Microsoft

PRODUIT OFFICIEL DE FORMATION MICROSOFT

22341B

Solutions principales de Microsoft® Exchange Server 2013

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

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

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

© 2013 Microsoft Corporation. Tous droits réservés.

Microsoft et les marques répertoriées à l'adresse 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 : 22341B

Numéro de référence : X19-12635

Date de publication : 9/2013

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

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

Stan Reimer – Développeur de contenu

Stan Reimer est président de S. R. Technical Services Inc et travaille comme consultant, instructeur et auteur. Stan bénéficie d'une expérience approfondie en matière de conseil sur les déploiements Active Directory® et Exchange Server pour certaines des plus grandes entreprises du Canada. Stan est le principal auteur de deux ouvrages Active Directory pour Microsoft Press®. Au cours des dix dernières années, Stan a écrit des cours pour la Formation Microsoft, en se spécialisant dans les cours Active Directory et Exchange Server. Stan est instructeur certifié par Microsoft® (MCT) depuis plus de 14 ans.

Damir Dizdarevic – Concepteur de cours / développeur de contenu

Damir Dizdarevic est MCT (Microsoft Certified Trainer), MCSE (Microsoft Certified Solutions Expert), MCTS (Microsoft Certified Technology Specialist) et MCITP (Microsoft Certified IT Professional). Il est l'un des responsables et instructeurs du centre de formation de Logosoft d.o.o. (Sarajevo, Bosnie-Herzégovine). Damir a plus de 17 années d'expérience en matière de plateformes Microsoft et il est spécialiste de Microsoft Windows Server®, Exchange Server, en termes de sécurité et de virtualisation. Il a travaillé en tant qu'expert technique et auteur sur de nombreux cours MOC (Microsoft Official Courses), principalement consacrés à Exchange et Windows Server, et a publié plus de 400 articles dans différents magazines informatiques, tels que *Windows ITPro*. Il intervient aussi fréquemment et avec brio dans la plupart des conférences Microsoft en Europe du Sud et de l'Est. En outre, il est membre du programme Microsoft MVP (Most Valuable Professional) et président du groupe d'utilisateurs MSCommunity de Bosnie. Son blog sur les technologies MS est disponible à l'adresse suivante : http://dizdarevic.ba/ddamirblog.

Siegfried Jagott – Développeur de contenu

Siegfried Jagott est consultant principal et responsable de l'équipe dédiée aux solutions de messagerie et de collaboration chez Atos Germany, Allemagne. Il est auteur-lauréat de *Microsoft Exchange Server 2010 Best Practices* (Microsoft Press) et il a écrit et effectué la révision technique de plusieurs cours MOC (Microsoft Official Curriculum) sur différents sujets tels que MOC 10165 : Mise à niveau des compétences concernant Microsoft Exchange Server 2003 ou Exchange Server 2007 vers Exchange Server 2010 SP1. Il a été coauteur de différents manuels sur Windows, Microsoft System Center Virtual Machine Manager et Exchange, et il a souvent présenté ces sujets lors de conférences internationales, telles que la conférence « IT & Dev Connections » au printemps 2012 à Las Vegas. Siegfried a planifié, conçu et implémenté certaines des plus grandes infrastructures Exchange Server et Windows® au monde pour des clients internationaux. Il est titulaire d'un MBA obtenu à l'université Open University, Royaume-Uni, et il est certifié MCSE depuis 1997.

Vladimir Meloski – Développeur de contenu

Vladimir est MCT (Microsoft Certified Trainer), MVP sur Exchange Server et consultant ; il fournit des solutions de communications et d'infrastructure unifiées basées sur Microsoft Exchange Server, Lync Server et System Center. Vladimir a 16 ans d'expérience professionnelle en informatique et a participé à des conférences Microsoft en Europe et aux États-Unis en tant que présentateur, modérateur, surveillant d'ateliers pratiques et expert technique. Il a également travaillé en tant qu'expert technique et réviseur technique pour plusieurs cours MOC (Microsoft Official Curriculum).

Robert Genes – Développeur de contenu

Robert Genes est architecte de messagerie et MCM (Microsoft Certified Master) pour Exchange Server 2010. Comme responsable des solutions de messagerie, il a travaillé dans différents projets Exchange Server en Allemagne du Sud. Robert est spécialisé dans Exchange Server et a plus de 10 années d'expérience.

Chris Crandall – Réviseur technique

Chris Crandall est l'architecte principal des pratiques de messagerie chez CB5 Solutions, où il dirige et gère tous les engagements liés à l'infrastructure de messagerie pour les utilisateurs professionnels dans le secteur publique et le secteur privé. Chris est MCM (Microsoft Certified Master), MCT (Microsoft Certified Trainer), MCITP (Microsoft Certified IT Professional) et MCTS (Microsoft Certified Technology Specialist). Il écrit actuellement un livre sur Exchange 2013 en tant qu'expert technique (SME). Chris a servi comme SME et instructeur dans le cadre de ses fonctions d'ingénieur senior chez Microsoft où il a servi plus de 30 entreprises et obtenu de nombreuses récompenses consécutives aux performances et à la satisfaction des clients.

Sommaire

Module 1 : Déploiement et gestion de Microsoft® Exchange Server 2013

Leçon 1 : Configuration requise et conditions préalables pour l'installation d'Exchange Server 2013 **1-2**
Leçon 2 : Déploiement d'Exchange Server 2013 **1-13**
Leçon 3 : Gestion d'Exchange Server 2013 **1-29**
Atelier pratique : Déploiement et gestion d'Exchange Server 2013 **1-38**

Module 2 : Planification et configuration de serveurs de boîtes aux lettres

Leçon 1 : Vue d'ensemble du rôle serveur de boîtes aux lettres **2-2**
Leçon 2 : Planification du déploiement du serveur de boîtes aux lettres **2-14**
Leçon 3 : Configuration des serveurs de boîtes aux lettres **2-29**
Atelier pratique : Configuration de serveurs de boîtes aux lettres **2-36**

Module 3 : Gestion d'objets destinataires

Leçon 1 : Gérer les boîtes aux lettres Exchange Server 2013 **3-2**
Leçon 2 : Gestion d'autres destinataires Exchange **3-15**
Leçon 3 : Planification et implémentation des boîtes aux lettres de dossiers publics **3-21**
Leçon 4 : Gestion des stratégies et listes d'adresses **3-28**
Atelier pratique : Gestion d'objets destinataires **3-37**

Module 4 : Planification et déploiement des serveurs d'accès au client

Leçon 1 : Planification du déploiement du serveur d'accès au client **4-2**
Leçon 2 : Configuration du rôle serveur d'accès au client **4-12**
Leçon 3 : Gestion des services d'accès au client **4-22**
Atelier pratique : Déploiement et configuration d'un rôle serveur d'accès au client **4-32**

Module 5 : Planification et configuration de la connectivité pour les clients de messagerie

Leçon 1 : Connectivité client sur le serveur d'accès au client **5-2**
Leçon 2 : Configuration d'Outlook Web App **5-8**
Leçon 3 : Planification et configuration de la messagerie mobile **5-16**
Leçon 4 : Configuration de l'accès Internet sécurisé pour le serveur d'accès au client **5-26**
Atelier pratique : Planification et configuration de la connectivité pour les clients de messagerie **5-38**

Module 6 : Planification et implémentation de la haute disponibilité

Leçon 1 : Haute disponibilité dans Exchange Server 2013 **6-2**
Leçon 2 : Configuration de bases de données de boîtes aux lettres hautement disponibles **6-12**
Leçon 3 : Configuration des serveurs d'accès au client hautement disponibles **6-28**
Atelier pratique : Implémentation de la haute disponibilité **6-32**

Module 7 : Planification et implémentation d'une solution de récupération d'urgence

Leçon 1 : Planification de l'atténuation des risques **7-2**
Leçon 2 : Planification et implémentation de la sauvegarde d'Exchange Server 2013 **7-11**
Leçon 3 : Planification et implémentation de la récupération d'Exchange Server 2013 **7-18**
Atelier pratique : Implémentation d'une solution de récupération d'urgence pour Exchange Server 2013 **7-29**

Module 8 : Planification et configuration du transport des messages

Leçon 1 : Vue d'ensemble du transport et du routage des messages **8-2**
Leçon 2 : Planification et configuration du transport des messages **8-22**
Leçon 3 : Gestion des règles de transport **8-31**
Atelier pratique : Planification et configuration du transport des messages **8-38**

Module 9 : Planification et configuration de l'hygiène des messages

Leçon 1 : Planification de la sécurité de la messagerie **9-2**
Leçon 2 : Implémentation d'une solution antivirus pour Exchange Server 2013 **9-12**
Leçon 3 : Implémentation d'une solution anti-courrier indésirable pour Exchange Server 2013 **9-19**
Atelier pratique : Planification et configuration de la sécurité des messages **9-34**

Module 10 : Planification et configuration de la sécurité et de l'audit administratifs

Leçon 1 : Configuration du contrôle d'accès basé sur les rôles **10-2**
Leçon 2 : Configuration de la journalisation d'audit **10-16**
Atelier pratique : Configuration de la sécurité et de l'audit administratifs **10-21**

Module 11 : Analyse et résolution des problèmes de Microsoft® Exchange Server 2013

Leçon 1 : Analyse d'Exchange Server 2013 **11-2**
Leçon 2 : Maintenance d'Exchange Server 2013 **11-17**
Leçon 3 : Résolution des problèmes liés à Exchange Server 2013 **11-25**
Atelier pratique : Analyse et résolution des problèmes d'Exchange Server 2013 **11-35**

Corrigés des ateliers pratiques

Atelier pratique du module 1 : Déploiement et gestion d'Exchange Server 2013 **L1-1**
Atelier pratique du module 2 : Configuration de serveurs de boîtes aux lettres **L2-7**
Atelier pratique du module 3 : Gestion d'objets destinataires **L3-15**
Atelier pratique du module 4 : Déploiement et configuration d'un rôle serveur d'accès au client **L4-25**
Atelier pratique du module 5 : Planification et configuration de la connectivité pour les clients de messagerie **L5-31**
Atelier pratique du module 6 : Implémentation de la haute disponibilité **L6-41**
Atelier pratique du module 7 : Implémentation d'une solution de récupération d'urgence pour Exchange Server 2013 **L7-47**
Atelier pratique du module 8 : Planification et configuration du transport des messages **L8-55**
Atelier pratique du module 9 : Planification et configuration de la sécurité des messages **L9-61**
Atelier pratique du module 10 : Configuration de la sécurité et de l'audit administratifs **L10-67**
Atelier pratique du module 11 : Analyse et résolution des problèmes d'Exchange Server 2013 **L11-73**

À propos de ce cours

Cette section décrit brièvement le cours et ses objectifs, le public visé, ainsi que les connaissances préalables requises.

Description du cours

Ce cours apporte les connaissances et compétences nécessaires pour planifier, déployer, gérer, sécuriser et prendre en charge Microsoft Exchange® Server 2013. Il explique comment configurer Exchange Server 2013 et vous fournit les informations dont vous avez besoin pour surveiller, maintenir et dépanner Exchange Server 2013. Il propose également les instructions, meilleures pratiques et éléments à prendre en compte qui vous aideront à optimiser les performances, ainsi qu'à réduire les erreurs et les menaces de sécurité dans Exchange Server 2013.

Public visé

Ce cours est destiné aux personnes souhaitant devenir administrateurs de messagerie au niveau de l'entreprise. Il s'adresse également aux généralistes de l'informatique et aux professionnels du support technique qui souhaitent découvrir Microsoft Exchange Server 2013. Les participants doivent avoir travaillé au moins trois ans dans le domaine informatique, notamment dans l'administration de réseau, l'assistance technique ou l'administration système. Une connaissance des versions précédentes d'Exchange Server n'est pas requise.

Le public secondaire visé par cette formation se compose de candidats professionnels de l'informatique qui souhaitent passer l'examen 70-341 : Solutions principales de Microsoft Exchange Server 2013 comme solution autonome, ou dans le cadre de la configuration requise pour la certification MSCE (Microsoft Certified Solutions Expert).

Connaissances préalables des stagiaires

Pour suivre ce cours, vous devez disposer de connaissances pratiques dans les domaines suivants :

- Connaissance de TCP/IP et des concepts réseau.
- Connaissance de Windows® Server 2008 ou 2012 et AD DS, y compris la planification, la conception et le déploiement.
- Connaissance des concepts de sécurité tels que l'authentification et l'autorisation.
- Travail en équipe, ou en tant qu'équipe virtuelle.
- Connaissance pratique des technologies d'infrastructure à clé publique (PKI) – Services de certificats Active Directory (AD CS).
- Connaissance pratique de DNS (Domain Name System).

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 :

- exécuter un déploiement Exchange Server 2013 et gérer Exchange Server 2013 ;
- planifier le déploiement d'un rôle serveur de boîtes aux lettres et configurer les serveurs de boîtes aux lettres et les bases de données de boîtes aux lettres ;
- gérer des destinataires dans Exchange Server 2013 ;
- planifier le déploiement du serveur d'accès au client et configurer les rôles serveurs d'accès au client ;
- planifier et configurer la messagerie mobile et sécuriser l'accès Internet pour le serveur d'accès au client ;
- configurer les bases de données de boîtes aux lettres hautement disponibles et les serveurs d'accès au client ;
- préparer et implémenter une solution de récupération d'urgence pour Exchange Server 2013 ;
- planifier et configurer le transport de messages et gérer les règles de transport ;
- planifier une hygiène de messages et implémenter une solution antivirus et anti-courrier indésirable pour Exchange Server 2013 ;
- gérer les autorisations de contrôle d'accès basé sur les rôles et les autorisations fractionnées ;
- analyser, maintenir et dépanner Exchange Server 2013.

Plan du cours

Le plan du cours est le suivant :

Module 1, « Déploiement et gestion de Microsoft® Exchange Server 2013 »

Module 2, « Planification et configuration de serveurs de boîtes aux lettres »

Module 3, « Gestion d'objets destinataires »

Module 4, « Planification et déploiement des serveurs d'accès au client »

Module 5, « Planification et configuration de la connectivité pour les clients de messagerie »

Module 6, « Planification et implémentation de la haute disponibilité »

Module 7, « Planification et implémentation d'une solution de récupération d'urgence »

Module 8, « Planification et configuration du transport des messages »

Module 9, « Planification et configuration de l'hygiène des messages »

Module 10, « Planification et configuration de la sécurité et de l'audit administratifs »

Module 11, « Analyse et résolution des problèmes de Microsoft® Exchange Server 2013 »

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 de correction pas à pas.



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

- **Modules** : 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 de l'atelier pratique, ainsi que des sections sur les contrôles des acquis et éléments à retenir, qui contiennent les questions et réponses de contrôle des acquis, les meilleures pratiques, des astuces et réponses sur les problèmes courants et la résolution des problèmes, des scénarios et problèmes concrets avec les réponses.
- **Ressources** : incluent des ressources supplémentaires présentées par catégories qui vous donnent un accès immédiat à du contenu utile et à jour disponible sur TechNet, MSDN® ou Microsoft Press®.

- ***Évaluation du cours :*** à la fin du cours, vous aurez la possibilité 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'ordinateur virtuel

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 de l'ordinateur virtuel

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

Important : à la fin de chaque atelier pratique, vous devez revenir à une capture instantanée précédente des ordinateurs virtuels. Vous trouverez les instructions correspondant à cette procédure à la fin de chaque atelier pratique.

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

Ordinateur virtuel	Rôle
22341B-LON-DC1	Contrôleur de domaine exécutant Windows Server 2012 dans le domaine Adatum.com.
22341B-LON-DC1-B	Contrôleur de domaine exécutant Windows Server 2012 dans le domaine Adatum.com (utilisé pour l'atelier pratique d'installation)
22341B-LON-EX1-B	Serveur membre Windows Server 2013 pour l'atelier pratique d'installation d'Exchange Server 2013
22341B-LON-CAS1	Serveur Windows Server 2012, avec le rôle serveur d'accès au client Exchange Server 2013 installé
22341B-LON-CAS2	Serveur Windows Server 2012, avec le rôle serveur d'accès au client Exchange Server 2013 installé
22341B-LON-MBX1	Serveur Windows Server 2012, avec le rôle serveur de boîtes aux lettres Exchange Server 2013 installé
22341B-LON-MBX2	Serveur Windows Server 2012, avec le rôle serveur de boîtes aux lettres Exchange Server 2013 installé
22341B-LON-SVR1	Serveur Windows Server 2012, membre du domaine Adatum.com
22341B-LON-TMG	Serveur Threat Management Gateway dans le domaine Adatum.com
22341B-LON-CL1	Ordinateur client exécutant Windows 8 et Office 2013 dans le domaine Adatum.com

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration logicielle

Les logiciels suivants sont installés sur chaque ordinateur virtuel :

- Windows Server 2012
- Windows® 8
- Microsoft Office 2013
- Mise à jour cumulative 1 (CU1) d'Exchange Server 2013
- Windows Server 2008 R2 et Microsoft Forefront® Threat Management Gateway

Configuration de la classe

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

Niveau des éléments matériels du cours

Pour garantir une utilisation satisfaisante, Microsoft Learning requiert 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.

- Processeur Intel VT (Intel Virtualization Technology) ou AMD-V (AMD Virtualization)
- Deux disques durs SATA (Serial ATA) de 120 Go à 7 200 tr/min ou supérieurs. Les disques durs doivent être configurés avec un volume distinct (lecteur C: et lecteur D:) sur chaque disque dur.
- 16 Go de RAM
- Lecteur de DVD
- Carte réseau
- Écran SVGA (Super VGA) de 17 pouces
- Souris Microsoft ou dispositif de pointage compatible
- Carte audio avec haut-parleurs

En outre, l'ordinateur de l'instructeur doit être connecté à un projecteur vidéo prenant en charge la carte SVGA 1024 x 768 pixels, couleurs 16 bits.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 1

Déploiement et gestion de Microsoft® Exchange Server 2013

Table des matières :

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

Leçon 1 : Configuration requise et conditions préalables pour l'installation d'Exchange Server 2013 **1-2**

Leçon 2 : Déploiement d'Exchange Server 2013 **1-13**

Leçon 3 : Gestion d'Exchange Server 2013 **1-29**

Atelier pratique : Déploiement et gestion d'Exchange Server 2013 **1-38**

Contrôle des acquis et éléments à retenir **1-44**

Vue d'ensemble du module

Exchange Server 2013 est la nouvelle version de la suite de messagerie et de collaboration de Microsoft. Il s'agit du successeur de Microsoft® Exchange Server 2010. Exchange Server 2013 offre de nombreuses améliorations en matière d'architecture, de fonctionnalités et de fonctions aux administrateurs et aux utilisateurs. Pour implémenter correctement Exchange Server 2013, vous devez connaître les conditions préalables, ainsi que la façon de le déployer dans votre infrastructure existante. Ce module explique comment déployer et gérer Exchange Server 2013.

Objectifs

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

- décrire la configuration requise et les conditions préalables pour l'installation d'Exchange Server 2013 ;
- effectuer un déploiement d'Exchange Server 2013 ;
- gérer Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Configuration requise et conditions préalables pour l'installation d'Exchange Server 2013

Avant de commencer le processus de déploiement d'Exchange Server 2013, vous devez vous assurer que vos services de domaine Active Directory® (AD DS) actuels et les composants d'infrastructure réseau répondent aux exigences d'un déploiement d'Exchange Server. En outre, vous devez planifier les ressources matérielles pour l'installation d'Exchange Server. Dans la mesure où Exchange Server 2013 s'intègre de manière importante à AD DS, vous devez étendre le schéma AD DS avant de commencer le processus d'installation. Dans cette leçon, nous allons examiner la configuration requise pour l'installation d'Exchange Server 2013.

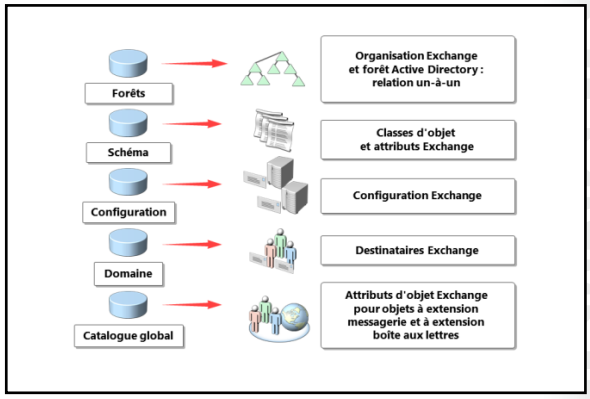
Objectifs de la leçon

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

- décrire les composants Active Directory et l'intégration d'Exchange Server ;
- décrire les exigences relatives au serveur DNS (Domain Name System) pour Exchange Server 2013 ;
- décrire la configuration logicielle requise pour Exchange Server 2013 ;
- décrire la configuration matérielle requise pour Exchange Server 2013 ;
- décrire la configuration d'infrastructure requise pour Exchange Server 2013 ;
- préparer AD DS pour un déploiement d'Exchange Server 2013.

Composants Active Directory et intégration d'Exchange Server

Les informations Active Directory se décomposent en quatre types de partition : domaine, configuration, schéma et application. Ces partitions d'annuaire correspondent aux unités de réplication dans AD DS.



Partition de domaine

Une partition de domaine contient tous les objets de l'annuaire pour le domaine. Les objets de domaine sont répliqués sur chaque contrôleur de domaine du domaine, et incluent les comptes d'utilisateurs et d'ordinateurs ainsi que les groupes.

Un sous-ensemble de la partition de domaine est répliqué sur tous les contrôleurs de domaine de la forêt qui sont configurés en tant que serveurs de catalogue global. Si vous configurez un contrôleur de domaine en tant que serveur de catalogue global, il contient une copie complète de tous les objets de son propre domaine et un sous-ensemble des attributs de tous les objets de chaque domaine de la forêt.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Partition de configuration

La partition de configuration contient des informations de configuration pour AD DS et pour les applications, notamment les informations de site et de lien de sites Active Directory. En outre, certaines applications et certains services distribués stockent des informations dans la partition de configuration. Ces informations sont répliquées via l'ensemble de la forêt afin que chaque contrôleur de domaine conserve un réplica de la partition de configuration.

Lorsque les développeurs d'applications choisissent de stocker des informations d'application dans la partition de configuration, ils n'ont pas besoin de créer leur propre mécanisme pour répliquer les informations. La partition de configuration stocke chaque type d'information de configuration dans des conteneurs séparés. Un conteneur est un objet Active Directory similaire à une unité d'organisation (UO) qui permet d'organiser d'autres objets.

Partition de schéma

La partition de schéma contient des informations de définition pour tous les types d'objet et leurs attributs que vous pouvez créer dans AD DS. Ces données sont communes à tous les domaines dans la forêt, et AD DS les réplique dans tous les contrôleurs de domaine de la forêt. Toutefois, un seul contrôleur de domaine contient une copie accessible en écriture du schéma. Par défaut, ce contrôleur de domaine, appelé contrôleur de schéma, est le premier contrôleur de domaine installé dans une forêt Active Directory.

Partitions d'application

Un administrateur peut créer des partitions d'application manuellement, et une application peut automatiquement créer des partitions au cours de son processus d'installation. Elles contiennent des données d'application spécifiques qui sont nécessaires à l'application. Le principal avantage des partitions d'application est la souplesse de la réplication. Vous pouvez spécifier les contrôleurs de domaine qui contiennent un réplica d'une partition d'application et ces contrôleurs de domaine peuvent inclure un sous-ensemble de contrôleurs de domaine dans la forêt. Exchange Server 2013 n'utilise pas de partition d'application pour stocker des informations.

Exchange Server 2013 et intégration des partitions AD DS

Pour garantir le positionnement correct des composants Active Directory par rapport aux ordinateurs qui exécutent Exchange Server, vous devez comprendre comment Exchange Server 2013 communique avec AD DS et utilise les informations Active Directory pour fonctionner. Les services de domaine Active Directory stockent la plupart des informations de configuration Exchange Server 2013.

Forêts

Une organisation Exchange Server et une forêt Active Directory ont une relation un-à-un. Une organisation Exchange Server ne peut pas couvrir plusieurs forêts Active Directory. De même, une forêt Active Directory ne peut pas contenir plusieurs organisations Exchange Server.

 **Remarque :** Dans Exchange Server 2013, vous pouvez également ajouter le domaine Office 365 à la console du Centre d'administration Exchange. Cela vous permet de gérer plusieurs organisations à partir d'une console de gestion unique.

Partition de schéma

La partition de schéma est modifiée pendant l'installation d'Exchange Server 2013 afin de permettre la création d'objets spécifiques d'Exchange Server. Pendant l'installation, les attributs spécifiques d'Exchange Server sont également ajoutés aux objets existants. Par exemple, le processus d'installation met à jour les objets utilisateur avec des attributs supplémentaires pour décrire les quotas de stockage et les fonctionnalités de boîte aux lettres.

Partition de configuration

La partition de configuration stocke des informations de configuration pour l'organisation Exchange Server 2013. Dans la mesure où AD DS réplique la partition de configuration dans tous les contrôleurs de domaine de la forêt, la configuration de l'organisation Exchange Server 2013 est répliquée dans la forêt. La partition de configuration inclut des objets de configuration Exchange Server tels que les paramètres globaux, les stratégies d'adresse de messagerie, les règles de transport et les listes d'adresses.

Partition de domaine

La partition de domaine contient des informations sur les objets destinataires. Cela inclut les utilisateurs à extension boîte aux lettres, ainsi que les contacts, les groupes et les utilisateurs à extension messagerie. Les objets à extension boîte aux lettres ou à extension messagerie ont des attributs déjà configurés, tels que les adresses de messagerie.

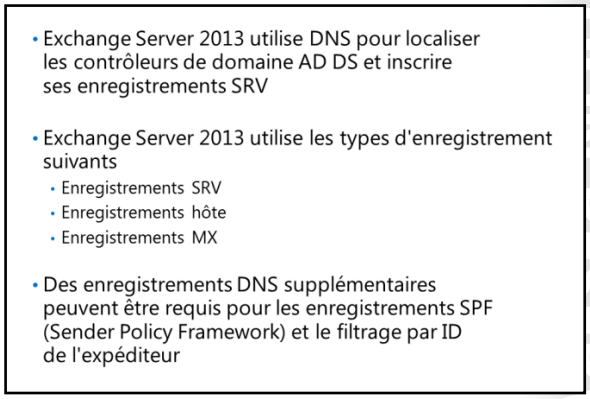
Catalogue global

- Lorsque vous installez Exchange Server 2013, les attributs de messagerie électronique des objets à extension messagerie et à extension boîte aux lettres sont répliqués dans le catalogue global. Dans le cadre d'Exchange Server, le catalogue global est utilisé pour ce qui suit : la liste d'adresses globale est générée à partir de la liste des destinataires dans le catalogue global d'une forêt Active Directory.
- Le service de transport Exchange Server 2013 accède au catalogue global pour rechercher l'emplacement de la boîte aux lettres d'un destinataire lors de la remise des messages.
- Les serveurs d'accès au client Exchange accèdent au serveur de catalogue global pour localiser le serveur de boîtes aux lettres de l'utilisateur et afficher la liste d'adresses globale sur les clients Microsoft Office Outlook®, Microsoft® Outlook Web App ou Exchange ActiveSync®.

 **Remarque :** En raison de l'importance du catalogue global dans une organisation Exchange Server, vous devez déployer au moins un serveur de catalogue global dans chaque site Active Directory qui contient un serveur Exchange 2013. Vous devez déployer suffisamment de serveurs de catalogue global pour garantir des performances adéquates. Exchange Server 2013 n'utilise pas de contrôleurs de domaine en lecture seule ni de contrôleurs de domaine en lecture seule que vous configurez comme serveurs de catalogue global. Cela signifie que vous ne devez pas déployer de serveur Exchange 2013 dans un site qui contient uniquement des contrôleurs de domaine en lecture seule ou des serveurs de catalogue global.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration requise des serveurs DNS pour Exchange Server 2013



Chaque ordinateur qui exécute Exchange Server doit utiliser un système DNS pour rechercher les serveurs de catalogue global et AD DS. En tant qu'application orientée site, Exchange Server 2013 préfère communiquer avec les contrôleurs de domaine qui se trouvent dans le même site que l'ordinateur exécutant Exchange Server.

Les services Exchange Server utilisent un système DNS pour rechercher un contrôleur de domaine ou un serveur de catalogue global valide. Par défaut, chaque fois qu'un contrôleur de domaine démarre le service Netlogon, il met à jour le système DNS (Domain Name System) avec les enregistrements de service (SRV) qui décrivent le serveur comme un contrôleur de domaine et un serveur de catalogue global (le cas échéant).

Pour garantir la mise à jour correcte des enregistrements DNS, tous les contrôleurs de domaine doivent utiliser un serveur DNS interne prenant en charge les mises à jour dynamiques. Une fois les enregistrements DNS enregistrés, les ordinateurs qui exécutent Exchange Server peuvent utiliser DNS pour rechercher des contrôleurs de domaine et des serveurs de catalogue global.

Enregistrements de ressources SRV

Les enregistrements de ressources SRV sont des enregistrements DNS qui identifient les serveurs qui fournissent des services spécifiques sur le réseau. Par exemple, un enregistrement de ressource SRV peut contenir des informations permettant aux clients de localiser un contrôleur de domaine dans un domaine ou un site spécifique.

Tous les enregistrements de ressources SRV utilisent un format standard composé de plusieurs champs contenant les informations qu'AD DS utilise afin de remapper un service à l'ordinateur qui fournit le service. Les enregistrements SRV pour les contrôleurs de domaine et les serveurs de catalogue global sont enregistrés avec différentes variations pour permettre de rechercher les contrôleurs de domaine et les serveurs de catalogue global de différentes manières.

Une option consiste à enregistrer les enregistrements DNS par nom de site, ce qui permet aux ordinateurs qui exécutent Exchange Server de rechercher des contrôleurs de domaine et des serveurs de catalogue global dans le site Active Directory local. Exchange Server exécute toujours les requêtes DNS concernant les ressources pour le site Active Directory local en premier.

Les enregistrements de ressources SRV utilisent le format suivant :

```
_Service_.Protocole.Nom Ttl classe SRV priorité poids port cible
```

Lorsqu'un ordinateur qui exécute Exchange Server est un serveur membre, Exchange Server le configure dynamiquement avec son site chaque fois qu'il s'authentifie auprès d'AD DS. Dans le cadre du processus d'authentification, le nom du site est stocké dans le Registre. Lorsque le serveur Exchange Server demande au serveur DNS de fournir les enregistrements de contrôleur de domaine ou de serveur de catalogue global, le serveur Exchange Server essaie toujours de se connecter aux contrôleurs de domaine qui ont le même attribut de site que lui.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Enregistrements hôte

Les enregistrements hôte fournissent un nom d'hôte à un mappage d'adresse IP. Ces enregistrements sont requis pour chaque contrôleur de domaine et pour les autres hôtes qui doivent être accessibles aux serveurs Exchange ou aux ordinateurs clients. Les enregistrements hôte peuvent utiliser le protocole IPv4 (Internet Protocol version 4), qui correspond aux enregistrements A. Par ailleurs, ils peuvent utiliser le protocole IPv6 (Internet Protocol version 6), qui correspond aux enregistrements AAAA.

Enregistrements MX

Un enregistrement de serveur de messagerie (MX) est un enregistrement de ressource qui permet aux serveurs de rechercher d'autres serveurs pour remettre le courrier électronique Internet à l'aide du protocole SMTP (Simple Mail Transfer Protocol). Un enregistrement MX identifie le serveur SMTP qui acceptera des messages entrants pour un domaine DNS spécifique. Chaque enregistrement MX contient un nom d'hôte et une valeur de préférence. Lorsque vous déployez plusieurs serveurs SMTP qui sont accessibles sur Internet, vous pouvez attribuer des valeurs de préférence équivalentes à chaque enregistrement MX afin d'activer l'équilibrage de charge entre les serveurs SMTP.

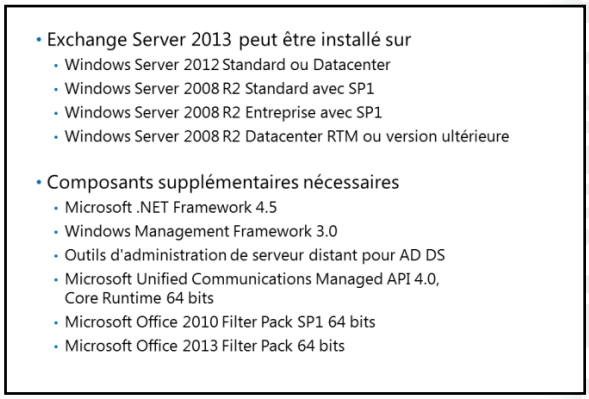
Vous pouvez également spécifier une valeur de préférence inférieure pour l'un des enregistrements MX. Tous les messages sont acheminés via le serveur SMTP qui possède l'enregistrement MX ayant la valeur de préférence inférieure, à moins que ce serveur ne soit pas disponible.

Remarque : Outre les enregistrements SRV, hôte et MX, vous devrez également peut-être configurer des enregistrements SPF (Sender Policy Framework) pour prendre en charge le filtrage anti-courrier indésirable par ID de l'expéditeur. De plus, certaines organisations utilisent des recherches inversées comme option de filtrage antispam. Vous devriez par conséquent envisager d'ajouter des enregistrements de recherche inversée pour tous les serveurs SMTP qui assurent la messagerie électronique de votre organisation.

Configuration logicielle requise pour Exchange Server 2013

Exchange Server 2013 nécessite que certains logiciels soient préinstallés avant le début du processus de déploiement. Tout d'abord, vous devez planifier les plateformes de système d'exploitation utilisées pour Exchange Server 2013. Les systèmes d'exploitation suivants sont pris en charge pour l'installation des rôles Exchange Server 2013 :

- Windows Server® 2012 Standard ou Datacenter.
- Windows Server® 2008 R2 Standard avec Service Pack 1 (SP1).



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Windows Server® 2008 R2 Entreprise avec SP1.
- Windows Server® 2008 R2 Datacenter RTM ou version plus récente.

Remarque : L'option d'installation minimale n'est pas une option de système d'exploitation prise en charge pour l'installation d'Exchange Server 2013. En outre, Windows Server 2008 R2 Standard ne prend pas en charge le clustering avec basculement et ne peut pas utiliser les groupes de disponibilité de la base de données (DAG) dans Exchange Server à des fins de haute disponibilité. Vous ne pouvez pas mettre à niveau Windows Server après avoir installé Exchange.

Selon le rôle Exchange Server installé, différents composants Windows peuvent être installés sur un serveur. Toutefois, vous n'avez pas besoin d'installer ces rôles et fonctionnalités avant l'installation d'Exchange Server, car le processus d'installation peut installer les rôles et fonctionnalités nécessaires automatiquement.

Remarque : Si vous choisissez d'installer les rôles et fonctionnalités Windows Server lors de l'installation d'Exchange Server, vous serez peut-être amené à redémarrer le serveur avant le début de l'installation du serveur Exchange. Il s'agit du comportement attendu.

