouton droit sur **Connexion au réseau local 2**, puis cliquez sur **Propriétés**.

b. Dans la fenêtre **Propriétés de Connexion au réseau local 2**, double-cliquez sur **Protocole Internet version 4 (TCP/IPv4)**.

c. Dans la boîte de dialogue **Proriétés de : Protocole Internet version 4 (TCP/IPv4)**, dans la zone de texte **Adresse IP**, saisissez **131.107.0.2**, et dans la zone de texte **Masque de sous-réseau**, saisissez **255.255.0.0**.

d. Cliquez sur **OK**, puis de nouveau sur **OK**.

e. Fermez Connexions réseau.

▶ Tâche 2 : Configurer les certificats

1. Pour configurer les paramètres de distribution de la liste de révocation de certificats (CRL), procédez comme suit :

a. Sur LON-DC1, dans le Gestionnaire de serveur, sur le menu **Outils,** cliquez sur **Autorité de certification**.

b. Dans le volet d'informations, cliquez avec le bouton droit sur **Adatum-LON-DC1-CA**, puis cliquez sur **Propriétés**.

c. Dans la boîte de dialogue **Propriétés de : Adatum-LON-DC1-CA**, cliquez sur l'onglet **Extensions**.

d. Dans l'onglet **Extensions**, cliquez sur **Ajouter**. Dans la zone de texte **Emplacement**, saisissez **http://crl.adatum.com/crld/**.

e. Sous **Variable**, cliquez sur <**NomAutoritéCertification**>, puis cliquez sur **Insérer**.

f. Sous **Variable**, cliquez sur <**SuffixeNomListeRévocationCertificats**>, puis cliquez sur **Insérer**.

g. Sous **Variable**, cliquez sur <**ListeRévocationCertificatsDeltaAutorisée**>, puis cliquez sur **Insérer**.

h. Dans la zone de texte **Emplacement**, à la fin de la chaîne **Emplacement**, saisissez **.crl**, puis cliquez sur **OK**.

i. Activez les cases à cocher **Inclure dans les listes de révocation de certificats. afin de pouvoir rechercher les listes de révocation des certificats delta** et **Inclure dans l'extension CDP des certificats émis**, puis cliquez sur **Appliquer**. Dans la boîte de dialogue demandant de redémarrer les services de certificats Active Directory, cliquez sur **Non**.

j. Cliquez sur **Ajouter**.

k. Dans la zone de texte **Emplacement**, saisissez **\\LON-RTR\crldist$**.

l. Sous **Variable**, cliquez sur <**NomAutoritéCertification**>, puis cliquez sur **Insérer**.

m. Sous **Variable**, cliquez sur <**SuffixeNomListeRévocationCertificats**>, puis cliquez sur **Insérer**.

n. Sous **Variable**, cliquez sur <**ListeRévocationCertificatsDeltaAutorisée**>, puis cliquez sur **Insérer**.

o. Dans la zone de texte **Emplacement**, à la fin de la chaîne, saisissez **.crl**, puis cliquez sur **OK**.

p. Activez les cases à cocher **Publier les listes de révocation des certificats à cet emplacement** et **Publier les listes de révocation des certificats delta à cet emplacement**, puis cliquez sur **OK**.

q. Cliquez sur **Oui** pour redémarrer les Services de certificats Active Directory.

2. Pour dupliquer le modèle de certificat Web et configurer une autorisation appropriée, procédez comme suit :

a. Dans la console Autorité de certification, développez **Adatum-LON-DC1-CA**, cliquez avec le bouton droit sur **Modèles de certificats**, puis cliquez sur **Gérer**.

Remarque : Les utilisateurs doivent posséder l'autorisation Inscription sur le certificat.

b. Dans la Console des modèles de certificat, dans le volet de contenu, cliquez avec le bouton droit sur le modèle **Serveur Web**, puis cliquez sur **Dupliquer le modèle**.

c. Cliquez sur l'onglet **Général** et dans la zone de texte **Nom complet du modèle**, saisissez **Certificat de serveur Web Adatum**.

d. Cliquez sur l'onglet **Traitement de la demande**, puis cliquez sur **Autoriser l'exportation de la clé privée**.

e. Cliquez sur l'onglet **Sécurité**, vérifiez que **Utilisateurs authentifiés** est sélectionné.

f. Dans la fenêtre Autorisations pour Utilisateurs authentifiés, sous **Autoriser**, cliquez sur **Inscrire**, puis cliquez sur **OK**.

g. Fermez la Console des modèles de certificat.

h. Dans la console Autorité de certification, cliquez avec le bouton droit sur **Modèles de certificats**, et naviguez jusqu'à **Nouveau/Modèle de certificat à délivrer**.

i. Cliquez sur **Certificat de serveur Web Adatum**, puis cliquez sur **OK**.

j. Dans certsrv – [Autorité de certification (local)], cliquez avec le bouton droit sur **Adatum-LON-DC1-CA**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Arrêter le service**.

k. Cliquez avec le bouton droit sur **Adatum-LON-DC1-CA**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Accueil le service**.

l. Fermez la console Autorité de certification.

3. Configurez l'inscription automatique de certificat de l'ordinateur en exécutant les étapes suivantes :

a. Sur LON-DC1, basculez sur le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de stratégie de groupe**.

b. Dans la Console de gestion des stratégies de groupe, développez **Forêt : Adatum.com**, développez **Domaines**, puis développez **Adatum.com**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

c. Dans la console Adatum.com, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.

d. Dans l'Éditeur de gestion des stratégies de groupe, développez successivement Configuration ordinateur,
Stratégies, Paramètres Windows, Paramètres de sécurité, puis Stratégies de clé publique.

e. Dans le volet d'informations de Stratégies de clé publique, cliquez avec le bouton droit sur **Paramètres de demande automatique de certificat**, pointez le curseur sur **Nouveau**, puis cliquez sur **Demande automatique de certificat**.

f. Dans l'Assistant Création de demandes automatiques de certificats, cliquez sur **Suivant**.

g. Sur la page **Modèle de certificat**, vérifiez que **Ordinateur** est sélectionné, cliquez sur **Suivant**, puis cliquez sur **Terminer**.

h. Fermez l'Éditeur et la Console de gestion des stratégies de groupe.

▶ Tâche 3 : Configurer les ressources internes

1. Demandez un certificat pour LON-SVR1 en procédant comme suit :

   a. Sur LON-SVR1, déplacez la souris vers le coin inférieur droit de l'écran, cliquez sur **Rechercher**, saisissez **cmd**, puis appuyez sur Entrée.

   b. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

   ```
   gpupdate /force
   ```

   c. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

   ```
   mmc
   ```

   d. Cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.

   e. Cliquez successivement sur **Certificats**, **Ajouter**, **Un compte d'ordinateur**, puis sur **Suivant**. Vérifiez que, **Ordinateur local** est sélectionné, Cliquez sur **Terminer**, puis sur **OK**.

   f. Dans la console du composant logiciel enfichable Certificats, développez Certificats (ordinateur local), Personnel, puis cliquez sur Certificats.

   g. Cliquez avec le bouton droit sur **Certificats**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.

   h. Cliquez sur **Suivant** à deux reprises.

   i. Sur la page **Demander des certificats**, cliquez sur **Certificat de serveur Web Adatum**, puis cliquez sur **L'inscription pour obtenir ce certificat nécessite des informations supplémentaires**.

   j. Dans l'onglet **Objet** de la boîte de dialogue **Propriétés du certificat**, sous **Nom du sujet**, sous **Type**, cliquez sur **Nom commun**.

   k. Dans la zone de texte **Valeur**, saisissez **nls.adatum.com**, puis cliquez sur **Ajouter**.

   l. Cliquez sur **OK**, cliquez sur **Inscription**, puis cliquez sur **Terminer**.

   m. Dans le volet d'informations du composant logiciel enfichable de certificats, vérifiez qu'un nouveau certificat avec le nom **nls.adatum.com** a été inscrit avec **Rôles prévus** de **Authentification du serveur**.

   n. Fermez la fenêtre de la console. Lorsque vous êtes invité à enregistrer les paramètres, cliquez sur **Non**.

2. Pour changer les liaisons HTTPS, procédez comme suit :

   a. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestionnaire des services Internet (IIS)**.

   b. Dans la console Gestionnaire des services Internet (IIS), cliquez sur **LON-SVR1.** Dans la zone de message du Gestionnaire des services Internet (IIS), cliquez sur **Non**. Cliquez sur **Sites** et sur **Default Web Site**.

   c. Dans le volet Actions, cliquez sur **Liaisons**, puis sur **Ajouter**.

   d. Dans la boîte de dialogue **Ajouter la liaison de site**, cliquez sur **https**, dans la boîte de dialogue **Certificat SSL**, cliquez sur le certificat avec le nom **nls.adatum.com**, cliquez sur **OK**, puis cliquez sur **Fermer**.

   e. Fermez la console Gestionnaire des services Internet (IIS).

▶ Tâche 4 : Configurer le serveur DirectAccess

1. Demandez les certificats nécessaires pour LON-RTR en procédant comme suit :

   a. Basculez vers LON-RTR.

   b. Ouvrez une invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

   ```
   gpupdate /force
   ```

   c. À l'invite de commandes, saisissez **mmc.exe**, et appuyez sur Entrée.

   d. Cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.

   e. Cliquez sur **Certificats**, cliquez sur **Ajouter**, cliquez sur **Un compte d'ordinateur**, cliquez sur **Suivant**, sélectionnez **L'ordinateur local**, cliquez sur **Terminer**, puis cliquez sur **OK**.

   f. Dans la console du composant logiciel enfichable Certificats, développez **Certificats (ordinateur local)**, **Personnel**, puis cliquez sur **Certificats**.

   g. Cliquez avec le bouton droit sur **Certificats**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.

   h. Cliquez sur **Suivant** à deux reprises.

   i. Sur la page **Demander des certificats**, cliquez sur **Certificat de serveur Web Adatum**, puis cliquez sur **L'inscription pour obtenir ce certificat nécessite des informations supplémentaires**.

   j. Dans l'onglet **Objet** de la boîte de dialogue **Propriétés du certificat**, sous **Nom du sujet**, sous **Type**, cliquez sur **Nom commun**.

   k. Dans la zone de texte **Valeur**, saisissez **131.107.0.2**, puis cliquez sur **Ajouter**.

   l. Cliquez sur **OK**, cliquez sur **Inscription**, puis cliquez sur **Terminer**.

   m. Dans le volet d'informations du composant logiciel enfichable Certificats, vérifiez qu'un nouveau certificat du nom de **131.107.0.2** a bien été délivré avec **Rôles prévus** de **Authentification serveur**.

   n. Cliquez avec le bouton droit sur le certificat, puis cliquez sur **Propriétés**.

   o. Dans la zone de texte **Nom convivial**, saisissez **Certificat IP-HTTPS**, puis cliquez sur **OK**.

   p. Fermez la fenêtre de la console. Si vous êtes invité à enregistrer les paramètres, cliquez sur **Non**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

2. Créez le point de distribution de liste de révocation de certificats sur LON-RTR en procédant comme suit :

   a. Basculez vers Gestionnaire de serveur.

   b. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Gestionnaire des services Internet (IIS)**.

   c. Dans l'arborescence de la console, développez **LON-RTR** (Si la zone de message du Gestionnaire des services Internet s'affiche, cliquez sur **Non**), **Sites**, cliquez sur **Default Web Site**, cliquez avec le bouton droit sur **Default Web Site**, puis cliquez sur **Ajouter un répertoire virtuel**.

   d. Dans la boîte de dialogue **Ajouter un répertoire virtuel**, dans la zone de texte **Alias**, saisissez **CRLD**. En regard de **Chemin d'accès physique**, cliquez sur le bouton de points de suspension (…).

   e. Dans la boîte de dialogue **Rechercher un dossier**, cliquez sur **Disque local (C:)**, puis sur **Créer un nouveau dossier**.

   f. Saisissez **CRLDist**, et appuyez sur Entrée.

   g. Dans la boîte de dialogue **Rechercher un dossier**, cliquez sur **OK**.

   h. Dans la boîte de dialogue **Ajouter un répertoire virtuel**, cliquez sur **OK**.

   i. Dans le volet central de la console, double-cliquez sur **Exploration de répertoire**, et dans le volet Actions, cliquez sur **Activer**.

   j. Dans la console, cliquez sur le dossier **CRLD**.

   k. Dans le volet central de la console, double-cliquez sur l'icône **Éditeur de configuration**.

   l. Cliquez sur la flèche vers le bas de la liste déroulante **Section**, développez **system.webServer**, **security**, puis cliquez sur **requestFiltering**.

   m. Dans le volet central de la console requestFiltering, double-cliquez sur **allowDoubleEscaping** pour modifier la valeur de Faux à **True**.

   n. Dans le volet Actions, cliquez sur **Appliquer**.

   o. Fermez le Gestionnaire des services Internet (IIS).

   Question : Pourquoi rendez-vous la liste de révocation de certificats disponible sur le serveur Edge ?

   Réponse : Vous rendez la liste de révocation de certificats disponible sur le serveur Edge de sorte que les clients DirectAccess Internet puissent y accéder.

3. Partagez et sécurisez le point de distribution de la liste de révocation de certificats en exécutant les étapes suivantes :

 **Remarque :** vous effectuez ces étapes pour attribuer des autorisations au point de distribution de liste de révocation de certificats.

   a. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.

   b. Dans l'Explorateur de fichiers, double-cliquez sur **Disque local (C:)**.

   c. Dans le volet d'informations de l'Explorateur de fichiers, cliquez avec le bouton droit sur le dossier **CRLDist**, puis cliquez sur **Propriétés**.

   d. Dans la boîte de dialogue **Propriétés de CRLDist**, cliquez sur l'onglet **Partage**, puis cliquez sur **Partage avancé**.

e. Dans la boîte de dialogue **Partage avancé**, cliquez sur **Partager ce dossier**.

f. Dans la zone de texte **Nom de partage**, ajoutez un symbole dollar ($) à la fin du nom de sorte que le nom de partage soit **CRLDist$**.

g. Dans la boîte de dialogue **Partage avancé**, cliquez sur **Autorisations**.

h. Dans la boîte de dialogue **Autorisations pour CRLDist$**, cliquez sur **Ajouter**.

i. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des contacts, des ordinateurs, des comptes de service ou groupes**, cliquez sur **Types d'objets**.

j. Dans la boîte de dialogue **Types d'objets**, sélectionnez **des ordinateurs**, puis cliquez sur **OK**.

k. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des contacts, des ordinateurs, des comptes de service ou groupes**, dans la zone de texte **Entrez les noms des objets à sélectionner**, saisissez **LON-DC1**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.

l. Dans la boîte de dialogue **Autorisations pour CRLDist$**, dans la liste **Noms de groupes ou d'utilisateurs**, cliquez sur **LON-DC1 (ADATUM\LON-DC1$)**. Dans la zone **Autorisations pour LON-DC1**, sous **Contrôle total**, cliquez sur **Autoriser**, puis cliquez sur **OK**.

m. Dans la boîte de dialogue **Partage avancé**, cliquez sur **OK**.

n. Dans la boîte de dialogue **Propriétés CRLDist**, cliquez sur l'onglet **Sécurité**.

o. Dans l'onglet **Sécurité**, cliquez sur **Modifier**.

p. Dans la boîte de dialogue **Autorisations pour CRLDist**, cliquez sur **Ajouter**.

q. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des contacts, des ordinateurs, des comptes de service ou groupes**, cliquez sur **Types d'objets**.

r. Dans la boîte de dialogue **Types d'objets**, cliquez sur **des ordinateurs**, puis cliquez sur **OK**.

s. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des contacts, des ordinateurs, des comptes de service ou groupes**, dans la zone de texte **Entrez les noms des objets à sélectionner**, saisissez **LON-DC1**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.

t. Dans la boîte de dialogue **Autorisations pour CRLDist**, dans la liste **Noms de groupes ou d'utilisateurs**, cliquez sur **LON-DC1 (ADATUM\LON-DC1$)**. Dans la zone **Autorisations pour LON-DC1**, sous **Contrôle total**, cliquez sur **Autoriser**, puis cliquez sur **OK**.

u. Dans la boîte de dialogue **Propriétés CRLDist**, cliquez sur **Fermer**.

v. Fermez la fenêtre de l'Explorateur de fichiers.