Toutefois, il existe des composants supplémentaires que vous devez installer manuellement. Ces composants, que vous pouvez télécharger librement à partir du site de Microsoft, sont les suivants :

- Microsoft .NET Framework 4.5 (uniquement pour Windows Server 2008 et 2008 R2) ;
- Windows Management Framework 3.0 (déjà inclus dans Windows Server 2012) ;
- Outils d'administration de serveur distant (RSAT) pour AD DS (peuvent être installés avec le Gestionnaire de serveur) ;
- Microsoft Unified Communications Managed API, Core Runtime 64 bits ;
- Microsoft® Office 2010 Filter Pack SP1 64 bits ou Microsoft Office 2013 Filter Pack ;
- mises à jour d'Exchange Server pour les articles de Base de connaissances KB974405, KB2619234 et KB2533623 lors de l'installation d'Exchange Server 2013 sur Windows Server 2008 R2.

Vous devez aussi vous assurer que le service Planificateur de tâches est activé et en cours d'exécution sur le serveur où vous prévoyez d'installer Exchange Server 2013.

Configuration matérielle requise pour Exchange Server 2013

L'identification de la configuration matérielle requise pour Exchange Server 2013 est plus complexe que la simple lecture des spécifications fournies par Microsoft. Beaucoup d'autres facteurs peuvent influer sur la conception du matériel Exchange Server, en dehors des spécifications générales qui fournissent des informations sur la configuration matérielle minimale prise en charge.

Ressource	Configuration requise
Processeur	• Architecture Intel 64 bits • Architecture AMD64
Mémoire	• 8 Go de RAM recommandés • Mémoire supplémentaire requise en fonction du rôle et de la charge du serveur
Disque	• 1,2 Go d'espace disque disponible pour les fichiers Exchange Server • 200 Mo d'espace libre sur le lecteur système • Espace supplémentaire pour le stockage des boîtes aux lettres
Système de fichiers	• Système de fichiers NTFS pour tous les lecteurs

Premièrement, le rôle serveur installé a une influence significative sur les spécifications matérielles. Par exemple, le serveur de boîtes aux lettres nécessite probablement un matériel plus puissant que le serveur d'accès au client. Deuxièmement, de nombreuses organisations installent tous les rôles Exchange Server sur un seul ordinateur, ce qui signifie que vous devez fusionner la configuration matérielle de chacun des rôles.

Le processeur d'un ordinateur Exchange Server doit être un processeur Intel® basé sur une architecture 64 bits qui prend en charge l'architecture Intel 64 (anciennement connue sous le nom d'Intel EM64T) ou un processeur AMD qui prend en charge la plateforme AMD64. Les processeurs Intel Itanium IA64 ne sont pas pris en charge.

Mémoire

Il est conseillé d'utiliser la configuration de mémoire maximale du serveur au moment de décider de la quantité de mémoire vive (RAM) dont vous avez besoin pour Exchange Server 2013. Les diverses architectures de serveur ont des limites de mémoire différentes. Vérifiez les spécifications techniques suivantes du serveur pour déterminer la configuration de mémoire maximale du serveur la plus efficace sur le plan du coût :

- Vitesse de la mémoire. Certaines architectures de serveur nécessitent des modules mémoire plus lents pour s'adapter à la quantité maximale de mémoire prise en charge pour un serveur spécifique. Par exemple, la mémoire maximale du serveur peut être limitée à 32 gigaoctets (Go) avec de la mémoire vive de type PC3 10666 (DDR3 1333) ou à 128 Go avec de la mémoire vive de type PC2 6400 (DDR2 800). Contactez votre fabricant pour vous assurer que la cible de la configuration de la mémoire pour Exchange Server 2013 est compatible en termes de vitesse.
- Taille du module mémoire. Choisissez la taille maximale de module mémoire prise en charge par le serveur. En général, les prix des modules mémoire varient en fonction de la taille. Assurez-vous que la taille maximale du module mémoire vous permet de répondre aux exigences de la configuration mémoire cible pour Exchange Server 2013.
- Nombre total d'emplacements mémoire. Tenez compte du nombre de modules mémoire qu'un serveur spécifique prend en charge. Le nombre total d'emplacements multiplié par la taille maximale du module mémoire représente la configuration mémoire maximale pour le serveur. Gardez à l'esprit que les modules mémoire doivent parfois être installés par paire.

Lorsque vous planifiez la quantité de mémoire à installer dans les serveurs Exchange, vous devez suivre ces instructions :

- Boîte aux lettres : 8 Go minimum
- Accès au client : 4 Go minimum
- Boîte aux lettres et accès au client combinés : 8 Go minimum

Certains serveurs voient leurs performances s'améliorer si plusieurs emplacements mémoire sont remplis, alors que d'autres rencontrent des problèmes de performances. Contactez votre fournisseur de matériel pour obtenir une explication pour votre architecture serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Espace disque disponible

Lors du choix et de la configuration des lecteurs de disques pour une installation d'Exchange Server 2013, vous devez tenir compte de plusieurs exigences de configuration requises. Vous devez avoir :

- au moins 30 Go sur le lecteur où vous installez Exchange ;
- 500 mégaoctets (Mo) supplémentaires d'espace disque disponible pour chaque module linguistique de la messagerie unifiée que vous prévoyez d'installer ;
- 200 Mo d'espace disque disponible sur le lecteur système ;
- un disque dur où est stockée la base de données des files d'attente de messages avec au moins 500 Mo d'espace disponible ;
- toutes les partitions qu'Exchange Server 2013 utilise doivent être formatées avec le système de fichiers NTFS.

Il est impossible de déterminer l'espace requis pour le rôle serveur de boîtes aux lettres sans connaître le nombre de boîtes aux lettres, la taille des boîtes aux lettres, ainsi que les exigences en matière de haute disponibilité, entre autres paramètres. Nous vous recommandons d'utiliser l'outil de calcul du rôle serveur de boîte aux lettres pour déterminer la configuration matérielle optimale du rôle serveur de boîtes aux lettres.

Configuration matérielle des serveurs avec plusieurs rôles serveur

Lorsque vous concevez la configuration matérielle des serveurs sur lesquels vous installez plusieurs rôles serveur, prenez en compte les recommandations suivantes :

- Prévoyez au moins deux cœurs de processeur. Le nombre recommandé de cœurs de processeur est huit, 24 étant le nombre recommandé maximal.
- Concevez un serveur doté de plusieurs rôles serveur de sorte que la moitié des cœurs de processeur disponibles soit utilisée par le rôle serveur de boîte aux lettres et l'autre moitié par le rôle serveur d'accès au client.
- Planifiez la configuration mémoire suivante pour un serveur avec plusieurs rôles serveur : 8 Go, et entre 2 et 10 Mo par boîte aux lettres. Ces valeurs peuvent varier selon le profil utilisateur et le nombre de bases de données de boîtes aux lettres. La quantité maximale de mémoire requise est 64 Go.
- Pour accueillir le rôle serveur d'accès au client sur le même serveur que le rôle serveur de boîtes aux lettres, réduisez de 20 % le nombre de boîtes aux lettres par calcul de cœur en fonction du profil de client moyen.
- Déployez plusieurs rôles serveur Exchange sur un serveur de boîtes aux lettres qui est membre du groupe de disponibilité de base de données (DAG), le cas échéant. Ce scénario permet de disposer d'une redondance complète pour les rôles serveur de boîtes aux lettres et d'accès au client sur seulement deux serveurs Exchange 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration d'infrastructure requise pour Exchange Server 2013

Avant de déployer Exchange Server 2013 dans votre organisation, vous devez vérifier que celle-ci est conforme à la configuration requise pour AD DS et DNS.

Composant d'infrastructure	Configuration requise
 Active Directory	• Le contrôleur de schéma doit exécuter Windows Server 2003 (SP2), Windows Server 2008, Windows Server 2008 R2 ou Windows Server 2012 • Dans chacun des sites où Exchange est installé, au moins un serveur de catalogue global doit exécuter Windows Server 2003 SP2, Windows Server 2008, Windows Server 2008 R2 ou Windows Server 2012 • Windows Server 2003 est requis au minimum pour les niveaux fonctionnels du domaine et de la forêt
DNS	• Doit être configuré pour activer la résolution de noms du contrôleur de domaine et du serveur de catalogue global

Configuration requise pour AD DS

La configuration requise suivante pour AD DS est nécessaire afin de pouvoir installer Exchange Server 2013 :

- Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 ou Windows Server 2003 avec Service Pack 2 (SP2) doit être installé sur le contrôleur de domaine représentant le contrôleur de schéma. Par défaut, le contrôleur de schéma s'exécute sur le premier contrôleur de domaine Windows installé dans une forêt.
- Dans chacun des sites où Exchange Server 2013 est déployé, au moins un serveur de catalogue global doit être installé et doit exécuter Windows Server 2012, Windows Server 2008, Windows Server 2008 R2 ou Windows Server 2003 SP2.
- Dans chaque site où vous envisagez d'installer Exchange Server 2013, au moins un contrôleur de domaine accessible en écriture doit exécuter Windows Server 2012, Windows Server 2008 ou Windows Server 2008 R2.
- Le domaine Active Directory et les niveaux fonctionnels de la forêt doivent exécuter au minimum Windows Server 2003 ou des versions ultérieures.

Configuration requise pour DNS

Avant d'installer Exchange Server 2013, vous devez configurer correctement DNS dans votre forêt Active Directory. Tous les serveurs qui exécutent Exchange Server 2013 doivent pouvoir localiser les contrôleurs de domaine Active Directory, les serveurs de catalogue global et les autres serveurs Exchange Server.

Préparation d'AD DS pour le déploiement d'Exchange Server 2013

Avant d'implémenter Exchange Server 2013 dans votre environnement, vous devez préparer AD DS. Par défaut, AD DS ne dispose pas des classes, objets et attributs nécessaires définis pour le serveur Exchange. En préparant AD DS, vous étendez le schéma AD DS et vous modifiez également les partitions de configuration et de domaine d'AD DS. En outre, Exchange Server nécessite plusieurs groupes et autorisations spéciales dans AD DS. Ces éléments sont également configurés lors de la préparation d'AD DS.

Paramètres d'installation	Description
/PrepareAD /OrganizationName: "nom_organisation"	• Prépare les objets Exchange globaux • Crée les groupes de sécurité universels Exchange dans le domaine racine • Prépare le domaine actuel
/PrepareSchema	• Prépare le schéma pour l'installation d'Exchange Server 2013
/PrepareDomain /PrepareDomain *nom_domaine* /PrepareAllDomains	• Prépare le domaine où se trouvent les destinataires Exchange Server

Vous pouvez préparer AD DS en exécutant l'Assistant Installation d'Exchange Server 2013 à l'aide d'un compte d'utilisateur qui dispose des autorisations nécessaires pour préparer Active Directory et le domaine. Pour préparer la partition de schéma et de configuration AD DS, vous devez utiliser un compte membre du groupe Administrateurs du schéma et du groupe Administrateurs d'entreprise. À l'aide de ce type de compte, l'Assistant prépare automatiquement Active Directory et le domaine.

Sinon, vous pouvez également préparer AD DS pour Exchange Server en exécutant l'utilitaire d'installation d'Exchange Server 2013 à partir de la ligne de commande. Si vous voulez préparer le schéma AD DS et le mettre à niveau vers une version prise en charge par Exchange Server 2013, vous devez exécuter l'une des commandes **setup** suivantes : **setup /PrepareSchema** ou **setup /ps.** Pour exécuter cette commande, vous devez être également membre du groupe Administrateurs d'entreprise ou du groupe Administrateurs du schéma.

Cette commande effectue les tâches suivantes :

- connexion du serveur Exchange au contrôleur de domaine principal du schéma ;
- importation des fichiers LDIF (LDAP Data Interchange Format) afin de mettre à jour le schéma à l'aide des attributs spécifiques à Exchange Server 2013 ;
- définition de la version du schéma (ms-Exch-Schema-Version-Pt) à 15132.

Remarque : Vous pouvez également préparer le schéma dans le cadre de la procédure PrepareAD, qui est décrite ci-dessous.

Pour préparer les objets AD DS et la partition de configuration AD DS pour Exchange Server 2013, vous devez exécuter **setup** avec le commutateur **/PrepareAD**. Pour ce faire, exécutez la commande suivante :

```
Setup.exe /PrepareAD /IAcceptExchangeServerLicenseTerms /OrganizationName:"Nom de
l'organisation"
```

Cette commande effectue les tâches suivantes :

- Elle crée le conteneur Microsoft Exchange s'il n'existe pas. Le conteneur est créé sous CN=Services,CN=Configuration,DC=<domaine racine>.
- Elle vérifie que le schéma a été mis à jour et que l'organisation est à jour en recherchant la présence de la propriété objectVersion dans Active Directory. La propriété objectVersion se trouve dans le conteneur CN=<votre organisation>,CN=Microsoft Exchange,CN=Services,CN=Configuration, DC=<domaine>. La valeur affectée à objectVersion pour Exchange Server 2013 est 15448.
- Elle crée tous les objets et conteneurs nécessaires pour Exchange Server 2013, sous CN=<Nom de l'organisation>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<domaine racine>.
- Elle crée l'entrée par défaut Domaines acceptés, si elle n'existe pas, en fonction de l'espace de noms racine de la forêt, sous CN=Transport Settings,CN=<Nom de l'organisation>, CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<domaine racine>.
- Elle affecte des autorisations spécifiques dans l'ensemble de la partition de configuration.
- Elle importe le fichier Rights.ldf. Cela entraîne l'ajout des droits étendus nécessaires à Exchange pour être installé dans Active Directory.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Elle crée l'unité d'organisation Microsoft Exchange Security Groups dans le domaine racine de la forêt, puis attribue des autorisations spécifiques à cette unité d'organisation.
- Elle crée les groupes de rôles de gestion au sein de l'unité d'organisation Microsoft Exchange Security Groups.
- Elle ajoute les nouveaux groupes de sécurité universels qui se trouvent dans l'unité d'organisation Microsoft Exchange Security Groups à l'attribut otherWellKnownObjects stocké dans le conteneur CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<domaine racine>.
- Elle crée le contact Unified Messaging Voice Originator dans le conteneur Microsoft Exchange System Objects du domaine racine.
- Elle prépare le domaine local pour Exchange Server 2013.

Pour exécuter cette commande, vous devez être membre du groupe de sécurité Administrateurs d'entreprise. Par ailleurs, vous devez exécuter cette commande sur l'ordinateur qui se trouve dans le même domaine que le contrôleur de domaine principal du schéma. Si vous disposez de plusieurs domaines, attendez un certain temps après l'exécution de cette commande, afin que les modifications apportées à AD DS soient répliquées sur tous les autres domaines et contrôleurs de domaine.

À la fin de ce processus, exécutez la commande **setup /PrepareDomain** dans chaque domaine contenant des destinataires Exchange. Vous n'avez pas besoin d'exécuter cette commande dans un domaine où vous avez exécuté **setup /PrepareAD**.

Sinon, vous pouvez également exécuter **setup /PrepareDomain:<nom de domaine complet du domaine à préparer>** pour préparer un domaine spécifique, ainsi que **setup /PrepareAllDomains** ou **setup /pad** pour préparer tous les domaines de votre organisation.

Cette commande effectue les tâches suivantes :

- Elle crée le conteneur Microsoft Exchange System Objects dans la partition de domaine racine d'AD DS, puis définit les autorisations de ce conteneur pour les groupes Serveurs Exchange, Administrateurs d'organisation Exchange et Utilisateurs authentifiés.
- Elle définit la propriété objectVersion dans le conteneur Microsoft Exchange System Objects sous DC=<domaine racine>. Cette propriété objectVersion contient la version de la préparation du domaine. La version pour Exchange Server 2013 est 13236.
- Elle crée un groupe global de domaine nommé Serveurs de domaine Exchange.
- Elle affecte les autorisations au niveau du domaine pour les groupes de sécurité universels Serveurs Exchange et Gestion de l'organisation.
- Une fois que toutes ces commandes ont été correctement exécutées, AD DS est prêt pour l'installation d'Exchange Server 2013. Vous pouvez vérifier si la préparation s'est bien passée en effectuant les tâches suivantes : dans le contexte d'appellation Schema, assurez-vous que la propriété rangeUpper de ms-Exch-Schema-Version-Pt a la valeur 15132.
- Dans le contexte d'appellation Configuration, assurez-vous que la propriété objectVersion située dans le conteneur CN=<votre organisation>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<domaine> a la valeur 15448.
- Dans le contexte d'appellation Default, assurez-vous que la propriété objectVersion située dans le conteneur Microsoft Exchange System Objects sous DC=<domaine racine> a la valeur 13236.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Déploiement d'Exchange Server 2013

Le déploiement d'Exchange Server 2013 requiert de votre part l'exécution de toutes les étapes de planification des conditions préalables, l'installation du logiciel, puis l'exécution des tâches de post-installation. Lors de la préparation de votre installation, déterminez le type de déploiement que vous allez effectuer, ainsi que la façon dont vous concevez le positionnement des rôles serveur. Cette leçon porte sur l'architecture des rôles serveur dans Exchange Server 2013, ainsi que sur divers scénarios de déploiement.

Objectifs de la leçon

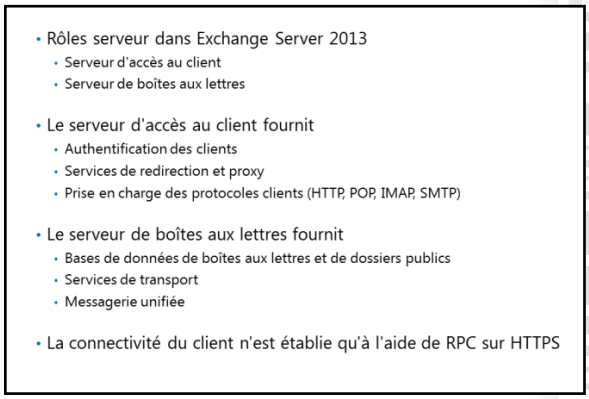
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire l'architecture des rôles serveur dans Exchange Server 2013 ;
- décrire les options de déploiement d'Exchange Server 2013 ;
- décrire les éléments à prendre en compte pour le déploiement hybride avec Microsoft® Office 365 ;
- décrire les options de mise à niveau et de migration ;
- déployer Exchange Server 2013 en tant qu'ordinateur virtuel ;
- décrire l'installation d'Exchange Server 2013 à l'aide de l'Assistant Installation ;
- décrire l'installation d'Exchange 2013 en mode sans assistance ;
- installer Exchange 2013 en mode sans assistance ;
- décrire et effectuer les tâches de post-installation ;
- résoudre les problèmes de l'installation d'Exchange Server.

Architecture des rôles serveur dans Exchange Server 2013

Dans Exchange Server 2013, Microsoft a apporté des changements majeurs à l'architecture des rôles serveur. Dans Exchange Server 2007 et Exchange Server 2010, il y avait cinq rôles serveur dédiés à différentes fonctionnalités :

- Rôle serveur de boîtes aux lettres
- Rôle d'accès au client
- Rôle de transport Hub
- Rôle de transport Edge
- Rôle de messagerie unifiée



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans Exchange Server 2013, le nombre de rôles serveur a été considérablement réduit, pour ne conserver que les deux rôles suivants :

- Rôle serveur de boîtes aux lettres
- Rôle serveur d'accès au client

Tous les autres rôles, à l'exception du rôle de transport Edge (qui n'existe pas dans Exchange Server 2013), sont intégrés au sein de ces deux rôles.

Rôles serveur dans Exchange Server 2013

Contrairement à Microsoft Exchange Server 2010, dans lequel le rôle serveur de boîte aux lettres hébergeait uniquement les bases de données de boîtes aux lettres et de dossiers publics, et permettait le stockage des messages électroniques, dans Exchange Server 2013, le rôle serveur de boîte aux lettres inclut également les protocoles d'accès au client, le service de transport Hub, les bases de données de boîtes aux lettres et les composants de la messagerie unifiée. Cela signifie que les fonctionnalités des trois rôles dans Exchange Server 2010 (boîte aux lettres, transport Hub et messagerie unifiée) sont maintenant intégrées dans un seul rôle au sein d'Exchange Server 2013.

Le rôle serveur d'accès au client a changé dans Exchange Server 2013. Le serveur d'accès au client est pour l'essentiel un serveur proxy qui gère toutes les connexions clientes, en autorisant toutes les requêtes des clients et en les acheminant vers la base de données de boîtes aux lettres active appropriée. Il fournit l'authentification, ainsi que les services de redirection et proxy. En outre, il assure une prise en charge des protocoles d'accès au client suivants : HTTP, POP, IMAP et SMTP.

Autres aspects n'ayant pas changé : le serveur d'accès au client ne stocke aucune donnée de l'utilisateur. De même, il n'effectue pas de mise en file d'attente des messages. Le rôle serveur d'accès au client fournit également des fonctionnalités de sécurité, en appliquant le protocole SSL lors des communications avec les clients. Dans certains scénarios où Exchange Server est déployé dans plusieurs sites au sein d'une organisation, le serveur d'accès au client peut également rediriger la requête vers un serveur d'accès au client plus approprié ou acheminer la connexion par l'intermédiaire d'un proxy au serveur de boîtes aux lettres approprié.

 **Remarque :** Le rôle de transport Edge n'est pas inclus dans Exchange Server 2013. Toutefois, vous pouvez utiliser le serveur de transport Edge Exchange Server 2010 avec les serveurs Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Serveur d'accès au client

Le serveur d'accès au client dans Exchange Server 2013 offre les fonctionnalités suivantes :

- Serveur sans état. Dans Exchange Server 2007 et 2010, la plupart des protocoles du serveur d'accès au client nécessitaient une affinité de session dans les scénarios où le serveur d'accès au client faisait partie d'un cluster d'équilibrage de charge. En d'autres termes, toutes les requêtes d'un client Outlook Web App unique devaient être traitées durant une session entière par un serveur d'accès au client spécifique au sein d'un groupe de serveurs d'accès au client à charge équilibrée. Dans Exchange Server 2013, ce n'est plus le cas. Le serveur d'accès au client est désormais sans état. Tout le traitement de la boîte aux lettres se passe désormais sur le serveur de boîtes aux lettres. Par conséquent, cela n'a pas d'importance de savoir quel est le serveur d'accès au client d'un groupe de serveurs d'accès au client qui reçoit chaque requête cliente. En implémentant cette configuration, vous pouvez utiliser l'équilibrage de charge de la couche 4 à la place de l'équilibrage de charge de la couche 7, qui est plus onéreux. Cela permet aux périphériques d'équilibrage de la charge matérielle de prendre en charge un nombre bien plus important de connexions simultanées.
- Regroupement de connexions. Comme dans les versions précédentes d'Exchange, le serveur d'accès au client gère l'authentification des clients pour les connexions clientes et envoie les données AuthN au rôle serveur de boîtes aux lettres. La connexion entre le serveur d'accès au client et le serveur de boîtes aux lettres est établie à l'aide d'un compte disposant de privilèges et qui est membre du groupe Serveurs Exchange. Cela permet aux serveurs d'accès au client de regrouper de manière efficace les connexions aux serveurs de boîtes aux lettres. Grâce à cette technologie, un groupe de serveurs d'accès au client peut gérer des millions de connexions clientes à partir d'Internet ou du réseau interne, mais en utilisant beaucoup moins de connexions pour transférer les requêtes vers les serveurs de boîtes aux lettres que dans les versions antérieures d'Exchange.

Serveur de boîtes aux lettres

Dans Exchange Server 2013, le rôle serveur de boîte aux lettres offre beaucoup plus de fonctionnalités que dans les versions antérieures d'Exchange Server. Cela inclut l'intégration du service de transport Hub (auparavant appelé rôle serveur de transport Hub) et du service de messagerie unifiée (auparavant appelé rôle serveur de messagerie unifiée). Il s'agit du rôle clé pour le stockage des données de boîtes aux lettres et de dossiers publics, ainsi que pour la fonctionnalité de messagerie unifiée et Message Queuing.

Le rôle serveur de boîte aux lettres interagit également avec le serveur d'accès au client, ainsi que les contrôleurs de domaine AD DS et les catalogues globaux. Le rôle serveur de boîte aux lettres ne communique jamais directement avec les clients, comme il le faisait dans les versions antérieures d'Exchange Server. Toutes les communications avec le client sont effectuées via le rôle serveur d'accès au client.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

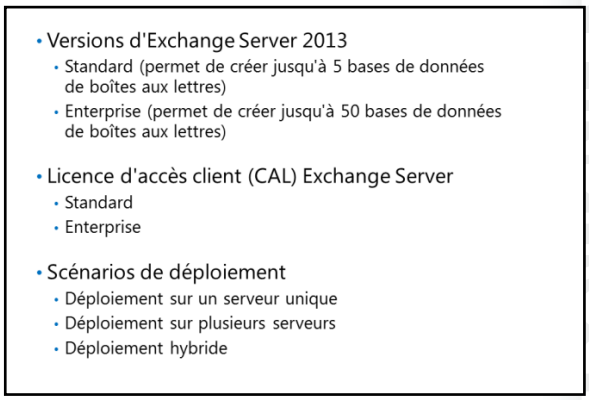
Communication entre le client et le serveur dans Exchange Server 2013

En raison des modifications apportées à l'architecture d'Exchange Server 2013, des changements ont également été apportés à la façon dont les clients communiquent avec Exchange Server, ainsi qu'à la façon dont les rôles Exchange Server 2013 communiquent entre eux et avec les composants AD DS.

Du point de vue du client, le changement le plus important en matière de connectivité vient du fait que l'appel de procédure distante (RPC) n'est plus pris en charge en tant que protocole d'accès au client direct. Dans les versions antérieures d'Exchange, les clients Outlook d'un réseau interne se connectaient à Exchange Server via RPC (ou MAPI). Dans Exchange Server 2013, toutes les connexions clientes sont établies à l'aide de RPC sur HTTPS. Cela signifie que tous les clients se connectent à l'aide du service Outlook Anywhere. Cela évite l'exécution du service RPC sur le serveur d'accès au client. En outre, vous aurez un nom de domaine complet en moins à gérer, car tous les clients utilisent un nouveau point de connexion composé du GUID de boîte aux lettres de l'utilisateur + @ + suffixe UPN. En raison de ces modifications, seul Outlook 2007 et les clients plus récents prennent en charge la connexion à Exchange Server 2013.

Options de déploiement pour Exchange Server 2013

Lors de la planification d'une installation d'Exchange Server 2013, vous devez déterminer comment vous allez organiser les rôles serveur. En outre, vous devez choisir la version appropriée d'Exchange Server 2013.



Exchange Server 2013 est disponible dans les versions Standard Edition et Enterprise Edition. La version Standard Edition est conçue pour répondre aux besoins de la plupart des petites et moyennes entreprises en matière de messagerie ; toutefois, elle peut également convenir pour des rôles serveur spécifiques ou des agences. La version Enterprise Edition, qui s'adresse aux grandes entreprises, permet de créer des bases de données supplémentaires et inclut d'autres fonctionnalités avancées. La principale différence entre les versions Standard et Enterprise est que cette dernière prend en charge jusqu'à 50 bases de données de boîtes aux lettres, alors que la version Standard ne permet de créer que 5 bases de données au plus. La version utilisée est déterminée par la clé de produit que vous entrez lors de l'activation de votre installation Exchange. Vous devez également vous assurer que vous sélectionnez la version appropriée en matière de licence d'accès client (CAL) parmi les options suivantes :

- Licence d'accès client standard Exchange Server. Cette licence permet d'accéder au courrier électronique, au calendrier partagé, ainsi qu'à Outlook Web App et ActiveSync.
- Licence d'accès client entreprise Exchange Server. Cette licence requiert une licence d'accès client standard et fournit l'accès à des fonctionnalités supplémentaires telles que la messagerie unifiée, la journalisation par utilisateur et par liste de diffusion, les dossiers de messagerie personnalisés gérés et Microsoft Forefront® Endpoint Protection pour Exchange Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

En général, vous avez le choix entre trois scénarios de déploiement :

- Déploiement sur un serveur unique. Dans ce scénario, vous déployez les deux rôles Exchange Server sur un serveur unique. Ce scénario est approprié pour les petites organisations aux ressources limitées. Le déploiement de l'ensemble des services Exchange Server sur un serveur unique présente plusieurs inconvénients. En effet, il n'existe qu'un seul point de défaillance pour l'ensemble de votre système de messagerie et vous ne disposez pas d'options de haute disponibilité. Si vous choisissez de déployer Exchange sur un seul serveur, il est recommandé de déployer Exchange Server sur un ordinateur virtuel qui soit hautement disponible ou qui soit au moins répliqué sur un autre hôte Hyper-V® dans Windows Server® 2012. Cela vous permettra de bénéficier d'une haute disponibilité et d'une redondance des services Exchange critiques.
- Déploiement sur plusieurs serveurs. Dans le scénario de déploiement sur plusieurs serveurs, vous installez généralement le rôle serveur d'accès au client et le rôle serveur de boîtes aux lettres sur des serveurs distincts, ou vous installez plusieurs serveurs avec les deux rôles présents. Cela exige que vous fournissiez au moins deux ordinateurs virtuels ou physiques pour le déploiement d'Exchange Server. Dans les scénarios où vous voulez également fournir une haute disponibilité, ajoutez davantage d'ordinateurs pour créer le cluster d'équilibrage de charge d'accès au client et les groupes de disponibilité de base de données. Vous ne pouvez pas utiliser les groupes de disponibilité de base de données et l'équilibrage de charge réseau sur le même ensemble d'ordinateurs. Pour obtenir une redondance complète d'Exchange Server, vous avez besoin d'au moins quatre serveurs pour Exchange et d'au moins deux contrôleurs de domaine.
- Déploiement hybride. Un déploiement hybride offre la possibilité d'étendre les fonctionnalités Exchange Server locales dans le cloud. Dans ce scénario, vous connectez vos services AD DS et Exchange Server à Microsoft® Office 365. Cela vous permet de déplacer certaines de vos ressources Exchange vers Office 365. Un déploiement hybride peut également servir d'étape intermédiaire avant de passer complètement à une organisation Exchange Online.

Déploiement hybride d'Exchange Server 2013 avec Office 365

Office 365 est une suite de quatre services Microsoft qui sont désormais disponibles dans une version en ligne : Exchange Online, Lync® Online, SharePoint® Online et Office Professionnel Plus. Il s'agit d'un service par abonnement qui propose différentes options tarifaires.

- Le déploiement hybride d'Exchange offre les fonctionnalités suivantes
  - Routage du courrier avec un espace de noms de domaine partagé
  - Liste d'adresses globale unifiée
  - Partage des informations de disponibilité et du calendrier
  - Contrôle centralisé du flux de messagerie
  - URL Outlook Web App unique
  - Possibilité de déplacer des boîtes aux lettres existantes vers le cloud
  - Gestion de boîte aux lettres centralisée
  - Archivage des messages dans le cloud
- Composants supplémentaires nécessaires au déploiement hybride
  - Microsoft Federation Gateway
  - Synchronisation Active Directory

Exchange Online apporte à Exchange Server des fonctionnalités telles que le courrier électronique, le calendrier et les contacts, ainsi qu'une protection antivirus et une protection contre le courrier indésirable. Vous pouvez connecter votre organisation Exchange Server 2013 existante à Exchange Online afin d'enrichir l'expérience Exchange des utilisateurs. Dans Exchange Server 2013, il est possible de créer un déploiement hybride entre une installation locale d'Exchange Server et Exchange Online à partir de Microsoft Office® 365. Un déploiement hybride offre aux organisations la possibilité d'étendre l'expérience utilisateur et le contrôle administratif de l'organisation Microsoft Exchange locale déjà existante au cloud d'Office 365. Un déploiement hybride vous permet de disposer d'une vue d'une organisation Exchange unique basée sur une organisation locale et une organisation de type cloud. En outre, un déploiement hybride peut servir d'étape intermédiaire pour passer complètement à une organisation Exchange de type cloud.

Un déploiement hybride d'Exchange Server et d'Office 365 offre les fonctionnalités suivantes :

- Routage du courrier avec un espace de noms de domaine partagé. Par exemple, l'organisation locale et l'organisation de type cloud utilisent le domaine SMTP @adatum.com.
- Liste d'adresses globale unifiée, également appelée carnet d'adresses partagé. Avec cette liste d'adresses, les utilisateurs peuvent voir tous les contacts de l'organisation Exchange locale et d'Office 365.
- Partage des informations de disponibilité et du calendrier entre l'organisation locale et l'organisation de type cloud.
- Contrôle centralisé du flux de messagerie. L'organisation locale peut contrôler le flux de messagerie de l'organisation locale et de l'organisation de type cloud.
- URL Outlook Web App unique pour l'organisation locale et l'organisation de type cloud.
- Possibilité de déplacer des boîtes aux lettres locales existantes vers l'organisation de type cloud.
- Gestion de boîte aux lettres centralisée via la console de gestion Exchange locale.
- Suivi des messages, infos-courrier et recherche dans plusieurs boîtes aux lettres entre l'organisation locale et l'organisation de type cloud.
- Archivage des messages dans le cloud pour les boîtes aux lettres Exchange locales. L'archivage Exchange Online peut être utilisé avec un déploiement hybride.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

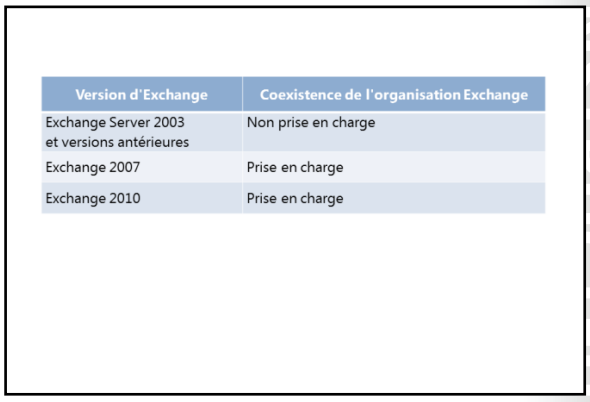
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si vous souhaitez implémenter Exchange Server 2013 dans un scénario de déploiement hybride, vous devez configurer deux éléments très importants pour connecter vos services AD DS locaux à l'infrastructure Exchange et Office 365. Il s'agit notamment des éléments suivants :

- Microsoft Federation Gateway. Microsoft Federation Gateway est un service gratuit qui fournit une connexion approuvée entre votre serveur Exchange Server (installé localement) et Exchange Online (en tant que partie intégrante d'Office 365). Il est indispensable que votre organisation Exchange locale approuve Microsoft Federation Gateway. Vous pouvez configurer cette relation d'approbation manuellement. Toutefois, cette dernière peut également être créée automatiquement lors de la configuration d'un déploiement hybride avec l'Assistant Configuration hybride. Une approbation de fédération avec Microsoft Federation Gateway pour votre client Office 365 est configurée automatiquement lorsque vous activez votre compte de service Office 365.
- Synchronisation Active Directory. Si vous souhaitez fournir des services Exchange Online à vos utilisateurs locaux, vous devez synchroniser les informations entre vos services AD DS et Exchange Online. La synchronisation Active Directory réplique les informations AD DS locales des objets à extension messagerie vers l'organisation Office 365, afin de permettre la prise en charge de la liste d'adresses globale (GAL). Les organisations qui configurent un déploiement hybride doivent déployer la synchronisation Active Directory sur un serveur local distinct.

Options de mise à niveau et de migration

Pour mettre à niveau votre organisation Exchange existante vers Exchange Server 2013, vous ne pouvez pas mettre à niveau directement votre serveur Exchange actuel en installant Exchange Server 2013 sur une version antérieure. Cette procédure, appelée mise à niveau sur place, n'est pas prise en charge pour Exchange Server 2013. En fait, vous ne pouvez mettre à niveau votre organisation Exchange Server existante qu'en installant Exchange Server 2013 sur un nouveau serveur, puis en faisant migrer toutes les ressources de votre ancien serveur Exchange Server vers Exchange Server 2013. Une fois la migration terminée, vous pouvez désactiver votre ancien serveur Exchange Server.

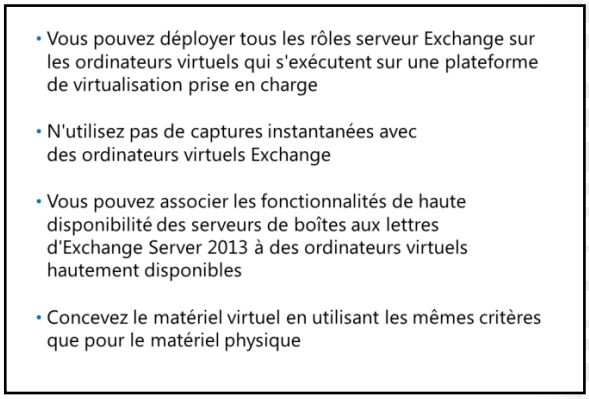


La coexistence d'Exchange Server 2013 et des versions antérieures d'Exchange Server est décrite dans le tableau suivant :

Version d'Exchange	Coexistence de l'organisation Exchange
Exchange Server 2003 et versions antérieures	Non prise en charge
Exchange 2007	Prise en charge
Exchange 2010	Prise en charge

Déploiement d'Exchange Server 2013 en tant qu'ordinateurs virtuels

Exchange Server 2013 vous permet de déployer tous les rôles serveur en tant qu'ordinateurs virtuels. Le recours à la virtualisation pour déployer des serveurs améliore considérablement l'utilisation des ressources, et simplifie également le déploiement et la gestion. Outre l'évaluation des avantages potentiels d'une mise à niveau, vous devez également prendre en compte les aspects relatifs au déploiement d'ordinateurs virtuels dans votre environnement Exchange Server actuel.



Avantages de l'utilisation d'ordinateurs virtuels

Le déploiement de serveurs Exchange Server 2013 en tant qu'ordinateurs virtuels présente les mêmes avantages et inconvénients que le déploiement de tout autre serveur en tant qu'ordinateur virtuel. De nombreuses organisations virtualisent les serveurs physiques pour réduire les coûts et s'assurer que le matériel lié aux serveurs est correctement utilisé.

Le déploiement de serveurs Exchange Server en tant qu'ordinateurs virtuels présente les avantages suivants :

- Augmentation de l'utilisation du matériel et réduction du nombre de serveurs physiques. Dans de nombreuses organisations, les serveurs déployés dans des centres de données présentent une faible utilisation du matériel. En déployant plusieurs ordinateurs virtuels sur un serveur physique unique, vous pouvez augmenter l'utilisation du matériel, tout en réduisant le nombre de serveurs physiques déployés. Cela vous permet de réaliser des économies considérables.
- Fourniture d'options de gestion de serveur qui ne sont pas disponibles pour les serveurs physiques. Les ordinateurs virtuels étant essentiellement constitués d'un ensemble de fichiers, vous pouvez disposer d'options de gestion supplémentaires avec ceux-ci. Par exemple, pour augmenter le niveau d'utilisation matérielle d'un ordinateur virtuel, vous pouvez attribuer des ressources hôtes supplémentaires à l'ordinateur virtuel ou déplacer les fichiers de l'ordinateur virtuel vers un serveur hôte plus puissant.

Bien que l'exécution de serveurs Exchange Server en tant qu'ordinateurs virtuels puisse offrir des avantages importants, vous devez également vous assurer que votre organisation dispose des ressources et des fonctionnalités de gestion nécessaires pour fournir un service aussi essentiel que la messagerie dans un environnement virtuel. L'implémentation de la virtualisation introduit un niveau supplémentaire de complexité, car vous êtes obligé de gérer à la fois les serveurs Exchange Server virtuels et les serveurs hôtes. En outre, l'hébergement de plusieurs ordinateurs virtuels sur un seul hôte peut augmenter le risque de défaillance d'un serveur physique unique, ce qui entraîne la défaillance de plusieurs ordinateurs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour le déploiement de serveurs Exchange Server 2013 en tant qu'ordinateurs virtuels

Bien que l'exécution de serveurs Exchange Server 2013 en tant qu'ordinateurs virtuels présente certains avantages, vous devez également prendre en compte les points suivants :

- Vous pouvez concevoir les serveurs Exchange Server de manière à ce qu'ils utilisent au maximum le matériel disponible. Par exemple, dans une grande organisation, vous pouvez déployer plusieurs milliers de boîtes aux lettres vers un serveur de boîtes aux lettres ou déployer un serveur d'accès au client avec les connexions clientes suffisantes afin de vous assurer que votre organisation utilise au maximum toutes les ressources matérielles.
- L'un des avantages que présente l'exécution d'ordinateurs virtuels est que vous pouvez configurer la haute disponibilité dans l'environnement d'ordinateur virtuel. Dans Exchange Server 2013, vous pouvez exécuter à la fois les groupes de disponibilité de base de données (DAG) et une solution à haute disponibilité basée sur les ordinateurs virtuels. Les DAG fournissent des fonctionnalités de basculement qui ne sont pas disponibles dans les solutions de haute disponibilité basées sur un ordinateur virtuel. Les fonctionnalités des DAG incluent notamment les copies multiples de la base de données, la sauvegarde de la base de données sur le nœud passif et les basculements d'applications. Les groupes de disponibilité de base de données peuvent être utilisés avec la technologie de migration et de clustering avec basculement basée sur l'hôte, tant que les ordinateurs virtuels sont configurés de sorte qu'ils n'enregistrent pas et ne restaurent pas l'état sur le disque lorsqu'ils sont déplacés ou mis hors connexion. Toute activité de basculement intervenant au niveau hyperviseur doit se traduire par un redémarrage complet quand l'ordinateur virtuel est activé sur le nœud cible. Toute la migration planifiée doit entraîner un arrêt et un redémarrage complet, ou une migration en ligne qui recourt à une technologie telle que la migration dynamique Hyper-V.
- Le stockage utilisé par l'ordinateur invité Exchange Server peut être un stockage virtuel de taille fixe, un stockage direct SCSI (Small Computer System Interface) ou un stockage iSCSI (Internet SCSI). Le stockage direct est configuré au niveau de l'hôte et est dédié à un ordinateur invité. Pour optimiser les performances de stockage du serveur Exchange Server, utilisez des disques directs ou des disques virtuels de taille fixe. Vous pouvez également utiliser la fonction SAN dans Hyper-V 3.0 pour fournir un stockage réseau SAN Fibre Channel à un ordinateur virtuel.
- Vous devez allouer un espace de stockage suffisant pour chaque ordinateur invité Exchange Server sur l'ordinateur hôte. Un espace de stockage est nécessaire pour le disque fixe qui contient le système d'exploitation de l'invité, les fichiers de stockage mémoire temporaires en cours d'utilisation et les fichiers des ordinateurs virtuels correspondants hébergés sur l'ordinateur hôte. En outre, pour chaque ordinateur invité Exchange Server, vous devez allouer un espace de stockage suffisant pour les files d'attente de messages, ainsi que pour les bases de données et les fichiers journaux des serveurs de boîtes aux lettres. Vous devez héberger le stockage utilisé par Exchange Server dans des piles de disque distinctes du stockage qui héberge le système d'exploitation de l'ordinateur virtuel invité. Le système d'exploitation d'un ordinateur invité Exchange doit utiliser un disque dur virtuel d'au moins 15 Go, plus la taille de la mémoire virtuelle qui est allouée à l'ordinateur invité. Cette capacité est nécessaire pour prendre en compte l'espace disque requis pour le système d'exploitation et le fichier de pagination. Par exemple, si 16 Go de mémoire sont alloués à l'ordinateur invité, l'espace disque minimum nécessaire pour le disque du système d'exploitation invité est de 31 Go.

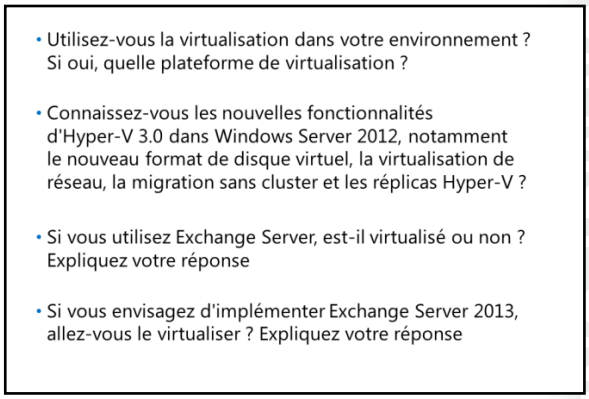
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Vous pouvez déployer uniquement des logiciels de gestion tels qu'un logiciel antivirus, un logiciel de sauvegarde et un logiciel de gestion de l'ordinateur virtuel, sur l'ordinateur de la racine physique. N'installez pas d'autres applications serveur, par exemple Exchange Server, Microsoft® SQL Server® ou les services AD DS, sur l'ordinateur racine. L'ordinateur de la racine doit être dédié à l'exécution des ordinateurs virtuels invités.
- L'exécution de serveurs Exchange Server en tant qu'ordinateurs virtuels peut rendre difficile l'analyse des performances. Les données de performance entre l'hôte et l'ordinateur virtuel ne sont pas cohérentes, car l'ordinateur virtuel utilise uniquement une partie des ressources de l'hôte.
- L'un des éléments ralentissant le plus souvent les performances des serveurs de boîtes aux lettres est l'entrée/la sortie (E/S) du réseau. Lorsque vous exécutez des serveurs de boîtes aux lettres dans un environnement virtuel, les ordinateurs virtuels doivent partager la bande passante d'E/S avec l'ordinateur hôte et d'autres serveurs de l'ordinateur virtuel déployés sur le même hôte. Si un ordinateur virtuel unique est exécuté sur le serveur physique, l'E/S réseau disponible pour l'ordinateur virtuel équivaut quasiment à l'E/S disponible pour un serveur physique. Un serveur de boîtes aux lettres très sollicité peut consommer toute la bande passante d'E/S disponible, ce qui rend impossible l'hébergement d'ordinateurs virtuels supplémentaires sur le serveur physique.
- Si vous envisagez de déployer Exchange Server 2013 en tant qu'ordinateur virtuel, veillez à planifier soigneusement la configuration matérielle virtuelle requise. L'exécution d'Exchange Server 2013 en tant qu'ordinateur virtuel ne modifie pas la configuration matérielle requise pour Exchange Server. Vous devez attribuer les mêmes ressources matérielles à l'ordinateur virtuel Exchange Server que pour un serveur physique exécutant la même charge de travail.

Remarque : N'utilisez pas de captures instantanées d'ordinateurs virtuels avec Exchange Server déployé au sein d'un ordinateur virtuel dans un environnement de production. Cela risque d'entraîner un comportement inattendu et n'est pas pris en charge.

Discussion : Implémentation de l'infrastructure Exchange dans un environnement virtuel

Discutez de la virtualisation d'Exchange et d'autres services avec les stagiaires. Menez la discussion à l'aide des questions suivantes :



- Utilisez-vous la virtualisation dans votre environnement ? Si oui, quelle plateforme de virtualisation utilisez-vous ?
- Connaissez-vous les nouvelles fonctionnalités d'Hyper-V 3.0 dans Windows Server 2012, notamment le nouveau format de disque virtuel, la virtualisation de réseau, la migration sans cluster, les réplicas Hyper-V, etc. ?
- Si vous utilisez Exchange Server, est-il virtualisé ou non ? Expliquez votre réponse.
- Si vous envisagez d'implémenter Exchange Server 2013, allez-vous le virtualiser ? Expliquez votre réponse.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure d'installation d'Exchange Server 2013 à l'aide de l'Assistant Installation

Exchange Server 2013 peut être installé via l'Assistant Installation (basé sur une interface graphique) ou à l'aide des utilitaires en ligne de commande. Si vous décidez d'utiliser l'interface graphique, exécutez le programme d'installation à partir du média d'installation. Toutefois, au préalable, assurez-vous d'avoir installé tous les composants requis par Exchange Server 2013.

Étapes d'installation de l'Assistant Installation d'Exchange Server

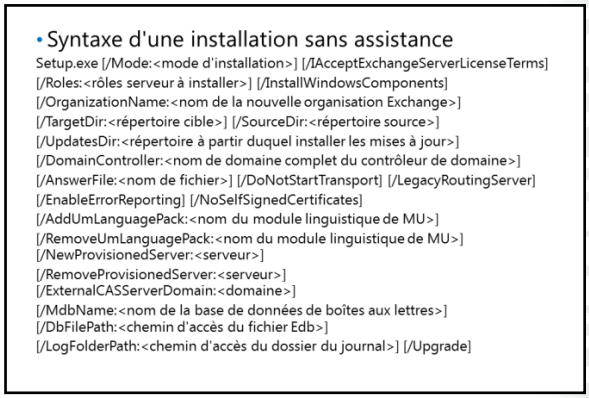
1. Rechercher des mises à jour
2. Contrat de licence
3. Paramètres recommandés
4. Sélection des rôles de serveur
5. Espace et emplacement d'installation
6. Organisation Exchange
7. Paramètres de protection contre les programmes malveillants
8. Tests de préparation

Vous effectuez les étapes suivantes lorsque vous installez Exchange Server 2013 à l'aide de l'Assistant Installation :

1. Dans la page **Rechercher des mises à jour**, vous pouvez choisir de mettre à jour le processus d'installation à l'aide des fichiers les plus récents, à partir de Microsoft Update. Il est recommandé de procéder de cette façon, si votre serveur Exchange est connecté à Internet.
2. Dans la page **Contrat de licence**, lisez les termes de votre contrat de licence passé avec Microsoft.
3. Dans la page **Paramètres recommandés**, vous pouvez choisir de configurer votre serveur pour signaler les erreurs à Microsoft. Il est recommandé de laisser ce paramètre par défaut.
4. Dans la page **Sélection des rôles serveur**, sélectionnez les rôles serveur que vous souhaitez installer. Vous pouvez choisir d'installer le rôle serveur de boîte aux lettres, le rôle serveur d'accès au client, ou les deux à la fois. Vous pouvez également choisir d'installer uniquement les outils de gestion. Dans cette même page, vous pouvez choisir d'installer l'ensemble des rôles et fonctionnalités Windows nécessaires à l'installation d'Exchange que vous souhaitez effectuer.
5. Dans la page **Espace et emplacement d'installation**, vous pouvez modifier le chemin d'accès d'installation du serveur Exchange Server.
6. Dans la page **Organisation Exchange**, vous pouvez choisir le nom de votre organisation Exchange, si vous en déployez une nouvelle. Si vous rejoignez une organisation Exchange existante, la valeur du nom est préalablement remplie. Dans cette même page, vous pouvez également choisir d'appliquer le modèle des autorisations fractionnées Active Directory à votre organisation Exchange.
7. Dans la page **Paramètres de protection contre les programmes malveillants**, vous pouvez choisir de désactiver la fonctionnalité intégrée de protection contre les programmes malveillants. Il est recommandé de ne pas désactiver cette protection contre les programmes malveillants, sauf si une autre solution de protection antivirus est déjà implémentée.
8. Dans la page **Tests de préparation**, la procédure d'installation vous informe s'il existe des obstacles à l'installation d'Exchange Server, et si votre matériel et vos logiciels respectent bien les prérequis. Si tout est en ordre, cliquez sur **Installer** et attendez qu'Exchange Server soit installé. Si vous n'avez pas préparé votre environnement AD DS avant de commencer l'installation d'Exchange Server, la procédure d'installation effectue cette tâche pendant l'installation.

L'installation d'Exchange Server 2013 peut prendre entre 20 et 50 minutes, selon les composants installés et les performances de votre serveur. Une fois l'installation terminée, vous pouvez commencer à configurer votre déploiement.

Procédure d'installation d'Exchange Server 2013 en mode sans assistance



L'installation d'Exchange Server 2013 peut également être effectuée sans utiliser l'interface graphique utilisateur de l'Assistant Installation. En utilisant la ligne de commande pour exécuter le programme setup.exe, vous pouvez installer Exchange Server 2013 en mode sans assistance. Cette méthode d'installation vous permet de fournir à l'avance toutes les réponses nécessaires à l'Assistant Installation. Par ailleurs, elle prend en charge l'installation de plusieurs serveurs Exchange Server avec les mêmes paramètres. Pour démarrer une installation sans assistance, exécutez le programme setup.exe à partir de la ligne de commande, puis fournissez les commutateurs appropriés afin de spécifier vos options d'installation d'Exchange.

Voici la syntaxe d'une installation sans assistance avec tous les commutateurs disponibles pour setup.exe :

```
Setup.exe [/Mode:<mode d'installation>] [/IAcceptExchangeServerLicenseTerms]
[/Roles:<rôles serveur à installer>] [/InstallWindowsComponents]
[/OrganizationName:<nom de la nouvelle organisation Exchange>]
[/TargetDir:<répertoire cible>] [/SourceDir:<répertoire source>]
[/UpdatesDir:<répertoire à partir duquel installer les mises à jour>]
[/DomainController:<nom de domaine complet du contrôleur de domaine>]
[/AnswerFile:<nom de fichier>] [/DoNotStartTransport] [/LegacyRoutingServer]
[/EnableErrorReporting] [/NoSelfSignedCertificates]
[/AddUmLanguagePack:<nom du module linguistique de MU>]
[/RemoveUmLanguagePack:<nom du module linguistique de MU>]
[/NewProvisionedServer:<serveur>]
[/RemoveProvisionedServer:<serveur>] [/ExternalCASServerDomain:<domaine>]
[/MdbName:<nom de la base de données de boîtes aux lettres>] [/DbFilePath:<chemin d'accès
du fichier Edb>]
[/LogFolderPath:<chemin d'accès du dossier du journal>] [/Upgrade]
```

Vous n'avez pas à fournir de valeur pour chacun de ces commutateurs. Vous devez seulement inclure les commutateurs qui se rapportent à votre scénario d'installation, ainsi que le niveau de détail que vous souhaitez offrir.

- Les éléments suivants constituent la liste des commutateurs les plus couramment utilisés : /Mode. Contrôle ce que fait le programme d'installation. Il peut prendre les valeurs suivantes : Install, Uninstall, RecoverServer.
- /roles. Spécifie les rôles que vous souhaitez installer. Si vous spécifiez plusieurs rôles, vous devez les séparer par des virgules. Vous pouvez indiquer les valeurs CA (pour le rôle d'accès au client) ou MB (pour le rôle de boîte aux lettres).
- /OrganizationName. Spécifie le nom que vous voulez donner à la nouvelle organisation Exchange Server. Ce paramètre est obligatoire pour l'installation du premier serveur d'une organisation.
- /TargetDir. Spécifie le dossier dans lequel Exchange Server 2013 doit être installé. Par défaut : %%programfiles%%\Microsoft\Exchange Server.
- /DomainController. Spécifie le contrôleur de domaine auquel le programme d'installation a accès en lecture et en écriture au cours du processus d'installation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION PRÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les éléments suivants sont des exemples de commandes qui peuvent être utilisées pour des installations sans assistance :

```
Setup.exe /mode:Install /role:ClientAccess,Mailbox /OrganizationName:MonOrg
/IAcceptExchangeServerLicenseTerms
```

Cette commande installe le rôle serveur d'accès au client, le rôle serveur de boîtes aux lettres et les outils de gestion à l'emplacement d'installation par défaut. En outre, elle indique que le nom de l'organisation est MonOrg.

```
Setup.exe /r:CA,MB /IAcceptExchangeServerLicenseTerms
```

Cette commande installe le rôle serveur d'accès au client, le rôle serveur de boîtes aux lettres et les outils de gestion à l'emplacement d'installation par défaut.

```
Setup.exe /role:ClientAccess,Mailbox /UpdatesDir:"C:\ExchangeServer\New Patches"
/IAcceptExchangeServerLicenseTerms
```

Cette commande met à jour ExchangeServer.msi avec les mises à jour provenant du répertoire spécifié, puis installe le rôle serveur d'accès au client, le rôle serveur de boîte aux lettres et les outils de gestion. Si un lot de modules linguistiques est inclus dans ce répertoire, le module linguistique est également installé.

```
Setup.exe /mode:Install /role:ClientAccess /AnswerFile:c:\ExchangeConfig.txt
/IAcceptExchangeServerLicenseTerms
```

Cette commande installe le rôle serveur d'accès au client à l'aide des paramètres du fichier ExchangeConfig.txt.

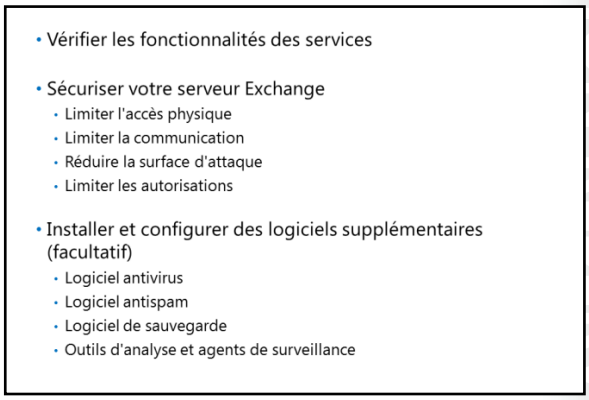
Démonstration : Installation d'Exchange Server 2013

Procédure de démonstration

1. Sur LON-DC1-B, attachez **D:\Program Files\Microsoft Learning\22341\Drives\ExchangeServer2013CU1.iso** en tant que lecteur de DVD.
2. Ouvrez Windows PowerShell.
3. Accédez au lecteur D:. Tapez **.\Setup.exe /PrepareAD /IAcceptExchangeServerLicenseTerms /OrganizationName:Adatum**, puis appuyez sur **Entrée**. Attendez la fin du processus.
4. Basculez vers LON-EX1.
5. Mappez **D:\Program Files\Microsoft Learning\22341\Drives\ExchangeServer2013CU1.iso** en tant que lecteur de DVD.
6. Ouvrez l'Explorateur Windows et accédez à D:\.
   - Exécutez setup.exe.
   - Ne recherchez pas les mises à jour.
   - Sélectionnez l'installation du Rôle de boîte aux lettres et du Rôle d'accès au client.
   - Ne désactivez pas l'analyse des programmes malveillants.
   - Démarrez la vérification des conditions préalables.
   - Redémarrez l'ordinateur et exécutez à nouveau setup.exe.

Tâches de post-installation

Une fois l'installation d'Exchange Server terminée, vous devrez peut-être exécuter des étapes supplémentaires pour finaliser le déploiement du serveur.



Configuration de la sécurité Exchange Server

La sécurité est importante pour tous les serveurs de votre déploiement. Toutefois, elle est encore plus importante pour les ordinateurs qui exécutent Exchange Server. Pour la plupart des organisations, la messagerie est une partie essentielle du réseau. Les utilisateurs comptent sur la messagerie pour effectuer leur travail. Par ailleurs, des informations confidentielles et personnelles sont souvent envoyées via le système de messagerie et stockées sur ce dernier. Les ordinateurs qui exécutent Exchange Server communiquent tous avec Internet d'une façon ou d'une autre, ce qui n'est pas le cas pour de nombreux autres serveurs. Même les serveurs de boîtes aux lettres sans communication directe avec Internet sont exposés à des messages provenant d'Internet.

Pour sécuriser les ordinateurs qui exécutent Exchange Server 2013, procédez comme suit :

- Limitez l'accès physique. Comme pour tous les serveurs, l'accès physique à un ordinateur qui exécute Exchange Server doit être limité. Tout serveur auquel vous pouvez accéder physiquement peut être compromis facilement.
- Limitez la communication. Vous pouvez utiliser des pare-feu pour limiter la communication entre les serveurs ainsi qu'entre les serveurs et les clients. Le fait de limiter la communication à des adresses IP ou des plages d'adresses IP spécifiques réduit le risque qu'un pirate accède au système ou le modifie. Un serveur de transport Edge (s'il est déployé) ou toute autre passerelle SMTP doit être disponible pour les connexions Internet anonymes, mais les pare-feu peuvent limiter l'accès à des ports spécifiques.
- Réduisez la surface d'attaque. Pour limiter les failles logicielles exploitables par les pirates, supprimez les logiciels et les services inutiles de vos serveurs Exchange Server. En particulier, si vous déployez des serveurs de transport Edge, seuls les services et les logiciels nécessaires doivent s'exécuter sur ces serveurs, car ils sont exposés à Internet.
- Limitez les autorisations. Identifiez qui dispose des autorisations pour gérer Active Directory dans votre organisation. Les utilisateurs qui sont des administrateurs de domaines peuvent s'ajouter à tout groupe, et ainsi, gérer tous les destinataires Exchange Server et ordinateurs exécutant Exchange Server dans ce domaine. Limitez plus précisément les autorisations de gestion AD DS déléguées si vous ne voulez pas que tous les administrateurs de domaine puissent également gérer Exchange Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

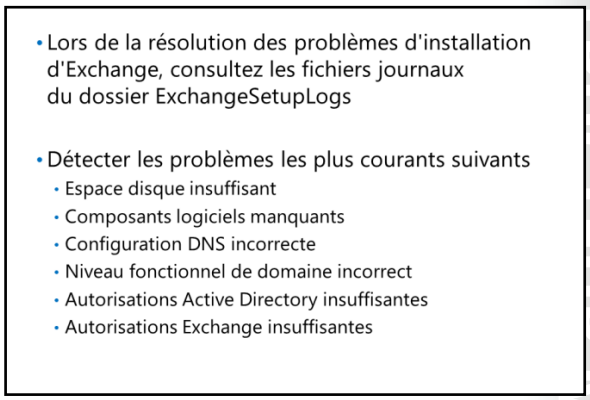
Configuration des logiciels supplémentaires

Avant d'installer tout logiciel supplémentaire, assurez-vous qu'il est certifié Microsoft pour une utilisation avec Exchange Server 2013. Dans le cas contraire, vous risquez d'être confronté à une perte de données ou une perte de disponibilité. Les produits spécifiquement conçus pour une utilisation avec Exchange Server 2013 tirent parti des nouvelles fonctionnalités.

Voici quelques-uns des logiciels supplémentaires que vous pouvez installer ou configurer :

- Logiciel antivirus. Vous pouvez choisir d'utiliser Forefront Online Protection ou une solution antivirus tierce. Vous pouvez aussi utiliser une protection anti-programmes malveillants intégrée.
- Logiciel anti-courrier indésirable. Ce type de logiciel peut réduire considérablement le nombre de messages électroniques publicitaires non sollicités que vos utilisateurs reçoivent et doivent gérer. De nombreuses organisations choisissent de déployer des solutions antispam tierces. Vous pouvez également utiliser la solution antispam intégrée à Exchange Server 2013.
- Logiciel de sauvegarde. Pour sauvegarder les serveurs Exchange Server 2013, vous devez déployer un logiciel de sauvegarde qui utilise le service VSS (Volume Shadow Copy Service) pour exécuter la sauvegarde.
- Outils d'analyse et agents de surveillance. Microsoft System Center Operations Manager (Operations Manager) est un exemple d'outil d'analyse. Il vous permet de gérer et d'analyser vos serveurs Exchange Server de manière proactive en y installant des agents de surveillance.

Résolution des problèmes d'installation d'Exchange Server



Même s'il est rare que l'installation d'Exchange Server échoue lorsque vous répondez à toutes les conditions requises, il existe certaines situations où vous devez dépanner l'installation d'Exchange. L'installation d'Exchange Server donne lieu à une journalisation extrêmement détaillée. Les journaux d'installation d'Exchange sont situés dans le dossier C:\ExchangeSetupLogs. Le fichier journal ExchangeSetup.log contient les informations sur l'état des contrôles de conditions préalables et de disponibilité du système effectués par Exchange Server avant le début de l'installation, ainsi que des informations sur chaque tâche réalisée lors de l'installation d'Exchange Server. Il s'agit du journal le plus complet disponible pour la résolution des erreurs d'installation. Ce dossier peut contenir d'autres fichiers .msilog ou .ps1, selon les rôles que vous installez sur le serveur.

Voici quelques problèmes d'installation courants et les solutions correspondantes :

- Espace disque insuffisant. Il est possible que votre serveur ne dispose pas de l'espace disque nécessaire pour installer Exchange Server 2013. Pour résoudre ce problème, augmentez l'espace disque de votre serveur ou supprimez des fichiers inutiles afin de libérer de l'espace.
- Composants logiciels manquants. Il est possible que votre serveur ne dispose pas de tous les composants logiciels requis pour les rôles serveur que vous souhaitez implémenter. Pour résoudre ce problème, déterminez les composants logiciels requis, téléchargez-les si besoin, puis installez-les.
- Configuration DNS incorrecte. Exchange Server 2013 dépend des serveurs de catalogue global pour l'exécution de nombreuses opérations et utilise DNS pour rechercher ces serveurs. Si la configuration DNS est incorrecte, votre serveur ne pourra peut-être pas rechercher un serveur de catalogue global. Pour analyser le problème, utilisez l'outil dcdiag. Pour résoudre le problème, assurez-vous que le serveur Exchange et les contrôleurs de domaine utilisent les serveurs DNS internes appropriés.
- Niveau fonctionnel de domaine incorrect. Tous les domaines contenant des serveurs ou des destinataires Exchange Server 2013 doivent être définis selon le niveau fonctionnel de Windows Server 2008 R2, Windows Server 2008 ou Windows Server 2003. Pour résoudre ce problème, élevez le niveau fonctionnel du domaine au niveau fonctionnel approprié.
- Autorisations Active Directory insuffisantes. Lorsque vous installez Exchange Server 2013, vous avez besoin des autorisations suffisantes pour étendre le schéma Active Directory et modifier la partition de configuration d'Active Directory. Pour exécuter l'extension de schéma initiale, vous devez être membre des groupes Administrateurs d'entreprise et Administrateurs de schéma.
- Autorisations Exchange insuffisantes. Pour installer Exchange Server 2013 dans une organisation existante, vous devez être membre du groupe Administrateurs Exchange pour la version Exchange Server antérieure.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Gestion d'Exchange Server 2013

Une fois Exchange Server 2013 installé, vous devez gérer votre déploiement d'Exchange. Les administrateurs Exchange peuvent gérer Exchange Server à l'aide d'une nouvelle interface graphique basée sur le Web, appelée Centre d'administration Exchange, ou via l'environnement de ligne de commande Exchange Management Shell. Les utilisateurs Exchange peuvent gérer un ensemble d'options disponibles via l'interface Outlook Web App. Cette leçon décrit chacune de ces techniques de gestion d'Exchange Server 2013.

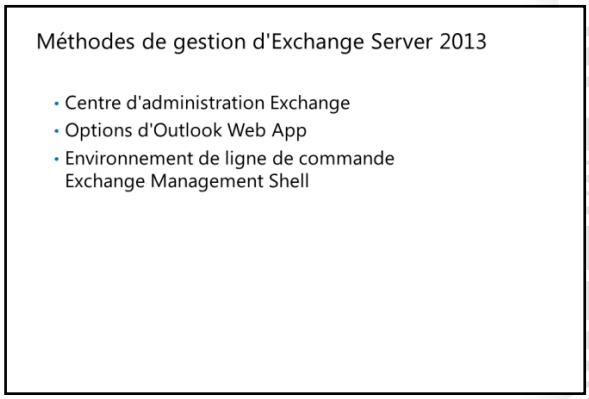
Objectifs de la leçon

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

- gérer Exchange Server 2013 ;
- décrire le Centre d'administration Exchange ;
- gérer les propriétés de boîte aux lettres utilisateur avec Outlook Web App ;
- décrire Windows PowerShell ;
- décrire la syntaxe de Windows PowerShell ;
- décrire la façon d'accéder à l'aide de Windows PowerShell ;
- décrire l'environnement de ligne de commande Exchange Management Shell ;
- effectuer des exemples d'administration de l'environnement de ligne de commande Management Shell ;
- utiliser les outils d'administration Exchange pour gérer Exchange.

Gestion d'Exchange Server 2013

Exchange Server 2013 prend en charge plusieurs méthodes pour gérer vos paramètres serveur et client. Contrairement à Exchange Server 2010 et aux versions antérieures, où la gestion était effectuée principalement à l'aide de la console MMC de gestion Exchange, Exchange Server 2013 ne fournit pas de console MMC pour la gestion de la configuration. À la place, Exchange Server 2013 utilise une nouvelle console Web appelée Centre d'administration Exchange.

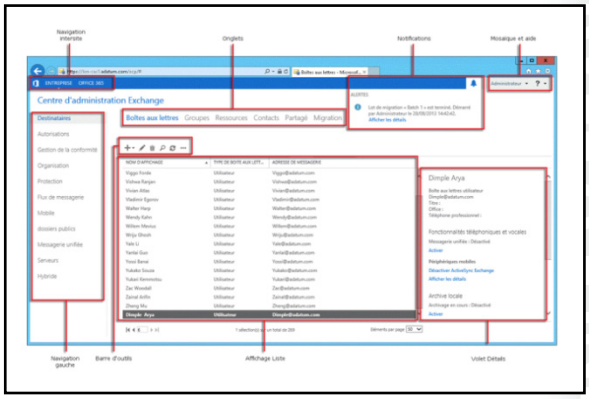


La gestion complète d'Exchange Server 2013 peut également être effectuée via l'environnement de ligne de commande Exchange Management Shell, une console Windows PowerShell qui fournit toutes les options disponibles pour la gestion de votre serveur Exchange Server. Dans la mesure où plusieurs options de gestion ne sont pas disponibles dans le Centre d'administration Exchange, certaines tâches avancées doivent être effectuées via l'environnement de ligne de commande Exchange Management Shell.

Les utilisateurs peuvent également gérer certains de leurs paramètres de boîte aux lettres via Outlook Web App. Il s'agit également d'une interface Web qui permet aux utilisateurs de configurer les options disponibles pour leurs boîtes aux lettres et les périphériques connectés. Les utilisateurs sont autorisés à configurer uniquement un sous-ensemble des options disponibles.

Il est important que vous suiviez les techniques de gestion appropriées lors de l'exécution de tâches d'administration spécifiques. Par exemple, si vous voulez créer des boîtes aux lettres pour plusieurs utilisateurs en même temps, il est beaucoup plus efficace de le faire via l'environnement de ligne de commande Exchange Management Shell qu'à l'aide du Centre d'administration Exchange.

Qu'est-ce que le Centre d'administration Exchange ?



Le Centre d'administration Exchange est la nouvelle console Web qui vous permet de gérer votre déploiement Exchange Server 2013. Il s'agit d'une console graphique qui vous permet de gérer à la fois un déploiement local d'Exchange Server et un déploiement d'Exchange Online (ou un déploiement hybride d'Exchange). Cette console remplace la console de gestion Exchange (présente dans Exchange Server 2007 et 2010) et le Panneau de configuration Exchange.