4. Publiez la liste de révocation de certificats vers LON-RTR en suivant la procédure ci-dessous :

 **Remarque :** Ces étapes rendent la liste de révocation de certificats disponible sur le serveur Edge pour les clients DirectAccess basés sur Internet.

a. Basculez vers LON-DC1.

b. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Autorité de certification**.

c. Dans la console Autorité de certification, développez **Adatum-LON-DC1-CA**, cliquez avec le bouton droit sur **Certificats révoqués**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Publier**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

d. Dans la boîte de dialogue **Publier la liste de révocation des certificats**, cliquez sur **Nouvelle liste de révocation des certificats**, puis cliquez sur **OK**.

e. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.

f. Dans la barre d'adresses de l'Explorateur de fichiers, saisissez **\\LON-RTR\CRLDist$**, puis appuyez sur Entrée.

g. Dans la fenêtre de l'Explorateur de fichiers, observez les fichiers **Adatum-LON-DC1-CA**.

h. Fermez la fenêtre de l'Explorateur de fichiers.

5. Terminez la procédure avec l'Assistant de configuration DirectAccess sur LON-RTR en procédant comme suit :

Remarque : Ces étapes configurent LON-RTR en tant que serveur DirectAccess.

a. Sur LON-RTR, ouvrez le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Routage et accès distant**. Si vous y êtes invité, cliquez sur **Annuler**, e puis sur **OK**.

b. Dans la console Routage et accès distant, cliquez avec le bouton droit sur **LON-RTR (local)**, puis cliquez sur **Désactiver le routage et l'accès à distance**. Cliquez sur **Oui** et fermez la console.

c. Dans le Gestionnaire de serveur, dans le menu **Outils**, cliquez sur **Gestion de l'accès à distance**.

d. Dans la console de Gestion de l'accès à distance, cliquez sur **Configuration**.

e. Dans le volet de résultats, cliquez sur **Exécuter l'Assistant Mise en route**.

Remarque : Si vous obtenez une erreur à ce stade, redémarrez LON-RTR, connectez-vous en tant qu'ADATUM\administrateur, puis recommencez la procédure à partir de l'étape c).

f. Dans l'Assistant **Configurer l'accès à distance,** cliquez sur **Déployer DirectAccess uniquement**.

g. Dans le volet Topologie du réseau, vérifiez que **Edge** est sélectionné, et que **131.107.0.2** est le nom public utilisé par les clients pour se connecter au serveur d'accès à distance.

h. Cliquez sur **Suivant**.

i. Sur la page **Configurer l'accès à distance**, cliquez sur **Terminer**.

j. Une fois la configuration terminée, cliquez sur **Fermer**.

k. Dans la console Gestion de l'accès à distance, sous **Étape 1**, cliquez sur **Modifier**, puis sur **Suivant+**.

l. Sous **Sélectionner les groupes**, dans le volet d'informations, cliquez sur **Ajouter**.

m. Dans la boîte de dialogue **Sélectionnez un groupe**, saisissez **DA_Clients**, puis cliquez sur **OK**.

n. Désactivez la case à cocher **Activer DirectAccess pour les ordinateurs portables uniquement**.

o. Supprimez le groupe Ordinateurs du domaine, puis cliquez sur **Suivant**. Cliquez sur **Terminer**.

p. Dans la console Gestion de l'accès à distance, sous **Étape 2**, cliquez sur **Modifier**.

q. Sur la page **Topologie du réseau**, vérifiez que **Edge** est sélectionné, saisissez **131.107.0.2**, puis cliquez sur **Suivant**.

r. Sur la page **Cartes réseau**, vérifiez que **CN=131.107.0.2** est utilisé comme certificat d'authentification des connexions IP-HTTPS, puis cliquez sur **Suivant**.

s. Sur la page **Authentification**, cliquez successivement sur **Utiliser les certificats d'ordinateur**, **Parcourir**, **Adatum-LON-DC1-CA**, **OK**, puis sur **Terminer**.

t. Dans le volet Configuration de l'accès à distance, sous **Étape 3**, cliquez sur **Modifier**.

u. Sur la page **Server Emplacement réseau**, cliquez sur **Le serveur Emplacement réseau est déployé sur un serveur Web distant (recommandé)**. Dans le champ URL du serveur d'emplacement réseau (NLS), saisissez **https://nls.adatum.com**, puis cliquez sur **Valider**.

v. Assurez-vous que l'URL est validée.

w. Cliquez sur **Suivant**, et sur la page **DNS**, vérifiez les valeurs, puis cliquez sur **Suivant**.

x. Dans la **Liste de recherche de suffixes DNS**, cliquez sur **Suivant**.

y. Sur la page **Gestion**, cliquez sur **Terminer**.

z. Sous **Étape 4**, cliquez sur **Modifier**.

aa. Sur la page **Installation du serveur d'applications DirectAccess**, cliquez sur **Terminer**.

bb. Cliquez sur **Terminer** pour appliquer les modifications.

cc. Dans **Vérification de l'accès à distance**, cliquez sur **Appliquer**.

dd. Sous **Application des paramètres de l'Assistant Configuration de l'accès à distance**, cliquez sur **Fermer**.

6. Mettez à jour les paramètres de la stratégie de groupe sur **LON-RTR** en procédant comme suit :

   a. Déplacez le pointeur de la souris sur le coin inférieur droit, et sur la barre de menus, cliquez sur **Rechercher**, saisissez **cmd**, puis appuyez sur Entrée.

   b. À l'invite de commandes, saisissez les commandes ci-dessous, en appuyant sur Entrée à la fin de chaque ligne :

```
gpupdate /force
Ipconfig
```

 **Remarque :** Vérifiez que **LON-RTR** a une adresse IPv6 pour **Interface IPHTTPS de la carte Tunnel** commençant par **2002**.

Résultats : À la fin de cet exercice, vous devez avoir configuré l'infrastructure DirectAccess.

Exercice 2 : Configuration des clients DirectAccess

▶ Tâche 1 : Configurer les paramètres de stratégie de groupe DirectAccess

1. Démarrez LON-CL1 et ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**. L'objectif consiste à garantir que l'ordinateur LON-CL1 se connecte au domaine en tant que membre du groupe de sécurité DA_Clients.
2. Dans le menu Accueil, saisissez **cmd** pour ouvrir une fenêtre d'invite de commandes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

4. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpresult /R
```

5. Vérifiez que **l'objet de la stratégie de groupe Paramètres client DirectAccess** s'affiche correctement dans la liste des objets de stratégie de groupe pour les **paramètres de l'ordinateur**.

Remarque : Si la stratégie n'est pas appliquée, exécutez à nouveau la commande **gpupdate /force**. Si la stratégie n'est toujours pas en cours d'application, redémarrez l'ordinateur. Après le redémarrage de l'ordinateur, connectez-vous en tant qu'**ADATUM\Administrateur** et exécutez à nouveau la commande **Gpresult –R**.

▶ Tâche 2 : Vérifier la distribution de certificats d'ordinateurs clients

1. À l'invite de commandes, saisissez **mmc.exe**, et appuyez sur Entrée.
2. Dans la console MMC, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
3. Cliquez sur **Certificats**, cliquez sur **Ajouter**, sélectionnez **Un compte d'ordinateur**, cliquez sur **Suivant**, sélectionnez **Ordinateur local**, cliquez sur **Terminer**, puis cliquez sur **OK**.
4. Dans la console du composant logiciel enfichable Certificats, cliquez sur Certificats (ordinateur local), développez Personnel, puis cliquez sur Certificats.
5. Dans le volet d'informations Certificats, vérifiez qu'un certificat avec le nom **LON-CL1.adatum.com** s'affiche avec **Rôles prévus** de **Authentification client** et **Authentification serveur**.
6. Fermez la fenêtre de la console. Lorsque vous êtes invité à enregistrer les paramètres, cliquez sur **Non**.

▶ Tâche 3 : Vérifier la connectivité interne aux ressources

1. Sur LON-CL1, sur le Bureau, dans la barre des tâches, cliquez sur **Internet Explorer**.
2. Dans la barre d'adresses Windows Internet Explorer®, saisissez **http://lon-svr1.adatum.com/**, et appuyez sur Entrée. La page Web par défaut IIS8 pour LON-SVR1 s'affiche.
3. Dans la barre d'adresses Internet Explorer, saisissez **https://nls.adatum.com/**, puis appuyez sur Entrée. La page Web par défaut IIS8 pour LON-SVR1 s'affiche.
4. Laissez la fenêtre Internet Explorer ouverte.
5. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
6. Dans la barre d'adresses de l'Explorateur de fichiers, saisissez **\\Lon-SVR1\Files**, puis appuyez sur Entrée. Une fenêtre avec les contenus du dossier partagé **Fichiers** s'affiche.
7. Fermez toutes les fenêtres.

Résultats : À la fin de cet exercice, vous devez avoir configuré les clients DirectAccess.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Vérification de la configuration DirectAccess

▶ Tâche 1 : Déplacer l'ordinateur client vers le réseau virtuel Internet

1. Basculez vers LON-CL1.
2. Sur LON-CL1, déplacez le pointeur de la souris dans le coin inférieur droit de l'écran, cliquez sur **Paramètres**, sélectionnez **Panneau de configuration**, puis cliquez sur **Réseau et Internet**.
3. Cliquez sur **Centre Réseau et partage**.
4. Cliquez sur **Modifier les paramètres de la carte**.
5. Cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, double-cliquez sur **Protocole Internet version 4 (TCP/IPv4)**.
7. Dans la boîte de dialogue **Propriétés de : Protocole Internet version 4 (TCP/IPv4)**, cliquez sur **Utiliser l'adresse IP suivante**.
8. Renseignez les paramètres suivants, puis cliquez sur **OK** :
   - Adresse IP : **131.107.0.10**
   - Masque de sous-réseau : **255.255.0.0**
   - Passerelle par défaut : **131.107.0.2**
9. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, cliquez sur **OK**.
10. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Désactiver**.
11. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur **Connexion au réseau local**, et cliquez sur **Activer**.
12. Sur votre hôte, dans Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22411B-LON-CL1**, puis cliquez sur **Paramètres**.
13. Modifiez la carte réseau héritée pour qu'elle soit sur le réseau **Réseau privé 2**, puis cliquez sur **OK**.

▶ Tâche 2 : Vérifier la connectivité vers le serveur DirectAccess

1. Sur LON-CL1, déplacez le pointeur de la souris sur le coin inférieur droit, et dans le menu droit, cliquez sur **Rechercher**, saisissez **cmd**, puis appuyez sur Entrée.
2. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
ipconfig
```

3. Notez que l'adresse IP renvoyée commence par **2002**. Il s'agit d'une adresse IP-HTTPS.
4. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Netsh name show effectivepolicy
```

5. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
powershell
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans l'interface de ligne de commande Windows PowerShell®, saisissez la commande suivante, puis appuyez sur Entrée :

```
Get-DAClientExperienceConfiguration
```

Remarque : Observez les paramètres du client DirectAccess.

▶ Tâche 3 : Vérifier la connectivité vers les ressources du réseau interne

1. Basculez vers **Internet Explorer**, et dans la barre d'adresses, saisissez **http://lon-svr1.adatum.com**, et appuyez sur Entrée. La page Web par défaut IIS8 pour LON-SVR1 s'affiche.
2. Laissez la fenêtre Internet Explorer ouverte.
3. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
4. Dans la barre d'adresses de l'Explorateur de fichiers, saisissez **\\LON-SVR1\Files**, puis appuyez sur Entrée. Une fenêtre de dossier avec les contenus du dossier partagé Fichiers s'affiche.
5. Revenez à la fenêtre d'invite de commandes.
6. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
ping lon-dc1.adatum.com
```

7. Vérifiez que vous recevez les réponses de lon-dc1.adatum.com.
8. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

9. Fermez toutes les fenêtres.
10. Basculez vers LON-RTR.
11. Basculez vers **Gestion de l'accès à distance**.
12. Dans la console, cliquez sur **STATUT DU CLIENT DISTANT**.

Remarque : Vous remarquerez que LON-CL1 est connecté via IP-HTTPS (IP sur HTTPS). Dans le volet d'informations de connexion en bas à droite de l'écran, observez l'utilisation de Kerberos pour l'ordinateur et l'utilisateur.

13. Fermez toutes les fenêtres.

▶ Pour préparer le module suivant

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22411B-LON-CL1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22411B-LON-SVR1**, **22411B-LON-RTR** et **22411B-LON-DC1**.