Le Centre d'administration Exchange présente plusieurs avantages par rapport à la console MMC utilisée dans les versions antérieures d'Exchange. Dans la mesure où le Centre d'administration Exchange est une console Web, il est beaucoup plus rapide et plus réactif que la console de gestion Exchange. Le Centre d'administration Exchange vous permet d'administrer les déploiements d'Exchange locaux et les déploiements d'Exchange Online à partir du même emplacement. Le Centre d'administration Exchange est accessible via une interface de navigateur Web à partir d'un réseau interne et d'Internet. Toutefois, si vous souhaitez désactiver la gestion d'Exchange depuis l'extérieur de votre réseau, vous pouvez partitionner l'accès depuis Internet/l'intranet à partir du répertoire virtuel IIS du Panneau de configuration Exchange pour autoriser ou interdire les fonctionnalités de gestion. Cela vous permet d'autoriser ou d'interdire l'accès aux utilisateurs qui tentent d'accéder au Centre d'administration Exchange à partir d'Internet en dehors de l'environnement de votre organisation, tout en permettant l'accès aux options Outlook Web App d'un utilisateur final.

Vous pouvez accéder au Centre d'administration Exchange à l'aide de la même syntaxe d'URL que celle utilisée dans les versions antérieures. Il est situé dans le répertoire virtuel du Panneau de configuration Exchange. Lorsque vous vous connectez au Centre d'administration Exchange, vous avez la possibilité de gérer les composants suivants de votre infrastructure Exchange :

- *Destinataires*. Dans ce nœud, vous gérez les boîtes aux lettres, les groupes, les boîtes aux lettres de ressources, les contacts, les boîtes aux lettres partagées, ainsi que les migrations et déplacements de boîtes aux lettres.
- *Autorisations*. Ce nœud contient des options permettant de gérer les rôles d'administrateur, les rôles d'utilisateur et les stratégies Outlook Web App.
- *Gestion de la conformité*. Le centre Gestion de la conformité permet de gérer la recherche eDiscovery sur place, l'archive permanente, la prévention de la perte de données, les stratégies de rétention, les balises de rétention et la journalisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Organisation*. Ce nœud comprend les tâches liées à l'organisation Exchange, notamment le partage fédéré, les applications Outlook et les listes d'adresses.
- *Protection*. Exchange Server 2013 intègre les fonctionnalités anti-programmes malveillants que vous pouvez gérer à partir du Centre de protection, si vous choisissez d'implémenter la protection anti-programmes malveillants d'Exchange à la place de la protection offerte par les logiciels tiers.
- *Flux de messagerie*. Dans ce nœud, vous gérez les règles, les rapports de remise, les domaines acceptés et les stratégies d'adresses de messagerie, ainsi que les connecteurs d'envoi et de réception.
- *Mobile*. À cet emplacement de la console du Centre d'administration Exchange, vous pouvez gérer les appareils mobiles qui vous permettent de vous connecter à votre organisation. Vous pouvez gérer l'accès et les stratégies des appareils mobiles.
- *Dossiers publics*. Contrairement aux précédentes versions d'Exchange Server, dans lesquelles l'administration de dossiers publics n'était pas possible à partir de la console de gestion Exchange, dans Exchange Server 2013, les dossiers publics peuvent être gérés depuis le centre Dossiers publics.
- *Messagerie unifiée*. Le centre Messagerie unifiée est l'emplacement où vous gérez les plans de numérotation et les passerelles IP de la messagerie unifiée.
- *Serveurs*. Le centre Serveurs est l'emplacement où vous gérez les serveurs de boîtes aux lettres et d'accès au client, les bases de données, les groupes de disponibilité de la base de données, les répertoires virtuels et les certificats.
- *Hybride*. Le centre Hybride est l'emplacement où vous accédez à l'installation et à la configuration hybride.

Dans la mesure où le Centre d'administration Exchange est désormais une console de gestion Web, vous devez y accéder via votre navigateur Web à l'aide de l'URL de répertoire virtuel du Panneau de configuration Exchange. Pour trouver l'URL de répertoire virtuel du Panneau de configuration Exchange, qui permet d'accéder au Centre d'administration Exchange, exécutez la commande suivante :

```
Get-ECPVirtualDirectory | Format-List InternalURL,ExternalURL
```

Utilisez la valeur InternalURL ou ExternalURL dans votre navigateur Web pour lancer le Centre d'administration Exchange.

Gestion des propriétés de boîte aux lettres utilisateur avec Outlook Web App

Dans Exchange Server 2013, les utilisateurs peuvent gérer leurs comptes et leurs boîtes aux lettres à l'aide de l'interface Outlook Web App. Lorsque les utilisateurs se connectent à Outlook Web App, ils peuvent voir le courrier électronique et les éléments correspondants. En outre, ils peuvent également gérer leurs paramètres de boîte aux lettres.



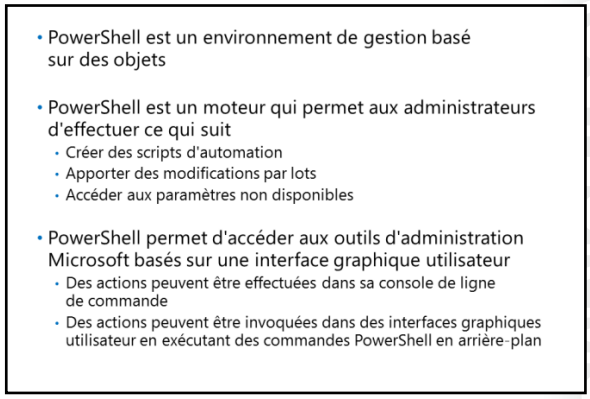
Cela permet à tous les utilisateurs de boîtes aux lettres de configurer la plupart de leurs paramètres de boîte aux lettres, notamment :

- gérer les paramètres Outlook Web App, tels que les signatures électroniques et les messages d'absence du bureau ;
- gérer les règles de la boîte de réception pour la gestion automatique des messages ;
- effectuer le suivi des messages envoyés ou reçus à partir de leur boîte aux lettres ;
- gérer les boîtes aux lettres des sites dont ils sont membres ;
- afficher et gérer les appareils mobiles connectés à leurs boîtes aux lettres ;
- gérer les notifications de messagerie texte ;
- afficher les appartenances aux groupes et demander à rejoindre des groupes publics ;
- récupérer les messages supprimés ;
- gérer les listes verte et rouge ;
- changer de mot de passe ;
- gérer les applications pour Outlook Web App.

Cela permet aux utilisateurs d'effectuer certaines tâches qui étaient auparavant réservées aux administrateurs. Ainsi, les utilisateurs ont davantage de contrôle sur l'apparence et les performances de leur système de messagerie.

Qu'est-ce que Windows PowerShell ?

Windows PowerShell est une interface de gestion de ligne de commande que vous pouvez utiliser pour configurer Windows Server 2012 et des produits tels que System Center 2012, Exchange Server 2013 et Microsoft SharePoint® Server 2013. Cette interface de gestion, qui offre une solution de remplacement en matière d'outil de gestion d'interface graphique utilisateur, permet aux administrateurs d'effectuer les tâches suivantes :



- créer des scripts d'automation ;
- apporter des modifications par lots ;
- accéder aux paramètres qui peuvent être inaccessibles ou plus difficiles à configurer dans l'interface graphique utilisateur.

Une interface graphique utilisateur peut se révéler inefficace pour les tâches que vous devez effectuer à plusieurs reprises, comme créer des comptes d'utilisateurs. En créant une fonctionnalité administrative sous forme de commandes Windows PowerShell, vous pouvez sélectionner la méthode appropriée pour une tâche donnée.

Plus vous vous familiarisez avec Windows PowerShell, plus vous pouvez l'utiliser à la place d'autres outils d'administration de bas niveau que vous utilisiez jusqu'à présent. Par exemple, Windows PowerShell a accès aux mêmes fonctionnalités que VBScript, mais il permet souvent d'effectuer plus facilement les mêmes tâches.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

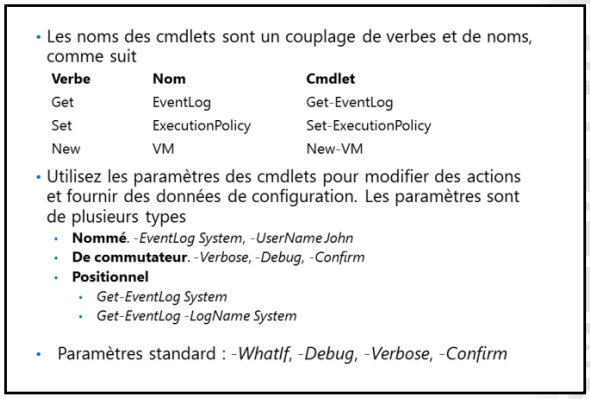
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Windows PowerShell peut également modifier la façon dont vous utilisez Windows Management Instrumentation (WMI). Windows PowerShell peut regrouper des commandes spécifiques aux tâches dans la fonctionnalité WMI sous-jacente. Quand vous utilisez Windows PowerShell avec WMI, votre travail est simplifié car Windows PowerShell fournit des commandes basées sur les tâches faciles à utiliser.

Bien que Windows PowerShell soit un excellent outil en ligne de commande pour effectuer des tâches spécifiques, il offre également des fonctionnalités supplémentaires. Windows PowerShell peut gérer des rôles et des fonctionnalités Windows Server, et peut être utilisé pour mettre en service et gérer divers objets, répertoires et composants, ainsi que pour générer des rapports sur ces éléments.

Syntaxe Windows PowerShell

Windows PowerShell utilise des commandes, appelées cmdlets, pour exécuter des tâches spécifiques. La convention d'affectation des noms pour une cmdlet comprend un verbe ou une action, un tiret, puis un nom ou un objet. Par exemple, pour récupérer une liste d'utilisateurs, servez-vous de la cmdlet **Get-User**. Cette convention d'affectation des noms normalisée est conçue pour permettre aux utilisateurs de se rappeler plus facilement la façon dont s'effectuent les tâches d'administration. Par exemple, pour modifier les paramètres d'une boîte aux lettres, vous pouvez utiliser la cmdlet **Set-Mailbox**.



Éventuellement, un ou plusieurs paramètres peuvent être utilisés avec une cmdlet pour modifier son comportement ou pour spécifier des paramètres. Lorsque vous tapez une cmdlet sur une ligne de commande, les paramètres sont entrés après le nom de la cmdlet. Chaque paramètre utilisé doit commencer par un tiret, et si plusieurs paramètres sont entrés, ces derniers doivent être séparés par un espace.

Toutes les cmdlets n'utilisent pas les mêmes paramètres. Certaines cmdlets ont des paramètres spécifiques à leur fonctionnalité. Par exemple, la cmdlet **Move-Item** inclut le paramètre *-Destination* pour spécifier l'emplacement vers lequel déplacer l'objet, tandis que la cmdlet **Get-ChildItem** accepte le paramètre *-Recurse*. Il existe plusieurs types de paramètre, notamment :

- Nommé. Il s'agit des paramètres les plus couramment utilisés. Ils peuvent exiger une valeur ou un modificateur. Par exemple, avec la cmdlet **Move-Item**, vous pouvez spécifier le paramètre *-Destination*, avec la destination exacte vers laquelle l'élément doit être déplacé.
- De commutateur. Les paramètres de commutateur modifient le comportement de la cmdlet, mais ne requièrent aucun modificateur ni aucune valeur supplémentaire. Par exemple, vous pouvez spécifier le paramètre **-***Recurse* sans spécifier la valeur $True.
- Positionnel. Les paramètres positionnels sont des paramètres qui peuvent être omis et qui peuvent accepter des valeurs en fonction de l'emplacement des informations dans la commande. Par exemple, vous pouvez exécuter **Get-EventLog -EventLog System** pour récupérer les informations du journal des événements système. Cependant, étant donné que le paramètre positionnel *-EventLog* accepte des valeurs pour la première position, vous pouvez également exécuter **Get-EventLog System** pour obtenir les mêmes résultats. Lorsque le paramètre **-***EventLog* est absent, la cmdlet accepte tout de même la valeur System car il s'agit du premier élément après le nom de la cmdlet.

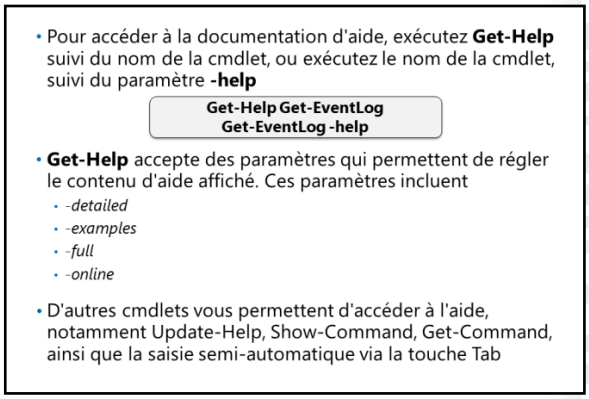
Les paramètres communs à de nombreuses applets de commande incluent des options qui permettent de tester les actions de l'applet de commande ou de générer des informations détaillées sur l'exécution de l'applet de commande. Les paramètres communs incluent :

- **-***Verbose*. Ce paramètre affiche des informations détaillées sur la commande exécutée. Vous pouvez utiliser ce paramètre pour obtenir des informations supplémentaires sur l'exécution de la commande.
- **-***WhatIf*. Ce paramètre affiche les résultats de l'exécution de la commande sans l'exécuter en réalité. Cela est utile pour tester une nouvelle cmdlet ou un nouveau script, lorsque vous ne voulez pas exécuter la cmdlet.
- **-***Confirm*. Ce paramètre affiche une invite de confirmation avant l'exécution de la commande. Ce paramètre est utile lorsque vous exécutez des scripts et que vous souhaitez inviter l'utilisateur à confirmer l'exécution d'une étape spécifique dans le script.

Documentation supplémentaire : Pour plus d'informations sur les verbes des applets de commande, accédez à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=290957.

Accès à l'aide dans Windows PowerShell

Que vous soyez un professionnel expérimenté ou que vous découvriez Windows PowerShell, la documentation d'aide relative aux applets de commande est une précieuse source d'informations. Pour accéder à la documentation d'aide, utilisez la cmdlet **Get-Help** (ou son alias, **help**) suivie du nom de la cmdlet, ou entrez le nom de la cmdlet suivi du paramètre **-help**. **Get-Help** inclut les paramètres suivants pour régler le contenu de l'aide affichée :



- *-Detailed*. Affiche une aide plus détaillée que l'option par défaut.
- *-Examples*. Affiche uniquement les exemples d'utilisation de la cmdlet.
- *-Full*. Affiche l'aide avancée et des exemples d'utilisation.
- *-Online*. Ouvre un navigateur Web vers la documentation relative aux applets de commande sur le site Web de Microsoft.

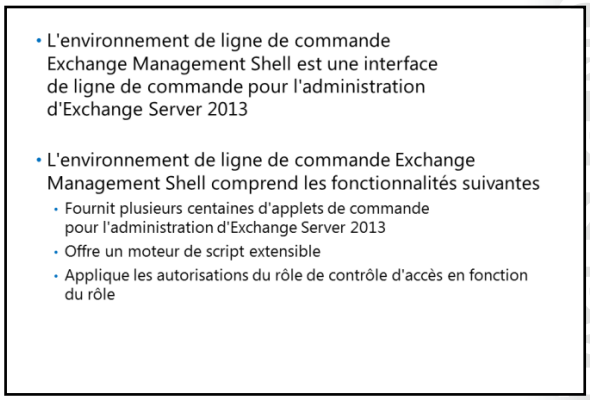
Windows PowerShell 3.0 inclut la possibilité de télécharger la dernière version de la documentation d'aide à partir de Microsoft. Pour afficher la documentation d'aide localement, vous devez utiliser la cmdlet **Update-Help**. Autre nouveauté dans Windows PowerShell 3.0, la cmdlet **Show-Command**. Cette cmdlet permet aux utilisateurs novices de PowerShell d'interagir avec les options d'entrée et de sortie pour une cmdlet à l'aide d'une interface graphique.

La cmdlet **Get-Command** renvoie une liste de tous les cmdlets, fonctions et alias disponibles en local. Vous pouvez l'utiliser pour découvrir de nouvelles cmdlets à l'aide des recherches par caractères génériques. Par exemple, pour renvoyer une liste de toutes les cmdlets qui comprennent les lettres VM dans leur nom, vous pouvez exécuter **Get-Command *VM***.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que l'environnement de ligne de commande Exchange Management Shell ?

L'environnement de ligne de commande Exchange Management Shell et la console de gestion Exchange s'exécutent sur l'interface de ligne de commande Windows PowerShell version 3.0. Ces outils utilisent également des applets de commande qui sont des commandes s'exécutant au sein de Windows PowerShell. Chaque applet de commande exécute une seule tâche d'administration, et vous pouvez combiner des applets de commande pour effectuer des tâches d'administration complexes.



Dans l'environnement de ligne de commande Exchange Management Shell, il existe plus de 700 applets de commande qui exécutent des tâches de gestion Exchange Server. Par ailleurs, il existe un nombre encore plus important d'applets de commande non Exchange Server dans la conception de l'interpréteur de commandes Windows PowerShell de base.

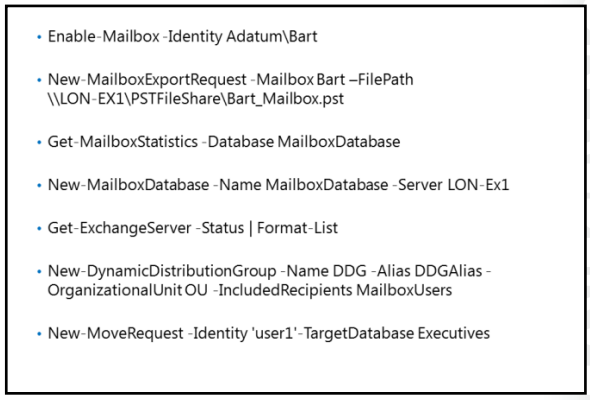
L'environnement de ligne de commande Exchange Management Shell ne se limite pas à une interface de ligne de commande que vous pouvez utiliser pour gérer Exchange Server 2013. Il s'agit d'un environnement de gestion complet qui offre un moteur de script complexe et extensible doté de fonctions de bouclage, de variables et d'autres fonctionnalités de programmation vous permettant de créer rapidement des scripts d'administration complets.

Lorsque vous exécutez des applets de commande dans l'environnement de ligne de commande Exchange Management Shell, le rôle de contrôle d'accès en fonction du rôle permet de déterminer si vous avez les autorisations requises pour exécuter les applets de commande. Le rôle de contrôle d'accès en fonction du rôle vous permet d'affecter des autorisations granulaires aux administrateurs (ainsi que l'étendue des objets modifiables) et d'ajuster plus étroitement les rôles que vous affectez aux utilisateurs et administrateurs aux rôles réels qu'ils occupent au sein de votre organisation. Dans la mesure où tous les outils d'administration Exchange Server 2013 exécutent les cmdlets de l'environnement de ligne de commande Exchange Management Shell pour apporter des modifications à l'environnement Exchange, les autorisations du rôle de contrôle d'accès en fonction du rôle sont appliquées de manière uniforme dans tous les outils d'administration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exemples d'administration de l'environnement de ligne de commande Exchange Management Shell

Dans l'environnement de ligne de commande Exchange Management Shell, vous pouvez également utiliser la commande **get-help** pour accéder à l'aide de n'importe quelle applet de commande. Par exemple, si vous voulez en savoir plus sur les options disponibles pour l'applet de commande Set-Mailbox, tapez **get-help Set-Mailbox**. Si vous souhaitez accéder à l'aide étendue, vous pouvez taper **get-help Set-Mailbox -detailed**. Et si vous voulez voir une liste d'exemples d'utilisation de l'applet de commande Set-Mailbox, tapez **get-help Set-Mailbox -examples**.



Lorsque vous tapez une applet de commande, il est très utile d'utiliser la touche Tab. L'environnement de ligne de commande Exchange Management Shell prend en charge la saisie semi-automatique des commandes à l'aide de la touche Tab. Il vous suffit de taper les premières lettres d'une applet de commande, puis d'appuyer sur la touche Tab pour permettre la saisie automatique du reste de la commande. Si plusieurs cmdlets commencent par les mêmes lettres, continuez à appuyer sur la touche Tab pour parcourir toutes les cmdlets.

Chaque commande qui apporte une modification dans l'environnement de ligne de commande Exchange Management Shell peut se terminer par le paramètre **-WhatIf**, qui indique à l'applet de commande de simuler les actions applicables à l'objet. À l'aide du paramètre **-WhatIf**, vous pouvez avoir un aperçu des modifications sans les appliquer réellement.

Vous pouvez également utiliser le paramètre **-Confirm** si vous êtes sur le point d'exécuter une commande qui affecte plusieurs objets. Le paramètre **-Confirm** suspend de force le traitement de la cmdlet et demande à l'administrateur de confirmer les actions que la cmdlet va effectuer avant de continuer le traitement.

Si vous pensez que la sortie de votre cmdlet sera trop longue, vous pouvez diriger cette sortie vers un fichier texte. Par exemple, vous pouvez taper **Get-Mailbox | Format-List > file.txt**.

Exemples de commandes de l'environnement de ligne de commande Exchange Management Shell :

- **Enable-Mailbox -Identity Adatum\Bart -Database MailboxDatabase**. Cette commande active la boîte aux lettres d'un utilisateur Active Directory existant (Bart) avec le domaine et l'alias Adatum\Bart en créant une boîte aux lettres dans la base de données de boîtes aux lettres nommée MailboxDatabase.
- **New-MailboxExportRequest -Mailbox Bart -FilePath \\LON-EX1\PSTFileShare\Bart_Mailbox.pst**. Cette commande récupère le contenu de la boîte aux lettres avec l'alias Bart, et stocke le fichier PST dans \\LON-EX1\PSTFileShare\Bart_Mailbox.pst.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- **Get-MailboxStatistics -Database MailboxDatabase**. Cette commande récupère les statistiques de boîte aux lettres pour toutes les boîtes aux lettres figurant dans la base de données de boîtes aux lettres nommée MailboxDatabase.
- **New-MailboxDatabase -Name MailboxDatabase -Server LON-Ex1**. Cette commande crée une base de données de boîtes aux lettres nommée MailboxDatabase sur le serveur LON-EX1.
- **Get-ExchangeServer -Status | Format-List**. Cette commande récupère une liste détaillée de tous les serveurs existants et force un appel à l'actualisation de l'état actuel du serveur. Sans le paramètre Status, certains champs qui changent en temps réel ne sont pas renseignés.
- **New-DynamicDistributionGroup -Name DDG -Alias DDGAlias -OrganizationalUnit OU -IncludedRecipients MailboxUsers**. Cette commande crée un groupe de distribution dynamique basé sur une requête portant le nom DDG, qui se trouve dans l'unité d'organisation et possède l'alias DDGAlias.
- **New-MoveRequest -Identity 'user1'-TargetDatabase Executives**. Cette commande crée une requête de déplacement de la boîte aux lettres associée à l'alias user1 vers la base de données de boîtes aux lettres nommée Executives.

Démonstration : Utilisation des outils d'administration Exchange pour gérer Exchange

Procédure de démonstration

1. Sur LON-EX1, vérifiez les options du Centre d'administration Exchange.
2. Créez la boîte aux lettres de l'utilisateur Aidan.
3. Connectez-vous à Outlook Web App en tant qu'Aidan.
4. Vérifiez les options d'Outlook Web App pour un utilisateur non-administrateur.
5. À partir de l'environnement de ligne de commande Exchange Management Shell, exécutez les cmdlets suivantes :
   - **Get-Command *mailbox***
   - **Get-Mailbox Aidan | Format-List alias,*quota**
   - **Enable-MailContact -Identity "John Woods" -Alias woods -ExternalEmailAddress woods@adatum.com**
   - **Get-MailboxStatistics -Server LON-EX1**
   - **Get-Recipient -RecipientType UserMailbox**
   - **New-MailboxDatabase -Name AdatumExec -Server LON-EX1**

Atelier pratique : Déploiement et gestion d'Exchange Server 2013

Scénario

Vous êtes un administrateur de messagerie pour A. Datum Corporation. Votre organisation se prépare à installer son premier serveur Exchange Server 2013. Votre première tâche consiste à déployer Exchange Server 2013 dans un environnement de test. Avant d'installer Exchange Server 2013 dans l'environnement de test, vous devez d'abord vérifier que les services AD DS sont prêts pour l'installation. Vous devez également vérifier que tous les ordinateurs qui exécuteront Exchange Server 2013 répondent aux conditions préalables à l'installation d'Exchange. Une fois l'environnement préparé, vous déploierez Exchange Server 2013.

Objectifs

- Évaluation de la configuration requise et des conditions préalables pour le déploiement d'Exchange Server 2013.
- Déploiement d'Exchange Server 2013.
- Gestion d'Exchange Server 2013.

Configuration de l'atelier pratique

Durée approximative : **60 minutes**

Ordinateurs virtuels	22341B-LON-DC1-B 22341B-LON-EX1-B
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22341B-LON-DC1-B**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous avec les informations d'identification suivantes :
   a. Nom d'utilisateur : **ADATUM\Administrateur**
   b. Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22341B-LON-EX1-B**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Évaluation de la configuration requise et des conditions préalables pour une installation d'Exchange Server 2013

Scénario

Les administrateurs Active Directory d'A. Datum ont préparé un environnement AD DS de test pour le déploiement d'Exchange Server 2013. L'équipe d'administration de serveur a déployé un serveur Windows Server 2012 que vous pouvez utiliser pour déployer le premier serveur Exchange Server 2013 dans l'organisation test. Vous devez vérifier que l'environnement Active Directory et le serveur répondent à toutes les conditions préalables à l'installation d'Exchange Server 2013.

Les tâches principales de cet exercice sont les suivantes :

1. Évaluer la configuration requise pour Active Directory.
2. Évaluer la configuration requise pour DNS.

▶ Tâche 1 : Évaluer la configuration requise pour Active Directory

- Sur LON-DC1-B, évaluez si la configuration requise pour le contrôleur de domaine est satisfaite :
    - Utilisez Utilisateurs et ordinateurs Active Directory pour évaluer si la configuration requise au niveau fonctionnel de la forêt et du domaine est satisfaite. (Remarque : il doit s'agir au moins de Windows Server 2003).
    - Utilisez Adsiedit.msc pour évaluer si les modifications de schéma Exchange sont appliquées.

▶ Tâche 2 : Évaluer la configuration requise pour DNS

1. Sur LON-EX1-B, assurez-vous que les paramètres DNS sont correctement configurés.
2. Effectuez un test Ping du contrôleur de domaine LON-DC1.adatum.com pour vérifier la connectivité réseau.
3. Démarrez l'utilitaire **Nslookup** à partir de Windows PowerShell.
4. Tapez **set type=all**.
5. Effectuez une recherche nslookup de l'enregistrement SRV **_ldap._tcp.dc._msdcs.adatum.com**.
6. Vérifiez qu'un enregistrement SRV pour lon-dc1.adatum.com est renvoyé.
7. Fermez Windows PowerShell.

Résultats : Après avoir terminé cet exercice, les stagiaires auront évalué la configuration requise pour les services AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Déploiement d'Exchange Server 2013

Scénario

Après avoir évalué la configuration requise pour Exchange Server 2013, vous êtes prêt à commencer le processus de déploiement. Vous devez d'abord préparer les services AD DS, puis effectuer l'installation d'Exchange sur un seul serveur. À des fins d'évaluation, tous les rôles seront installés sur un serveur unique. Pour finir, vous vérifierez si les services et composants Exchange principaux sont correctement installés.

Les tâches principales de cet exercice sont les suivantes :

1. Préparation d'AD DS pour le déploiement d'Exchange Server 2013.
2. Exécuter l'installation d'Exchange Server 2013 sur un serveur unique.
3. Vérifier l'installation d'Exchange Server.

▶ Tâche 1 : Préparation d'AD DS pour le déploiement d'Exchange Server 2013

1. Sur LON-DC1-B, attachez **C:\Programmes\Microsoft Learning\22341B\Drives\ExchangeServer2013CU1.iso** à l'ordinateur virtuel.
2. Sur LON-DC1, ouvrez une fenêtre Windows PowerShell. Basculez vers D:\.
3. Exécutez la commande appropriée pour préparer les services AD DS pour votre installation d'Exchange Server.

```
.\Setup.exe /PrepareAD /IAcceptExchangeServerLicenseTerms /OrganizationName:Adatum
```

4. Patientez jusqu'à la fin du processus.
5. Fermez Windows PowerShell.

▶ Tâche 2 : Exécuter l'installation d'Exchange Server 2013 sur un serveur unique

1. Sur LON-EX1, attachez **C:\Programmes\Microsoft Learning\22341\Drives\ExchangeServer2013CU1.iso** à l'ordinateur virtuel.
2. Installez les composants Windows pour Exchange Server, en tapant :

   Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, puis appuyez sur Entrée. (Si vous ne voulez pas taper cette commande, copiez le contenu du fichier **cmdlet.txt** à partir du lecteur C:\.)

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Une fois les rôles installés, redémarrez le serveur.
4. Connectez-vous à LON-EX1-B en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**, puis démarrez l'installation d'Exchange Server à partir de D:\.
   - Ne recherchez pas les mises à jour.
   - Sélectionnez les options permettant d'installer le **Client Access role** et le **Mailbox role**.
   - Ne désactivez pas la protection contre les programmes malveillants.
   - Assurez-vous que les conditions préalables sont remplies.
   - Installez le serveur Exchange. Attendez que l'installation se termine. Cela peut prendre entre 30 et 40 minutes.
   - Dans la page **Installation terminée**, cliquez sur **finish**.
   - Redémarrez LON-EX1 et ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$word**.

▶ Tâche 3 : Vérifier l'installation d'Exchange Server

1. Sur LON-EX1-B, dans le Gestionnaire de serveur, ouvrez la console Services.
2. Examinez l'état de chaque service Exchange Server. Vérifiez que tous les services qui sont configurés pour démarrer automatiquement sont exécutés.
3. À l'aide de l'Explorateur de fichiers, accédez à **C:\Programmmes\Microsoft\Exchange Server\v15**. Cette liste de dossiers inclut ClientAccess, Mailbox et TransportRoles. Ces trois rôles ont été installés dans le cadre de l'installation par défaut.
4. À l'aide d'Internet Explorer, ouvrez **https://lon-ex1.adatum.com/owa**.
5. Connectez-vous à Outlook Web App en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**. Envoyez un nouveau message à l'**Administrateur**, et assurez-vous que le message a été remis dans la boîte de réception.
6. Fermez Outlook Web App.

Résultats : À la fin de cet exercice, les stagiaires auront déployé Exchange Server 2013.

Exercice 3 : Gestion d'Exchange Server 2013

Scénario

Exchange Server 2013 est déployé dans l'environnement de test et vous souhaitez explorer les outils de gestion Exchange Server 2013. Vous cherchez à découvrir les fonctionnalités du nouveau Centre d'administration Exchange, ainsi que celles d'Outlook Web App et de l'environnement de ligne de commande Exchange Management Shell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Explorer le Centre d'administration Exchange Server 2013.
2. Gérer Exchange Server à l'aide de l'environnement de ligne de commande Exchange Management Shell.
3. Explorer Outlook Web App.

▶ Tâche 1 : Explorer le Centre d'administration Exchange Server 2013

1. Sur LON-EX1-B, ouvrez Internet Explorer.
2. Connectez-vous à **https://lon-ex1.adatum.com/ecp** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Créez une boîte aux lettres pour l'utilisateur existant **Aidan Delaney**.
4. Créez un groupe de distribution ouvert appelé **Adatum News**.
5. Déconnectez-vous du Centre d'administration Exchange.

▶ Tâche 2 : Gérer Exchange Server à l'aide de l'environnement de ligne de commande Exchange Management Shell

- Sur LON-EX1-B, utilisez Exchange Management Shell pour effectuer les tâches suivantes :
  a. Affichez la liste de tous les utilisateurs du domaine Adatum.com.
  b. Activez la boîte aux lettres de l'utilisateur Robert.
  c. Affichez la liste de toutes les boîtes aux lettres dans Adatum.com.
  d. Définissez le quota d'avertissement à 200 Mo, puis configurez le quota d'interdiction d'envoi à 250 Mo pour toutes les boîtes aux lettres.
  e. Activez les boîtes aux lettres pour tous les utilisateurs de l'unité d'organisation IT.

▶ Tâche 3 : Explorer Outlook Web App

1. Sur LON-EX1-B, ouvrez Internet Explorer et connectez-vous à Outlook Web App à l'adresse **https://lon-ex1.adatum.com/owa** en tant qu'**Adatum\Aidan** avec le mot de passe **Pa$$w0rd**.
2. Envoyez un message électronique de test à l'administrateur.
3. Rejoignez le groupe Adatum News.
4. Créez une signature pour Aidan Delaney.
5. Modifiez le thème de l'interface Outlook Web App.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1-B**, puis cliquez sur **Rétablir**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-EX1-B**.

Résultats : À la fin de cet exercice, les stagiaires auront exploré les outils de gestion Exchange.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

- Toujours planifier les ressources du serveur Exchange avant de commencer un processus d'installation.
- Déployer le rôle serveur d'accès au client et le rôle serveur de boîtes aux lettres sur des serveurs distincts.
- Surveiller les services et les journaux Exchange avec un logiciel de surveillance tel que SCOM 2012.
- Apprendre à utiliser l'environnement de ligne de commande Exchange Management Shell.
- Installer les rôles et fonctionnalités Windows Server nécessaires à Exchange Server avant d'installer Exchange pour éviter les redémarrages.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Échec de Setup.exe /PrepareAD	

Questions de contrôle des acquis

Question : Quel est le rôle serveur dans Exchange Server 2013 qui gère le transport des messages ?

Question : Comment les clients Outlook d'un réseau interne peuvent-ils se connecter à Exchange Server 2013 ?

Question : Sur quoi repose le Centre d'administration Exchange ?

Outils

- CAE
- Environnement de ligne de commande Exchange Management Shell

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 2

Planification et configuration de serveurs de boîtes aux lettres

Table des matières :

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

Leçon 1 : Vue d'ensemble du rôle serveur de boîtes aux lettres **2-2**

Leçon 2 : Planification du déploiement du serveur de boîtes aux lettres **2-14**

Leçon 3 : Configuration des serveurs de boîtes aux lettres **2-29**

Atelier pratique : Configuration de serveurs de boîtes aux lettres **2-36**

Contrôle des acquis et éléments à retenir **2-43**

Vue d'ensemble du module

L'élément principal de l'infrastructure de Microsoft® Exchange Server 2013 est le serveur de boîtes aux lettres, qui héberge les bases de données de boîtes aux lettres et les carnets d'adresses, gère le transport et le routage des messages, et fournit des services de messagerie unifiée. Lorsque vous planifiez un déploiement Exchange Server 2013, il est très important de prendre en compte tous les aspects du déploiement qui peuvent affecter la conception du rôle serveur de boîtes aux lettres. Dans ce module, nous parlerons de la planification et de la configuration du rôle serveur de boîtes aux lettres.

Objectifs

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

- décrire le rôle serveur de boîtes aux lettres ;
- planifier un déploiement du rôle serveur de boîtes aux lettres ;
- configurer les serveurs de boîtes aux lettres.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble du rôle serveur de boîtes aux lettres

Le rôle serveur de boîtes aux lettres fournit une solution de stockage pour la plupart des données avec lesquelles Exchange Server fonctionne. Il héberge les boîtes aux lettres des utilisateurs, les dossiers publics, les listes d'adresses et d'autres types de données. Dans Exchange 2013, la plupart des fonctionnalités, telles que le transport de messages et la messagerie unifiée, font partie du rôle serveur de boîtes aux lettres ; par conséquent, il est très important de planifier et déployer correctement ce rôle.

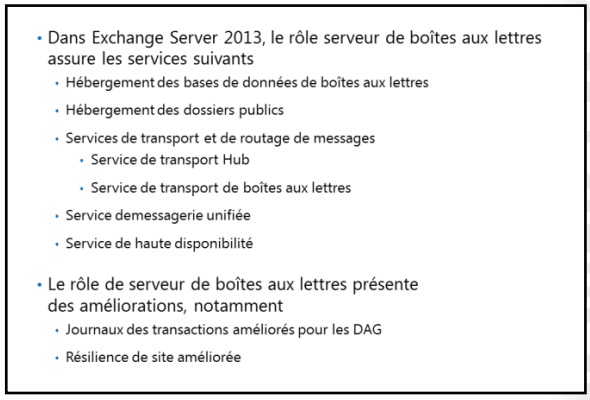
Objectifs de la leçon

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

- décrire le rôle serveur de boîtes aux lettres dans Exchange Server 2013 ;
- décrire comment le rôle serveur de boîtes aux lettres interagit avec les clients et le rôle serveur d'accès au client ;
- décrire la banque de boîte aux lettres dans Exchange Server 2013 ;
- décrire les éléments à prendre en compte pour le journal de base de données ;
- décrire la manière dont la base de données de boîtes aux lettres est mise à jour ;
- décrire les options de stockage pour les bases de données de boîtes aux lettres ;
- expliquer comment importer et exporter des données de la base de données de boîtes aux lettres.

Rôle serveur de boîtes aux lettres dans Exchange Server 2013

Dans Exchange Server 2013, le serveur de boîtes aux lettres fait beaucoup plus qu'il ne le fait dans Microsoft® Exchange Server 2010. Dans Exchange Server 2010, le serveur de boîtes aux lettres héberge les bases de données et propose le stockage des messages électroniques. Dans Exchange Server 2013, le serveur de boîtes aux lettres héberge également les protocoles d'accès au client, les composants du service de transport, les bases de données de boîtes aux lettres et les composants de la messagerie unifiée.



Bien que les clients ne communiquent jamais directement avec le serveur de boîtes aux lettres, ce serveur interagit activement avec les composants des services de domaine Active Directory® (AD DS) et le serveur d'accès au client. Il utilise le protocole LDAP (Lightweight Directory Access Protocol) pour localiser et accéder aux informations sur les destinataires, les serveurs et les informations de configuration de l'organisation qui sont enregistrées dans AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le serveur de boîtes aux lettres participe également aux configurations haute disponibilité via des groupes de disponibilité de base de données (DAG, Database Availability Group). Ce concept offre une haute disponibilité au niveau base de données en implémentant plusieurs copies de la même base de données sur différents serveurs de boîtes aux lettres. Un DAG est un groupe comprenant jusqu'à 16 serveurs de boîtes aux lettres, qui héberge un ensemble de bases de données et assure la récupération automatique au niveau base de données des défaillances qui affectent chaque serveur ou base de données.

La plupart des fonctionnalités de transport de messages internes et de routage, précédemment hébergées sur le serveur de transport Hub, font à présent partie du rôle serveur de boîtes aux lettres. Le service de transport Hub, exécuté par le rôle serveur de boîtes aux lettres, gère tout le flux de courrier interne SMTP (Simple Mail Transfer Protocol) et effectue la catégorisation des messages et l'inspection du contenu. Outre ce service, deux services de transport supplémentaires sont exécutés par le rôle serveur de boîtes aux lettres : le dépôt du transport de boîtes aux lettres et la remise du transport de boîte aux lettres. Ces deux services communiquent avec le service de transport Hub pour envoyer des messages à d'autres serveurs, et également avec la base de données de boîtes aux lettres pour récupérer ou envoyer des données à la base de données.

Le rôle serveur de messagerie unifiée, qui était précédemment un rôle serveur distinct, est maintenant également intégré au rôle serveur de boîtes aux lettres.

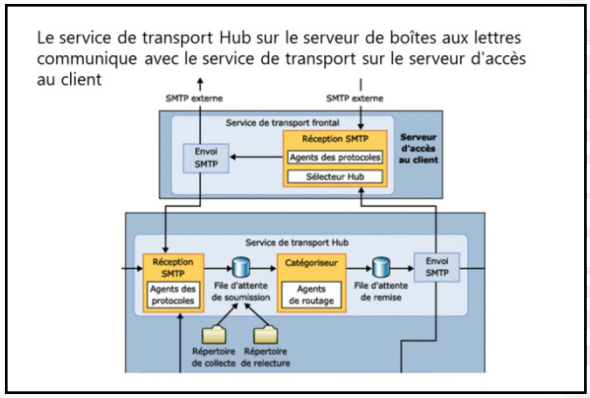
 **Remarque :** Le rôle serveur de boîtes aux lettres dans Exchange Server 2013 héberge également les boîtes aux lettres des dossiers publics. Contrairement à Exchange Server 2010, les dossiers publics n'utilisent pas de bases de données distinctes ou un mécanisme de réplication distinct. Pour plus d'informations sur les dossiers publics dans Exchange Server 2013, voir le module 3.

Le rôle serveur de boîtes aux lettres dans Exchange Server 2013 présente les nouvelles caractéristiques suivantes :

- Dans une évolution du DAG Exchange 2010, le code du journal des transactions a été refactorisé pour permettre un basculement rapide, avec des points de contrôle approfondis sur les copies de bases de données passives.
- Les serveurs peuvent se trouver à des emplacements divers afin d'assurer une résilience améliorée du site.
- Exchange Server 2013 héberge désormais certains composants d'accès au client, notamment les composants de transport et les composants de messagerie unifiée.
- La banque d'informations Exchange a été ré-écrite en code managé afin d'améliorer les performances en termes de réduction et de fiabilité des E/S supplémentaires.
- Chaque base de données Exchange Server 2013 s'exécute désormais sous son propre processus.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Interaction du rôle serveur de boîtes aux lettres avec les clients et le serveur d'accès au client



Outre sa communication avec AD DS, le rôle serveur de boîtes aux lettres communique de manière intensive avec le serveur d'accès au client. Cette communication utilise toujours les mêmes chemins d'accès, même lorsque le rôle serveur d'accès au client est installé sur le même serveur que le rôle serveur de boîtes aux lettres.

Étant donné que les clients ne communiquent jamais directement avec le serveur de boîtes aux lettres, le serveur d'accès au client accepte les demandes des clients et les envoie au serveur de boîtes aux lettres. Le service de transport frontal, qui s'exécute sur le serveur d'accès au client, accepte et envoie des messages à partir d'Internet, et les transfère ensuite au service de transport Hub qui s'exécute sur le serveur de boîtes aux lettres.

Le serveur d'accès au client renvoie également les données (le contenu de la boîte aux lettres du client) du serveur de boîtes aux lettres aux clients. En outre, le serveur d'accès au client utilise le partage de fichiers NETBIOS pour accéder aux données du carnet d'adresses en mode hors connexion (OAB, Offline Address Book) à partir du rôle serveur de boîtes aux lettres. Ces données sont ensuite envoyées aux clients via le répertoire virtuel OAB sur le serveur d'accès au client. Le serveur d'accès au client envoie également des messages, des données de disponibilité et des paramètres de profil de client entre le serveur du client et le serveur de boîtes aux lettres.

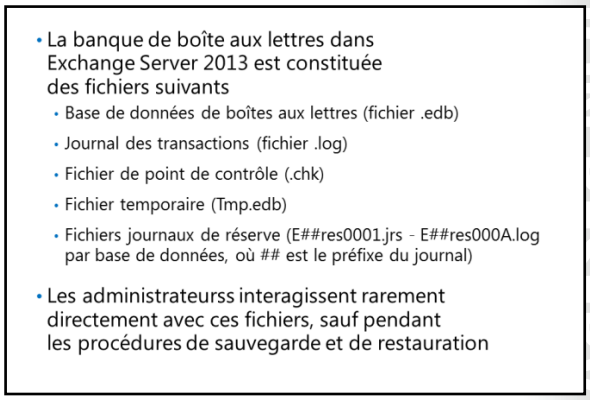
Dans les versions précédentes d'Exchange Server, telles que Microsoft® Exchange Server 2007 et Exchange Server 2010, les clients internes communiquaient directement via l'interface MAPI (Messaging Application Program Interface) avec le rôle serveur de boîtes aux lettres dans certains scénarios. Par exemple, lorsque le client accédait aux dossiers publics dans Exchange Server 2010, il communiquait directement avec le rôle serveur de boîtes aux lettres. Dans Exchange Server 2007, pour tous les scénarios, les clients internes communiquaient directement avec le rôle serveur de boîtes aux lettres à l'aide de l'interface MAPI.

Dans Exchange Server 2013, les clients ne communiquent plus directement avec le rôle serveur de boîtes aux lettres ; les communications client internes et externes sont transmises par proxy via le serveur d'accès au client. Le serveur d'accès au client utilise le protocole LAPD ou l'interface NSPI (Name Service Provider Interface) pour contacter le serveur Active Directory et récupérer les informations Active Directory de l'utilisateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Banque de boîtes aux lettres dans Exchange Server 2013

Dans Exchange Server 2013, le composant principal de la banque de boîte aux lettres est la base de données de boîtes aux lettres. Contrairement aux versions précédentes d'Exchange Server, dans lesquelles les bases de données des dossiers publics étaient également présentes, Exchange Server 2013 fonctionne uniquement avec les bases de données de boîtes aux lettres.



Les bases de données de boîtes aux lettres contiennent des données, des définitions de données, des index, des sommes de contrôle, des indicateurs, et d'autres informations qui constituent les boîtes aux lettres dans Exchange Server 2013. Les bases de données de boîtes aux lettres contiennent des données propres à chaque utilisateur, ainsi que les dossiers de boîte aux lettres générés lors de la création d'une boîte aux lettres pour cet utilisateur. La base de données de boîtes aux lettres peut être hébergée sur un seul serveur, ou elle peut être répartie sur plusieurs serveurs de boîtes aux lettres si des DAG sont déployés.

La base de données de boîtes aux lettres est stockée dans un fichier de base de données, également appelé fichier (.edb) de base de données Exchange. Toutefois, ce n'est pas le seul fichier associé à la base de données de boîtes aux lettres. Exchange Server 2013 utilise un groupe de fichiers de données pour héberger et gérer la base de données de boîtes aux lettres.

Il s'agit des fichiers suivants :

- *Base de données de boîtes aux lettres (fichier .edb)* Il s'agit du référentiel principal pour les données de boîtes aux lettres. Ce fichier est directement accessible via le moteur de stockage extensible (ESE, Extensible Storage Engine). Il a une structure d'arbre B (B-tree) qui favorise un accès rapide et permet aux utilisateurs d'accéder aux données sur n'importe quelle page en un seul cycle d'entrée-sortie.
- *Journal des transactions (fichier .log).* Chaque opération qui doit être effectuée sur une base de données, tel que l'envoi ou la réception d'un message, est stockée dans le fichier journal des transactions. Ces opérations sont appelées transactions. Les opérations qui sont enregistrées dans le journal des transactions sont écrites ultérieurement dans la base de données elle-même (dans un fichier .edb). Jusqu'à ce que la transaction soit enregistrée dans la base de données de boîtes aux lettres, ces données existent uniquement dans la mémoire RAM et dans les journaux des transactions. Toutes les transactions, finalisées ou non finalisées, sont enregistrées afin d'assurer l'intégrité des données en cas d'interruption du service. Chaque base de données possède son propre ensemble de journaux des transactions.

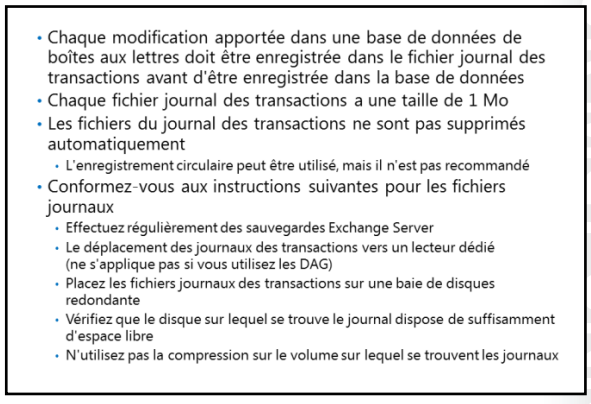
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Fichier de point de contrôle (.chk).* Les fichiers de point de contrôle stockent les données qui indiquent qu'une transaction a été correctement enregistrée dans la base de données. L'objet du fichier de point de contrôle est d'aider l'ESE à relire les fichiers journaux d'une base de données incohérente en cas de récupération de base de données. Grâce aux informations du fichier de point de récupération, l'ESE commencera par la transaction qui se trouve dans le fichier journal, mais n'est pas encore écrite dans le fichier de point de contrôle. Le préfixe de journal de chaque base de données détermine son nom de fichier de point de contrôle. Par exemple, le nom de fichier de point de contrôle pour une base de données avec le préfixe E00 sera E00.chk. La taille de ce fichier de point de contrôle, de plusieurs kilo-octets, n'augmente pas.
- *Fichier temporaire (Tmp.edb).* Il s'agit d'un emplacement temporaire destiné au traitement des transactions. Le fichier Tmp.edb contient des informations temporaires qui sont supprimées lorsque toutes les banques du groupe de stockage sont démontées ou que le service Banque d'informations Exchange est arrêté. La taille de ce fichier ne dépasse pas 1 Mo.
- *Fichiers journaux de réserve (E##res0001.jrs - E##res000A.log par base de données, où ## est le préfixe du journal).* Ces fichiers permettent de réserver de l'espace pour des fichiers journaux supplémentaires si le disque qui stocke les fichiers journaux est plein. Exchange Server 2013 utilise ces fichiers uniquement comme stockage d'urgence lorsque le disque est plein et qu'aucune nouvelle transaction ne peut être écrite sur le disque. Lorsque Exchange Server 2013 manque d'espace disque, il écrit la transaction actuelle sur le disque, en utilisant l'espace réservé par les 10 journaux des transactions de réservation, puis démonte la base de données. Les journaux des transactions réservés permettent de limiter au maximum la perte des données en transit vers la base de données. La taille de chaque journal des transactions réservé est toujours de 1 Mo.

Bien qu'il soit important de comprendre l'objet de chaque fichier de base de données de boîtes aux lettres, vous serez rarement amené à interagir directement avec ces fichiers. Exchange Server les gère automatiquement, aussi n'ont-ils pas besoin de l'intervention de l'administrateur, sauf en cas de sauvegarde et de restauration de base de données.

Éléments à prendre en compte en matière de fichiers journaux de base de données

Chaque modification effectuée sur une base de données de boîtes aux lettres Exchange Server doit être enregistrée dans un fichier journal des transactions préalablement à la modification dans la base de données. Une fois chaque transaction enregistrée dans le fichier journal des transactions, elle peut être écrite dans le fichier .edb. Pour améliorer les performances, les utilisateurs peuvent généralement accéder aux modifications effectuées sur la base de données juste après leur enregistrement dans le fichier journal des transactions.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exchange Server met également des transactions en cache en mémoire RAM, pour des raisons de redondance et de performance. Si la base de données s'arrête, ou si le serveur tombe en panne ou rencontre toute autre défaillance système, Exchange Server analyse les fichiers journaux, puis reconstruit et applique les modifications n'ayant pas encore été écrites dans la base de données. Ce processus est appelé relecture de fichiers journaux.

Le journal des transactions n'est pas constitué d'un seul fichier mais d'une série de fichiers journaux. La taille de chaque fichier journal des transactions est exactement de 1 024 Ko. Lorsqu'un fichier journal des transactions est plein, l'ESE le ferme, le renomme, puis ouvre un nouveau fichier journal des transactions.

La syntaxe de dénomination du fichier journal des transactions est Enn0000000x.log, où nn fait référence à un nombre à deux chiffres appelé préfixe de base de nom ou de journal, et où x est le numéro séquentiel du fichier journal. Il est important de savoir que les fichiers journaux sont numérotés dans un système hexadécimal et non dans un système décimal. Par exemple, le fichier journal venant après E0000000009.log n'est pas E0000000010.log mais E000000000A.log.

Les fichiers du journal des transactions ne sont pas supprimés automatiquement. En général, lorsqu'une base de données est sauvegardée, le logiciel de sauvegarde supprime les fichiers du journal des transactions. Dans la mesure où une base de données de boîtes aux lettres ne peut pas être sauvegardée de la même manière que d'autres fichiers, il est très important de disposer d'un logiciel de sauvegarde pour Exchange qui gère correctement les fichiers du journal des transactions lors des opérations de sauvegarde et de restauration. Si les fichiers du journal des transactions ne sont pas supprimés régulièrement, ils peuvent remplir l'espace disque, ce qui peut entraîner l'arrêt des services Exchange. Nous ne recommandons pas de supprimer manuellement les fichiers du journal des transactions, car cette approche peut interférer avec votre procédure de sauvegarde normale.

Vous pouvez configurer Exchange Server de manière à ce qu'il effectue un enregistrement circulaire. Si l'option d'enregistrement circulaire est activée, les fichiers du journal des transactions seront remplacés une fois que les transactions du fichier journal auront été enregistrées dans la base de données de boîtes aux lettres. Toutefois, cette approche n'est pas recommandée dans un environnement de production, car elle affecte la capacité de sauvegarde et de restauration de la base de données de boîtes aux lettres. Par exemple, si l'enregistrement circulaire est activé, vous ne pouvez récupérer des données que jusqu'au moment où vous avez effectué la dernière sauvegarde complète de votre base de données. Si vous n'utilisez pas l'enregistrement circulaire, vous avez la possibilité d'utiliser les sauvegardes incrémentielles, de même que vous pouvez restaurer la base de données à partir de la sauvegarde incrémentielle. Par défaut, l'enregistrement circulaire est désactivé.

Pour gérer correctement les journaux des transactions ainsi que la base de données de boîtes aux lettres, nous recommandons de procéder comme suit :

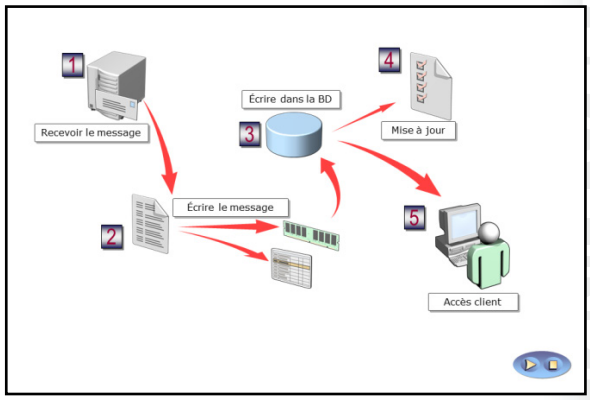
- Effectuez régulièrement des sauvegardes Exchange Server avec un logiciel de sauvegarde pour Exchange.
- Déplacez les journaux des transactions vers un lecteur dédié acceptant une charge d'écriture importante.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Placez les fichiers du journal des transactions sur une baie de disques redondante, à l'aide de la technologie RAID (Redundant Array of Independent Disks). Nous recommandons d'utiliser un volume RAID 1. Cependant, si vous protégez vos bases de données de boîtes aux lettres avec un DAG, il peut être superflu d'utiliser un espace de stockage dédié pour les fichiers du journal des transactions. Cette option est décrite plus loin dans ce module.
- Vérifiez que le volume qui héberge les fichiers du journal des transactions dispose de suffisamment d'espace disque libre pour stocker tous les fichiers créés entre deux cycles de sauvegarde.
- N'utilisez pas la compression sur les lecteurs qui stockent les fichiers du journal des transactions.
- N'utilisez pas l'enregistrement circulaire, sauf dans un environnement de test.

Mise à jour des bases de données de boîtes aux lettres

Bien que la modification de base de données soit un processus automatisé, l'administrateur ou l'utilisateur final ne le voit pas directement. Il est important que vous compreniez comment la base de données est modifiée lors d'opérations classiques.



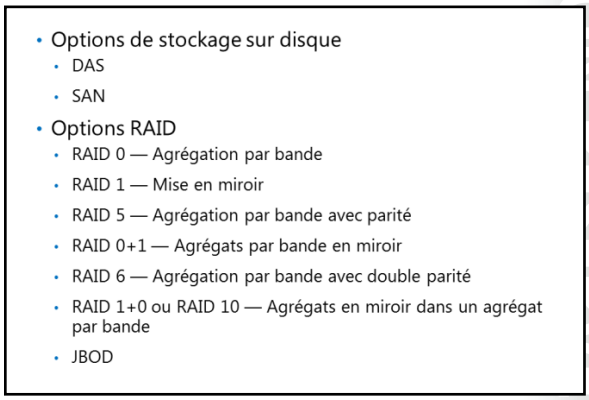
Le processus suivant a lieu lorsqu'un serveur de boîtes aux lettres reçoit un message :

1. Le serveur de boîtes aux lettres reçoit le message. Cela se produit lorsque le service de transport Hub sur le serveur de boîtes aux lettres accepte le message du service de transport frontal qui s'exécute sur le serveur d'accès au client. Une fois le message accepté par le service de transport Hub, il est transmis au service de transport de boîtes aux lettres.
2. Avant que le message ne soit écrit dans les bases de données, le serveur de boîtes aux lettres écrit simultanément le message dans le journal des transactions actuel et dans le cache mémoire.
3. Le serveur de boîtes aux lettres écrit la transaction du cache mémoire dans la base de données appropriée.
4. Le serveur de boîtes aux lettres met à jour le fichier de point de contrôle pour indiquer que la transaction a été enregistrée dans la base de données.
5. Les clients peuvent accéder au message et le lire dans la base de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options de stockage pour le rôle serveur de boîtes aux lettres Exchange Server 2013



Exchange Server 2013 prend en charge différentes technologies de matériel pour le stockage sur disque, notamment la technologie SATA (Serial Advanced Technology Attachment), le disque SSD (Solid-State Drive) et l'interface Serial Attached SCSI, appelée SAS (Serial Attached SCSI) ou pilotes iSCSI. Lors de la sélection de la solution de stockage à utiliser, l'objectif est de s'assurer que le stockage fournira les performances exigées par votre environnement. Dans Exchange Server 2013, les E/S de disque sont encore réduites par rapport aux versions précédentes d'Exchange Server. Cela vous permet d'utiliser des disques et des systèmes de stockage moins rapides et moins coûteux, sans diminution importante des performances. Lorsque vous choisissez une technologie de stockage pour Exchange Server, les choix les plus courants sont DAS, SAN ou RAID.

DAS

Le stockage DAS (Direct Attached Storage) correspond à un système de disque physiquement connecté à votre serveur. Il comprend les disques durs au sein du serveur ou ceux connectés via un boîtier externe. Certains boîtiers externes incluent la technologie RAID basée sur le matériel. Par exemple, des boîtiers de disques externes peuvent combiner plusieurs disques d'un agrégat RAID 5 qui apparaissent au serveur comme un grand disque unique.

En général, le stockage DAS offre de bonnes performances, mais il fournit une évolutivité limitée en raison de la taille physique de l'unité. Vous devez gérer le stockage DAS par serveur. Exchange Server 2013 fonctionne bien avec les caractéristiques d'évolutivité et de performance du stockage DAS.

Cette technologie présente les avantages suivants :

- *Solution Exchange Server à coût réduit*. Le stockage à connexion directe offre généralement un coût d'achat significativement inférieur à celui d'autres technologies.
- *Facilité d'implémentation*. Le stockage à connexion directe est généralement plus simple à gérer et n'exige qu'une formation minimale.
- *Points de défaillance distribués*. Chaque serveur Exchange dispose de systèmes de disques distincts. La défaillance d'un seul système n'affecte donc pas la totalité du système de messagerie Exchange dans la mesure où vous configurez vos serveurs Exchange pour la haute disponibilité.

SAN

Un réseau SAN (Storage Area Network) est un réseau permettant aux serveurs d'accéder aux périphériques de stockage. Il fournit des fonctionnalités avancées en matière de gestion et de stockage, telles que des captures instantanées des données et des performances élevées. Les réseaux SAN utilisent une commutation Fibre Channel ou iSCSI (Internet SCSI) qui assure une connectivité rapide et fiable entre le stockage et les applications. La commutation Fibre Channel ou iSCSI permet à un grand nombre de serveurs de se connecter à un seul réseau SAN.

Fibre Channel offre une architecture SAN standard sur un câblage à fibre optique. La plupart des réseaux SAN l'utilisent, car Fibre Channel est conçue spécifiquement pour ces réseaux et il s'agit de l'architecture la plus rapide disponible.

Les réseaux SAN sont complexes, et des connaissances spécialisées sont indispensables pour les concevoir, les faire fonctionner et les mettre à jour. La plupart des réseaux SAN sont également plus coûteux que des options DAS.

Les réseaux SAN offrent les avantages suivants :

- Un réseau SAN inclut généralement un important cache mémoire qui empêche tout goulet d'étranglement au niveau de l'accès au disque. Étant donné que les besoins d'E/S sont réduits dans Exchange Server 2013, un réseau SAN basé sur iSCSI répondra probablement à vos besoins lors de déploiements de petite et de moyenne taille. Toutefois, vous devez tester entièrement toutes les configurations matérielles avant le déploiement pour vérifier qu'elles répondent aux caractéristiques de performance requises de votre organisation.
- Solutions de stockage très évolutives. Les systèmes de messagerie se développent sans cesse et les besoins de stockage sont de plus en plus importants. Au fur et à mesure de la croissance de vos besoins, un réseau SAN vous permet d'ajouter des disques à votre stockage. La plupart des réseaux SAN intègrent une virtualisation du stockage, ce qui vous permet d'ajouter des disques et d'affecter les nouveaux disques à votre serveur Exchange Server.
- Association de plusieurs serveurs à un réseau SAN unique. Si vous utilisez un réseau SAN, vous pouvez connecter plusieurs ordinateurs exécutant Exchange Server et répartir le stockage entre ces ordinateurs.
- Sauvegarde, récupération et disponibilité améliorées. Les réseaux SAN utilisent la mise en miroir de volumes et les sauvegardes de captures instantanées. Étant donné que ces réseaux autorisent plusieurs connexions, vous pouvez y connecter des périphériques de sauvegarde très performants. Les réseaux SAN vous permettent également de définir différents niveaux RAID pour des partitions de stockage distinctes.

Pour implémenter un réseau SAN de manière économique, il peut être intéressant de prendre en compte la commutation iSCSI. Un réseau iSCSI encapsule les commandes SCSI dans des paquets TCP/IP sur des commutateurs et un câblage Ethernet standard. Vous ne devez implémenter cette technologie que sur des réseaux de stockage dédiés de 1 gigabit par seconde (Gbps) ou plus.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

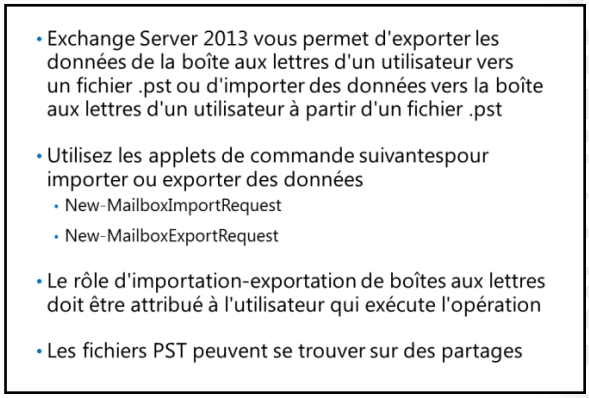
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

RAID

Pour permettre la redondance sur n'importe quelle option de stockage, vous devez utiliser la technologie RAID. La technologie RAID permet de fournir de meilleures performances disque ou la tolérance de panne. Les options RAID les plus courantes sont les suivantes :

- *RAID 0 (agrégation par bande)*. Augmente les performances de lecture et d'écriture en répartissant les données entre plusieurs disques. Toutefois, cette option n'offre aucune tolérance de panne. Les performances augmentent lorsque vous ajoutez des disques supplémentaires. Vous ajoutez la tolérance de panne en utilisant plusieurs copies des bases de données sur des agrégats RAID distincts.
- *RAID 1 (mise en miroir*). Augmente la tolérance de panne en plaçant des copies redondantes de données sur deux disques. Les performances de lecture sont plus rapides qu'avec un seul disque, mais les performances d'écriture sont plus lentes qu'avec RAID 0. La moitié des disques est utilisée pour la redondance de données.
- *RAID 5 (agrégation par bande avec parité)*. Augmente la tolérance de panne en répartissant les données et les informations de parité entre trois disques ou plus. Si un disque tombe en panne, les données manquantes sont calculées sur la base des disques restants. Les performances de lecture et d'écriture pour RAID 5 sont plus lentes que pour RAID 0. Au maximum, seul un tiers des disques est utilisé pour stocker les informations de parité.
- *RAID 0+1 (agrégats par bande en miroir)*. Augmente la tolérance de panne via la mise en miroir de deux agrégats RAID 0. Fournit des performances de lecture et d'écriture très rapides avec une excellente tolérance de panne.
- *RAID 6 (agrégation par bande avec double parité)*. Augmente la tolérance de panne en répartissant les données et les informations de parité entre quatre disques ou plus. Si un ou deux disques au maximum tombent en panne, RAID 6 calcule les données manquantes sur la base des données et des informations de parité stockées sur les disques restants. Les performances de lecture et d'écriture pour RAID 6 sont généralement plus lentes qu'avec RAID 0 et RAID 6 n'a pas de pénalité de lecture. Le principal avantage de RAID 6 consiste en sa capacité à régénérer les données manquantes si vous avez deux défaillances par groupe RAID et à réduire l'impact de la reconstruction de l'agrégat RAID lorsqu'un disque tombe en panne.
- *RAID 1+0 ou RAID 10 (agrégats en miroir dans un agrégat par bande)*. Fournit une tolérance de panne et des performances améliorées, mais augmente la complexité. La différence entre RAID 0+1 et RAID 1+0 est que RAID 1+0 crée un agrégat par bande à partir d'une série de disques en miroir. Dans le cas d'une panne de disque, RAID 1+0 est plus efficace et a plus de tolérance de panne que RAID 0+1.
- *JBOD (Just a Bunch Of Disks)*. JBOD est un ensemble de disques qui n'ont pas de redondance ou de tolérance de panne. Les solutions JBOD sont habituellement moins coûteuses que les solutions qui utilisent RAID. JBOD ajoute une tolérance de panne en utilisant plusieurs copies des bases de données sur des disques distincts, dont vous pouvez vous servir lorsque vous protégez vos bases de données à l'aide de DAG.

Importation et exportation des données d'une base de données de boîtes aux lettres



Dans certains scénarios, vous pouvez souhaiter exporter des données de la base de données utilisateur ou importer des données vers la base de données utilisateur. Par exemple, pour des raisons juridiques ou de conformité, vous pouvez devoir exporter le contenu de la boîte aux lettres d'un utilisateur spécifique vers un fichier de stockage personnel (.pst). À d'autres fins, vous pouvez souhaiter effectuer une capture instantanée d'une boîte aux lettres spécifique.

Dans un autre scénario encore, vous pouvez vouloir importer des données à partir d'un fichier .pst d'une application héritée vers la boîte aux lettres d'un utilisateur sur Exchange Server. Par exemple, si un utilisateur utilisait une application Windows Mail, toutes les données de l'utilisateur étaient stockées dans un fichier .pst. Il est courant d'importer des données à partir du fichier .pst de l'utilisateur vers la nouvelle boîte aux lettres de l'utilisateur sur Exchange Server, ou vers la boîte aux lettres d'archivage de l'utilisateur.

Dans Exchange Server 2013, vous pouvez utiliser les applets de commande **New-MailboxImportRequest** ou **New-MailboxExportRequest** pour importer ou exporter des données de la boîte aux lettres de l'utilisateur. Les demandes d'importation ou d'exportation de la boîte aux lettres doivent être exécutées à partir de l'environnement de ligne de commande Exchange Management Shell. Une fois que vous avez exécuté une de ces applets de commande, le processus est achevé de manière asynchrone par le service de réplication de boîte aux lettres Microsoft Exchange. Ce service tire profit des infrastructures de mise en file d'attente et de limitation des données pour optimiser les performances d'Exchange lors des opérations d'importation ou d'exportation.

Remarque : Pour utiliser les applets de commande **New-MailboxImportRequest** ou **New-MailboxExportRequest**, le rôle d'importation-exportation de boîtes aux lettres doit vous avoir été attribué. Par défaut, ce rôle n'est pas attribué.

Exchange Server 2013 comprend un fournisseur de fichiers de dossiers personnels (.pst), ce qui lui permet de lire et d'écrire les fichiers .pst en mode natif. Les fichiers .pst peuvent être stockés localement ou résider sur un dossier partagé. Toutefois, si vous utilisez des dossiers partagés comme emplacement .pst, vous devez vous assurer d'accorder les autorisations de lecture/écriture au groupe Sous-système approuvé Exchange pour le dossier partagé spécifique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exchange Server 2013 prend uniquement en charge les fichiers Unicode créés par Office® Outlook 2007, Outlook 2010 et versions plus récentes. Les données d'un fichier .pst peuvent être importées vers la boîte aux lettres d'un utilisateur ou vers une archive en ligne si elle est activée pour la boîte aux lettres d'un utilisateur. En outre, Exchange Server 2013 peut importer ou exporter plusieurs fichiers .pst en même temps, ce qui peut accélérer le processus. Toutefois, le processus d'importation ou d'exportation peut prendre plusieurs heures, selon la taille du fichier et la bande passante réseau.

 **Remarque :** La taille maximale prise en charge pour un fichier .pst est de 50 gigaoctets (Go). Si vous souhaitez exporter une boîte aux lettres faisant plus de 50 Go, créez plusieurs fichiers .pst. Vous pouvez utiliser des filtres pour spécifier les dossiers sélectionnés pour l'exportation au lieu de spécifier l'intégralité de la boîte aux lettres. Vous pouvez également inclure ou exclure des dossiers spécifiques à l'aide des paramètres IncludeFolders ou ExcludeFolders.

Lorsque vous importez des données à partir d'un fichier .pst, vous devez vérifier que la boîte aux lettres existe avant de commencer le processus d'importation. Vous pouvez importer des données dans un compte utilisateur différent de celui à partir duquel il a été exporté.

Démonstration : Importer des données dans la boîte aux lettres d'un utilisateur

Procédure de démonstration

1. Ouvrez une session sur Outlook Web App (OWA) en tant qu'**Adatum\Aidan**.
2. Assurez-vous que la boîte aux lettres d'archivage sur place est vide. Déconnectez-vous d'Outlook Web App.
3. Ouvrez l'environnement de ligne de commande Exchange Management Shell sur LON-MBX1.
4. Tapez **New-ManagementRoleAssignment –Role "Mailbox Import Export" –User Administrator**.
5. Redémarrez l'environnement de ligne de commande Exchange Management Shell.
6. Tapez le texte suivant : **New-MailboxImportRequest -Mailbox Aidan -IsArchive -FilePath \\LON-DC1\MailboxExport\backup.pst**.
7. Une fois l'importation terminée, sur LON-CAS1, connectez-vous à Outlook Web App en tant qu'**Adatum\Aidan** et vérifiez que le contenu a été importé dans l'archive personnelle.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Planification du déploiement du serveur de boîtes aux lettres

La planification du déploiement du rôle serveur de boîtes aux lettres constitue une partie essentielle de la planification d'une infrastructure Exchange Server. Avant de déployer un serveur de boîtes aux lettres Exchange Server 2013, vous devez planifier le matériel et le stockage de manière à répondre aux besoins de votre environnement. Vous devez également planifier et concevoir l'organisation de la base de données de boîtes aux lettres, ainsi que les options de haute disponibilité. Certains éléments particuliers doivent être pris en compte si vous décidez de virtualiser vos serveurs de boîtes aux lettres. Dans cette leçon, nous allons discuter du déploiement de serveurs de boîtes aux lettres.