Résultats : À la fin de cet exercice, vous devez avoir vérifié la configuration DirectAccess.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 8: Installation, configuration et résolution des problèmes du rôle de serveur NPS

Atelier pratique : Installation et configuration d'un serveur NPS

Exercice 1 : Installation et configuration de NPS pour prendre en charge RADIUS

▶ Tâche 1 : Installer et configurer le Serveur NPS

1. Basculez vers LON-DC1.
2. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Si nécessaire, cliquez sur **Gestionnaire de serveur** dans la barre des tâches.
4. Dans le volet Détails, cliquez sur **Ajouter des rôles et des fonctionnalités**.
5. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner le type d'installation**, vérifiez que **Installation basée sur un rôle ou une fonctionnalité** est sélectionné, puis cliquez sur **Suivant**.
7. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services de stratégie et d'accès réseau**.
9. Cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant** à deux reprises.
10. Sur la page **Services de stratégie et d'accès réseau**, cliquez sur **Suivant**.
11. Sur la page **Sélectionner des services de rôle**, vérifiez que la case à cocher **Serveur NPS (Network Policy Server)** est activée, puis cliquez sur **Suivant**.
12. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
13. Vérifiez que l'installation a réussi, puis cliquez sur **Fermer**.
14. Fermez la fenêtre du Gestionnaire de serveur.
15. Suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
16. Cliquez sur **Serveur NPS**.
17. Dans le volet de navigation du Gestionnaire de stratégies réseau, cliquez avec le bouton droit sur **NPS (local)**, puis cliquez sur **Inscrire un serveur dans Active Directory**.
18. Dans la zone de message **Serveur NPS (Network Policy Server)**, cliquez sur **OK**.
19. Dans la boîte de dialogue Serveur NPS (Network Policy Server) suivante, cliquez sur **OK**.
20. Laissez la fenêtre de la console Serveur NPS (Network Policy Server) ouverte.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer des modèles NPS

1. Dans la console Serveur NPS, dans le volet de navigation, développez **Gestion des modèles**.
2. Dans le volet de navigation, cliquez avec le bouton droit de la souris sur **Secrets partagés**, puis cliquez sur **Nouveau**.
3. Dans la boîte de dialogue **Nouveau modèle de secret partagé RADIUS**, dans la zone **Nom du modèle**, saisissez **Secret Adatum**.
4. Dans les zones **Secret partagé** et **Confirmez le secret partagé**, tapez **Pa$$w0rd**, puis cliquez sur **OK**.
5. Dans le volet de navigation, cliquez avec le bouton droit de la souris sur **Clients RADIUS**, puis cliquez sur **Nouveau**.
6. Dans la boîte de dialogue **Nouveau client RADIUS**, dans le champ **Nom convivial**, tapez **LON-RTR**.
7. Cliquez sur **Vérifier** et dans la boîte de dialogue **Vérifier l'adresse**, dans le champ **Adresse**, tapez **LON-RTR**, puis cliquez sur **Résoudre**.
8. Cliquez sur **OK**.
9. Dans la boîte de dialogue **Nouveau client RADIUS**, sous **Secret partagé**, dans **Sélectionnez un modèle de secrets partagés existant**, cliquez sur **Secret Adatum**, puis cliquez sur **OK**.
10. Laissez la console ouverte.

▶ Tâche 3 : Configurer la gestion de comptes RADIUS

1. Dans le serveur NPS, dans le volet de navigation, cliquez sur **Gestion**.
2. Dans le volet d'informations, cliquez sur **Configurer la gestion des comptes**.
3. Dans l'Assistant Configuration de la gestion des comptes, cliquez sur **Suivant**.
4. Sur la page **Sélectionner les options de gestion**, cliquez sur **Enregistrer les données dans un fichier texte sur l'ordinateur local**, puis cliquez sur **Suivant**.
5. Sur la page **Configurer la journalisation dans un fichier local**, cliquez sur **Suivant**.
6. Sur la page **Résumé**, cliquez sur **Suivant**.
7. Sur la page **Conclusion**, cliquez sur **Fermer**.
8. Laissez la console ouverte.

Résultats : À la fin de cet exercice, vous devez avoir activé et configuré NPS pour prendre en charge l'environnement requis.

Exercice 2 : Configuration et test d'un client RADIUS

▶ Tâche 1 : Configurer un client RADIUS

1. Dans la console Serveur NPS, développez **Clients et serveurs RADIUS**.
2. Cliquez avec le bouton droit sur **Clients RADIUS**, et cliquez sur **Nouveau**.
3. Dans la boîte de dialogue **Nouveau client RADIUS**, désactivez la case à cocher **Activer ce client RADIUS**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Activez la case à cocher **Sélectionner un modèle existant**.
5. Cliquez sur **OK**.
6. Laissez la console Serveur NPS ouverte.
7. Basculez vers LON-RTR.
8. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
9. Suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
10. Dans Accueil, cliquez sur **Outils d'administration**, puis double-cliquez sur **Routage et accès distant**.
11. Si nécessaire, dans la boîte de dialogue **Assistant Activation de DirectAccess**, cliquez sur **Annuler**. Cliquez sur **OK**.
12. Dans la console Routage et accès distant, cliquez avec le bouton droit sur **LON-RTR (local)**, puis cliquez sur **Désactiver le routage et l'accès à distance**.
13. Dans la boîte de dialogue, cliquez sur **Oui**.
14. Dans la console Routage et accès distant, cliquez avec le bouton droit sur **LON-RTR (local)**, puis cliquez sur **Configurer et activer le routage et l'accès à distance**.
15. Cliquez sur **Suivant**, vérifiez que **Accès à distance (connexion à distance ou VPN)** est sélectionné**,** puis cliquez sur **Suivant**.
16. Activez la case à cocher **VPN**, puis cliquez sur **Suivant**.
17. Cliquez sur l'interface réseau intitulée **Connexion au réseau local 2**. Désactivez la case à cocher **Sécuriser l'interface sélectionnée en configurant des filtres de paquet statiques**, puis cliquez sur **Suivant**.
18. Sur la page **Attribution d'adresses IP**, sélectionnez **À partir d'une plage d'adresses spécifiée**, puis cliquez sur **Suivant**.
19. Sur la page **Assignation de plages d'adresses**, cliquez sur **Nouveau**. Tapez **172.16.0.100** en regard de **Adresse IP de début** et **172.16.0.110** en regard de **Adresse IP de fin**, puis cliquez sur **OK**. Vérifiez que 11 adresses IP ont été attribuées aux clients distants, puis cliquez sur **Suivant**.
20. Sur la page **Gestion de serveurs d'accès à distance multiples**, cliquez sur **Oui, configurer ce serveur pour travailler avec un serveur RADIUS**, puis cliquez sur **Suivant**.
21. Sur la page **Sélection des serveurs RADIUS**, dans le champ **Serveur RADIUS principal**, tapez **LON-DC1**.
22. Dans le champ **Secret partagé** tapez **Pa$$w0rd**, puis cliquez sur **Suivant**.
23. Cliquez sur **Terminer**.
24. Dans la boîte de dialogue **Routage et accès distant**, cliquez sur **OK**.
25. Si vous y êtes invité à nouveau, cliquez sur **OK**.

▶ Tâche 2 : Configurez une stratégie réseau pour RADIUS :

1. Basculez vers l'ordinateur LON-DC1.
2. Basculez vers **Serveur NPS (Network Policy Server)**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans Serveur NPS (Network Policy Server), développez **Stratégies**, puis cliquez sur **Stratégies réseau**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur la première stratégie de la liste, puis cliquez sur **Désactiver**.
5. Dans le volet d'informations, cliquez avec le bouton droit sur la dernière stratégie de la liste, puis cliquez sur **Désactiver**.
6. Dans le volet de navigation, cliquez avec le bouton droit sur **Stratégies réseau**, puis cliquez sur **Nouveau**.
7. Dans l'Assistant Nouvelle stratégie réseau, dans le champ **Nom de la stratégie**, tapez **Stratégie VPN Adatum**.
8. Dans la liste **Type de serveur d'accès réseau**, cliquez sur **Serveur d'accès à distance (VPN-Dial up)**, puis sur **Suivant**.
9. Sur la page **Spécifier les conditions**, cliquez sur **Ajouter**.
10. Dans la boîte de dialogue **Sélectionner une condition** , cliquez sur **Type de port NAS**, puis cliquez sur **Ajouter**.
11. Dans la boîte de dialogue **Type de port NAS**, cochez la case **Virtuel (VPN)**, puis cliquez sur **OK**.
12. Cliquez sur **Suivant**, et sur la page **Spécifier l'autorisation d'accès**, vérifiez que **Accès accordé** est sélectionné, puis cliquez sur **Suivant**.
13. Sur la page **Configurer les méthodes d'authentification**, cliquez sur **Suivant**.
14. Sur la page **Configurer des contraintes**, cliquez sur **Suivant**.
15. Sur la page **Configurer les paramètres**, cliquez sur **Suivant**.
16. Sur la page **Fin de la configuration de la nouvelle stratégie réseau**, cliquez sur **Terminer**.

▶ Tâche 3 : Tester la configuration RADIUS

1. Basculez vers LON-CL2.
2. Ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans l'écran d'accueil, tapez **Panneau**, puis dans la liste **Applications**, cliquez sur **Panneau de configuration**.
4. Dans le Panneau de configuration, cliquez sur **Réseau et Internet**.
5. Cliquez sur **Centre Réseau et partage**.
6. Cliquez sur **Configurer une nouvelle connexion ou un nouveau réseau**.
7. Sur la page **Choisir une option de connexion**, cliquez sur **Connexion à votre espace de travail**, puis sur **Suivant**.
8. Sur la page **Comment voulez-vous vous connecter ?**, cliquez sur **Utiliser ma connexion Internet (VPN)**.
9. Cliquez sur **Je configurerai une connexion Internet ultérieurement**.
10. Sur la page **Entrez l'adresse Internet à laquelle vous souhaitez vous connecter**, dans le champ **Adresse Internet**, tapez **10.10.0.1**.
11. Dans la zone **Nom de la destination**, tapez **VPN Adatum**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

12. Activez la case à cocher **Autoriser d'autres personnes à utiliser cette connexion**, puis cliquez sur **Créer**.
13. Dans la fenêtre Centre Réseau et partage, cliquez sur **Modifier les paramètres de la carte**.
14. Cliquez avec le bouton droit sur la connexion **VPN Adatum**, cliquez sur **Propriétés**, puis cliquez sur l'onglet **Sécurité**.
15. Dans la liste **Type de réseau VPN**, cliquez sur **Protocole PPTP (Point to Point Tunneling Protocol)**.
16. Sous **Authentification**, cliquez sur **Autoriser ces protocoles**, puis cliquez sur **OK**.
17. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur la connexion **VPN Adatum**, puis cliquez sur **Connecter/Déconnecter**.
18. Dans la liste **Réseaux** de droite, cliquez sur **VPN Adatum**, puis sur **Connexion**.
19. Dans Authentification réseau, dans le champ **Nom d'utilisateur**, tapez **ADATUM\Administrateur**.
20. Dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **OK**.
21. Attendez que la connexion VPN soit établie. La connexion a réussi.

Résultats : À la fin de cet exercice, vous devriez avoir déployé un serveur VPN, et l'avoir configuré en tant que client RADIUS.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial de tous les ordinateurs virtuels. Pour cela, 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 **22411B-LON-CL2**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22411B-LON-RTR** et **22411B-LON-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 9: Implémentation de la protection d'accès réseau

Atelier pratique : Implémentation de la protection d'accès réseau

Exercice 1 : Configuration des composants NAP

▶ Tâche 1 : Configurer les exigences des certificats clients et de serveur

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Autorité de certification**.
2. Dans la console de gestion certsrv, développez **Adatum-LON-DC1-CA**, cliquez avec le bouton droit sur **Modèles de certificats**, puis sélectionnez **Gérer** dans le menu contextuel.
3. Dans le volet d'informations de la Console des modèles de certificat, cliquez avec le bouton droit sur **Ordinateur**, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Sécurité** dans la boîte de dialogue **Propriétés de : Ordinateur**, puis sélectionnez **Utilisateurs authentifiés**.
5. Dans **Autorisations pour Utilisateurs authentifiés**, activez la case à cocher **Autoriser** pour l'autorisation **Inscrire**, puis cliquez sur **OK**.
6. Fermez la Console des modèles de certificat.
7. Dans **certsrv – [Autorité de certification (local)]**, cliquez avec le bouton droit sur **Adatum-LON-DC1-CA**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Arrêter le service**.
8. Cliquez avec le bouton droit sur **Adatum-LON-DC1-CA**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Accueil le service.**
9. Fermez la console de gestion certsrv.

▶ Tâche 2 : Configurer les stratégies de contrôle d'intégrité

1. Basculez vers l'ordinateur LON-RTR.
2. Connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
4. Dans l'écran Accueil, tapez **mmc.exe** et appuyez sur Entrée.
5. Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
6. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur**Certificats**, sur **Ajouter**, sélectionnez **Un Compte d'ordinateur**, cliquez sur **Suivant**, puis sur **Terminer**.
7. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **OK**.
8. Dans l'arborescence de la console, développez **Certificats**, cliquez avec le bouton droit sur **Personnel**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Demander un Nouveau certificat**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. La boîte de dialogue **Inscription de certificats** s'ouvre. Cliquez sur **Suivant**.
10. Sur la page **Sélectionner la stratégie d'inscription de certificat**, cliquez sur **Stratégie d'inscription à Active Directory**, puis sur **Suivant**.
11. Activez la case à cocher **Ordinateur**, puis cliquez sur **Inscription**.
12. Vérifiez que l'état d'installation du certificat indique **réussie**, puis cliquez sur **Terminer**.
13. Fermez la fenêtre Console1.
14. Cliquez sur **Non** lorsque vous êtes invité à enregistrer les paramètres de la console.
15. Sur LON-RTR, basculez vers **Gestionnaire de serveur**.
16. Dans le Gestionnaire de serveur, dans le volet d'informations, cliquez sur **Ajouter des rôles et des fonctionnalités**.
17. Cliquez sur **Suivant**.
18. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
19. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
20. Sur la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services de stratégie et d'accès réseau**.
21. Cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant** à deux reprises.
22. Sur la page **Services de stratégie et d'accès réseau**, cliquez sur **Suivant**.
23. Dans la page **Sélectionner des services de rôle**, cliquez sur **Suivant**.
24. Cliquez sur **Installer**.
25. Vérifiez que l'installation a réussi, puis cliquez sur **Fermer**.
26. Fermez la fenêtre du Gestionnaire de serveur.
27. Suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
28. Cliquez sur **Serveur NPS**.
29. Développez successivement **Protection d'accès réseau**, **Programmes de validation d'intégrité système**, **Programme de validation d'intégrité de la sécurité Windows**, puis cliquez sur **Paramètres**.
30. Dans le volet de droite, sous **Nom**, double-cliquez sur **Configuration par défaut**.
31. Dans l'onglet **Windows 8/Windows 7/Windows Vista**, désactivez toutes les cases à cocher, sauf **Un pare-feu est activé pour toutes les connexions réseau**, puis cliquez sur **OK**.
32. Dans le volet de navigation, développez **Stratégies**.
33. Cliquez avec le bouton droit sur **Stratégies de contrôle d'intégrité**, puis cliquez sur **Nouveau**.
34. Dans la boîte de dialogue **Créer une stratégie de contrôle d'intégrité**, sous **Nom de la stratégie**, tapez **Conforme**.
35. Sous **Contrôles du client par les programmes de validation d'intégrité système (SHV)**, vérifiez que la case à cocher **Réussite de tous les contrôles SHV pour le client** est activée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

36. Sous **Programmes de validation d'intégrité système (SHV) utilisés dans cette stratégie de contrôle d'intégrité**, activez la case à cocher **Programme de validation d'intégrité de la sécurité Windows**.
37. Cliquez sur **OK**.
38. Cliquez avec le bouton droit sur **Stratégies de contrôle d'intégrité**, puis cliquez sur **Nouveau**.
39. Dans la boîte de dialogue **Créer une stratégie de contrôle d'intégrité**, sous **Nom de la stratégie**, tapez **Non conforme**.
40. Sous **Contrôles du client par les programmes de validation d'intégrité système (SHV)**, sélectionnez **Échec d'un ou de plusieurs contrôles SHV pour le client**.
41. Sous **Programmes de validation d'intégrité système (SHV) utilisés dans cette stratégie de contrôle d'intégrité**, activez la case à cocher **Programme de validation d'intégrité de la sécurité Windows**.
42. Cliquez sur **OK**.