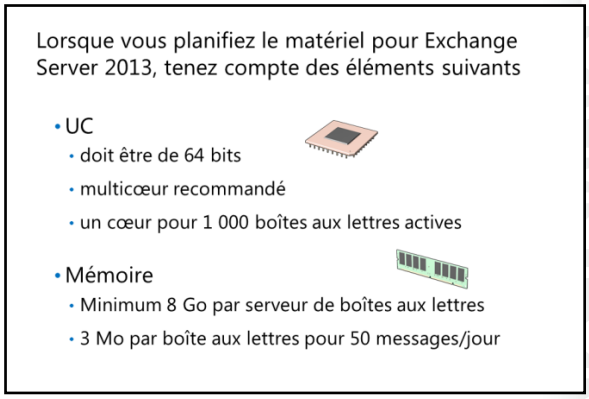
Objectifs de la leçon

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

- planifier le matériel et le stockage pour les serveurs de boîtes aux lettres ;
- concevoir des bases de données de boîtes aux lettres ;
- planifier la haute disponibilité pour les serveurs de boîtes aux lettres ;
- décrire les éléments à prendre en compte pour la virtualisation des serveurs de boîte aux lettres ;
- décrire les éléments à prendre en compte pour planifier les bases de données de boîtes aux lettres ;
- décrire l'outil Exchange Mailbox Server Role Requirements Calculator ;
- utiliser Exchange Mailbox Server Role Requirements Calculator ;
- vérifier les performances du rôle serveur de boîtes aux lettres.

Planification du matériel pour le rôle serveur de boîtes aux lettres

Contrairement au serveur d'accès au client, dont l'encombrement matériel est réduit, le serveur de boîtes aux lettres peut être assez exigeant en termes de conditions matérielles dans les scénarios dans lesquels il héberge un grand nombre de boîtes aux lettres. D'autre part, vous n'aurez peut-être pas besoin de matériel très puissant si vous implémentez Exchange Server dans de petites ou moyennes entreprises. Dans l'un ou l'autre cas, il est très important de planifier correctement les conditions matérielles requises pour le rôle serveur de boîtes aux lettres Exchange.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration requise pour le processeur

Exchange Serveur 2013 requiert un processeur 64 bits et un système d'exploitation 64 bits. Exchange Serveur 2013 prend en charge deux architectures de processeur spécifiques : AMD64 et la technologie Intel EM64T (Extended Memory 64 Technology). Les processeurs Itanium ne sont pas pris en charge.

Exchange Server 2013 peut tirer parti des processeurs multicœurs, qui peuvent traiter plusieurs tâches en même temps. Un processeur de serveur traditionnel possède au moins quatre cœurs.

Le nombre de cœurs de processeur requis pour un serveur de boîtes aux lettres varie selon le nombre de boîtes aux lettres et l'intensité de leur utilisation. Dans le cas d'une utilisation moyenne, un seul cœur de processeur peut prendre en charge environ 1 000 boîtes aux lettres actives. L'utilisation moyenne est définie comme étant celle d'un utilisateur qui envoie 10 messages par jour et reçoit 40 messages par jour. Si le processeur prend en charge le hyperthreading, nous vous recommandons de le désactiver. Le hyperthreading pose des problèmes de planification de la capacité et offre peu d'amélioration des performances.

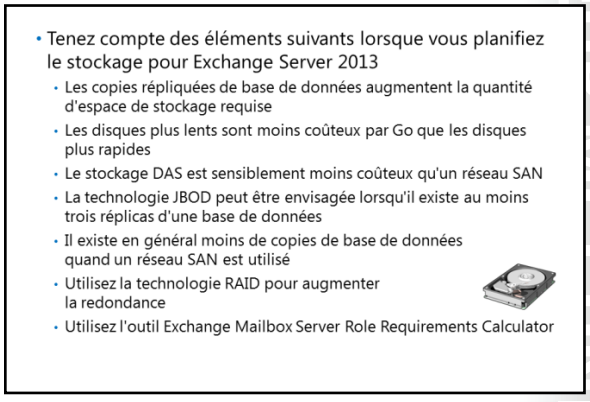
Mémoire requise

La quantité de mémoire requise pour Exchange Server 2013 varie en fonction du nombre de boîtes aux lettres et de l'intensité de leur utilisation. La quantité de RAM minimale recommandée pour un serveur de boîtes aux lettres est de 8 Go. Un serveur qui combine plusieurs rôles doit disposer d'un minimum de 8 Go de RAM.

Lors du calcul de la mémoire requise pour votre serveur de boîtes aux lettres, prenez le minimum requis, puis ajoutez de la mémoire supplémentaire pour chaque utilisateur en fonction du volume de sa messagerie. Pour chaque ensemble de 50 messages envoyés ou reçus par jour, vous devez allouer 3 mégaoctets (Mo) par utilisateur. Par exemple, si l'utilisateur moyen de votre organisation envoie et reçoit 100 messages par jour, vous devez allouer 6 Mo par utilisateur, en plus de la quantité de RAM minimale requise pour la configuration de votre serveur de boîtes aux lettres.

Planification du stockage pour le rôle serveur de boîtes aux lettres

Pour de nombreux utilisateurs, l'accès à la messagerie électronique est indispensable pour leur travail, car ils l'utilisent pour communiquer en interne avec des collègues et en externe avec des clients et des partenaires. La quantité de données conservées dans les boîtes aux lettres augmente sans cesse et toutes ces données doivent pouvoir faire l'objet d'une recherche.



Les disques durs de nouvelles générations deviennent plus volumineux, mais les vitesses de rotation et les temps d'accès ne s'améliorent pas. Les taux de lecture séquentielle augmentent en raison d'une densité de données supérieure, mais les taux de lecture en accès aléatoire restent les mêmes. Exchange Server 2013 tire profit de la taille croissante des disques pour que vous puissiez offrir des boîtes aux lettres plus grandes aux utilisateurs sans augmentation des coûts ou diminution des performances.

Grâce aux améliorations d'E/S dans Exchange Server 2013, vous pouvez utiliser des disques plus volumineux et moins coûteux dans de nombreux scénarios. Les E/S de disque sont liées au nombre de boîtes aux lettres stockées sur un disque plutôt qu'au volume des données de boîte aux lettres stockées sur le disque. Les boîtes aux lettres volumineuses réduisent les besoins d'E/S de disque pour un serveur de boîtes aux lettres car elles réduisent le nombre de boîtes aux lettres stockées sur un disque. Un nombre réduit de boîtes aux lettres sur un disque se traduit par un nombre inférieur des E/S de disque.

En raison du nombre inférieur des E/S de disque, vous pouvez envisager d'utiliser des disques volumineux à 7 200 tours/minute plutôt que des disques plus petits et plus rapides à 15 000 tours/minute. Un disque classique à 7 200 tours/minute stocke entre 1 et 3 téraoctets. Un disque classique à 15 000 tours/minute stocke moins de 1 téraoctet. Les disques à 7 200 tours/minute sont sensiblement moins chers par Go.

Dans Exchange Server 2013, vous pouvez stocker les archives personnelles et les boîtes aux lettres principales dans des bases de données distinctes. Cela est utile si vous souhaitez utiliser des stratégies de sauvegarde différentes pour les archives personnelles et pour les boîtes aux lettres principales. Toutefois, il peut en résulter un déséquilibre des E/S de disque. Les disques qui stockent les bases de données avec les boîtes aux lettres principales subissent un nombre d'E/S relativement élevé, tandis que les disques qui stockent les bases de données avec les archives personnelles subissent un nombre d'E/S relativement bas. Le fait de conserver des boîtes aux lettres principales plus petites vous permet de placer un nombre plus élevé de boîtes aux lettres sur le même jeu de disques, ce qui peut également augmenter les E/S de disque. Le fait de conserver une archive personnelle dans la même base de données que la boîte aux lettres principale ne modifie pas le nombre des E/S de disque dans la mesure où vous disposez uniquement de grandes boîtes aux lettres.

En raison des améliorations de stockage introduites dans Exchange Server 2010, et qui sont également prises en charge dans Exchange Serveur 2013, vous pouvez envisager d'utiliser des types de stockage sur disque plus lents et moins coûteux, que vous n'auriez pas pu utiliser dans les versions précédentes d'Exchange Server. Toutefois, vous devez continuer à tester la configuration de stockage que vous sélectionnez afin de vous assurer qu'elle répond à vos besoins. Prenez en compte les éléments suivants :

- Les copies répliquées de base de données augmentent la quantité d'espace de stockage requise. Si votre organisation utilise des DAG pour répliquer des bases de données de boîtes aux lettres pour la haute disponibilité, tenez compte du nombre de copies de base de données lorsque vous calculez la quantité d'espace disque dont vous avez besoin, ainsi que son coût.
- Les disques plus lents sont beaucoup moins coûteux par Go que les disques plus rapides. La réduction des besoins d'E/S de disque d'Exchange Server 2013 signifie que les disques de grande capacité à 7 200 tours/minute conviennent à de nombreuses organisations. Vous pouvez obtenir des disques à 7 200 tours/minute d'une taille égale avec l'interface SATA ou SAS. Les disques SAS sont légèrement plus coûteux que les disques SATA, mais lors des tests effectués par Microsoft, les disques SAS ont eu un taux d'échec de 50 % inférieur à celui des disques SATA.
- Le stockage DAS (Direct Access Storage) est moins coûteux qu'un réseau SAN (Storage Area Network). Par conséquent, le système DAS est préférable si vous utilisez des DAG pour créer plusieurs copies répliquées des données. Vous pouvez acheter des baies de disques externes et les utiliser pour relier un grand nombre de disques à un serveur unique. La fiabilité inférieure du système DAS est compensée par le nombre de copies de base de données du DAG. Si vous disposez d'un réseau SAN avec de l'espace disponible, vous préfèrerez peut-être l'utiliser en raison de sa fiabilité supérieur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Vous pouvez envisager d'utiliser la technologie JBOD si vous disposez d'au moins trois réplicas d'une base de données dans un DAG. JBOD ne permet pas la redondance, mais cela est acceptable car le DAG contient plusieurs copies de base de données. JBOD est utilisé avec le stockage DAS.
- Certaines organisations ont considérablement investi dans les réseaux SAN pour le stockage de tous les serveurs. Si vous utilisez un réseau SAN, la fiabilité accrue peut signifier que vous choisissez d'implémenter moins de copies de base de données dans un DAG. Vous pouvez également conserver quelques copies de base de données sur un réseau SAN et d'autres sur un système DAS. Même lorsque vous utilisez un réseau SAN, nous vous recommandons d'avoir deux copies de base de données.
- Une interface SCSI (iSCSI) SAN Internet offre généralement des performances inférieures à un réseau SAN Fibre Channel, mais elle est également beaucoup moins coûteuse. Si vous utilisez un réseau SAN, les besoins inférieurs en termes d'E/S dans Exchange Server 2013 font d'iSCSI une alternative à Fibre Channel dans un large éventail de scénarios.
- Utilisez RAID pour augmenter la redondance du système de disque s'il y a moins de trois copies de base de données dans un DAG. Divers types de RAID sont disponibles pour augmenter les performances et la redondance du système de disque. RAID 10 est l'option RAID la plus performante, car elle a la vitesse d'un agrégat par bande et la redondance de la mise en miroir. Toutefois, cette option est relativement onéreuse, car 50 % de l'espace disque est utilisé pour les données redondantes. Vous pouvez utiliser l'outil Exchange Mailbox Server Role Requirements Calculator pour vous aider à planifier la configuration de stockage des serveurs de boîtes aux lettres. Cette feuille de calcul permet d'estimer avec précision les conditions matérielles requises pour prendre en charge un nombre d'utilisateurs donné avec une configuration de stockage spécifique. Vous pouvez télécharger cet outil, mis à jour régulièrement, à partir du site Web de Microsoft.

Documentation supplémentaire : Vous trouverez plus d'informations sur les options de configuration du stockage pour Exchange Server 2013 sur : http://go.microsoft.com/fwlink/?LinkId=290958.

Conception de bases de données de boîtes aux lettres

Pour concevoir des services de boîte aux lettres, vous devez identifier les informations requises pour les boîtes aux lettres et pour les dossiers publics. En général, les informations que vous recueillez vous aident à déterminer la taille des bases de données qui doivent être adaptées, et la charge de traitement que ces bases de données placeront sur les serveurs de boîtes aux lettres.

Lorsque vous concevez des bases de données, tenez compte des recommandations suivantes

- Utilisez des fichiers journaux fractionnés et un stockage de base de données pour améliorer la capacité de récupération quand la réplication n'est pas utilisée
- Allouez de l'espace pour les index
- Allouez de l'espace pour la récupération d'élément unique
- Allouez de l'espace pour les archives personnelles
- Allouez de l'espace pour une base de données de récupération

Pour concevoir des bases de données de boîtes aux lettres, vous devez tenir compte des facteurs relatifs aux boîtes aux lettres suivants :

- *Nombre d'utilisateurs*. Un grand nombre d'utilisateurs augmente généralement l'utilisation du disque.
- *Fréquence d'utilisation*. Une fréquence d'utilisation plus élevée augmente généralement l'utilisation du disque.
- *Taille des boîtes aux lettres*. Des boîtes aux lettres de plus grande taille associées à un nombre plus élevé d'utilisateurs augmentent la taille globale de la base de données.
- *Contrats SLA*. Pour répondre aux besoins en matière de récupération, il se peut que vous deviez conserver des bases de données de petite taille afin que les durées de restauration soient réduites.

Dans les versions précédentes d'Exchange Server, telles qu'Exchange Server 2007, nous recommandions de conserver les fichiers journaux et les bases de données sur des disques distincts. Ainsi, en cas de défaillance du disque et de perte de la base de données, vous disposiez toujours des fichiers journaux après une restauration. Vous pouviez donc les relire pour récupérer les messages reçus depuis la dernière sauvegarde. Dans Exchange Server 2013, la même recommandation est toujours applicable dans les petits environnements qui n'utilisent pas les DAG. Toutefois, s'il existe plusieurs copies répliquées d'une base de données, vous n'avez pas besoin de conserver les journaux des transactions et les bases de données sur des disques distincts, car la récupération est effectuée à partir un réplica différent et non à partir d'une sauvegarde.

Dans Exchange Server 2013, il est recommandé de localiser plusieurs bases de données sur un seul numéro d'unité logique (LUN, Logical Unit Number), car les E/S de disque sont aléatoires. Vous pouvez répartir les journaux des transactions sur différents disques physiques pour augmenter les performances, mais ce n'est généralement pas nécessaire. Dans la plupart des cas, étant donné qu'Exchange Server 2013 a des besoins inférieurs en termes d'E/S, vous pouvez conserver les fichiers journaux et les fichiers de base de données sur le même volume sans affecter les performances.

Vous pouvez séparer les fichiers journaux des fichiers de base de données pour leur faculté de récupération lors de l'utilisation de sauvegardes. En stockant les fichiers de base de données et les fichiers journaux sur des volumes ou des disques distincts, vous pouvez relire les journaux des transactions après une restauration de base de données lorsque celle-ci a été perdue en raison d'un volume ou d'un disque défectueux.

Éléments à prendre en compte concernant l'espace disque

Lorsque vous calculez l'espace disque requis pour une base de données sur un serveur de boîtes aux lettres, vous ne devez pas uniquement prendre en compte les bases de données de boîtes aux lettres. Dans la plupart des cas, vous souhaitez autoriser l'indexation sur les bases de données pour accélérer les recherches. Chaque index utilise environ 5 % de l'espace disque de la base de données de boîtes aux lettres. Cet index est placé au même emplacement que celui de la base de données.

La récupération d'élément unique conserve les messages supprimés dans une base de données pendant un laps de temps spécifié. Lorsque vous activez la récupération d'élément unique, la taille de la base de données augmente.

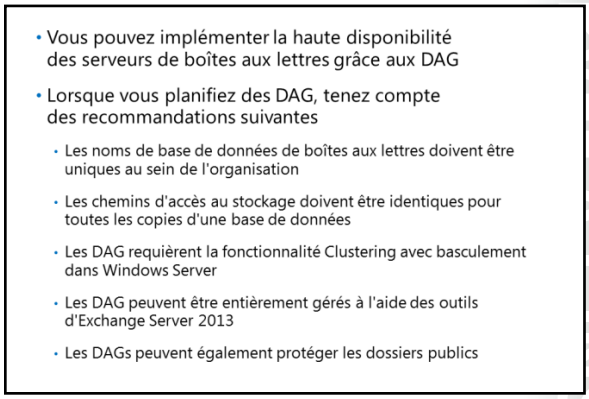
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous devez également inclure les archives personnelles lors de la planification des bases de données de boîtes aux lettres. Une archive personnelle est généralement utilisée pour conserver le contenu de boîte aux lettres pendant une période plus longue. Si vous activez les archives personnelles, la taille de la base de données peut augmenter.

Vous pouvez utiliser une base de données de récupération dans divers scénarios de récupération pour extraire les données des boîtes aux lettres. Pour utiliser une base de données de récupération, vous devez disposer de suffisamment d'espace disque pour restaurer la base de données et les journaux des transactions.

Planification de serveurs de boîtes aux lettres pour la haute disponibilité

L'utilisation d'un DAG est requis pour l'implémentation de la haute disponibilité des bases de données de boîtes aux lettres. Un DAG vous permet de répliquer des bases de données de boîtes aux lettres sur plusieurs serveurs. Si le serveur qui dessert les clients tombe en panne, un réplica sur un autre serveur du DAG commence à traiter les demandes des clients.



Éléments à prendre en compte pour l'implémentation de DAG :

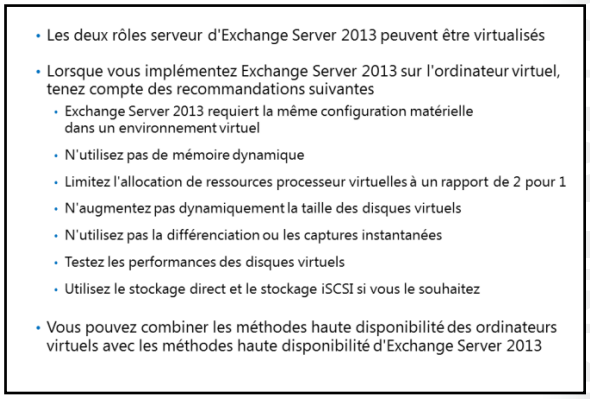
- Les noms de base de données de boîtes aux lettres doivent être uniques dans l'organisation Exchange Server 2013. Cela peut nécessiter le développement d'une convention d'affectation de noms. Cette convention d'affectation de noms ne doit pas inclure le nom du serveur, car la base de données peut être déplacée entre les membres du DAG.
- Le chemin d'accès au stockage doit être identique pour toutes les copies d'une base de données. Cela signifie que tous les membres d'un DAG doivent avoir la même configuration de disque avec les mêmes lettres de lecteur. Pour une plus grande flexibilité, vous pouvez utiliser des points de montage au lieu de diverses lettres de lecteur, mais cela n'est pas obligatoire.
- L'implémentation d'un DAG recourt à la fonctionnalité de clustering avec basculement du système d'exploitation Windows Server. Cette fonctionnalité est disponible dans Windows Server® 2012 Éditions Standard ou Datacenter. Si vous utilisez Windows Server 2008, installez Windows Server 2008 Enterprise ou Windows Server 2008 Datacenter afin de prendre en charge le clustering avec basculement. Toutefois, les DAG sont pris en charge dans les éditions Standard et Entreprise d'Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Les DAG peuvent être gérés à partir des outils de gestion d'Exchange Server 2013. Cela simplifie le processus de configuration des DAG et masque la complexité du clustering avec basculement pour les administrateurs.
- Dans Exchange Server 2013, les DAG peuvent également être utilisés pour rendre les dossiers publics disponibles. Dans la mesure où les dossiers publics résident dans la base de données de boîtes aux lettres, la même technologie de haute disponibilité peut leur être appliquée.
- Il est possible d'installer des rôles serveur supplémentaires sur un serveur membre d'un DAG. Par exemple, vous pouvez installer l'accès au client sur un serveur membre d'un DAG.

Éléments à prendre en compte pour la virtualisation des serveurs de boîtes aux lettres

Tous les rôles serveur d'Exchange Server 2013 peuvent être virtualisés. Une implémentation virtualisée d'Exchange Server 2013 est prise en charge lorsque l'exécution s'effectue sur une des plateformes de virtualisation suivantes :



- Windows Server® 2008 R2 avec la technologie Hyper-V®.
- Microsoft Hyper-V® dans Windows Server® 2008 R2.
- Windows Server® 2012.
- Microsoft Hyper-V® dans Windows Server® 2012.
- Tout hyperviseur tiers ayant été validé par le programme Windows Server Virtualization Validation Program.

Lorsque vous implémentez Exchange Server 2013 sur un ordinateur virtuel, tenez compte des recommandations suivantes :

- Lorsque Exchange Server 2013 s'exécute sur un ordinateur virtuel, ses exigences en matière de performances matérielles sont identiques à celles qu'il a lorsqu'il n'est pas virtualisé. Les conditions requises pour la mémoire et la puissance de traitement sont identiques. Par exemple, si la planification indique qu'un serveur exécutant Exchange Server 2013 requiert 16 Go de mémoire, une version virtualisée de ce serveur requerra également 16 Go de mémoire.
- Vous ne devez installer aucun logiciel supplémentaire sur la partition racine physique du serveur qui héberge les ordinateurs virtuels.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- N'utilisez pas de mémoire dynamique. Exchange Server 2013 utilise la mise en cache dans la mémoire pour améliorer les performances. Si la mémoire est dynamique, Exchange Server 2013 ne contrôle pas totalement l'allocation de mémoire dans l'ordinateur virtuel, ce qui peut réduire les performances.
- N'allouez pas de processeurs virtuels à des ordinateurs virtuels dans des proportions supérieures à deux processeurs virtuels par cœur de processeur. Par exemple, si l'hôte physique comporte deux processeurs à six cœurs chacun, vous ne devez pas allouer plus de 24 processeurs virtuels.

Voici quelques éléments à prendre en compte pour le stockage :

- L'augmentation dynamique de la taille des disques virtuels n'est pas prise en charge. Cela est dû à des problèmes de performance à mesure que la taille du disque augmente.
- Les mécanismes de différenciation ou mécanismes delta tels que les captures instantanées ne sont pas pris en charge. Cela est dû au fait que les mécanismes de captures instantanées ne prennent pas en charge les applications et, par conséquent, la récupération vers une capture instantanée est imprévisible.
- Un ordinateur virtuel Exchange Server doit utiliser un disque dur virtuel d'au moins 15 Go, plus la taille de la mémoire virtuelle qui est allouée à l'ordinateur invité. Cette capacité est nécessaire pour prendre en compte l'espace disque requis pour le système d'exploitation et le fichier de pagination. Par exemple, si 8 Go de mémoire sont alloués à l'ordinateur invité, l'espace disque minimum nécessaire pour le disque du système d'exploitation invité est de 23 Go.
- Testez les performances du disque virtuel pour vous assurer que ce dernier répond à vos besoins. Les performances d'un disque virtuel sont généralement légèrement inférieures à celles d'un disque physique.
- Le stockage direct et le stockage iSCSI sont tous deux pris en charge. Toutefois, les performances du stockage iSCSI sont réduites si la pile réseau de l'environnement de virtualisation ne prend pas en charge les trames Jumbo. Les trames Jumbo sont prises en charge par Hyper-V dans Windows Server 2008 R2, mais elles doivent être activées dans la partition parente et sur l'ordinateur virtuel.

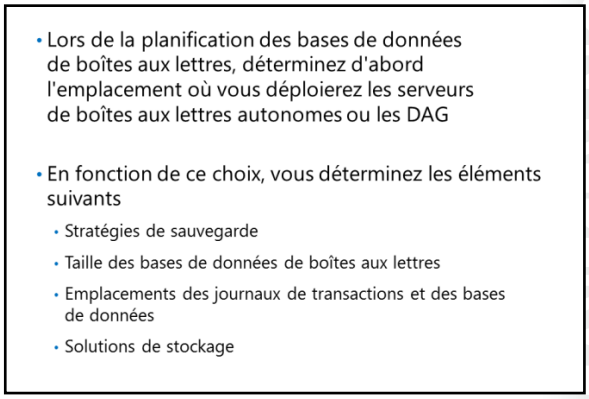
Vous pouvez utiliser la haute disponibilité de l'ordinateur virtuel fournie par votre environnement de virtualisation dans Exchange Server 2013. Elle est prise en charge, même pour les serveurs qui font partie d'un DAG. Voici certains des éléments à prendre en compte pour la haute disponibilité des ordinateurs virtuels :

- Les ordinateurs virtuels ne doivent pas enregistrer puis restaurer l'état lorsqu'ils sont migrés entre les hôtes. Toutes les migrations entre les hôtes doivent être des migrations en ligne, comme la technologie de migration dynamique Hyper-V dans Windows Server 2008 R2 et Windows Server 2012. Sinon, les ordinateurs virtuels peuvent être arrêtés, migrés, puis redémarrés.
- Les méthodes de migration en ligne doivent être prises en charge par le fournisseur de l'hyperviseur.
- Si un ordinateur virtuel ou un hôte est défaillant, l'ordinateur virtuel doit être redémarré sur un autre hôte avec un processus de démarrage complet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour planifier les bases de données de boîtes aux lettres

Lors de la planification d'un déploiement de bases de données de boîtes aux lettres, la première décision critique est de déterminer si les organisations déploieront les DAG ou si elles choisiront d'implémenter des serveurs indépendants sans solution de haute disponibilité. Cette décision aura un impact important sur la façon dont la solution de base de données et de stockage sera implémentée.



Éléments à prendre en compte pour planifier les déploiements de bases de données de boîtes aux lettres sans DAG

Lorsque les organisations choisissent de ne pas implémenter de DAG, le processus de planification pour le déploiement de bases de données de boîtes aux lettres est similaire à celui concernant les déploiements sans haute disponibilité des versions Exchange Server antérieures. Avec ce déploiement, les organisations doivent être conscientes qu'en cas de défaillance de quelque type que ce soit, leur solution de messagerie s'arrêtera et elles devront restaurer leurs données et leurs services à l'aide de stratégies et de procédures de sauvegarde soigneusement planifiées.

Appliquez les recommandations suivantes si votre entreprise choisit de ne pas implémenter les DAG :

- Stratégies de sauvegarde. Comme vous n'avez qu'une seule copie de la base de données, la sauvegarde et la restauration sont vos principaux moyens de récupération en cas de défaillance de base de données. Il s'ensuit qu'il est essentiel que vous sauvegardiez régulièrement la base de données.
- Taille des bases de données de boîtes aux lettres. La taille maximale de base de données est déterminée par la capacité du processus de sauvegarde et de restauration, ainsi que par le contrat de niveau de service (SLA) en matière de récupération des bases de données. L'outil Exchange Mailbox Server Role Requirements Calculator recommande une limite de 200 Go pour les bases de données sans DAG.
- Emplacements des journaux de transactions et des bases de données. Avec une seule copie des bases de données, il est important que les journaux des bases de données et les journaux des transactions soient stockés sur des disques séparés, pour des raisons de performance et de récupération.
- Solution de stockage. Avec une seule copie de la base de données, il est très important de fournir la redondance au niveau du stockage. Vous devez utiliser les SAN avec de hauts niveaux de redondance pour supprimer un seul point de défaillance. Utilisez RAID 5 pour améliorer les performances et la tolérance de panne pour les bases de données, RAID 1 pour fournir la tolérance de panne pour les journaux des transactions et les bases de données, et RAID 10 pour les journaux des transactions si la demande de performances est élevée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour planifier les déploiements de bases de données de boîtes aux lettres avec DAG

Lorsque les organisations choisissent d'implémenter les DAG, le processus de planification du déploiement des bases de données de boîtes aux lettres change. Lorsque les bases de données sont stockées sur plusieurs serveurs, les utilisateurs peuvent ne pas être conscients d'une défaillance du serveur ou de la base de données, car les bases de données peuvent être automatiquement montées sur un autre serveur. Ces entreprises peuvent choisir de ne pas effectuer de sauvegarde et d'utiliser à la place la protection native des données d'Exchange pour protéger leurs données. Si votre entreprise choisit de déployer les DAG, les recommandations suivantes s'appliquent :

- Stratégie de sauvegarde. Avec les DAG, la haute disponibilité est assurée par l'existence de plusieurs copies de bases de données et, par conséquent, la sauvegarde et la restauration deviennent beaucoup moins importantes. Avec un nombre suffisant de bases de données, les entreprises peuvent envisager d'effectuer des sauvegardes à intervalles plus grands ou peuvent même supprimer totalement les procédures de sauvegarde.
- Taille des bases de données de boîtes aux lettres. En raison de la moindre importance de la sauvegarde et de la restauration, le principal élément à prendre en compte quant à la taille de la base de données devient le temps qu'il faudra pour réamorcer la base de données en cas de perte d'un exemplaire. De ce fait, les bases de données peuvent être beaucoup plus volumineuses. L'outil Exchange Mailbox Server Role Requirements Calculator recommande une limite de 2 To pour les bases de données avec DAG.
- Emplacements des journaux de transactions et des bases de données. Avec plusieurs copies de base de données, la séparation des bases de données et des fichiers journaux des transactions est moins importante. Les compagnies peuvent continuer à vouloir procéder ainsi pour des raisons de performance, mais ce choix n'est nullement obligatoire pour des motifs de redondance et de récupération. Si l'organisation n'effectue pas de sauvegarde, activez la journalisation circulaire pour empêcher que les journaux des transactions n'occupent trop de place sur les disques.
- Solution de stockage. Avec plusieurs copies de bases de données qui fournissent la redondance, il devient moins important d'envisager un système disque onéreux (SAN, par exemple). Il est probable que vous préfèrerez utiliser DAS en raison de son coût inférieur. En outre, si votre organisation possède trois copies ou plus des bases de données, il est fort probable que vous utiliserez une solution JBOD.

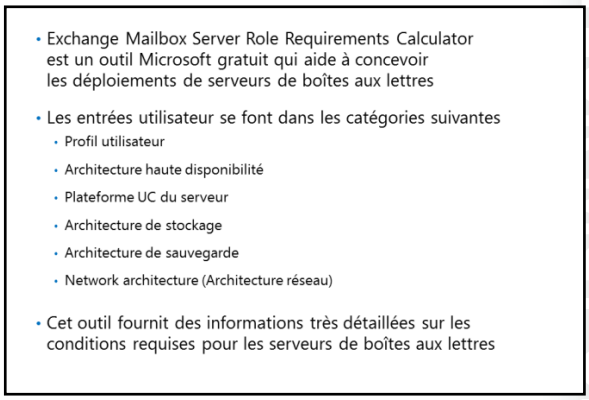
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour planifier les déploiements de bases de données de boîtes aux lettres

Lors de la conception des déploiements de bases de données de boîtes aux lettres, certains critères s'appliquent que vous déployiez ou non les DAG. Ces facteurs sont les suivants :

- Nombre de bases de données déployées. Pensez à déployer plusieurs bases de données, plutôt que d'avoir une seule base de données volumineuse. Vous pouvez choisir de placer les boîtes aux lettres utilisateurs aux besoins métier communs dans une seule base de données (Direction, Ressources humaines ou Marketing, par exemple). Le fait d'avoir plusieurs bases de données offre une plus grande souplesse aux administrateurs Exchange Server, car ils peuvent configurer les limites de boîte aux lettres, les paramètres de suppression et les procédures de sauvegarde/restauration de chaque base de données.
- Éléments à prendre en compte pour la dénomination des bases de données. À compter d'Exchange Server 2010, les bases de données ne sont plus la propriété d'objets serveur, et une base de données peut être répliquée sur plusieurs serveurs de boîtes aux lettres si vous les configurez pour la haute disponibilité. Cela signifie que les noms des bases de données doivent aussi être uniques à travers toute l'organisation, y compris les bases de données des serveurs hérités. Par conséquent, nous vous recommandons de ne pas utiliser les éléments suivants dans les conventions de nomination de base de données :
  - Nom du serveur
  - Nom du site Active Directory (pour le cas de tolérance aux pannes de site)
  - Nom du centre de données physique (pour le cas de tolérance aux pannes de site)
  - Nom de l'organisation Exchange

Qu'est-ce que l'outil Exchange Mailbox Server Role Requirements Calculator ?



Pour permettre aux administrateurs et aux concepteurs de systèmes de planifier le rôle serveur de boîte aux lettres Exchange Server aussi exactement que possible, Microsoft fournit un outil qui permet d'estimer la configuration requise pour votre serveur de boîtes aux lettres en fonction de vos propriétés environnementales actuelles. Il s'agit de l'outil Exchange Mailbox Server Role Requirements Calculator. Cet outil se présente sous la forme d'une feuille de calcul Excel prenant en charge les macros, qui collecte les entrées utilisateur, puis en fonction de ces entrées, calcule diverses conditions requises pour l'implémentation du rôle serveur de boîtes aux lettres Exchange Server.

Remarque : Exchange Mailbox Server Role Requirements Calculator est un téléchargement gratuit, disponible à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=290959.

Actuellement, seule la version pour Exchange Server 2010 est disponible. Toutefois, elle s'applique également à Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour que vous puissiez ouvrir l'outil et l'utiliser, Microsoft Excel® 2007, Microsoft Excel® 2010 ou Microsoft Excel® 2013 doit être installé. Cet outil comprend les sections suivantes (feuilles de calcul) :

- Input (Entrée)
- Role Requirements (Conditions requises pour le rôle)
- Activation Scenarios (Scénarios d'activation)
- Distribution
- LUN Requirements (Conditions requises pour LUN)
- Backup Requirements (Conditions requises pour la sauvegarde)
- Log Replication Requirements (Conditions requises pour la réplication des journaux)
- Storage Design (Conception du stockage)

Nous vous recommandons de renseigner uniquement les données dans la première feuille de calcul (entrée). En fonction de ces entrées, l'outil calcule les conditions requises pour le rôle serveur de boîtes aux lettres et présente ces conditions sur les autres feuilles. Sur la feuille d'entrée, fournissez les données des catégories suivantes :

- User profile (Profil utilisateur) : profil du message, taille de la boîte aux lettres et nombre d'utilisateurs.
- High-availability architecture (Architecture haute disponibilité) : nombre de copies de base de données que vous envisagez de déployer, résilience éventuelle du site et nombre de serveurs de boîtes aux lettres souhaité.
- Server's CPU platform (Plateforme UC du serveur).
- Storage architecture (Architecture de stockage) : capacité/type du disque et solution de stockage.
- Backup architecture (Architecture de sauvegarde) : indiquez si vous souhaitez utiliser le service VSS (Volume Shadow Copy Service) matériel ou logiciel et la fréquence des sauvegardes, ou si vous préférez tirer parti des fonctionnalités de protection des données natives Exchange.
- Network architecture (Architecture réseau) : utilisation, débit et aspects de latence.