▶ Tâche 3 : Configurer les stratégies réseau

1. Dans le volet de navigation, sous **Stratégies**, cliquez sur **Stratégies réseau**.

 **Important :** Désactivez les deux stratégies par défaut indiquées sous **Nom de la stratégie** en cliquant avec le bouton droit sur chacune d'elles puis en cliquant sur **Désactiver**.

2. Cliquez avec le bouton droit sur **Stratégies réseau**, puis cliquez sur **Nouveau**.
3. Sur la page **Spécifier le nom de la stratégie réseau et le type de connexion**, sous **Nom de la stratégie**, tapez **Conforme-accès complet**, puis cliquez sur **Suivant**.
4. Sur la page **Spécifier les conditions**, cliquez sur **Ajouter**.
5. Dans la boîte de dialogue **Sélectionner une condition**, double-cliquez sur **Stratégies de contrôle d'intégrité**.
6. Dans la boîte de dialogue **Stratégies de contrôle d'intégrité**, sous **Stratégies de contrôle d'intégrité**, sélectionnez **Conforme**, puis cliquez sur **OK**.
7. Sur la page **Spécifier les conditions**, cliquez sur **Suivant**.
8. Sur la page **Spécifier l'autorisation d'accès**, cliquez sur **Suivant**.
9. Sur la page **Configurer les méthodes d'authentification,** désactivez toutes les cases à cocher, sélectionnez la case à cocher **Vérifier uniquement l'intégrité de l'ordinateur**, puis cliquez sur **Suivant**.
10. Cliquez à nouveau sur **Suivant**.
11. Sur la page **Configurer les paramètres**, cliquez sur **Contrainte de mise en conformité NAP**. Vérifiez que l'option **Autoriser un accès complet au réseau** est sélectionnée, puis cliquez sur **Suivant**.
12. Sur la page **Fin de la configuration de la nouvelle stratégie réseau**, cliquez sur **Terminer**.
13. Cliquez avec le bouton droit sur **Stratégies réseau**, puis cliquez sur **Nouveau**.
14. Sur la page **Spécifier le nom de la stratégie réseau et le type de connexion**, sous **Nom de la stratégie**, tapez **Non conforme-restreint**, puis cliquez sur **Suivant**.

15. Sur la page **Spécifier les conditions**, cliquez sur **Ajouter**.
16. Dans la boîte de dialogue **Sélectionner une condition**, double-cliquez sur **Stratégies de contrôle d'intégrité**.
17. Dans la boîte de dialogue **Stratégies de contrôle d'intégrité**, sous **Stratégies de contrôle d'intégrité**, sélectionnez **Non conforme**, puis cliquez sur **OK**.
18. Sur la page **Spécifier les conditions**, cliquez sur **Suivant**.
19. Sur la page **Spécifier l'autorisation d'accès**, vérifiez que l'option **Accès accordé** est sélectionnée, puis cliquez sur **Suivant**.
20. Sur la page **Configurer les méthodes d'authentification,** désactivez toutes les cases à cocher, sélectionnez la case à cocher **Vérifier uniquement l'intégrité de l'ordinateur**, puis cliquez sur **Suivant**.
21. Cliquez à nouveau sur **Suivant**.
22. Sur la page **Configurer les paramètres**, cliquez sur **Contrainte de mise en conformité NAP**. Cliquez sur **Autoriser un accès limité**.
23. Désactivez la case à cocher **Activer la mise à jour automatique des ordinateurs clients**.
24. Dans la fenêtre Configurer les paramètres, cliquez sur **Filtres IP**.
25. Sous **IPv4**, cliquez sur **Filtres d'entrée**, puis sur **Nouveau**.
26. Dans la boîte de dialogue **Ajouter le filtre IP**, sélectionnez **Réseau de destination**.
27. Dans la zone **Adresse IP**, tapez **172.16.0.10**.
28. Dans le champ **Masque de sous-réseau**, tapez **255.255.255.255**, puis cliquez sur **OK**.
29. Cliquez sur **Autoriser uniquement les trafics listés ci-dessous**, puis sur **OK**.
30. Sous **IPv4**, cliquez sur **Filtres de sortie**, puis sur **Nouveau**.
31. Dans la boîte de dialogue **Ajouter le filtre IP**, sélectionnez **Réseau source**.
32. Dans la zone **Adresse IP**, tapez **172.16.0.10**.
33. Dans le champ **Masque de sous-réseau**, tapez **255.255.255.255**, puis cliquez sur **OK**.
34. Cliquez sur **Autoriser uniquement les trafics listés ci-dessous**, puis sur **OK**.
35. Sur la page **Configurer les paramètres**, cliquez sur **Suivant**.
36. Sur la page **Fin de la configuration de la nouvelle stratégie réseau**, cliquez sur **Terminer**.

▶ Tâche 4 : Configurer des stratégies de demande de connexion pour VPN

1. Cliquez sur **Stratégies de demande de connexion**.
2. Désactivez les stratégies de demande de connexion par défaut indiquée sous **Nom de la stratégie** en cliquant avec le bouton droit sur les stratégies, puis en cliquant sur **Désactiver**.
3. Cliquez avec le bouton droit sur **Stratégies de demande de connexion**, puis cliquez sur **Nouveau**.
4. Sur la page **Spécifier le nom de la stratégie de demande de connexion et le type de connexion**, dans le champ **Nom de la stratégie**, tapez **Connexions VPN**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Sous **Type de serveur d'accès réseau**, sélectionnez **Serveur d'accès à distance (VPN-Dial up)**, puis cliquez sur **Suivant**.
6. Sur la page **Spécifier les conditions**, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Sélectionner une condition**, double-cliquez sur **Type de tunnel**, puis sélectionnez **PPTP**, **SSTP**, et **L2TP**. Cliquez sur **OK**, puis sur **Suivant**.
8. Sur la page **Spécifier le transfert de la demande de connexion**, vérifiez que l'option **Authentifier les demandes sur ce serveur** est sélectionnée, puis cliquez sur **Suivant**.
9. Sur la page **Spécifier les méthodes d'authentification**, activez la case à cocher **Remplacer les paramètres d'authentification de stratégie réseau**.
10. Sous **Types de protocoles EAP**, cliquez sur **Ajouter**.
11. Dans la boîte de dialogue **Ajouter des protocoles EAP**, sous **Méthodes d'authentification**, cliquez sur **Microsoft : PEAP (Protected EAP)**, puis cliquez sur **OK**.
12. Sous **Types de protocoles EAP**, cliquez sur **Ajouter**. Dans la boîte de dialogue **Ajouter des protocoles EAP**, sous **Méthodes d'authentification**, cliquez sur **Microsoft : Mot de passe sécurisé (EAP-MSCHAP version 2)**, puis cliquez sur **OK**.
13. Sous **Types de protocoles EAP**, cliquez sur **Microsoft : PEAP (Protected EAP)**, puis cliquez sur **Modifier**.
14. Vérifiez que l'option **Appliquer la protection d'accès réseau** est sélectionnée, puis cliquez sur **OK**.
15. Cliquez sur **Suivant** à deux reprises, puis sur **Terminer**.

Résultats : À la fin de cet exercice, vous devriez avoir installé et configuré les composants requis de protection d'accès réseau (NAP), créé les stratégies d'intégrité et réseau et créé les stratégies de demande de connexion.

Exercice 2 : Configuration de l'accès VPN

▶ Tâche 1 : Configurer un serveur VPN

1. Sur LON-RTR, suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
2. Cliquez sur **Routage et accès distant**. Si vous y êtes invité, dans la boîte de dialogue **Assistant Activation de DirectAccess**, cliquez sur **Annuler**, puis sur **OK**.
3. Dans la console Routage et accès distant, cliquez avec le bouton droit sur **LON-RTR (local)**, puis cliquez sur **Désactiver le routage et l'accès à distance**.
4. Dans la boîte de dialogue, cliquez sur **Oui**.
5. Dans la console Routage et accès distant, cliquez avec le bouton droit sur **LON-RTR (local)**, puis cliquez sur **Configurer et activer le routage et l'accès à distance**.
6. Cliquez sur **Suivant**, vérifiez que **Accès à distance (connexion à distance ou VPN)** est sélectionné, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Activez la case à cocher **VPN**, puis cliquez sur **Suivant**.
8. Cliquez sur l'interface réseau intitulée **Connexion au réseau local 2**. Désactivez la case à cocher **Sécuriser l'interface sélectionnée en configurant des filtres de paquet statiques**, puis cliquez sur **Suivant**.
9. Sur la page **Attribution d'adresses IP**, sélectionnez **À partir d'une plage d'adresses spécifiée**, puis cliquez sur **Suivant**.
10. Sur la page **Assignation de plages d'adresses**, cliquez sur **Nouveau**. Tapez **172.16.0.100** en regard de **Adresse IP de début** et **172.16.0.110** en regard de **Adresse IP de fin**, puis cliquez sur **OK**. Vérifiez que 11 adresses IP ont été attribuées aux clients distants, puis cliquez sur **Suivant**.
11. Sur la page **Gestion de serveurs d'accès à distance multiples**, vérifiez que la case à cocher **Non, utiliser Routage et accès distant pour authentifier les demandes de connexion** est activée, puis cliquez sur **Suivant**.
12. Cliquez sur **Terminer**.
13. Cliquez sur **OK** à deux reprises, et attendez que le service Routage et accès distant démarre.
14. Basculez vers **Serveur NPS (Network Policy Server)**.
15. Dans **Serveur NPS**, cliquez sur le nœud **Stratégies de demande de connexion**, et dans le volet de résultats, vérifiez que **Stratégie du service Routage et accès à distance Microsoft** est **Désactivé**.

Remarque : Cliquez sur **Action**, puis sur **Actualiser**. Si l'option **Stratégie du service Routage et accès à distance Microsoft** est activée, cliquez dessus avec le bouton droit, puis cliquez sur **Désactiver**.

16. Fermez la console de gestion NPS.
17. Fermez la console Routage et accès distant.

▶ Tâche 2 : Autoriser les tests ping à des fins de test

1. Sur LON-RTR, suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
2. Cliquez sur **Outils d'administration**, puis double-cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité**.
3. Cliquez sur **Règles de trafic entrant**, cliquez avec le bouton droit sur **Règles de trafic entrant**, puis cliquez sur **Nouvelle règle**.
4. Sélectionnez **Personnalisée**, puis cliquez sur **Suivant**.
5. Vérifiez que **Tous les programmes** est sélectionné, puis cliquez sur **Suivant**.
6. En regard de **Type de protocole**, sélectionnez **ICMPv4**, puis cliquez sur **Perso...**.
7. Sélectionnez **Certains types ICMP**, activez la case à cocher **Requête d'écho**, cliquez sur **OK**, puis sur **Suivant**.
8. Cliquez sur **Suivant** pour accepter l'étendue par défaut.
9. Dans la fenêtre Action, vérifiez que l'option **Autoriser la connexion** est sélectionnée et cliquez sur **Suivant**.
10. Cliquez sur **Suivant** pour accepter le profil par défaut.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans la fenêtre Nom, sous **Nom**, tapez **ICMPv4 echo request**, puis cliquez sur **Terminer**.
12. Fermez la console Pare-feu Windows avec fonctions avancées de sécurité.

Résultats : À la fin de cet exercice, vous aurez créé un serveur VPN et configuré des communications entrantes.

Exercice 3 : Configuration des paramètres clients pour prendre en charge la protection d'accès réseau (NAP)

▶ Tâche 1 : Activer une méthode de contrainte de mise en conformité NAP d'un client

1. Basculez vers l'ordinateur LON-CL2.
2. Sur l'écran d'accueil, saisissez **napclcfg.msc**, puis appuyez sur Entrée.
3. Dans NAPCLCFG – [configuration de client NAP (ordinateur local)], dans le volet de navigation, cliquez sur **Clients de contrainte**.
4. Dans le volet de résultats, cliquez avec le bouton droit sur **Client de contrainte de quarantaine EAP**, puis cliquez sur **Activer**.
5. Fermez NAPCLCFG – [configuration du client NAP (ordinateur local)].
6. Positionnez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
7. Dans Accueil, tapez **Services.msc**, puis appuyez sur Entrée.
8. Dans Services, dans le volet de résultats, double-cliquez sur **Agent de protection d'accès réseau**.
9. Dans la boîte de dialogue **Propriétés de Agent de protection d'accès réseau (ordinateur local)**, dans la liste **Type de démarrage**, cliquez sur **Automatique**.
10. Cliquez sur **Accueil**, puis sur **OK**.
11. Positionnez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
12. Dans Accueil, tapez **gpedit.msc**, puis appuyez sur Entrée.
13. Dans l'arborescence de la console, développez successivement (si nécessaire) **Stratégie Ordinateur local**, **Ordinateur Configuration**, **Modèles d'administration**, **Composants Windows**, puis cliquez sur **Centre de sécurité**.
14. Double-cliquez sur **Activer le Centre de sécurité (ordinateurs appartenant à un domaine uniquement)**, cliquez sur **Activé**, puis sur **OK**.
15. Fermez la fenêtre de la console.
16. Fermez la console Services, puis fermez les fenêtres Outils d'administration et Système et sécurité.

▶ Tâche 2 : Établir une connexion VPN

1. Sur LON-CL2, sur le Bureau, indiquez votre souris le coin inférieur droit de la barre des tâches, puis cliquez sur **Paramètres**.
2. Cliquez sur **Panneau de configuration**, puis sur **Réseau et Internet**.
3. Cliquez sur **Centre Réseau et partage**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Cliquez sur **Configurer une nouvelle connexion ou un nouveau réseau**.
5. Sur la page **Choisir une option de** connexion, cliquez sur **Connexion à votre espace de travail**, puis sur **Suivant**.
6. Sur la page **Comment voulez-vous vous connecter ?**, cliquez sur **Utiliser ma connexion Internet (VPN)**.
7. Cliquez sur **Je configurerai une connexion Internet ultérieurement**.
8. Sur la page **Entrez l'adresse Internet à laquelle vous souhaitez vous connecter**, dans le champ **Adresse Internet**, tapez **10.10.0.1**.
9. Dans la zone **Nom de la destination**, tapez **VPN Adatum**.
10. Activez la case à cocher **Autoriser d'autres personnes à utiliser cette connexion**, puis cliquez sur **Créer**.
11. Dans la fenêtre Centre Réseau et partage, cliquez sur **Modifier les paramètres de la carte**.
12. Cliquez avec le bouton droit sur la connexion **VPN Adatum**, cliquez sur **Propriétés**, puis cliquez sur l'onglet **Sécurité**.
13. Sous **Authentification**, cliquez sur **Utiliser le protocole EAP (Extensible Authentication Protocol)**.
14. Dans la liste **Microsoft : Mot de passe sécurisé (EAP-MSCHAP v2) (chiffrement activé)**, sélectionnez **Microsoft : PEAP (Protected EAP) (chiffrement activé)**, puis cliquez sur **Propriétés**.
15. Vérifiez que la case à cocher **Vérifier l'identité du serveur en validant le certificat** est activée.
16. Désactivez la case à cocher **Connexion à ces serveurs**, puis sous **Sélectionner la méthode d'authentification**, vérifiez que **Mot de passe sécurisé (EAP-MSCHAP version 2)** est sélectionné.
17. Désactivez la case à cocher **Activer la reconnexion rapide**, puis activez la case à cocher **Appliquer la protection d'accès réseau**.
18. Cliquez deux fois sur **OK** pour accepter ces paramètres.
19. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur la connexion **VPN Adatum**, puis cliquez sur **Connecter/Déconnecter**.
20. Dans la liste **Réseaux** de droite, cliquez sur **VPN Adatum**, puis sur **Connexion**.
21. Dans Authentification réseau, dans le champ **Nom d'utilisateur**, tapez **ADATUM\Administrateur**.
22. Dans le champ **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **OK**.
23. La fenêtre Alerte de sécurité Windows s'affiche la première fois que cette connexion VPN est utilisée. Cliquez sur **Afficher les détails du certificat**.
24. Cliquez sur **Connecter**. Attendez que la connexion VPN soit établie. Étant donné que l'ordinateur LON-CL2 est conforme, il doit bénéficier d'un accès illimité au sous-réseau intranet.
25. Positionnez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
26. Dans Accueil, tapez **cmd.exe**, puis appuyez sur Entrée.
27. Tapez **ipconfig /all**, puis appuyez sur Entrée. Affichez la configuration IP. L'option **État de quarantaine du système** doit être définie sur **Non restreint**.
28. À l'invite de commandes, tapez **ping 172.16.0.10**, puis appuyez sur Entrée. L'opération doit réussir. Le client répond à présent au critère défini pour une connectivité VPN satisfaisante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

29. Basculez vers Connexions réseau.
30. Cliquez avec le bouton droit sur **VPN Adatum**, puis cliquez sur **Connecter/Déconnecter**.
31. Dans la liste **Réseaux** de droite, cliquez sur **VPN Adatum,** puis sur **Déconnexion**.
32. Basculez vers LON-RTR.
33. Dans Outils d'administration, double-cliquez sur **Serveur NPS**.
34. Développez successivement **Protection d'accès réseau**, **Programmes de validation d'intégrité système**, **Programme de validation d'intégrité de la sécurité Windows**, puis cliquez sur **Paramètres**.
35. Dans le volet de droite, sous **Nom**, double-cliquez sur **Configuration par défaut**.
36. Sur l'onglet **Windows 8/Windows 7/Windows Vista**, sélectionnez la case à cocher **Restreindre l'accès des clients qui n'ont pas intallé toutes les mises à jour de sécurité disponibles ne sont pas installées**, puis cliquez sur **OK**.
37. Basculez vers LON-CL2.
38. Dans la liste **Réseaux** de droite, cliquez sur **VPN Adatum**, puis sur **Connexion**.
39. Revenez à l'invite de commandes.
40. Tapez **ipconfig /all**, puis appuyez sur Entrée. Affichez la configuration IP. L'option **État de quarantaine du système** doit avoir la valeur **Restreint**.
41. Basculez vers Connexions réseau.
42. Cliquez avec le bouton droit sur **VPN Adatum, puis cliquez sur** Connecter/Déconnecter.
43. Dans la liste **Réseaux** de droite, cliquez sur **VPN Adatum,** puis sur **Déconnexion**.

Résultats : À la fin de cet exercice, vous devriez avoir créé une nouvelle connexion VPN sur LON-CL2, et avoir activé et testé NAP sur LON-CL2.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial de tous les ordinateurs virtuels. Pour cela, 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 **22411B-LON-CL2**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22411B-LON-RTR** et **22411B-LON-DC1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 10: Optimisation des services de fichiers

Atelier pratique A : Configuration des quotas et du filtrage des fichiers à l'aide de FSRM

Exercice 1 : Configuration des quotas FSRM

▶ Tâche 1 : Créer un modèle de quota

1. Connectez-vous à LON-SVR1 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la barre des tâches, cliquez sur le raccourci **Gestionnaire de serveur**.
3. Dans le **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
4. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
5. Vérifiez que l'installation basée sur un rôle ou une fonctionnalité est sélectionnée, puis cliquez sur **Suivant**.
6. Vérifiez que **LON-SVR1.Adatum.com** est sélectionné, puis cliquez sur **Suivant**.
7. Dans la page **Sélectionner des rôles de serveurs**, développez **Service de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, puis activez la case à cocher **Gestionnaire de ressources du serveur de fichiers**.
8. Dans la fenêtre contextuelle, cliquez sur **Ajouter des fonctionnalités**.
9. Cliquez sur **Suivant** deux fois pour confirmer la sélection du service de rôle et de la fonctionnalité.
10. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. Une fois l'installation réussie, cliquez sur **Fermer**.
12. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire de ressources du serveur de fichiers**.
13. Dans la console Gestionnaire de ressources du serveur de fichiers, développez **Gestion de quota**, puis cliquez sur **Modèles de quotas**.
14. Cliquez avec le bouton droit sur **Modèles de quotas**, puis cliquez sur **Créer un modèle de quota**.
15. Dans la boîte de dialogue **Créer un modèle de quota**, dans le champ **Nom du modèle**, tapez **Journal limité à 100 Mo dans l' Observateur d'événements**.
16. Sous **Seuils de notification**, cliquez sur **Ajouter**.
17. Dans la boîte de dialogue **Ajouter un seuil**, cliquez sur l'onglet **Journal des événements**.
18. Sous l'onglet **Journal des événements**, activez la case à cocher **Envoyer un avertissement au journal des événements**, puis cliquez sur **OK**.
19. Dans la boîte de dialogue **Créer un modèle de quota**, cliquez sur **Ajouter**.
20. Dans la boîte de dialogue **Ajouter un seuil**, dans le champ **Générer des notifications lorsque l'utilisation atteint (%)**, tapez **100**.
21. Cliquez sur l'onglet **Journal des événements**, activez la case à cocher **Envoyer un avertissement au journal des événements**, puis cliquez sur **OK** deux fois.

▶ Tâche 2 : Configurer un quota à partir du modèle de quota

1. Dans la console Gestionnaire de ressources du serveur de fichiers, cliquez sur **Quotas**.
2. Cliquez avec le bouton droit sur **Quotas**, puis cliquez sur **Créer un quota**.
3. Dans la boîte de dialogue **Créer un quota**, dans le champ **Chemin d'accès du quota**, tapez **E:\Labfiles\Mod10\Users**.
4. Cliquez sur **Appliquer automatiquement le modèle et créer des quotas sur les sous-dossiers existants et nouveaux**.
5. Dans la liste **Dériver les propriétés de ce modèle de quota (recommandé)**, cliquez sur **Journal limité à 100 Mo dans l' Observateur d'événements**, puis cliquez sur **Créer**.
6. Dans le volet de détails, vérifiez que le chemin d'accès **E:\Labfiles\Mod10\Users** a été configuré avec sa propre entrée de quota. Vous devrez peut-être actualiser le dossier **Quotas** pour afficher les modifications.
7. À partir de la barre des tâches, ouvrez l'Explorateur de fichiers.
8. Dans la fenêtre de l'Explorateur de fichiers, cliquez sur le lecteur **E:**, développez **Labfiles** (si nécessaire), **Mod10**, puis **Users**.
9. Dans le dossier **Users**, créez un dossier nommé **Max**.
10. Dans le Gestionnaire de ressources du serveur de fichiers, dans le menu **Action**, cliquez sur **Actualiser**.
11. Dans le volet de détails, vous noterez que le dossier que vous venez de créer s'affiche désormais dans la liste.

▶ Tâche 3 : Vérifier que le quota est fonctionnel

1. Sur LON-SVR1, cliquez sur le raccourci **Windows PowerShell** dans la barre des tâches.
2. Dans la fenêtre Windows PowerShell, tapez les commandes suivantes. Appuyez sur Entrée à la fin de chaque ligne :

```
E:
cd \Labfiles\Mod10\Users\Max
fsutil file createnew file1.txt 89400000
```

   Cette opération crée un fichier de plus de 85 mégaoctets (Mo), ce qui génère un avertissement dans l'Observateur d'événements.