 **Remarque :** L'outil est fourni avec certaines données pré-renseignées dans la feuille d'entrée. Ces données constituent un exemple de configuration, et tous les points de données entrés dans la feuille de calcul sont spécifiques à cet exemple particulier et ne s'appliquent pas à d'autres configurations. Assurez-vous que vous utilisez les points de données corrects pour votre conception.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Utilisation de l'outil Exchange Mailbox Server Role Requirements Calculator

Cette démonstration s'appuie sur une version modifiée de l'outil Exchange Mailbox Server Role Requirements Calculator (version Exchange Server 2010).

Remarque : Veillez à télécharger et à utiliser la version Exchange Server 2013 lors de l'évaluation des configurations matérielles requises pour les serveurs Exchange Server 2013.

Procédure de démonstration

1. Sur LON-CL1, ouvrez l'**Explorateur de fichiers**, accédez à **C:\Files**, puis double-cliquez sur **E2013Calc.xlsm**.
2. Dans le fichier **E2013Calc**, dans la feuille **Input**, entrez les valeurs suivantes pour chaque section :
   - Exchange Environment Configuration (Configuration de l'environnement Exchange)
     - Server Multi-Role Configuration (MBX+CAS) (Configuration de plusieurs rôles serveur (MBX+CAS)) : **Yes** (Oui)
     - Server Role Virtualization (Virtualisation du rôle serveur) : **Yes** (Oui)
     - High Availability Deployment (Déploiement de la haute disponibilité) : **Yes** (Oui)
     - Number of Mailbox Servers Hosting Active Mailboxes / DAG (Nombre de serveurs de boîtes aux lettres hébergeant des boîtes aux lettres actives/DAG) : **4**
     - Number of Database Availability Groups (Nombre de groupes de disponibilité de la base de données) : **2**
     - Mailbox Database Copy Configuration (Configuration d'une copie de base de données de boîtes aux lettres)
     - Total Number of HA Database Copy Instances (Includes Active Copy) within DAG (Nombre total d'instances de copie de base de données HA [y compris la copie active] dans le DAG) : **3**
     - Total number of Lagged Database Copy Instances within DAG (Nombre total d'instances de copie de base de données décalée dans le DAG) : **1**
   - Exchange Data Configuration (Configuration des données Exchange)
     - Mailbox Moves/Week Percentage (Pourcentage de déplacement de boîtes aux lettres par semaine) : **1%**
     - LUN Free Space Percentage (Pourcentage d'espace libre par LUN) : **15%**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

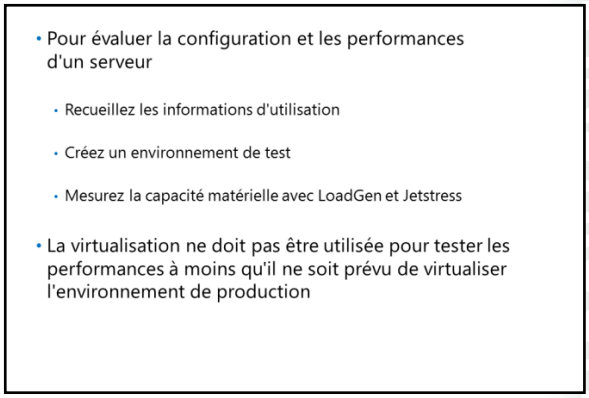
- Tier-1 User Mailbox Configuration (Configuration de boîtes aux lettres d'utilisateur de niveau 1)
  - Total Number of Tier-1 User Mailboxes/Environment (Nombre total de boîtes aux lettres d'utilisateur de niveau 1/environnement) : **500**
  - Projected Mailbox Number Growth Percentage (Pourcentage d'augmentation prévu du nombre de boîtes aux lettres) : **5%**
  - Total Send/Receive Capability/ Mailbox/Day (Capacité totale d'envoi/de réception par boîte aux lettres et par jour) : **50 messages**
  - Average Message Size (KB) (Taille moyenne des messages [Ko]) : **50**
  - Mailbox Size Limit (MB) (Taille maximale des boîtes aux lettres [Mo]) : **1024**
  - Personal Archive Mailbox Size Limit (MB) (Taille maximale des boîtes aux lettres d'archivage personnel [Mo]) : **2048**
  - Deleted Item Recovery Window (Days) (Fenêtre de récupération des éléments supprimés [jours]) : **20**
  - Single Item Recovery (Récupération d'élément unique) : **Enabled** (Activé)
  - Calendar Version Storage (Stockage des versions de calendrier) : **Enabled** (Activé)
- Backup Configuration (Configuration de la sauvegarde)
  - Backup Methodology (Méthodologie de sauvegarde) : **Software VSS Backup/Restore** (Sauvegarde/restauration VSS logicielle)
  - Backup Frequency (Fréquence des sauvegardes) : **Weekly Full / Daily incremental** (Complète hebdomadaire/incrémentielle quotidienne)
  - Database and Log Isolation Configured (Isolation de base de données et de journal configurée) : **Yes** (Oui)
  - Backup/Truncation Failure Tolerance (Tolérance d'échec des sauvegardes/troncations) : **3**
  - Network Failure Tolerance (Days) (Tolérance de défaillance réseau [jours]) : **0**
  - Primary Datacenter Disk Configuration (Configuration des disques du centre de données principal)
  - Database (Base de données) : **1,000 GB, 7.2K RPM SAS 3.5"** (Lecteur SAS 3,5 pouces, 7 200 tours/minute, 1 000 Go)
  - Log (Journal) : **500 GB, 7.2K RPM SAS 3.5"** (Lecteur SAS 3,5 pouces, 7 200 tours/minute, 500 Go)
  - Restore LUN (LUN de restauration) : **1500 GB, 7.2K RPM SAS 3.5"** (Lecteur SAS 3,5 pouces, 7 200 tours/minute, 1 500 Go)

3. Dans le fichier **E2013Calc**, cliquez sur l'onglet **Role Requirements** (Configuration requise pour le rôle).
4. Vérifiez les conditions requises indiquées sur cette feuille.
5. Cliquez sur la feuille **Distribution**.

6. Cliquez sur le bouton **Fail Server** (Serveur en échec) pour chaque serveur. Observez où les bases de données seront distribuées.
7. Cliquez sur le bouton **Export DAG Scripts** (Exporter les scripts DAG).
8. Dans la fenêtre **Storage Calculator – Export Scripts** (Outil de calcul de stockage – Exporter les scripts), cliquez sur **OK** deux fois.
9. Cliquez sur la feuille **LUN Requirements** (Conditions requises pour LUN). Vérifiez les conditions requises indiquées sur cette feuille.
10. Cliquez sur la feuille **Backup Requirements** (Conditions requises pour les sauvegardes). Vérifiez les conditions requises indiquées sur cette feuille.
11. Cliquez sur la feuille **Replication Requirements** (Conditions requises pour les réplications). Vérifiez les conditions requises indiquées sur cette feuille.
12. Cliquez sur la feuille **Storage Design** (Conception du stockage). Vérifiez les conditions requises indiquées sur cette feuille.

Vérification des performances du rôle serveur de boîtes aux lettres

Pour concevoir un plan de test pour les performances des serveurs de boîtes aux lettres, vous devez comprendre la manière exacte dont le serveur sera utilisé. Cela comprend des facteurs tels que le nombre de boîtes aux lettres, le nombre de messages que les utilisateurs enverront, et le type des clients qui accèderont aux boîtes aux lettres. Si vous ne comprenez pas exactement la charge qui sera placée sur le serveur, vous ne pouvez pas être certain que les performances du serveur répondront à vos besoins.



Lorsque vous créez votre environnement de test, vérifiez qu'il réplique les conditions de votre environnement de production aussi fidèlement que possible. Cela signifie que vous devez utiliser le même matériel, ainsi que les mêmes logiciels et pilotes sur le système de test et le système de production.

Pour tester les performances du serveur, il n'est pas possible de répliquer complètement les utilisateurs dans un environnement de production. Toutefois, Microsoft fournit deux outils servant à générer des charges simulées sur le serveur :

- **Exchange Load Generator (LoadGen)**. Vous pouvez utiliser cet outil pour créer une charge simulée de clients MAPI, Outlook® Web App, Microsoft Exchange ActiveSync®, IMAP (Internet Message Access Protocol) POP3 et SMTP (Simple Mail Transfer Protocol) sur vos serveurs Exchange. Vous pouvez configurer cet outil en fonction des données d'utilisation que vous avez recueillies pour déterminer si les performances sont acceptables.
- **Jetstress**. Cet outil permet de vérifier les performances du disque en simulant les charges de base de données Exchange Server et de fichiers journaux produites par un nombre spécifique d'utilisateurs. Cet outil est également capable de simuler la charge générée par la réplication de la base de données dans un DAG.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Configuration des serveurs de boîtes aux lettres

Une des tâches les plus importantes que vous effectuerez après que le déploiement initial d'Exchange Server 2013 est la configuration des serveurs de boîtes aux lettres. Vous devez sécuriser le serveur de boîtes aux lettres autant que possible, planifier et configurer le stockage approprié, puis créer et configurer des bases de données de boîtes aux lettres. Dans cette leçon, nous allons discuter de la configuration des serveurs de boîtes aux lettres.

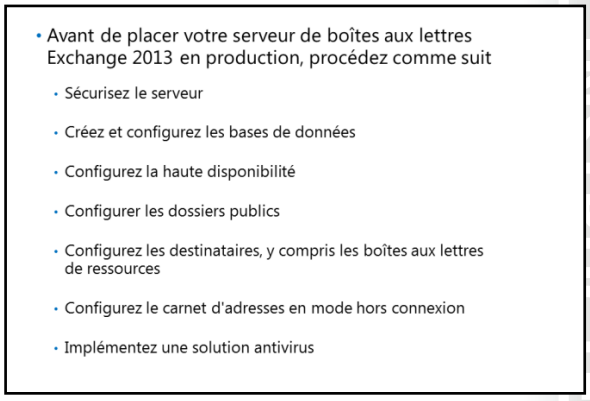
Objectifs de la leçon

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

- décrire les tâches de configuration initiale pour les serveurs de boîtes aux lettres ;
- configurer le stockage iSCSI ;
- créer et gérer les bases de données de boîtes aux lettres.

Tâches initiales de configuration des serveurs de boîtes aux lettres

Plusieurs tâches doivent être effectuées après l'installation d'Exchange Server 2013 et avant sa mise en production.



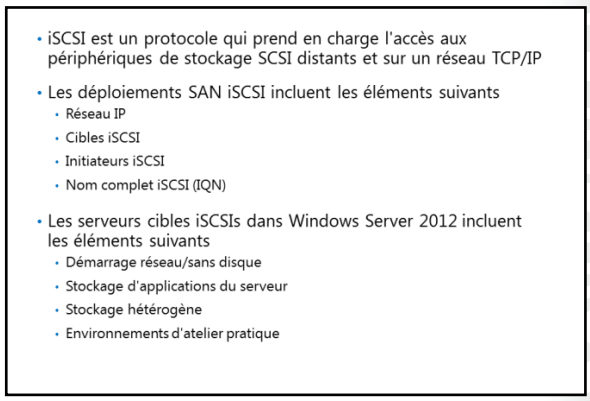
Effectuez la procédure suivante après avoir déployé le rôle serveur de boîtes aux lettres :

- *Sécurisez le serveur*. Avant de déployer les boîtes aux lettres pour le rôle serveur de boîtes aux lettres, vous devez sécuriser le serveur, ce qui inclut la configuration des autorisations à l'aide du contrôle d'accès basé sur les rôles (RBAC). Vous pouvez utiliser les groupes de rôles intégrés ou créer des groupes de rôles personnalisés pour déléguer les autorisations. Vous réduirez ainsi la surface d'attaque d'Exchange Server.
- *Créez et configurez des bases de données*. Exchange Server 2013 utilise des bases de données de boîtes aux lettres pour stocker les messages et les dossiers publics. Avant de créer des boîtes aux lettres sur le serveur, vous devez créer les bases de données requises.
- *Configurez la haute disponibilité*. Exchange Server 2013 utilise des DAG pour offrir une haute disponibilité aux bases de données de boîtes aux lettres. Nous recommandons de configurer les DAG avant de déployer les boîtes aux lettres dans les bases de données de boîtes aux lettres.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Configurez des dossiers publics*. Si vous effectuez une migration d'une version précédente d'Exchange Server, envisagez de migrer vos dossiers publics vers Exchange Server 2013 avant de déplacer toutes les boîtes aux lettres.
- *Configurez les destinataires, y compris les boîtes aux lettres de ressources*. Le rôle serveur de boîtes aux lettres gère toutes les boîtes aux lettres des utilisateurs. Ainsi, le déploiement du rôle serveur de boîtes aux lettres inclut la configuration des destinataires.
- *Configurez le carnet d'adresses en mode hors connexion*. Les clients Outlook 2007 (et version ultérieure) prennent en charge la récupération de carnet d'adresses en mode hors connexion avec HTTP, plutôt qu'avec uniquement des dossiers publics, comme dans les versions précédentes de Microsoft Office Outlook.
- *Implémentez une solution antivirus*. Nous vous conseillons vivement d'implémenter et de configurer une solution antivirus et antiprogramme malveillant avant de placer votre serveur Exchange en production.

Configuration du stockage iSCSI dans Windows Server 2012



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

iSCSI s'appuie sur l'architecture de mise en réseau Ethernet standard, et l'utilisation de matériel spécialisé tel qu'un HBA ou des commutateurs réseau est facultative. iSCSI utilise TCP/IP (en général, le port TCP 3260). Ainsi, iSCSI permet simplement à deux hôtes de négocier (l'établissement de session, le contrôle de flux et la taille de paquet, par exemple) et d'échanger ensuite des commandes SCSI à l'aide d'un réseau Ethernet existant. Ce faisant, iSCSI prend une architecture de sous-système de bus de stockage local hautes performances répandue et l'émule sur des LAN et des WAN en créant un SAN.

À la différence de certains protocoles SAN, iSCSI ne nécessite aucun câblage spécialisé. Il peut être exécuté sur une infrastructure de commutation et une infrastructure IP existante. Toutefois, les performances d'un déploiement de SAN iSCSI peuvent être considérablement réduites si ce déploiement n'est pas exécuté sur un réseau ou sous-réseau dédié, comme il est recommandé dans les meilleures pratiques.

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

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Un déploiement de SAN iSCSI comprend les éléments suivants :

- *Réseau IP*. Vous pouvez utiliser des cartes d'interface réseau standard et des commutateurs réseau Ethernet standard pour connecter les serveurs au périphérique de stockage. Pour offrir des performances suffisantes, le réseau doit fournir des vitesses d'au moins 1 gigabit par seconde (Gbit/s) et différents chemins d'accès à la cible iSCSI. Nous vous recommandons d'utiliser un réseau physique et logique dédié pour obtenir un débit rapide et fiable.
- *Cibles iSCSI*. Les cibles iSCSI présentent ou annoncent le stockage, de la même façon que les contrôleurs des disques durs de stockage connectés localement. Toutefois, ce stockage est accessible sur un réseau, et pas localement. Beaucoup de fournisseurs de stockage implémentent les cibles iSCSI au niveau matériel comme faisant partie du matériel de leur périphérique de stockage. D'autres périphériques ou appareils, tels que les périphériques de Windows Storage Server, implémentent les cibles iSCSI à l'aide d'un pilote logiciel et d'au moins une carte Ethernet. Windows Server 2012 fournit le serveur cible iSCSI, qui est en fait un pilote du protocole iSCSI, en tant que service de rôle.
- *Initiateurs iSCSI*. La cible iSCSI affiche le stockage pour l'initiateur iSCSI (également appelé le client), qui agit en tant que contrôleur de disque local pour les disques distants. Toutes les versions de Windows Server à partir de Windows Server 2008 comprennent l'initiateur iSCSI et peuvent se connecter aux cibles iSCSI.
- *Nom complet iSCSI (IQN)*. Les IQN sont des identificateurs uniques qui servent à adresser les initiateurs et cibles d'un réseau iSCSI. Lorsque vous configurez une cible iSCSI, vous devez configurer l'IQN des initiateurs iSCSI qui se connecteront à cette cible. Les initiateurs iSCSI utilisent également les IQN pour se connecter aux cibles iSCSI. Toutefois, si la résolution de noms sur le réseau iSCSI est un problème possible, des points de terminaison iSCSI (à la fois cible et initiateur) peuvent toujours être identifiés par leurs adresses IP.

Le service initiateur iSCSI est un composant standard du système d'exploitation depuis Windows Server 2008. Mais avant Windows Server 2012 le téléchargement et l'installation de la cible logicielle iSCSI étaient facultatifs. Elle est désormais intégrée à Windows Server 2012 sous forme de service de rôle. Les nouvelles fonctionnalités de Windows Server 2012 comprennent :

- *Authentification*. Vous pouvez activer Challenge Handshake Authentication Protocol (CHAP) pour authentifier les connexions d'initiateur ou CHAP inversé pour permettre à l'initiateur d'authentifier la cible iSCSI.
- *Ordinateur initiateur de requête d'ID*. Cette fonctionnalité n'est prise en charge qu'avec Windows 8 et Windows Server 2012.

Serveur cible iSCSI

Le service de rôle de serveur cible iSCSI fournit un sous-système de disques iSCSI de type logiciel indépendant du matériel. Vous pouvez utiliser le serveur cible iSCSI pour créer des cibles iSCSI et des disques virtuels iSCSI. Vous pouvez utiliser ensuite le Gestionnaire de serveur pour gérer ces cibles et disques virtuels iSCSI.

Le serveur cible iSCSI compris dans Windows Server 2012 comporte les fonctionnalités suivantes :

- *Démarrage réseau/sans disque*. En utilisant des cartes réseau compatibles pour le démarrage ou un chargeur de logiciels, vous pouvez utiliser des cibles iSCSI pour déployer rapidement des serveurs sans disque. En utilisant des disques virtuels de différenciation, vous pouvez économiser jusqu'à 90 % de l'espace de stockage pour les images du système d'exploitation. C'est idéal pour les grands déploiements d'images de système d'exploitation identiques, tels qu'une batterie de serveurs Hyper-V ou des clusters HPC (High Performance Computing).
- *Stockage d'applications du serveur*. Certaines applications, telles que Hyper-V et Exchange Server, nécessitent un stockage basé sur les blocs. Le serveur cible iSCSI peut fournir à ces applications un stockage basé sur les blocs disponible en permanence. Étant donné que le stockage est accessible à distance, il peut également combiner le stockage basé sur les blocs pour les sites principaux ou les sites de filiale.
- *Stockage hétérogène*. Le serveur cible iSCSI prend en charge les initiateurs iSCSI qui ne sont pas basés sur Windows. Vous pouvez donc partager le stockage sur des serveurs Windows dans les environnements mixtes.
- *Environnements d'atelier pratique*. Le rôle de serveur cible iSCSI permet à vos ordinateurs Windows Server 2012 d'être des périphériques de stockage basés sur les blocs accessibles sur le réseau. Cela est très utile dans les situations dans lesquelles vous souhaitez tester les applications avant leur déploiement sur un stockage SAN.

L'activation du serveur cible iSCSI pour fournir le stockage basé sur les blocs tire parti de votre réseau Ethernet existant. Aucun matériel supplémentaire n'est nécessaire. Si la haute disponibilité est un critère important, pensez à installer un cluster haute disponibilité. Avec un cluster haute disponibilité, vous aurez besoin d'un stockage partagé pour le cluster, soit un stockage Fibre Channel matériel ou une baie de stockage SAS (Serial Attached SCSI). Un serveur cible iSCSI est directement intégré à la fonctionnalité de cluster de basculement sous forme de rôle de cluster.

Initiateur iSCSI

L'initiateur iSCSI est compris dans Windows Server 2012 et Windows 8 sous forme de service et est installé par défaut. Pour connecter votre ordinateur à une cible iSCSI, il vous suffit de démarrer le service et de le configurer.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

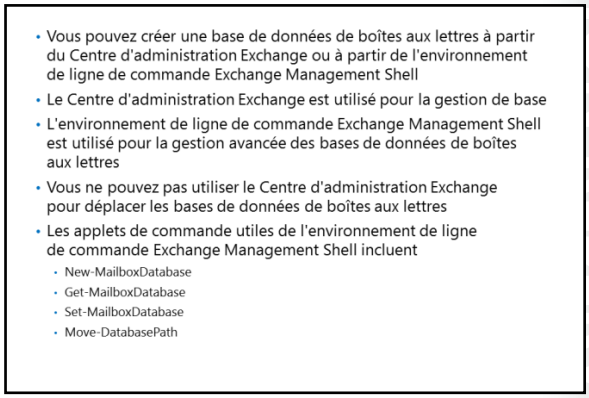
Démonstration : Configurer le stockage iSCSI pour le rôle serveur de boîtes aux lettres

Procédure de démonstration

1. Sur LON-DC1, démarrez le Gestionnaire de serveur, démarrez l'Assistant **Ajout de rôles et de fonctionnalités**, puis installez les rôles et fonctionnalités suivantes sur le serveur local et acceptez les valeurs par défaut :
   - **Services de fichiers et de stockage (Installés)\Services de fichiers et iSCSI (Installés)\Serveur cible iSCSI**
2. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez dans le volet de navigation sur **Services de fichiers et de stockage**, puis cliquez sur **iSCSI**.
3. **Créez un nouveau disque virtuel iSCSI** avec les paramètres suivants :
   - Emplacement de stockage : **C:**
   - Nom du disque : **iSCSIDisk1**
   - Taille : **2 Go**
   - Cible iSCSI : **Nouveau**
   - Nom de la cible : **lon-mbx1**
   - Serveurs d'accès : **LON-MBX1**
4. Dans la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.
5. Créez un nouveau disque virtuel iSCSI avec les paramètres suivants :
   - Emplacement de stockage : **C:**
   - Nom du disque : **iSCSIDisk2**
   - Taille : **500 Mo**
   - Cible iSCSI : **lon-mbx1**
6. Exécutez l'initiateur iSCSI sur LON-MBX1.
7. Connectez-vous au portail avec l'adresse 172.16.0.10.
8. Ajoutez la connexion à la liste des cibles favorites.

Créer et gérer des bases de données de boîtes aux lettres

L'une des premières choses à faire après avoir déployé l'infrastructure Exchange Server 2013 est de créer des bases de données de boîtes aux lettres, ou de configurer les paramètres des bases de données de boîtes aux lettres existantes. Exchange Server 2013 est fourni avec une base de données de boîtes aux lettres créée par défaut. Elle se trouve sur un lecteur système et fournit le stockage initial pour les boîtes aux lettres système et la boîte aux lettres de l'administrateur.



Dans la plupart des cas, vous n'utiliserez pas la base de données de boîtes aux lettres par défaut, sauf si vous disposez d'un petit environnement peu sollicité. Sinon, vous devrez créer une nouvelle base de données de boîtes aux lettres sur le stockage pris en charge. Il est recommandé de ne pas supprimer la base données de boîtes aux lettres par défaut, car elle contient les boîtes aux lettres système. Cependant, vous pouvez la renommer de telle sorte qu'elle respecte votre convention d'affectation de noms.

Vous pouvez créer une base de données de boîtes aux lettres à partir du Centre d'administration Exchange (CAE) ou à partir de l'environnement de ligne de commande Exchange Management Shell. Toutefois, la gestion avancée des bases de données existantes peut être effectuée uniquement à partir de l'environnement de ligne de commande Exchange Management Shell.

Lorsque vous créez une base de données de boîtes aux lettres à partir d'EAC, vous devez spécifier le nom de la base de données de boîtes aux lettres, le serveur qui hébergera la base de données, et les chemins d'accès du fichier de base de données et des journaux. Par défaut, chaque emplacement de base de données se trouve dans le répertoire d'installation Exchange Server, mais nous vous recommandons de les modifier, car vous devez héberger les bases de données sur un volume dédié.

Si vous souhaitez créer une base de données de boîtes aux lettres à l'aide de l'environnement de ligne de commande Exchange Management Shell, utilisez l'applet de commande **New-MailboxDatabase**. Lorsque vous créez une base de données de boîtes aux lettres, cette applet de commande fournit plus d'options et de paramètres que le Centre d'administration Exchange.

Lorsque vous ouvrez les propriétés de la base de données de boîtes aux lettres dans le Centre d'administration Exchange, vous pouvez configurer les options des onglets suivants :

- **Général** : Utilisez cet onglet pour configurer uniquement le nom de la base de données. Tous les autres paramètres et propriétés sont en lecture seule, mais vous pouvez voir quand la dernière sauvegarde de la base de données a été effectuée, sur quel serveur la base de données est montée et quel est le serveur maître pour la base de données. Vous pouvez également afficher la date de la dernière modification.
- **Maintenance** : Utilisez cet onglet pour configurer le destinataire du journal pour la base de données et le calendrier de maintenance. Vous pouvez également activer la maintenance de base de données en arrière-plan et configurer l'enregistrement circulaire. À des fins de restauration, vous pouvez activer le remplacement de données dans la base de données et configurer la base de données de sorte qu'elle ne soit pas montée au démarrage.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- **Limites** : Cet onglet vous permet de configurer les limites de taille et de rétention des boîtes aux lettres. Vous pouvez configurer les limites auxquelles les clients seront avertis de la taille de leurs boîtes aux lettres et également des limites au-delà desquelles l'envoi et la réception de messages seront interdits. Pour la rétention, vous pouvez configurer le nombre de jours pendant lequel le système conservera les boîtes aux lettres et les éléments supprimés.
- **Paramètres du client** : Cet onglet contient une seule option configurable ; il s'agit du carnet d'adresses en mode hors connexion (OAB, Offline Address Book). Vous pouvez configurer l'OAB des utilisateurs d'une base de données de boîtes aux lettres pour chacune des bases de données.

Pour afficher la liste complète des propriétés de la base de données de boîtes aux lettres, exécutez l'applet de commande suivante :

```
Get-MailboxDatabase -Identity MailboxName | FL
```

Pour une gestion et une configuration avancées de la base de données de boîtes aux lettres, utilisez l'applet de commande**Set-MailboxDatabase**.

Si vous souhaitez déplacer les fichiers de la base de données de boîtes aux lettres vers un autre emplacement, utilisez l'environnement de ligne de commande Exchange Management Shell. Vous ne pouvez pas utiliser l'applet de commande **Set-MailboxDatabase** pour déplacer la base de données de boîtes aux lettres ; à la place, utilisez **Move-DatabasePath**. Voici un exemple de l'applet de commande **Move-DatabasePath** :

```
Move-DatabasePath –Identity MailboxDatabaseName –EdbFilePath E:\DB1\DB1.edb –
LogFolderPath G:\Logs\DB1
```

Cet exemple illustre le déplacement d'une base de données nommée MailboxDatabaseName vers le chemin d'accès E:\DB1\DB1.edb, ainsi que le déplacement des fichiers journaux vers G:\Logs\DB1.

Démonstration : Créer et gérer des bases de données de boîtes aux lettres

Procédure de démonstration

1. Sur LON-MBX1, ouvrez l'outil **Gestion des disques**.
2. Mettez les trois nouveaux disques en ligne, puis initialisez-les.
3. Créez un volume simple sur chaque disque et formatez-le avec le système NTFS.
4. Nommez le volume sur le Disque 1 **DB2**.
5. Nommez le volume sur le Disque 2 **Logs**.
6. Dans la fenêtre du CAE, créez une base de données de boîtes aux lettres avec les propriétés suivantes :
   - Nom de la base de données : **DB2**
   - Chemin d'accès du fichier de base de données : **E:\DB2\DB2.edb**
   - Chemin d'accès du dossier des fichiers journaux : **F:\Logs\DB2**
7. Définissez les propriétés de la nouvelle base de données en exécutant l'applet de commande suivante : **Set-MailboxDatabase –identity DB2 –DeletedItemRetention 20.00:00:00 –CircularLoggingEnabled $true –ProhibitSendQuota "2.2GB"**.
8. Démontez et remontez la base de données DB2.

Atelier pratique : Configuration de serveurs de boîtes aux lettres

Scénario

Après avoir effectué un déploiement de test, A. Datum envisage désormais le déploiement d'Exchange Server 2013 dans un environnement de production. L'entreprise souhaite d'abord récapituler toutes les conditions requises et toutes les ressources disponibles, puis planifier le déploiement des serveurs de boîtes aux lettres. Après le déploiement, vous devrez configurer le stockage connecté aux serveurs, puis configurez les bases de données de boîtes aux lettres. Une fois les tâches de configuration terminées, il vous faudra exporter les données des boîtes aux lettres des utilisateurs vers les fichiers .pst.

Objectifs

- Planifier la configuration des serveurs de boîtes aux lettres.
- Configurer le stockage sur les serveurs de boîtes aux lettres.
- Créer et configurer les bases de données de boîtes aux lettres.

Configuration de l'atelier pratique

Durée approximative : **60 minutes**

Ordinateurs virtuels	22341B-LON-DC1 22341B-LON-CAS1 22341B-LON-MBX1 22341B-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 débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22341B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous avec les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22341B-LON-MBX1**, **22341B-LON-CAS1** et **22341B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Planifier la configuration des serveurs de boîtes aux lettres

Scénario

Utilisez l'outil applicable au rôle serveur de boîtes aux lettres pour concevoir l'infrastructure Exchange pour A. Datum. Les conditions requises suivantes doivent être réunies :

- A. Datum doit fournir des boîtes aux lettres à 5 000 utilisateurs. Le nombre de boîtes aux lettres augmente de 5 % par an.
- Tous les utilisateurs doivent être dotés d'une boîte aux lettres de 1 Go. En outre, chaque utilisateur doit disposer d'une archive en ligne de 2 Go.
- La taille moyenne des messages est de 75 Ko et le nombre total de messages envoyés/reçus par boîte aux lettres et par jour est de 150.
- Tous les messages supprimés doivent avoir une période de rétention de 30 jours et la récupération d'élément unique doit être activée.
- A. Datum souhaite déployer quatre serveurs de boîtes aux lettres.
- Les bases de données de boîtes aux lettres doivent être hautement disponibles.
- Chaque base de données doit avoir trois instances : 1 instance active, 1 instance passive et 1 copie décalée avec un délai de 24 heures.
- Environ 2 % des boîtes aux lettres sont déplacés par semaine.
- Les bases de données et les journaux doivent être séparés.
- A. Datum envisage d'implémenter une solution de sauvegarde tierce. Les sauvegardes seront effectuées d'après un schéma de sauvegardes complètes hebdomadaires et de sauvegardes incrémentielles quotidiennes.

Actuellement, A. Datum dispose d'un seul centre de données, et pour le moment la société n'envisage pas de solution de résilience de site. Les serveurs disposent actuellement de disques de 1 000 Go pour les bases de données, de disques de 500 Go pour les journaux des transactions, et de disques de 1 500 Go pour les LUN de restauration. A. Datum souhaite également tirer profit de la virtualisation autant que possible.

 **Remarque :** Cet atelier pratique s'appuie sur une version modifiée de l'outil Exchange Mailbox Server Role Requirements Calculator (version Exchange Server 2010). Veillez à télécharger et à utiliser la version Exchange Server 2013 lors de l'évaluation des configurations matérielles requises pour les serveurs Exchange Server 2013.

Les tâches principales de cet exercice sont les suivantes :

1. Analyser les conditions requises pour le déploiement Exchange Server d'A. Datum.
2. Utiliser Exchange Mailbox Server Role Requirements Calculator.
3. Analyser les résultats de l'outil Exchange Mailbox Server Role Requirements Calculator.
4. Comparer votre solution avec celle de l'instructeur et des autres stagiaires.

▶ Tâche 1 : Analyser les conditions requises pour le déploiement Exchange Server d'A. Datum

- Lisez le scénario de l'exercice et de l'atelier pratique. Résumez les conditions requises à partir du scénario de l'exercice.

▶ Tâche 2 : Utiliser Exchange Mailbox Server Role Requirements Calculator

1. Sur LON-CL1, ouvrez l'Explorateur de fichiers, accédez à **C:\Files** et ouvrez le fichier **E2013Calc.xlsm**. Dans l'avertissement de sécurité, cliquez sur **Activer le contenu**.
2. Selon les exigences de l'atelier pratique et du scénario de l'exercice, complétez les champs appropriés dans la feuille Input (Entrée) du fichier **E2013Calc**.

▶ Tâche 3 : Analyser les résultats de l'outil Exchange Mailbox Server Role Requirements Calculator

1. Dans le fichier **E2013Calc**, cliquez sur l'onglet **Role Requirements** (Configuration requise pour le rôle).
2. Vérifiez les conditions requises indiquées sur cette feuille.
3. Cliquez sur la feuille **Distribution**.
4. Cliquez sur le bouton **Fail Server** (Serveur en échec) pour chaque serveur. Observez où les bases de données seront distribuées.
5. Cliquez sur **Export DAG Scripts** (Exporter les scripts DAG).
6. Dans la fenêtre **Storage Calculator – Export Scripts** (Outil de calcul de stockage – Exporter les scripts), cliquez sur **OK** deux fois.
7. Cliquez sur la feuille **LUN Requirements** (Conditions requises pour LUN). Vérifiez les conditions requises indiquées sur cette feuille.
8. Cliquez sur la feuille **Backup Requirements** (Conditions requises pour les sauvegardes). Vérifiez les conditions requises indiquées sur cette feuille.
9. Cliquez sur la feuille **Replication Requirements** (Conditions requises pour les réplications). Vérifiez les conditions requises indiquées sur cette feuille.
10. Cliquez sur la feuille **Storage Design** (Conception du stockage). Vérifiez les conditions requises indiquées sur cette feuille.
11. Ouvrez l'**Explorateur de fichiers**, et accédez à **C:\Files**.
12. Cliquez avec le bouton droit sur le fichier **CreateMBDatabases.ps1**, puis sélectionnez **Modifier**. Examinez le contenu du script qui est généré.
13. Cliquez avec le bouton droit sur le fichier **CreateMBDatabaseCopies.ps1**, puis sélectionnez **Modifier**. Examinez le contenu du script qui est généré.
14. Cliquez avec le bouton droit sur le fichier **Diskpart.ps1**, puis sélectionnez **Modifier**. Examinez le contenu du script qui est généré.
15. Fermez la fenêtre **Windows PowerShell ISE**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION – RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Comparer votre solution avec celle de l'instructeur et des autres stagiaires

1. Discutez de la solution fournie par l'outil de calcul de configuration requise pour le rôle serveur de boîtes aux lettres d'Exchange avec les autres stagiaires et avec l'instructeur.
2. Modifiez les valeurs figurant dans l'onglet **Input** (Entrée) d'Exchange Mailbox Server Role Requirements Calculator et observez la façon dont cela se reflète dans les résultats obtenus par l'outil.

Résultats : À la fin de cet exercice, les stagiaires auront créé un plan pour la configuration de leurs serveurs de boîtes aux lettres.

Exercice 2 : Configurer le stockage sur les serveurs de boîtes aux lettres

Scénario

Actuellement, aucun stockage n'est lié localement au serveur de boîtes aux lettres pour la base de données de boîtes aux lettres. Vous disposez d'un stockage iSCSI disponible qui doit être utilisé pour les bases de données de boîtes aux lettres et les journaux. Ces lecteurs seront suffisants pour le déploiement initial chez A. Datum, mais l'organisation compte ajouter plusieurs lecteurs iSCSI supplémentaires pendant le déploiement.

Vous devez configurer Windows Server 2012 pour qu'il se connecte aux lecteurs iSCSI, et configurer un stockage pour les journaux et les bases de données de boîtes aux lettres.