3. Dans la barre des tâches, cliquez sur le raccourci **Gestionnaire de serveur**.
4. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Observateur d'événements**.
5. Dans la console Observateur d'événements, développez **Journaux Windows**, puis cliquez sur **Application**.
6. Dans le volet de détails, notez l'événement ayant l'**ID événement 12325**.
7. Dans la fenêtre Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
fsutil file createnew file2.txt 16400000
```

   Remarquez que le fichier ne peut pas être créé. Le message retourné par Windows fait référence à l'espace disque, mais la création du fichier a échoué car sa taille dépasserait la limite de quota.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Dans la fenêtre Windows PowerShell, tapez **exit**, puis appuyez sur Entrée.
9. Fermez toutes les fenêtres ouvertes sur LON-SVR1.

Résultats : À la fin de cet exercice, vous devez avoir configuré un quota FSRM.

Exercice 2 : Configuration du filtrage de fichiers et des rapports de stockage

▶ Tâche 1 : Créer un filtre de fichiers

1. Sur LON-SVR1, ouvrez le Gestionnaire de serveur, puis, dans le menu **Outils**, cliquez sur **Gestionnaire de ressources du serveur de fichiers**.
2. Dans l'arborescence de la console **Gestionnaire de ressources du serveur de fichiers**, développez **Gestion du filtrage de fichiers**, puis cliquez sur **Filtres de fichiers**.
3. Cliquez avec le bouton droit sur **Filtres de fichiers**, puis cliquez sur **Créer un filtre de fichiers**.
4. Dans la fenêtre Créer un filtre de fichiers, dans la zone de texte **Chemin d'accès du filtre de fichiers**, tapez **E:\Labfiles\Mod10\Users**.
5. Dans la fenêtre Créer un filtre de fichiers, dans la zone de liste déroulante **Dériver les propriétés de ce modèle de filtre de fichiers (recommandé)**, vérifiez que **Bloquer les fichiers audio et vidéo** est sélectionné.
6. Cliquez sur **Créer**.

▶ Tâche 2 : Créer un groupe de fichiers

1. Sur LON-SVR1, cliquez avec le bouton droit sur **Gestionnaire de ressources du serveur de fichiers (local)**, puis sur cliquez sur **Configurer les options**.
2. Dans la boîte de dialogue **Options du Gestionnaire de ressources du serveur de fichiers**, cliquez sur l'onglet **Vérification du filtrage de fichiers**.
3. Sous l'onglet **Vérification du filtrage de fichiers**, activez la case à cocher **Enregistrer l'activité de filtrage de fichiers dans la base de données de vérification**, puis cliquez sur **OK**.

Remarque : cette étape consiste à enregistrer les événements de filtrage de fichiers. Les enregistrements générés fournissent des données pour un rapport de vérification du filtrage des fichiers, qui sera exécuté ultérieurement dans cet exercice.

4. Dans l'arborescence de la console Gestionnaire de ressources du serveur de fichiers, développez **Gestion du filtrage de fichiers**, puis cliquez sur **Groupes de fichiers**.
5. Cliquez avec le bouton droit sur **Groupes de fichiers**, puis cliquez sur **Créer un groupe de fichiers**.
6. Dans la fenêtre Créer les propriétés du groupe de fichiers, dans la zone **Nom du groupe de fichiers**, tapez **Fichiers multimédias de multiplexeur**.
7. Dans la zone Fichiers à inclure, tapez ***.mp***, puis cliquez sur **Ajouter**.
8. Dans la zone **Fichiers à exclure**, tapez ***.mpp**, cliquez sur **Ajouter**, puis cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Dans l'arborescence de la console Gestionnaire de ressources du serveur de fichiers, développez **Gestion du filtrage de fichiers**, puis cliquez sur **Modèles de filtres de fichiers**.
10. Cliquez avec le bouton droit sur le modèle **Bloquer les fichiers audio et vidéo**, puis cliquez sur **Modifier les propriétés du modèle**.
11. Sous l'onglet **Paramètres**, sous **Groupes de fichiers**, désactivez la case à cocher en regard de **Fichiers audio et vidéo**.
12. Activez la case à cocher en regard de **Fichiers multimédias de multiplexeur**.
13. Cliquez sur **OK**. Cliquez sur **Oui** à l'invite de message.
14. Dans le message qui s'affiche, cliquez sur **OK**.

▶ Tâche 3 : Tester le filtre de fichiers

1. Dans la barre des tâches, cliquez sur le raccourci de l'**Explorateur de fichiers**.
2. Dans la fenêtre de l'Explorateur de fichiers, dans le volet gauche, cliquez sur **Allfiles (E:)**.
3. Dans le volet droit, cliquez avec le bouton droit et pointez sur **Nouveau**, puis cliquez sur **Document texte**.
4. Renommez **New Text Document.txt** en **musicfile.mp3**. Cliquez sur **Oui** pour modifier l'extension du nom de fichier.
5. Cliquez avec le bouton droit sur **musicfile.mp3**, puis cliquez sur **Copier**.
6. Dans le volet gauche, développez **Allfiles (E:)**, développez **Labfiles**, développez **Mod10**, cliquez avec le bouton droit sur **Users**, puis cliquez sur **Coller**. Vous allez être averti que le système n'a pas pu copier le fichier vers E:\Labfiles\Mod10\Users.
7. Cliquez sur **Annuler**.

▶ Tâche 4 : Générer un rapport de stockage à la demande

1. Dans la console Gestionnaire de ressources du serveur de fichiers, cliquez sur **Gestion des rapports de stockage**.
2. Cliquez avec le bouton droit sur **Gestion des rapports de stockage**, puis cliquez sur **Générer les rapports maintenant**.
3. Sous **Sélectionner les rapports à générer**, activez la case à cocher **Vérification du filtrage des fichiers**.
4. Cliquez sur l'onglet **Étendue**, puis sur **Ajouter**.
5. Dans la boîte de dialogue **Rechercher un dossier**, accédez à **E:\Labfiles\Mod10\Users**, puis cliquez sur **OK**.
6. Cliquez sur **OK** pour fermer la fenêtre **Propriétés des tâches de rapports de stockage**.
7. Dans la boîte de dialogue **Générer des rapports de stockage**, vérifiez que l'option **Attendre que les rapports soient générés avant de les afficher**, puis cliquez sur **OK**.
8. Dans Windows Internet Explorer, examinez les rapports HTML générés.
9. Fermez toutes les fenêtres ouvertes sur LON-SVR1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Pour préparer l'atelier suivant

- Une fois l'atelier pratique terminé, n'arrêtez pas les ordinateurs virtuels. Vous allez en avoir besoin pour l'atelier pratique suivant.

Résultats : À la fin de cet exercice, vous aurez configuré des rapports de filtrage de fichiers et de stockage dans FSRM.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique B : Implémentation de DFS

Exercice 1 : Installation du service de rôle DFS

▶ Tâche 1 : Installer le service de rôle DFS sur LON-SVR1

1. Basculez vers LON-SVR1.
2. Dans la barre des tâches, cliquez sur **Gestionnaire de serveur**.
3. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
4. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
7. Dans la page **Sélectionner des rôles de serveurs,** développez **Service de fichiers et de stockage (Installé)**, **Services de fichiers et iSCSI (Installé)**, puis activez la case à cocher **Espaces de noms DFS**.
8. Dans la fenêtre contextuelle Ajouter des rôles et fonctionnalités, cliquez sur **Ajouter des fonctionnalités**.
9. Activez la case à cocher **Réplication DFS**, puis cliquez sur **Suivant**.
10. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
11. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
12. Une fois l'installation réussie, cliquez sur **Fermer**.
13. Fermez le Gestionnaire de serveur.

▶ Tâche 2 : Installer le service de rôle DFS sur LON-SVR4

1. Basculez vers LON-SVR4.
2. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, 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,** développez **Service de fichiers et de stockage (Installé)**, **Services de fichiers et iSCSI (Installé)**, puis activez la case à cocher **Espaces de noms DFS**.
7. Dans la fenêtre contextuelle Ajouter des rôles et fonctionnalités, cliquez sur **Ajouter des fonctionnalités**.
8. Activez la case à cocher **Réplication DFS**, puis cliquez sur **Suivant**.
9. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
10. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Une fois l'installation réussie, cliquez sur **Fermer**.
12. Fermez le Gestionnaire de serveur.

Résultats : À la fin de cet exercice, vous aurez installé le service de rôle DFS sur LON-SVR1 et sur LON-SVR4.

Exercice 2 : Configuration d'un espace de noms DFS

▶ Tâche 1 : Créer l'espace de noms BranchDocs

1. Basculez vers LON-SVR1, puis ouvrez le **Gestionnaire de serveur**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion du système de fichiers distribués DFS**.
3. Dans le volet de navigation, cliquez sur **Espaces de noms**.
4. Cliquez avec le bouton droit sur **Espaces de noms**, puis cliquez sur **Nouvel espace de noms**.
5. Dans l'Assistant Nouvel espace de noms, dans la page **Serveur d'espaces de noms**, sous **Serveur**, tapez LON-SVR1, puis cliquez sur **Suivant**.
6. Dans la page **Nom et paramètres de l'espace de noms**, sous **Nom**, tapez **BranchDocs**, puis cliquez sur **Suivant**.
7. Dans la page **Type d'espace de noms**, vérifiez que l'option **espace de noms de domaine** est sélectionnée. Notez que l'espace de noms sera accessible via **\\Adatum.com\BranchDocs**.
8. Vérifiez que la case à cocher **Activer le mode Windows Server 2008** est activée, puis cliquez sur **Suivant**.
9. Dans la page **Revoir les paramètres et créer l'espace de noms**, cliquez sur **Créer**.
10. Dans la page **Confirmation**, vérifiez que la tâche **Créer un espace de noms** a réussi, puis cliquez sur **Fermer**.
11. Dans le volet de navigation, développez **Espaces de noms**, puis cliquez sur **\\Adatum.com\BranchDocs**.
12. Dans le volet de détails, cliquez sur l'onglet **Serveurs d'espaces de noms**, et assurez-vous qu'il existe une entrée activée pour **\\LON-SVR1\BranchDocs**.

▶ Tâche 2 : Activer l'énumération basée sur l'accès pour l'espace de noms BranchDocs

1. Dans le volet de navigation, sous **Espaces de noms**, cliquez avec le bouton droit sur **\\Adatum.com\BranchDocs**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés de : \\Adatum.com\BranchDocs**, cliquez sur l'onglet **Avancé**.
3. Sous l'onglet **Avancé**, activez la case à cocher **Activer l'énumération basée sur l'accès pour cet espace de noms**, puis cliquez sur **OK**.

▶ Tâche 3 : Ajouter le dossier ResearchTemplates à l'espace de noms BranchDocs

1. Dans Gestion du système de fichiers distribués DFS, cliquez avec le bouton droit sur **Adatum.com\BranchDocs**, puis cliquez sur **Nouveau dossier**.
2. Dans la boîte de dialogue **Nouveau dossier**, sous **Nom**, tapez **ResearchTemplates**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la boîte de dialogue **Nouveau dossier**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Ajouter une cible de dossier**, tapez **\\LON-SVR4\ResearchTemplates**, puis cliquez sur **OK**.
5. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
6. Dans la boîte de dialogue **Créer un partage**, dans le champ **Chemin d'accès local du dossier partagé**, tapez **C:\BranchDocs\ResearchTemplates**.
7. Cliquez sur **Tous les utilisateurs disposent d'autorisations de lecture/écriture**, puis cliquez sur **OK**.
8. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
9. Cliquez à nouveau sur **OK** pour fermer la boîte de dialogue **Nouveau dossier**.

▶ Tâche 4 : Ajouter le dossier DataFiles à l'espace de noms BranchDocs

1. Dans Gestion du système de fichiers distribués DFS, cliquez avec le bouton droit sur **Adatum.com\BranchDocs**, puis cliquez sur **Nouveau dossier**.
2. Dans la boîte de dialogue **Nouveau dossier**, sous **Nom**, tapez **DataFiles**, puis cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une cible de dossier**, tapez **\\LON-SVR1\DataFiles**, puis cliquez sur **OK**.
4. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
5. Dans la boîte de dialogue **Créer un partage**, dans le champ **Chemin d'accès local du dossier partagé**, tapez **C:\BranchDocs\DataFiles**.
6. Cliquez sur **Tous les utilisateurs disposent d'autorisations de lecture/écriture**, puis cliquez sur **OK**. Les autorisations seront configurées plus tard.
7. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
8. Cliquez à nouveau sur **OK** pour fermer la boîte de dialogue **Nouveau dossier**.

▶ Tâche 5 : Vérifier l'espace de noms BranchDocs

1. Sur **LON-SVR1**, ouvrez l'Explorateur de fichiers, puis dans la barre d'adresses, tapez **\\Adatum.com\BranchDocs**, puis appuyez sur Entrée.
2. Dans la fenêtre BranchDocs, vérifiez que **ResearchTemplates** et **DataFiles** s'affichent.
3. Fermez la fenêtre BranchDocs.

Résultats : À la fin de cet exercice, vous aurez configuré un espace de noms DFS.

Exercice 3 : Configuration de la réplication DFS

▶ Tâche 1 : Créer une autre cible de dossier pour DataFiles

1. Dans Gestion du système de fichiers distribués DFS, développez **Adatum.com\BranchDocs**, puis cliquez sur **DataFiles**.
2. Dans le volet de détails, vous constatez qu'il n'existe actuellement qu'une seule cible de dossier.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Cliquez avec le bouton droit sur **DataFiles**, puis cliquez sur **Ajouter une cible de dossier**.
4. Dans la boîte de dialogue **Nouvelle cible de dossier**, sous **Chemin d'accès à la cible de dossier**, tapez **\\LON-SVR4\DataFiles**, puis cliquez sur **OK**.
5. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui** pour créer le dossier partagé sur LON-SVR4.
6. Dans la boîte de dialogue **Créer un partage**, sous **Chemin d'accès local du dossier partagé**, tapez **C:\BranchDocs\DataFiles**.
7. Dans la boîte de dialogue **Créer un partage**, sous **Autorisations du dossier partagé**, sélectionnez **Tous les utilisateurs disposent d'autorisations de lecture/écriture**, puis cliquez sur **OK**.
8. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui** pour créer le dossier sur LON-SVR4.
9. Dans la boîte de dialogue **Réplication**, cliquez sur **Oui**. L'Assistant Réplication de dossier démarre.

▶ Tâche 2 : Configurer la réplication pour l'espace de noms

1. Dans Gestion du système de fichiers distribués DFS, dans l'Assistant Réplication de dossier, dans les pages **Nom du groupe de réplication et du dossier répliqué**, acceptez les paramètres par défaut, puis cliquez sur **Suivant**.
2. Dans la page **Éligibilité de réplication**, cliquez sur **Suivant**.
3. Dans la page **Membre principal**, sélectionnez **LON-SVR1**, puis cliquez sur **Suivant**.
4. Dans la page **Sélection de topologie**, sélectionnez **Aucune topologie**, puis cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Avertissement**, cliquez sur **OK**.
6. Dans la page **Vérifier les paramètres et créer le groupe de réplication**, cliquez sur **Créer**.
7. Dans la page **Confirmation**, cliquez sur **Fermer**.
8. Dans la boîte de dialogue **Délai de réplication**, cliquez sur **OK**.
9. Dans la console Gestion du système de fichiers distribués DFS, cliquez avec le bouton droit sur **Réplication**, puis cliquez sur **Adatum.com\BranchDocs\DataFiles**.
10. Dans le volet Actions, cliquez sur **Nouvelle topologie**.
11. Dans l'Assistant Nouvelle topologie, dans la page **Sélection de topologie**, vérifiez que **Maille pleine** est sélectionné, puis cliquez sur **Suivant**.
12. Dans la page **Planification du groupe de réplication et bande passante**, cliquez sur **Suivant**.
13. Dans la page **Vérifier les paramètres et créer la topologie**, cliquez sur **Créer**.
14. Dans la page **Confirmation**, cliquez sur **Fermer**, puis dans la boîte de dialogue **Délai de réplication**, cliquez sur **OK**.
15. Dans le volet de détails, sous l'onglet **Appartenances**, vérifiez que le dossier répliqué s'affiche à la fois sur LON-SVR4 et LON-SVR1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : 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 **22411B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez ces étapes pour **22411B-LON-SVR1** et **22411B-LON-SVR4**.

Résultats : À la fin de cet exercice, vous aurez configuré la réplication DFS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 11: Configuration du chiffrement et de l'audit avancé

Atelier pratique : Configuration du chiffrement et de l'audit avancé

Exercice 1 : Chiffrement et récupération des fichiers

▶ Tâche 1 : Mettre à jour le certificat d'agent de récupération pour le système EFS

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans Gestion des stratégies de groupe, développez **Forêt : Adatum.com**, développez **Domaines**, développez **Adatum.com**, puis cliquez sur **Default Domain Policy**.
3. Dans la boîte de dialogue **Console de gestion des stratégies de groupe**, cliquez sur **OK** pour effacer le message.
4. Cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
5. Dans la fenêtre Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, développez successivement **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, **Stratégies de clé publique**, puis cliquez sur **Système de fichiers EFS (Encrypting File System)**.
6. Cliquez avec le bouton droit sur le certificat **Administrateur**, puis cliquez sur **Supprimer**.
7. Dans la fenêtre Certificats, cliquez sur **Oui**.
8. Cliquez avec le bouton droit sur **Système de fichiers EFS (Encrypting File System)**, puis cliquez sur **Créer un agent de récupération de données**.
9. Lisez les informations pour le nouveau certificat créé. Notez que ce certificat a été obtenu à partir d'AdatumCA.
10. Fermez l'Éditeur de gestion des stratégies de groupe.
11. Fermez Gestion des stratégies de groupe.

▶ Tâche 2 : Mettre à jour la stratégie de groupe sur les ordinateurs

1. Sur LON-DC1, cliquez sur le raccourci de l'interface de ligne de commande Windows PowerShell® dans la barre des tâches.
2. Sur invitation de Windows PowerShell, tapez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

3. Fermez la fenêtre d'invite de commandes.
4. Basculez vers LON-CL1.
5. Sur LON-CL1, dans l'écran Accueil, tapez **cmd**, puis appuyez sur Entrée.
6. Dans l'invite, tapez la commande suivante, puis appuyez sur Entrée :

```
gpupdate /force
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Fermez la fenêtre d'invite de commandes.
8. Fermez la session sur LON-CL1.

▶ Tâche 3 : Obtenir un certificat pour EFS

1. Sur LON-CL1, connectez-vous en tant qu'**ADATUM\Doug** avec le mot de passe **Pa$$w0rd**.
2. Dans l'écran Accueil, tapez **mmc**, puis appuyez sur Entrée.
3. Dans Console1, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
4. Dans la liste des composants logiciels enfichables disponibles, cliquez sur **Certificats**, puis sur **Ajouter**.
5. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **OK**.
6. Dans le volet de gauche, cliquez sur **Certificats – Utilisateur actuel**, cliquez avec le bouton droit sur **Personnel**, pointez sur **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.
7. Dans l'Assistant Inscription de certificat, cliquez sur **Suivant**.
8. Dans la page **Sélectionner la stratégie d'inscription de certificat**, cliquez sur **Suivant** pour utiliser la stratégie d'inscription Active Directory.
9. Dans la page **Demander des certificats**, activez la case à cocher **EFS basique**, puis cliquez sur **Inscription**.
10. Dans la page **Résultats de l'installation des certificats**, cliquez sur **Terminer**.
11. Dans la fenêtre Console1, dans le volet de gauche, développez **Certificats – Utilisateur actuel**, développez **Personnel**, puis cliquez sur **Certificats**.
12. Lisez les détails du certificat, et notez qu'il a été émis par AdatumCA.
13. Fermez la fenêtre Console1 sans enregistrer les paramètres.

▶ Tâche 4 : Chiffrer un fichier

1. Sur LON-CL1, ouvrez l'**Explorateur de fichiers** et tapez **\\LON-DC1\Mod11Share\Marketing** dans la barre d'adresse, puis appuyez sur Entrée.
2. Cliquez avec le bouton droit sur **DougFile**, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Général**, cliquez sur **Avancé**.
4. Dans la boîte de dialogue **Attributs avancés**, activez la case à cocher **Chiffrer le contenu pour sécuriser les données**, puis cliquez sur **OK**.
5. Dans la boîte de dialogue **Propriétés de : DougFile**, cliquez sur **OK**.
6. Dans la boîte de dialogue **Avertissement de chiffrement**, sélectionnez **Chiffrer le fichier uniquement**, puis cliquez sur **OK**. Patientez quelques secondes pendant le chiffrement du fichier.
7. Examinez la couleur du nom de fichier.
8. Fermez la fenêtre de l'Explorateur de fichiers®.
9. Fermez la session sur LON-CL1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Utiliser l'agent de récupération pour ouvrir le fichier

1. Sur LON-DC1, cliquez sur le raccourci de l'**Explorateur de fichiers** sur la barre des tâches.
2. Dans l'Explorateur de fichiers, accédez à **E:\Labfiles\Mod11\Mod11Share\Marketing**.
3. Double-cliquez sur **DougFile.txt**.
4. Dans le Bloc-notes, ajoutez du texte au fichier, cliquez sur **Fichier**, puis sur **Enregistrer**.
5. Fermez le Bloc-notes et l'Explorateur de fichiers.

Résultats : À la fin de cet exercice, vous aurez chiffré et récupéré des fichiers.

Exercice 2 : Configuration de l'audit avancé

▶ Tâche 1 : Créer un objet de stratégie de groupe pour l'audit avancé

1. Sur LON-DC1, ouvrez le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Adatum.com**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
3. Tapez **Serveurs de fichiers**, puis appuyez sur Entrée.
4. Cliquez sur le conteneur **Computers**, cliquez avec le bouton droit sur **LON-SVR1**, cliquez sur **Déplacer**, sur l'unité d'organisation **Serveurs de fichiers**, puis sur **OK**.
5. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
6. Dans Gestion des stratégies de groupe, développez **Forêt : Adatum.com**, développez **Domaines**, développez **Adatum.com**, cliquez avec le bouton droit sur **Serveurs de fichiers**, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**.
7. Dans la fenêtre Nouvel objet de stratégie de groupe, tapez **Audit de fichier**, puis appuyez sur Entrée.
8. Double-cliquez sur le conteneur **Objets de stratégie de groupe**, cliquez avec le bouton droit sur **Audit de fichier**, puis cliquez sur **Modifier**.
9. Dans l'Éditeur de gestion de stratégies de groupe, sous **Configuration ordinateur**, développez successivement **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, **Configuration avancée de la stratégie d'audit**, **Stratégies d'audit**, puis cliquez sur **Accès à l'objet**.
10. Double-cliquez sur **Auditer le partage de fichiers détaillé**.
11. Dans la boîte de dialogue **Propriétés**, activez la case à cocher **Configurer les événements d'audit suivants**.
12. Activez les cases à cocher **Succès** et **Échec**, puis cliquez sur **OK**.
13. Double-cliquez sur **Auditer le stockage amovible**.
14. Dans la boîte de dialogue **Propriétés**, activez la case à cocher **Configurer les événements d'audit suivants**.
15. Activez les cases à cocher **Succès** et **Échec**, puis cliquez sur **OK**.
16. Fermez l'Éditeur de gestion des stratégies de groupe.
17. Redémarrez LON-SVR1.
18. Connectez-vous à LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

▶ Tâche 2 : Vérifier les entrées d'audit

1. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Allan** avec le mot de passe **Pa$$w0rd**.
2. Dans l'écran Accueil, tapez **\\LON-SVR1\Mod11**, puis appuyez sur Entrée.
3. Double-cliquez sur le fichier **Testfile.txt** pour l'ouvrir dans le Bloc-notes.
4. Fermez le Bloc-notes.
5. Basculez vers LON-SVR1.
6. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Observateur d'événements**.
7. Dans l'Observateur d'événements, double-cliquez sur **Journaux Windows**, puis cliquez sur **Sécurité**.
8. Double-cliquez sur l'une des entrées du journal dont la **Source** est **Microsoft Windows security auditing** et la **Catégorie de tâche** est **Partage de fichiers détaillé**.
9. Cliquez sur l'onglet **Détails** et notez l'accès exécuté.

Résultats : À la fin de cet exercice, vous aurez configuré l'audit avancé.

▶ Tâche 3 : 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 **22411B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez ces étapes pour **22411B-LON-SVR1** et **22411B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 12: Implémentation de la gestion des mises à jour

Atelier pratique : Implémentation de la gestion des mises à jour

Exercice 1 : Implémentation du rôle serveur WSUS

▶ Tâche 1 : Installation du rôle serveur Windows Server Update Services (WSUS)

1. Connectez-vous sur LON-SVR4 en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur LON-SVR4, dans **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
3. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Suivant**.
4. 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**.
5. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, sélectionnez la case à cocher **Windows Server Update Services**.
7. Dans la fenêtre contextuelle, cliquez sur **Ajouter des fonctionnalités**.
8. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
9. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
10. Sur la page **Services WSUS (Windows Server Update Services)**, cliquez sur **Suivant**.
11. Sur la page **Sélectionner des services de rôle**, confirmez que **WID Database** et **WSUS Services** sont sélectionnés, puis cliquez sur **Suivant**.
12. Sur la page **Sélection de l'emplacement du contenu**, dans la zone de texte, saisissez **C:\MisesajourWSUS**, puis cliquez sur **Suivant**.
13. Dans la page **Rôle Serveur Web (IIS)**, cliquez sur **Suivant**.
14. Dans la page **Sélectionner des services de rôle**, cliquez sur **Suivant**.
15. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
16. Une fois l'installation terminée, cliquez sur **Fermer**.
17. Dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Windows Server Update Services**.
18. Dans la fenêtre Terminer l'installation de WSUS, cliquez sur **Exécuter** et attendez la fin de la tâche. Cliquez sur **Fermer**.
19. Ne fermez pas la fenêtre Assistant de configuration de Windows Server Update Services.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configuration de WSUS pour qu'il se synchronise avec un serveur WSUS en amont

1. Dans la fenêtre Assistant de configuration de Windows Server Update Services:LON-SVR4, cliquez deux fois sur **Suivant**.
2. Sur la page **Choisir le serveur en amont**, cliquez sur l'option **Synchroniser à partir d'un autre serveur Windows Server Update Services**, dans la zone de texte **Nom du serveur**, tapez **LON-SVR1.Adatum.com**, puis cliquez sur **Suivant**.
3. Sur la page **Définir le serveur proxy**, cliquez sur **Suivant**.
4. Sur la page **Se connecter au serveur en amont**, cliquez sur **Démarrer la connexion**. Attendez que les paramètres du serveur en amont soient appliqués, puis cliquez sur **Suivant**.
5. Dans la page **Choisir les langues**, cliquez sur **Suivant**.
6. Dans la page **Définir la planification de la synchronisation**, cliquez sur **Suivant**.
7. Dans la page **Terminé**, cliquez sur l'option **Commencer la synchronisation initiale**, puis sur **Terminer**.
8. Dans le volet de navigation de la console WSUS, double-cliquez sur **LON-SVR4**, puis cliquez sur **Options**.
9. Dans le volet d'options, cliquez sur **Ordinateurs**. Dans la boîte de dialogue Ordinateurs, sélectionnez **Utiliser les paramètres de stratégie de groupe ou de Registre sur les ordinateurs**. Cliquez sur **OK**.

Résultats : À la fin de cet exercice, vous devez avoir implémenté le rôle serveur WSUS.

Exercice 2 : Configuration des paramètres de mise à jour

▶ Tâche 1 : Configuration des groupes WSUS

1. Dans le volet de navigation de la console WSUS de LON-SVR4, double-cliquez sur **LON-SVR4**, puis sur **Ordinateurs**.
2. Cliquez sur **Tous les ordinateurs**, puis, dans le volet Actions, cliquez sur **Ajouter un groupe d'ordinateurs**.
3. Dans la boîte de dialogue **Ajouter un groupe d'ordinateurs**, dans la zone de texte **Nom**, tapez **Recherche** puis cliquez sur **Ajouter**.

▶ Tâche 2 : Configuration de la stratégie de groupe pour déployer les paramètres de WSUS

1. Basculez vers LON-DC1.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la console de gestion des stratégies de groupe, double-cliquez sur **Forêt : Adatum.com**, double-cliquez sur **Domaines**, puis sur **Adatum.com**.
4. Cliquez avec le bouton droit sur l'unité d'organisation **Research**, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**.
5. Dans la boîte de dialogue **Nouvel objet GPO**, dans la zone de texte **Nom**, tapez **Recherche WSUS**, puis cliquez sur **OK**.
6. Double-cliquez sur l'unité d'organisation **Research**, cliquez avec le bouton droit sur **Recherche WSUS**, puis cliquez sur **Modifier**.
7. Dans l'Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, double-cliquez sur **Stratégies**, **Modèles d'administration**, **Composants Windows**, puis cliquez sur **Windows Update**.
8. Dans le volet Paramètre, double-cliquez sur **Configuration du service Mises à jour automatiques**, puis cliquez sur l'option **Activé**.
9. Dans le champ **Configuration de la mise à jour automatique**, sélectionnez **4 – Téléchargement automatique et planification des installations**, puis cliquez sur **OK**.
10. Dans le volet Paramètre, double-cliquez sur **Spécifier l'emplacement intranet du service de mise à jour Microsoft**, puis cliquez sur l'option **Activé**.
11. Dans les zones de texte **Configurer le service de Mise à jour pour la détection des mises à jour** et **Configurer le serveur intranet de statistiques**, tapez **http://LON-SVR4.Adatum.com:8530**, puis cliquez sur **OK**.
12. Dans le volet Paramètre, double-cliquez sur **Autoriser le ciblage côté client**.
13. Dans la boîte de dialogue **Autoriser le ciblage côté client**, cliquez sur l'option **Activé**. Dans la zone de texte **Nom du groupe cible de cet ordinateur**, saisissez **Research**, puis cliquez sur **OK**.
14. Fermez l'Éditeur de gestion des stratégies de groupe et la Console de gestion des stratégies de groupe.
15. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
16. Dans Utilisateurs et ordinateurs Active Directory, double-cliquez sur **Adatum.com**, cliquez sur **Computers**, cliquez avec le bouton droit sur **LON-CL1**, puis cliquez sur **Déplacer**.
17. Dans la boîte de dialogue **Déplacer**, cliquez sur l'unité d'organisation **Research**, puis sur **OK**.
18. Fermez la fenêtre Utilisateurs et ordinateurs Active Directory.

▶ Tâche 3 : Vérification de l'application des paramètres de la Stratégie de groupe

1. Basculez vers LON-CL1.
2. Sur LON-CL1, déplacez le pointeur de la souris à droite de l'écran, cliquez sur l'icône **Paramètres**, cliquez sur **Marche/Arrêt**, puis sur **Redémarrer**.
3. Une fois que LON-CL1 a redémarré, connectez-vous en tant que **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

4. Sur l'écran d'accueil, tapez **cmd**, cliquez avec le bouton droit sur **Invite de commande**, puis cliquez sur **Exécuter comme administrateur**.
5. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Gpresult /r
```

6. Dans la sortie de la commande, confirmez que sous **Paramètres de l'ordinateur**, **Recherche WSUS** est listé sous **Objets Stratégie de groupe appliqués**.

▶ Tâche 4 : Initialisation de Windows Update

1. Sur LON-CL1, à l'invite de commandes, tapez la commande suivante et appuyez sur ENTRÉE :

```
Wuauclt.exe /reportnow /detectnow
```

2. Basculez vers LON-SVR4.
3. Dans la console Update Services, développez **Ordinateurs**, **Tous les ordinateurs**, puis cliquez sur **Recherche**.
4. Vérifiez que LON-CL1 apparaît dans le groupe Recherche. S'il n'apparaît pas, répétez les étapes 1 à 3. L'affichage de LON-CL1 peut prendre plusieurs minutes.
5. Vérifiez que des mises à jour sont indiquées comme étant nécessaires. Si aucune mise à jour n'est indiquée, répétez les étapes 1 à 3. L'enregistrement des mises à jour peut prendre 10 à 15 minutes.

Résultats : À la fin de cet exercice, vous devez avoir configuré des paramètres de mise à jour pour les ordinateurs client.

Exercice 3 : Approbation et déploiement d'une mise à jour à l'aide de WSUS

▶ Tâche 1 : Approbation des mises à jour de WSUS pour le groupe d'ordinateurs Recherche

1. Sur LON-SVR4, dans Windows Server Update Services, sous **Mises à jour**, cliquez sur **Mises à jour de sécurité**, cliquez avec le bouton droit sur **Mise à jour de sécurité pour Microsoft Office 2010 (KB2553371), édition 32 bits**, puis cliquez sur **Approuver**.
2. Dans la fenêtre Approuver les mises à jour, dans la zone de liste déroulante **Recherche**, sélectionnez **Approuvée pour l'installation**.
3. Cliquez sur **OK**, puis sur **Fermer**.

▶ Tâche 2 : Déploiement des mises à jour sur LON-CL1.

1. Sur LON-CL1, à l'invite de commandes, tapez la commande suivante et appuyez sur ENTRÉE :