Les tâches principales de cet exercice sont les suivantes :

1. Créer et configurer une cible et des lecteurs iSCSI.
2. Connecter Exchange Server au stockage.
3. Configurer le stockage.

▶ Tâche 1 : Créer et configurer une cible et des lecteurs iSCSI

1. Sur LON-DC1, ouvrez le Gestionnaire de serveur, démarrez l'**Assistant Ajout de rôles et de fonctionnalités**, installez les rôles et fonctionnalités suivantes sur le serveur local et acceptez les valeurs par défaut :
   - **Service de fichiers et de stockage (Installé)\Services de fichiers et iSCSI (Installé)\ Serveur cible iSCSI**
2. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez dans le volet de navigation sur **Services de fichiers et de stockage**, puis cliquez sur **iSCSI**.
3. **Créez un nouveau disque virtuel iSCSI** avec les paramètres suivants :
   - Emplacement de stockage : **C:**
   - Nom du disque : **iSCSIDisk1**
   - Taille : **2 Go**
   - Cible iSCSI : **Nouveau**
   - Nom de la cible : **lon-mbx1**
   - Serveurs d'accès : **LON-MBX1**
4. Dans la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.

5. Créez un nouveau disque virtuel iSCSI avec les paramètres suivants :
   - Emplacement de stockage : **C:**
   - Nom du disque : **iSCSIDisk2**
   - Taille : **2 Go**
   - Cible iSCSI : **lon-mbx1**
6. Créez un nouveau disque virtuel iSCSI avec les paramètres suivants :
   - Emplacement de stockage : **C:**
   - Nom du disque : **iSCSIDisk3**
   - Taille : **500 Mo**
   - Cible iSCSI : **lon-mbx1**

▶ Tâche 2 : Connecter Exchange Server au stockage

1. Sur **LON-MBX1**, ouvrez le Gestionnaire de serveur et, dans le menu Outils, démarrez l'**Initiateur iSCSI**.
2. Connectez-vous au portail avec l'adresse **172.16.0.10**.
3. Ajoutez la connexion à la liste des cibles favorites.

▶ Tâche 3 : Configurer le stockage

1. Sur LON-MBX1, dans le Gestionnaire de serveur, ouvrez **Gestion des disques**.
2. Mettez les trois nouveaux disques en ligne, puis initialisez-les.
3. Créez un volume simple sur chaque disque et formatez-le avec le système NTFS.
4. Nommez le volume sur le Disque 1 **DB1**.
5. Nommez le volume sur le Disque 2 **DB2**.
6. Nommez le volume sur le Disque 3 **Logs**.

Résultats : À la fin de cet exercice, les stagiaires disposeront d'un stockage iSCSI configuré pour leurs bases de données de boîtes aux lettres et leurs journaux.

Exercice 3 : Créer et configurer des bases de données de boîtes aux lettres

Scénario

Lors de l'installation du rôle serveur de boîtes aux lettres, une base de données de boîtes aux lettres par défaut est créée sur le serveur. Vous devez modifier l'emplacement et la configuration de la base de données de boîtes aux lettres par défaut pour répondre aux normes de l'entreprise. La base de données doit avoir une limite d'avertissement définie sur 0,9 Go, le paramètre Interdire l'envoi à doit être défini sur 1 Go, et le paramètre Interdire l'envoi ou la réception défini sur 2,2 Go.

Outre la base de données de boîtes aux lettres par défaut, vous devez créer une autre base de données de boîtes aux lettres afin de répondre aux conditions requises pour le déploiement. La nouvelle base de données de boîtes aux lettres doit être placée sur le disque iSCSI et l'enregistrement circulaire doit être activé. Vous devez également définir différentes limites et périodes de rétention à partir de la base de données par défaut. Après avoir défini les limites et les rétentions, vous devez exporter la boîte aux lettres d'Aidan Delaney vers un fichier .pst.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les paramètres de boîte aux lettres pour la base de données de boîtes aux lettres existante.
2. Créer et configurer des bases de données de boîtes aux lettres supplémentaires.
3. Exportez les données de boîtes aux lettres dans le fichier .pst.

▶ Tâche 1 : Configurer les paramètres de boîte aux lettres pour la base de données de boîtes aux lettres existante

1. Sur LON-MBX1, ouvrez **Internet Explorer** et tapez **https://lon-cas1.**adatum**.com/ecp**, puis appuyez sur Entrée.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Définissez les propriétés de **Mailbox Database 1** comme suit :
   - Émettre un avertissement à (Go) : **0.9**
   - Interdire l'envoi à (Go) : **1**
   - Interdire l'envoi et la réception à (Go) : **1.3**
   - Conserver les éléments supprimés pendant (jours) : **30**
4. Ouvrez l'environnement de ligne de commande Exchange Management Shell.
5. Notez les noms de la base de données en exécutant l'applet de commande **Get-MailboxDatabase**.
6. Déplacez la base de données en exécutant l'applet de commande : **Move-DatabasePath –Identity "Mailbox Database 1" –EdbFilePath E:\DB1\DB1.edb –LogFolderPath G:\Logs\DB1**.
7. Vérifiez que le fichier de base de données et les journaux ont été déplacés vers le nouvel emplacement.

▶ Tâche 2 : Créer et configurer des bases de données de boîtes aux lettres supplémentaires

1. Dans la fenêtre du Centre d'administration Exchange, créez une base de données de boîtes aux lettres avec les propriétés suivantes :
   - Nom de la base de données : **DB2**
   - Chemin d'accès du fichier de base de données : **F:\DB2\DB2.edb**
   - C Chemin d'accès au dossier Journal : **G:\Logs\DB2**
2. Définissez les propriétés de la nouvelle base de données en exécutant l'applet de commande suivante : **Set-MailboxDatabase –identity DB2 –DeletedItemRetention 20.00:00:00 –CircularLoggingEnabled $true –ProhibitSendQuota "2.2GB"**.
3. Démontez et remontez la base de données DB2.

▶ Tâche 3 : Exportez les données de boîtes aux lettres dans le fichier .pst

1. Sur LON-MBX1, dans la fenêtre de l'environnement de ligne de commande Exchange Management Shell, exécutez l'applet de commande suivante : **New-ManagementRoleAssignment –Role "Mailbox Import Export" –User Administrateur**.
2. Redémarrez Exchange Management Shell.
3. Exportez la boîte aux lettres d'Aidan en exécutant l'applet de commande suivante : **New-MailboxExportRequest -Mailbox aidan -FilePath \\lon-dc1\MailboxExport\aidan.pst**.
4. Assurez-vous que l'exportation est terminée à l'aide de l'applet de commande **Get-MailboxExportrequest**.
5. Vérifiez que le fichier aidan.pst existe dans le dossier partagé.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1**, **22341B-LON-MBX1** et **22341B-LON-CL1**.

Résultats : À la fin de cet exercice, les stagiaires auront créé et configuré leurs bases de données de boîtes aux lettres.

Question : Quel est l'utilité de l'outil Exchange Mailbox Server Role Requirements Calculator ?

Question : Pouvez-vous déplacer des bases de données de boîtes aux lettres existantes vers un chemin d'accès différent en utilisant le Centre d'administration Exchange ?

Question : Que devez-vous faire avant de pouvoir exporter la boîte aux lettres de l'utilisateur vers le fichier .pst ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

- Utilisez l'outil Exchange Server Mailbox Server Role Calculator lorsque vous planifiez un déploiement de serveur de boîtes aux lettres.
- Fournissez toujours la haute disponibilité pour les serveurs de boîtes aux lettres.
- N'utilisez pas l'enregistrement circulaire pour des boîtes aux lettres dans un environnement de production.
- Pensez à utiliser la protection des données natives Exchange.

Questions de contrôle des acquis

Question : Pourquoi choisir d'utiliser des lecteurs SATA au lieu d'un lecteur SAN ou de lecteurs SCSI (Small Computer System Interface) pour vos serveurs de boîtes aux lettres ?

Question : Votre organisation doit déterminer la solution de stockage à déployer pour le nouvel environnement de messagerie Exchange Server 2013. Quelles informations devez-vous prendre en compte lors de la sélection du matériel ?

Outils

- Exchange Mailbox Server Role Calculator
- Centre d'administration Exchange
- Environnement de ligne de commande Exchange Management Shell

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 3

Gestion d'objets destinataires

Table des matières :

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

Leçon 1 : Gérer les boîtes aux lettres Exchange Server 2013 **3-2**

Leçon 2 : Gestion d'autres destinataires Exchange **3-15**

Leçon 3 : Planification et implémentation des boîtes aux lettres de dossiers publics **3-21**

Leçon 4 : Gestion des stratégies et listes d'adresses **3-28**

Atelier pratique : Gestion d'objets destinataires **3-37**

Contrôle des acquis et éléments à retenir **3-45**

Vue d'ensemble du module

Dans tout système de messagerie, vous devez créer des destinataires et les configurer pour envoyer et recevoir des messages électroniques. En tant qu'administrateur de la messagerie Microsoft® Exchange Server, vous devez souvent créer, modifier ou supprimer des objets destinataires. Il est par conséquent essentiel d'avoir bien compris le fonctionnement de la gestion des destinataires.

Ce module décrit comment gérer les objets destinataires, les stratégies d'adresse et les listes d'adresses dans Microsoft Exchange Server 2013.

Objectifs

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

- gérer les boîtes aux lettres dans Exchange Server 2013 ;
- gérer d'autres destinataires dans Exchange Server 2013 ;
- implémenter des dossiers publics ;
- configurer les stratégies et listes d'adresses.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Gérer les boîtes aux lettres Exchange Server 2013

Deux des tâches les plus courantes qu'exécutent les administrateurs Exchange Server sont la création et la configuration des destinataires de messagerie. Comme les organisations engagent de nouveaux employés, ou les employés changent de poste au sein de l'organisation, les administrateurs Exchange doivent s'assurer que les utilisateurs disposent de la fonctionnalité de messagerie dont ils ont besoin. La plupart des utilisateurs auront recours aux boîtes aux lettres Exchange Server, bien qu'Exchange Server 2013 offre également de nombreuses autres options de boîtes aux lettres à configurer.

Cette leçon fournit une vue d'ensemble des différents types de boîtes aux lettres Exchange Server 2013 et décrit comment gérer chaque type de boîte aux lettres.

Objectifs de la leçon

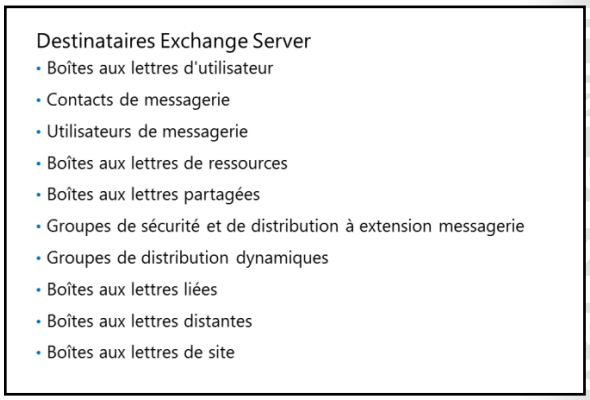
À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- identifier les différents objets destinataires dans Exchange Server 2013 ;
- décrire les boîtes aux lettres d'utilisateur ;
- créer et configurer les boîtes aux lettres d'utilisateur ;
- déplacer les boîtes aux lettres ;
- décrire les boîtes aux lettres de ressources ;
- créer et configurer des boîtes aux lettres de ressources ;
- décrire les boîtes aux lettres de site ;
- décrire les boîtes aux lettres partagées ;
- configurer les boîtes aux lettres partagées ;
- décrire les boîtes aux lettres liées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Types de destinataires Exchange Server

Les destinataires Exchange Server sont tous les objets au sein de la forêt Active Directory qui ont été configurés avec une adresse de messagerie. Lorsque des objets Active Directory sont configurés avec une adresse de messagerie, ils apparaissent dans la liste des adresses globale (LAG). Exchange Server 2013 prend en charge les types de destinataires suivants :



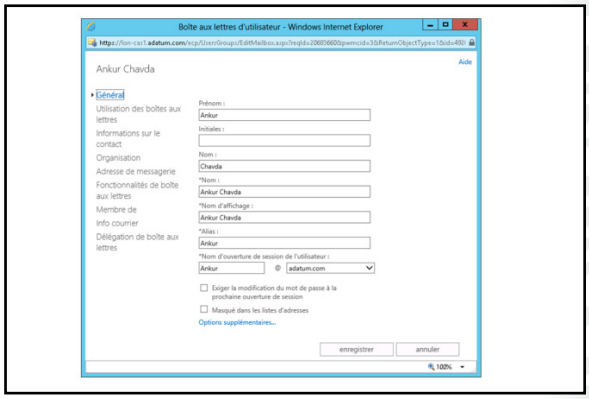
- *Boîtes aux lettres d'utilisateur*. Une boîte aux lettres que vous attribuez à un utilisateur individuel au sein de votre organisation Exchange Server. Il s'agit du type de destinataire le plus courant dans Exchange Server 2013.
- *Contacts de messagerie*. Contacts qui contiennent des informations sur les personnes ou les organisations qui existent en dehors d'une organisation Exchange Server et qui possèdent une adresse de messagerie externe. Exchange Server dirige tous les messages envoyés au contact de messagerie vers cette adresse de messagerie externe.
- *Utilisateurs de messagerie*. Les utilisateurs qui ont un compte d'utilisateur Active Directory, mais qui disposent d'une adresse de messagerie externe. Tous les messages envoyés à l'utilisateur de messagerie sont dirigés vers cette adresse de messagerie externe. Un utilisateur de messagerie est semblable à un contact de messagerie, à la différence près qu'un utilisateur de messagerie possède un compte d'utilisateur Active Directory avec un identificateur de sécurité (SID). Cela permet au compte d'utilisateur d'accéder aux ressources de l'environnement Active Directory.
- *Boîtes aux lettres de ressources (boîtes aux lettres de salle et boîtes aux lettres d'équipement)*. Une boîte aux lettres de ressources est configurée pour les objets, tels que les salles de réunion, ou les ressources, telles qu'un projecteur. Vous pouvez inclure les boîtes aux lettres de ressources en tant que ressources dans les demandes de réunion, ce qui représente un moyen simple et efficace de planification de l'utilisation des ressources.
- *Boîtes aux lettres partagées*. Une boîte aux lettres qui est utilisée par plusieurs utilisateurs plutôt que par un utilisateur principal. Les organisations ont souvent recours aux boîtes aux lettres partagées afin de fournir des services, tels que les demandes concernant les ventes, le support technique ou les informations à caractère général.
- *Groupes de sécurité et de distribution à extension messagerie*. Vous pouvez utiliser un objet groupe de sécurité Active Directory (AD DS) à extension messagerie pour accorder des autorisations d'accès aux ressources Active Directory, et vous pouvez également l'utiliser pour diffuser des messages. Vous pouvez utiliser un objet groupe de distribution Active Directory (AD DS) à extension messagerie pour distribuer des messages à un groupe de destinataires.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Groupes de distribution dynamiques*. Un groupe de distribution qui utilise une requête LDAP (Lightweight Directory Access Protocol) avec les filtres destinataires et les conditions pour générer son appartenance au moment où les messages sont envoyés.
- *Boîtes aux lettres liées*. Boîtes aux lettres normales qui sont associées à des utilisateurs individuels dans une forêt approuvée distincte. Lorsque vous créez une boîte aux lettres liée, un compte d'utilisateur désactivé est créé dans l'organisation Exchange et un compte d'utilisateur à partir d'une forêt approuvée obtient l'accès à la boîte aux lettres.
- *Boîtes aux lettres distantes*. Les boîtes aux lettres qui se situent dans l'environnement Exchange Online. Dans un déploiement hybride Exchange Server 2013, vous pouvez créer et gérer les boîtes aux lettres à distance dans l'environnement Exchange Online à l'aide du Centre d'administration Exchange.
- *Boîtes aux lettres de site*. Boîtes aux lettres qui comprennent à la fois une boîte aux lettres Exchange Server et un site Microsoft® SharePoint®. Avec les boîtes aux lettres de site, les messages sont stockés dans la boîte aux lettres, tandis que les documents sont stockés sur le site SharePoint.

Gestion des boîtes aux lettres

Création de boîtes aux lettres



- La plupart des boîtes aux lettres d'une organisation Exchange Server sont des boîtes aux lettres normales associées à un compte d'utilisateur dans la forêt Active Directory. Vous pouvez créer ces boîtes aux lettres à l'aide du Centre d'administration Exchange (CAE) ou de l'environnement de ligne de commande Exchange Management Shell. Lors de la création d'une boîte aux lettres, vous avez la possibilité de choisir entre les actions suivantes : Vous pouvez associer la boîte aux lettres à un compte d'utilisateur Active Directory existant, ou vous pouvez créer un compte Active Directory au moment de la création de la boîte aux lettres. Pour créer une boîte aux lettres et un compte d'utilisateur dans l'environnement de ligne de commande Exchange Management Shell, utilisez l'applet de commande **New-Mailbox**. Pour configurer un compte d'utilisateur existant avec une boîte aux lettres, utilisez l'applet de commande **Enable-Mailbox**.
- Vous pouvez choisir une base de données de boîtes aux lettres spécifique pour la boîte aux lettres, ou accepter la base par défaut ; autrement dit, Exchange attribuera la boîte aux lettres à toute base de données de boîtes aux lettres dans le même site Active Directory.
- Vous pouvez attribuer un affichage de carnet d'adresses à la boîte aux lettres.

Si vous créez ou activez la boîte aux lettres d'utilisateur à l'aide de l'environnement de ligne de commande Exchange Management Shell, vous pouvez y attribuer d'autres attributs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des boîtes aux lettres

Une fois la boîte aux lettres créée, vous pouvez configurer tous ses autres paramètres via le CAE ou l'environnement de ligne de commande Exchange Management Shell. Le tableau suivant répertorie certaines des options de configuration de la boîte aux lettres disponibles :

Onglet	Paramètres de configuration
Général	• Noms des utilisateurs et attributs personnalisés.
Espace de stockage utilisé	• Affiche les informations relatives à la dernière connexion. • Permet de configurer la taille totale de la boîte aux lettres et les paramètres de rétention.
Informations sur le contact	• Permet de configurer les informations, telles que les coordonnées (adresse, numéro de téléphone).
Organisation	• Permet de configurer les informations détaillées sur le rôle de l'utilisateur dans l'organisation : titre, service, société et gestionnaire.
Adresse de messagerie	• Permet de configurer les adresses de messagerie associées à la boîte aux lettres. • Peut comprendre les types d'adresses suivants : SMTP (Single Mail Transfer Protocol), EUM ou les adresses associés à d'autres systèmes de messagerie.
Fonctionnalités de boîte aux lettres	• Permet de configurer les stratégies qui s'appliquent à la boîte aux lettres. • Permet de configurer également les fonctionnalités vocales et téléphoniques, notamment leur activation et désactivation, ainsi que la configuration des stratégies pour les fonctionnalités activées. • Permet enfin de configurer les paramètres du flux de messagerie, notamment les options de remise, les restrictions de taille des messages et les restrictions de remise des messages.
Membre de	• Permet d'afficher les groupes auxquels le compte d'utilisateur appartient.
Infos-courrier	• Permet de configurer une Info courrier afin d'alerter les utilisateurs de problèmes potentiels s'ils envoient un message à ce destinataire.
Délégation de boîtes aux lettres	• Permet de configurer les autorisations suivantes : Envoyer sous, Envoyer au nom de et Accès total pour les attribuer à la boîte aux lettres utilisateur.

Pour modifier une boîte aux lettres existante, utilisez l'applet de commande **Set-Mailbox**

Remarque : Vous pouvez utiliser le CAE pour modifier certains attributs pour plusieurs boîtes aux lettres à la fois. Pour ce faire, sélectionnez plusieurs boîtes aux lettres dans l'affichage Liste. Le volet d'informations, sous Modifier en bloc, affichera les propriétés pouvant être modifiées en bloc disponibles pour les boîtes aux lettres. Vous remarquerez qu'il n'est pas possible de modifier l'intégralité des paramètres via ce processus.

Démonstration : Création et configuration des boîtes aux lettres

Au cours de cette démonstration, vous découvrirez comment créer et configurer les boîtes aux lettres d'utilisateur via le CAE et l'environnement de ligne de commande Exchange Management Shell.

Procédure de démonstration

1. Sur LON-CAS1, dans Internet Explorer, connectez-vous à **https://lon-cas1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la console de gestion Exchange, exécutez l'assistant Nouvelle boîte aux lettres et créez un compte d'utilisateur ainsi qu'une boîte aux lettres pour Alice Ciccu. Créez le compte d'utilisateur dans l'unité d'organisation (OU) Research et créez la boîte aux lettres dans la base de données de boîtes aux lettres Research.
3. Examinez les paramètres disponibles dans la boîte aux lettres d'Alice Ciccu.
4. Supprimez la boîte aux lettres d'Alice Ciccu.
5. Désactivez la boîte aux lettres d'Anil Elson.
6. Sur LON-DC1, dans Utilisateurs et ordinateurs Active Directory, vérifiez que le compte d'Alice a été supprimé de l'unité d'organisation Research, contrairement au compte d'Anil.

 **Remarque :** La suppression de la boîte aux lettres engendre la suppression du compte d'utilisateur spécifié ainsi que de la boîte aux lettres correspondante. La désactivation de la boîte aux lettres entraîne la suppression de la boîte aux lettres. Vous remarquerez toutefois que le compte d'utilisateur demeure activé.

7. Sur LON-CAS1, ouvrez l'environnement de ligne de commande Exchange Management Shell.
8. Utilisez l'applet de commande **Enable-Mailbox** pour attribuer au compte d'Anil Elson une boîte aux lettres de la base de données de boîtes aux lettres Research.
9. Utilisez les applets de commande **Get-User** et **Enable-**Mailbox pour créer les boîtes aux lettres pour tous les utilisateurs de l'unité d'organisation Développement. Placez les boîtes aux lettres dans la base de données de boîtes aux lettres 1.

Démonstration : Déplacement des boîtes aux lettres

Une des tâches courantes des administrateurs Exchange consiste à déplacer les boîtes aux lettres. Vous devrez peut-être déplacer des boîtes aux lettres vers une autre base de données de boîtes aux lettres sur le même serveur Exchange, vers une base de données de boîtes aux lettres sur un autre serveur Exchange ou vers une base de données de boîtes aux lettres sur un serveur Exchange dans une autre organisation Exchange. Dans Exchange Server 2013, vous pouvez déplacer les boîtes aux lettres une à une, ou créer des lots de migration pour déplacer plusieurs boîtes aux lettres à la fois.

Au cours de cette démonstration, vous découvrirez comment déplacer des boîtes aux lettres individuelles et comment configurer et contrôler les lots de migration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

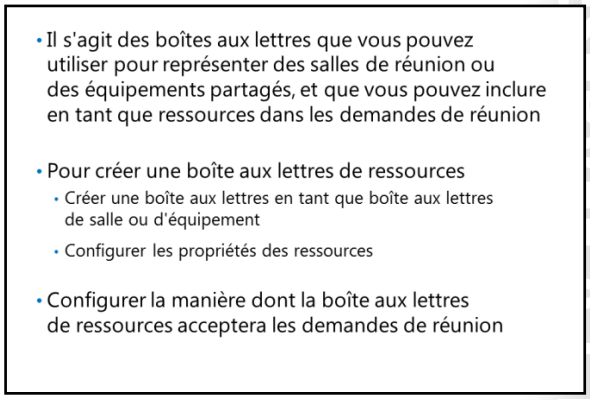
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Procédure de démonstration

1. Déplacez la boîte aux lettres d'April Reagan à partir de Mailbox Database 1 vers la base de données de boîtes aux lettres Research à l'aide du CAE. Vous pouvez également déplacer une boîte aux lettres à la fois en utilisant l'applet de commande **New-moverequest**.
2. Déplacez plusieurs boîtes aux lettres en créant un lot de migration.

Définition des boîtes aux lettres de ressources

Les boîtes aux lettres de ressources sont des types spécifiques de boîtes aux lettres que vous pouvez utiliser pour représenter des salles de réunion ou des équipements partagés, et vous pouvez les inclure en tant que ressources dans les demandes de réunion. Le compte d'utilisateur Active Directory qui est associé à une boîte aux lettres de ressources est un compte désactivé. Dans Exchange Server 2013, il est possible de créer les deux types suivants de boîtes aux lettres de ressources :



- *Boîtes aux lettres de salle*. Il s'agit des boîtes aux lettres de ressources que vous pouvez associer à des lieux de réunion, tels que des salles de conférence, des auditoriums et des salles de formation.
- *Boîtes aux lettres d'équipement*. Il s'agit des boîtes aux lettres de ressources que vous pouvez affecter à des ressources qui ne sont pas spécifiques à un emplacement, telles que des projecteurs d'ordinateur portable, des microphones ou encore des véhicules de société.

Les deux types de boîtes aux lettres de ressources peuvent être inclus comme ressources dans les demandes de réunion, offrant à vos utilisateurs un moyen simple et efficace de réserver ces ressources. Après avoir créé la boîte aux lettres de ressources, vous devez configurer des propriétés telles que l'emplacement et taille. Ces attributs sont utiles dans la mesure où ils permettent aux utilisateurs de rechercher des salles de réunion qui répondent à leurs exigences.

Configuration des paramètres de réservation des ressources

Lorsque vous configurez une boîte aux lettres de ressources, vous pouvez également configurer les paramètres qui déterminent la manière dont la boîte aux lettres des ressources répondra aux demandes de réunion. Vous pouvez configurer les boîtes aux lettres de ressources pour traiter automatiquement les demandes entrantes de réunion pour tous les utilisateurs, ou vous pouvez limiter le nombre de personnes habilitées à réserver la salle de réunion. Vous pouvez configurer les délégués qui doivent approuver toutes les demandes de réunion, et vous pouvez également configurer la boîte aux lettres de ressources pour accepter uniquement certains types de réunions. Par exemple, vous pouvez configurer une salle de conférence pour qu'elle accepte automatiquement les demandes de réunion entrantes, à l'exception des demandes de réunions récurrentes.

Lorsque vous créez une boîte aux lettres de ressources à l'aide du CAE, vous pouvez configurer les paramètres suivants qui déterminent la manière dont la boîte aux lettres acceptera les demandes de réunion.

Onglet	Paramètres
Délégués	Vous pouvez configurer les boîtes aux lettres de ressources pour traiter automatiquement les demandes de réunion pour tous les utilisateurs, ou vous pouvez sélectionner les délégués qui doivent accepter ou rejeter les demandes de réunion. En tant que délégués sur une boîte aux lettres, vous n'êtes habilité qu'à attribuer uniquement des boîtes aux lettres individuelles et non des listes de distribution.
Options de réservation	Vous pouvez configurer les éléments suivants : • Si la boîte aux lettres autorise la répétition ou la récurrence des réunions. • Si la boîte aux lettres autorise la planification des réunions uniquement pendant les heures de travail (de 8h à 17h, du lundi au vendredi). • Le nombre de jours pendant lesquels la réunion peut être planifiée à l'avance. • S'il faut refuser automatiquement les réunions qui vont au-delà de la durée maximale de réservation. • La durée de réservation des réunions pour la boîte aux lettres. • Le texte supplémentaire qui sera envoyé à l'utilisateur lorsque le demandeur réserve une réunion avec la boîte aux lettres.

Outre les paramètres disponibles dans le CAE, vous pouvez également configurer de nombreux paramètres supplémentaires concernant la façon dont la boîte aux lettres de ressources répondra aux demandes de réunion. Ces paramètres sont configurés avec l'applet de commande **set-calendarprocessing**. Parmi ces options disponibles, figurent les éléments suivants :

Option de configuration	Commande simple
Autoriser les demandes de réunion en conflit.	Set-CalendarProcessing –id MeetingRm1 –AllowConflicts $true
Autoriser certains utilisateurs à demander des réunions qui ne répondent pas aux stratégies en termes de durée maximale ou de total de réunions.	Set-CalendarProcessing –id MeetingRm1 –RequestOutOfPolicy adam
Empêcher la salle de réunion d'accepter automatiquement les demandes de réunion.	Set-CalendarProcessing -Identity MeetingRm1 -AutomateProcessing:None

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour la planification des boîtes aux lettres de ressources

Lorsque vous élaborez la manière dont les demandes de réunion seront acceptées, tenez compte des éléments suivants :

- *Les personnes habilitées à planifier une ressource*. Vous pouvez accepter les paramètres par défaut pour la plupart des ressources de l'organisation, mais vous devez envisager de limiter le cercle des personnes autorisées à réserver des ressources très utilisées ou importantes. Par exemple, si vous utilisez une boîte aux lettres de Salle de ressource pour gérer la planification d'une grande salle de conférence, vous pouvez restreindre le cercle des personnes autorisées à réserver des réunions dans cette salle de conférence.
- *Le moment où les utilisateurs peuvent planifier la ressource*. Vous pouvez définir des restrictions concernant l'heure à laquelle les réunions peuvent être réservées pour une ressource, ou encore restreindre la durée des réunions ou leur récurrence.
- *La stratégie d'acceptation automatique pour la ressource de réunion*. Par défaut, toutes les boîtes aux lettres de ressources sont configurées pour accepter toutes les nouvelles demandes de rendez-vous et pour bloquer toutes les demandes entrant en conflit. Vous pouvez modifier cela de sorte que toutes les demandes de réunion soient acceptées comme temporaires, ou permettre aux utilisateurs de réserver la ressource de réunion pour une même période.

Démonstration : Création et gestion des boîtes aux lettres de ressources

Dans cette démonstration, vous allez apprendre à utiliser la console de gestion Exchange (EMC) pour :

- créer et configurer une boîte aux lettres de ressources ;
- configurer un délégué pour une boîte aux lettres de ressources.

Procédure de démonstration

1. Sur LON-CAS1, dans le CAE, créez une boîte aux lettres de salle avec les informations suivantes :
    - Nom : **Salle de conférence 1**
    - Adresse de messagerie : **Salleconf1**
    - Unité d'organisation : **Sales**
    - Emplacement : **Londres**
    - Capacité : **20**
    - Base de données de boîtes aux lettres : **Mailbox Database 1**
2. Une fois la boîte aux lettres de salle créée, modifiez les propriétés pour :
    - Modifier la durée de réservation des réunions et la passer sur un an.
    - Envoyez le texte **Vous avez réservé avec succès la Salle de conférence 1** aux utilisateurs qui réservent la salle de réunion.

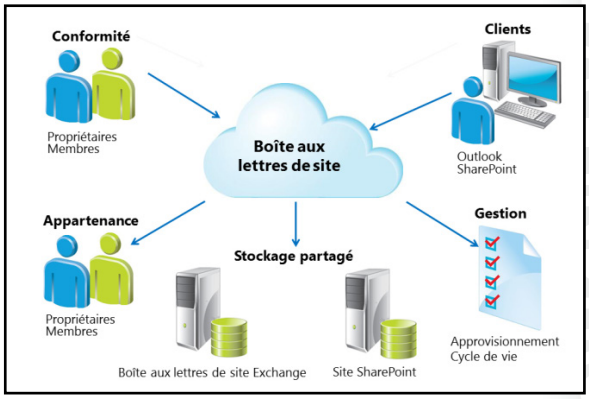
3. Sur LON-CL1, ouvrez une session en tant qu'Aidan, ouvrez Outlook 2013 et créez une demande de réunion. Invitez à la réunion l'administrateur et la boîte aux lettres de ressources Salle de conférence 1.

Remarque : Si nécessaire, exécutez l'Assistant **Bienvenue dans Microsoft Outlook 2013**.

4. Envoyez la demande de réunion et vérifiez que la ressource a accepté l'invitation.
5. Sur LON-CAS1, dans le CAE, accédez aux propriétés de la Salle de conférence 1.
6. Ajoutez **Amr Zaki** comme délégué sur la boîte aux lettres de ressources.
7. Vérifiez que le délégué a accepté la demande de réunion pour la boîte aux lettres de salle.

Définition des boîtes aux lettres de site

Un problème auquel les utilisateurs doivent faire face lorsqu'ils travaillent en collaboration est le stockage des informations dans divers emplacements. Les utilisateurs qui travaillent sur le même projet peuvent être amenés à échanger des messages à propos du projet, et sont également susceptibles d'accéder à des documents partagés stockés sur les partages de fichiers ou sur un site SharePoint® Server 2013.



Les boîtes aux lettres de site dans Exchange Server 2013 offrent un service mieux intégré aux utilisateurs qui doivent collaborer. Les boîtes aux lettres de site permettent aux utilisateurs d'accéder à la fois aux documents stockés sur SharePoint 2013 ainsi qu'aux messages électroniques stockés dans une boîte aux lettres Exchange Server 2013 à l'aide de la même interface client.

Comprendre le fonctionnement des boîtes aux lettres de site

Une boîte aux lettres de site permet l'intégration entre un site SharePoint et une boîte aux lettres Exchange. Par exemple, un groupe d'utilisateurs peut travailler sur un projet nécessitant une communication par e-mail ainsi qu'un processus d'examen de documents. Grâce aux boîtes aux lettres de site, les utilisateurs peuvent envoyer et lire des messages électroniques dans la boîte aux lettres de site. Les utilisateurs peuvent également publier des documents et les passer en revue sur le site SharePoint.

L'utilité des boîtes aux lettres de site réside dans le fait que les utilisateurs peuvent accéder à deux types de contenus à partir d'une seule et même interface. Les boîtes aux lettres de site sont disponibles dans Outlook 2013 et peuvent être utilisées pour visualiser à la fois les e-mails de la boîte aux lettres et les documents stockés dans SharePoint. Le même contenu est également accessible directement à partir du site SharePoint. Avec les boîtes aux lettres de site, Exchange stocke les courriers électroniques, offrant aux utilisateurs les mêmes conversations par courriers électroniques qu'ils utilisent chaque jour pour leurs propres boîtes aux lettres. SharePoint enregistre les documents et fournit les outils avancés de gestion de documents, tels que le contrôle de version.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des boîtes aux lettres de site

Les boîtes aux lettres de site sont gérées via SharePoint. Pour implémenter des boîtes aux lettres de site, il convient de configurer le protocole SSL (Secure Sockets Layer) ainsi que la norme d'autorisation OAuth entre le serveur SharePoint 2013 et le serveur Exchange Server 2013.

Une fois l'intégration configurée, les administrateurs ou les utilisateurs délégués peuvent créer des boîtes aux lettres de site sur le serveur SharePoint à l'aide de l'application Boîte aux lettres de site. Les utilisateurs Outlook peuvent ensuite ajouter la boîte aux lettres de site à leur profil Outlook 2013.

Gestion des boîtes aux lettres de site avec des stratégies

Les boîtes aux lettres de site peuvent être gérées à la fois à l'aide de stratégies Exchange Server 2013 et de stratégies SharePoint 2013.

Dans Exchange, vous pouvez configurer les quotas de boîte aux lettres de site à l'aide des applets de commande **SiteMailboxProvisioningPolicy** dans l'environnement de ligne de commande Exchange Management Shell. Vous pouvez configurer la taille maximale de la boîte aux lettres de site de même que la taille maximale des messages qui peuvent être envoyés à la boîte aux lettres.

Dans SharePoint, vous pouvez configurer les stratégies pour les personnes habilitées à créer des boîtes aux lettres de site, ou vous pouvez configurer les stratégies