```
Wuauclt.exe /detectnow
```

2. Cliquez sur l'écran d'accueil, puis tapez **Windows Update**.
3. Sous **Rechercher**, cliquez sur **Paramètres** puis sur **Windows Update**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Cliquez sur **Rechercher maintenant les mises à jour**.
5. Cliquez sur **Nous allons installer automatiquement 1 mise à jour importante**.
6. Cliquez sur **Installer** pour installer la mise à jour approuvée.
7. Fermez la fenêtre Paramètres du PC à la fin de l'installation.

▶ Tâche 3 : Vérification du déploiement de la mise à jour sur LON-CL1

1. Sur l'écran d'accueil de LON-CL1, saisissez **Observateur d'événements**, cliquez sur **Paramètres**, puis appuyez sur Entrée.
2. Dans l'observateur d'événements, développez **Journaux des applications et des services**, **Microsoft**, **Windows** et cliquez sur **WindowsUpdateClient** pour afficher les événements.
3. Confirmez que les événements relatifs à la mise à jour sont enregistrés.

Résultats : À la fin de cet exercice, vous devez avoir approuvé et déployé une mise à jour à l'aide de WSUS.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial de tous les ordinateurs virtuels. Pour cela, 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 **22411B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22411B-LON-SVR1**, **22411B-LON-SVR4** et **22411B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 13: Surveillance de Windows Server 2012

Atelier pratique : Surveillance de Windows Server 2012

Exercice 1 : Mise en place d'une base de référence des performances

▶ Tâche 1 : Créer et démarrer un ensemble de collecteurs de données

1. Basculez vers l'ordinateur LON-SVR1.
2. Suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
3. Dans le menu Accueil, tapez **Perf**, puis dans la liste **Applications**, cliquez sur **Analyseur de performances**.
4. Dans l'Analyseur de performances, dans le volet de navigation, développez **Ensembles de collecteurs de données**, puis cliquez sur **Définis par l'utilisateur**.
5. Cliquez avec le bouton droit sur **Définis par l'utilisateur**, pointez sur **Nouveau**, puis cliquez sur **Ensemble de collecteurs de données**.
6. Dans l'Assistant **Créer un nouvel ensemble de collecteurs de données**, dans la zone **Nom**, tapez **Performances de LON-SVR1**.
7. Cliquez sur **Créer manuellement (avancé)**, puis sur **Suivant**.
8. Dans la page **Quel type de données inclure ?**, activez la case à cocher **Compteur de performance**, puis cliquez sur **Suivant**.
9. Dans la page **Quels compteurs de performance enregistrer dans un journal ?**, cliquez sur **Ajouter**.
10. Dans la liste **Compteurs disponibles**, développez **Processeur**, cliquez sur **% temps processeur**, puis sur **Ajouter >>**.
11. Dans la liste **Compteurs disponibles**, développez **Mémoire**, cliquez sur **Pages/s**, puis sur **Ajouter >>**.
12. Dans la liste **Compteurs disponibles**, développez **Disque physique**, cliquez sur **Pourcentage du temps disque**, puis sur **Ajouter >>**.
13. Cliquez sur **Longueur moyenne de file d'attente du disque**, puis sur **Ajouter >>**.
14. Dans la liste **Compteurs disponibles**, développez **Système**, cliquez sur **Longueur de la file du processeur**, puis sur **Ajouter >>**.
15. Dans la liste **Compteurs disponibles**, développez **Interface réseau**, cliquez sur **Total des octets/s**, sur **Ajouter >>**, puis sur **OK**.
16. Dans la page **Quels compteurs de performance enregistrer dans un journal ?**, dans la zone **Intervalle d'échantillonnage**, tapez **1**, puis cliquez sur **Suivant**.
17. Dans la page **Où enregistrer les données ?**, cliquez sur **Suivant**.
18. Dans la page **Créer l'ensemble de collecteurs de données ?**, cliquez sur **Enregistrer et fermer**, puis cliquez sur **Terminer**.
19. Dans l'Analyseur de performances, dans le volet de résultats, cliquez avec le bouton droit sur **Performances de LON-SVR1**, puis cliquez sur **Accueil**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Créer une charge de travail classique sur le serveur

1. Positionnez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
2. Dans le menu Accueil, tapez **Cmd**, puis dans la liste **Applications**, cliquez sur **Invite de commandes**.
3. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Fsutil file createnew bigfile 104857600
```

4. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Copy bigfile \\LON-dc1\c$
```

5. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Copy \\LON-dc1\c$\bigfile bigfile2
```

6. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Del bigfile*.*
```

7. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Del \\LON-dc1\c$\bigfile*.*
```

8. Ne fermez pas la fenêtre d'invite de commandes.

▶ Tâche 3 : Analyser les données collectées

1. Basculez vers l'Analyseur de performances.
2. Dans le volet de navigation, cliquez avec le bouton droit sur **Performances de LON-SVR1**, puis cliquez sur **Arrêter**.
3. Dans l'Analyseur de performances, dans le volet de navigation, cliquez sur **Analyseur de performances**.
4. Dans la barre d'outils, cliquez sur **Affiche les données du journal**.
5. Dans la boîte de dialogue **Propriétés de : Analyseur de performances**, sous l'onglet **Source**, cliquez sur **Fichiers journaux**, puis sur **Ajouter**.
6. Dans la boîte de dialogue **Sélectionner le fichier journal**, double-cliquez sur **Admin**.
7. Double-cliquez sur **Performances de LON-SVR1**, sur le dossier **LON-SVR1_date-000001**, puis sur **DataCollector01.blg**.
8. Cliquez sur l'onglet **Données**, puis sur **Ajouter**.
9. Dans la boîte de dialogue **Ajouter des compteurs**, dans la liste **Compteurs disponibles**, développez **Mémoire**, cliquez sur **Pages/s**, puis sur **Ajouter >>**.
10. Développez **Interface réseau**, cliquez sur **Total des octets/s**, puis sur **Ajouter >>**.
11. Développez **Disque physique**, cliquez sur **Pourcentage du temps disque**, puis sur **Ajouter >>**.
12. Cliquez sur **Longueur moyenne de file d'attente du disque**, puis sur **Ajouter >>**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

13. Développez **Processeur**, cliquez sur **% temps processeur**, puis sur **Ajouter >>**.
14. Développez **Système**, cliquez sur **Longueur de la file du processeur**, cliquez sur **Ajouter >>**, puis sur **OK**.
15. Dans la boîte de dialogue **Propriétés de : Analyseur de performances**, cliquez sur **OK**.
16. Dans la barre d'outils, cliquez sur la flèche vers le bas, puis sur **Rapport**.
17. Enregistrez les valeurs répertoriées dans le rapport pour une analyse ultérieure.

Résultats : À la fin de cet exercice, vous devez avoir établi une base de référence pour la comparaison des performances.

Exercice 2 : Identification de la source des problèmes de performance

▶ Tâche 1 : Créer une charge de travail supplémentaire sur le serveur

1. Sur LON-SVR1, basculez vers l'invite de commandes.
2. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
C:
```

3. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Cd\Labfiles
```

4. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
StressTool 95
```

▶ Tâche 2 : Capturer les données de performances avec un ensemble de collecteurs de données

1. Basculez vers l'Analyseur de performances.
2. Dans l'Analyseur de performances, cliquez sur **Définis par l'utilisateur**, et dans le volet de résultats, cliquez avec le bouton droit sur **Performances de LON-SVR1**, puis cliquez sur **Accueil**.
3. Patientez une minute pour permettre la capture des données.

▶ Tâche 3 : Supprimer la charge de travail et examiner les données de performances

1. Au bout d'une minute, basculez vers la fenêtre d'invite de commandes.
2. Appuyez sur Ctr+C.
3. Ne fermez pas la fenêtre d'invite de commandes.
4. Basculez vers l'**Analyseur de performances**.
5. Dans le volet de navigation, cliquez avec le bouton droit sur **Performances de LON-SVR1**, puis cliquez sur **Arrêter**.
6. Dans l'**Analyseur de performances**, dans le volet de navigation, cliquez sur **Analyseur de performances**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Dans la barre d'outils, cliquez sur **Affiche les données du journal**.
8. Dans la boîte de dialogue **Propriétés de : Analyseur de performances**, sous l'onglet **Source**, cliquez sur **Fichiers journaux**, puis sur **Supprimer**.
9. Cliquez sur **Ajouter**.
10. Dans la boîte de dialogue **Sélectionner le fichier journal**, cliquez sur **Dossier parent**.
11. Double-cliquez sur le dossier **LON-SVR1_date-000002**, puis sur **DataCollector01.blg**.
12. Cliquez sur l'onglet **Données**, puis sur **OK**.

Remarque : si vous recevez un message d'erreur à ce stade ou si les valeurs de votre rapport sont nulles, répétez les étapes 4 à 11.

Question : Par rapport à votre précédent rapport, quelles valeurs ont changé ?

Réponse : L'activité de la mémoire et du disque est réduite tandis que l'activité du processeur a augmenté considérablement.

Question : Quelle solution conseillez-vous ?

Réponse : Vous devez continuer à surveiller le serveur pour vérifier que la charge de travail du processeur n'atteint pas la capacité définie.

Résultats : À la fin de cet exercice, vous devez avoir utilisé les outils de performances pour identifier un goulot d'étranglement potentiel au niveau des performances.

Exercice 3 : Affichage et configuration des journaux d'événements centralisés

▶ Tâche 1 : Configurer les éléments préalables aux abonnements

1. Sur LON-SVR1, basculez vers l'invite de commandes.
2. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
winrm quickconfig
```

3. Lorsque vous y êtes invité, tapez **O,** puis appuyez sur Entrée.
4. Dans la barre des tâches, cliquez sur **Gestionnaire de serveur**.
5. Dans le Gestionnaire de serveur, dans le volet de navigation, cliquez sur **Serveur local**. Dans la barre d'outils, cliquez sur **Outils**, puis sur **Gestion de l'ordinateur**.
6. Dans Gestion de l'ordinateur (local), développez **Outils système**, développez **Utilisateurs et groupes locaux**, puis cliquez sur **Groupes**.
7. Dans le volet de résultats, double-cliquez sur **Administrateurs**.
8. Cliquez sur **Ajouter**, et dans la boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, cliquez sur **Types d'objets**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Dans la boîte de dialogue **Types d'objets**, activez la case à cocher des ordinateurs, puis cliquez sur **OK**.
10. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, dans la zone **Entrez les noms des objets à sélectionner**, tapez **LON-DC1**, puis cliquez sur **OK**.
11. Dans la boîte de dialogue **Propriétés de : Administrateurs**, cliquez sur **OK**.
12. Basculez vers LON-DC1.
13. Positionnez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
14. Dans le menu Accueil, tapez **Cmd**, puis dans la liste **Applications**, cliquez sur **Invite de commandes**.
15. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Wecutil qc
```

16. Lorsque vous y êtes invité, tapez **O**, puis appuyez sur Entrée.

▶ Tâche 2 : Créer un abonnement

1. Positionnez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
2. Dans le menu Accueil, tapez **Événement**, puis dans la liste **Applications**, cliquez sur **Observateur d'événements**.
3. Dans l'Observateur d'événements, dans le volet Actions, cliquez sur **Abonnements**.
4. Cliquez avec le bouton droit de la souris sur **Abonnements**, puis cliquez sur **Créer un abonnement**.
5. Dans la boîte de dialogue **Propriétés de l'abonnement**, dans la zone **Nom d'abonnement**, tapez **Événements de LON-SVR1**.
6. Vérifiez que **Initialisation par le collecteur** est sélectionné, puis cliquez sur **Sélectionner des ordinateurs**.
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**, tapez **LON-SVR1**, puis cliquez sur **OK**.
9. Dans la boîte de dialogue **Ordinateurs**, cliquez sur **OK**.
10. Dans la boîte de dialogue **Propriétés de l'abonnement – Événements de LON-SVR1**, cliquez sur **Sélectionner des événements**.
11. Dans la boîte de dialogue **Filtre de requête**, activez les cases à cocher **Critique, Avertissement, Information**, **Commentaires** et **Erreur**.
12. Dans la liste **Connecté**, cliquez sur **Les 7 derniers jours**.
13. Dans la liste **Journaux d'événements**, développez successivement **Journaux des applications et des services**, **Microsoft**, **Windows**, **Diagnosis-PLA**, puis activez la case à cocher **Opérationnel**.
14. Cliquez à nouveau dans la boîte de dialogue **Filtre de requête**, puis cliquez sur OK.
15. Dans la boîte de dialogue **Propriétés de l'abonnement - Événements de LON-SVR1**, cliquez sur **OK**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer une alerte de compteur de performance

1. Basculez vers l'ordinateur LON-SVR1.
2. Dans l'Analyseur de performances, dans le volet de navigation, développez **Ensembles de collecteurs de données**, puis cliquez sur **Définis par l'utilisateur**.
3. Cliquez avec le bouton droit sur **Définis par l'utilisateur**, pointez sur **Nouveau**, puis cliquez sur **Ensemble de collecteurs de données**.
4. Dans l'Assistant Créer un nouvel ensemble de collecteurs de données, dans la zone **Nom**, tapez **Alerte de LON-SVR1**.
5. Cliquez sur **Créer manuellement (avancé)**, puis sur **Suivant**.
6. Dans la page **Quel type de données inclure ?**, activez la case à cocher **Alerte de compteur de performance**, puis cliquez sur **Suivant**.
7. Sur la page **Quels compteurs de performance voulez-vous contrôler ?**, cliquez sur **Ajouter**.
8. Dans la liste **Compteurs disponibles**, développez **Processeur**, cliquez sur **% temps processeur**, sur **Ajouter >>**, puis sur **OK**.
9. Sur la page **Quels compteurs de performance voulez-vous contrôler ?**, dans la liste **Alerter lorsque**, cliquez sur **Au-dessus de**.
10. Dans la zone **Limite**, tapez **10**, puis cliquez sur **Suivant**.
11. Sur la page **Créer l'ensemble de collecteurs de données ?**, cliquez sur **Terminer**.
12. Dans le volet de navigation, développez le nœud **Définis par l'utilisateur**, puis cliquez sur **Alerte de LON-SVR1**.
13. Dans le volet de résultats, cliquez avec le bouton droit sur **DataCollector01**, puis cliquez sur **Propriétés**.
14. Dans la boîte de dialogue **Propriétés de : DataCollector01**, dans la zone **Intervalle d'échantillonnage**, tapez **1**, puis cliquez sur l'onglet **Action de l'alerte**.
15. Activez la case à cocher **Ajouter une entrée dans le journal des événements des applications**, puis cliquez sur **OK**.
16. Dans le volet de navigation, cliquez avec le bouton droit sur **Alerte de LON-SVR1**, puis cliquez sur **Accueil**.

▶ Tâche 4 : Ajouter une charge de travail supplémentaire sur le serveur

1. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
C:
```

2. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
Cd\Labfiles
```

3. À l'invite de commandes, saisissez la commande suivante et appuyez sur Entrée :

```
StressTool 95
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Patientez une minute pour permettre la génération des alertes.
5. Appuyez sur Ctr+C.
6. Fermez la fenêtre d'invite de commandes.

▶ Tâche 5 : Vérifier les résultats

1. Basculez vers LON-DC1.
2. Dans l'**Observateur d'événements**, dans le volet de navigation, développez **Journaux Windows**.
3. Cliquez sur **Événements transférés**.

   Question : Y-a-t-il des alertes liées aux performances ?

   Réponse : Les réponses peuvent varier, mais il doit y avoir des événements liés à la charge de travail imposée sur LON-SVR1. Les événements ont l'identificateur 2031.

Résultats : À la fin de cet exercice, vous aurez centralisé les journaux d'événements et examiné ces journaux pour les événements liés aux performances.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial de tous les ordinateurs virtuels. Pour cela, 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 **22411B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir les ordinateurs virtuels**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22411B-LON-SVR1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT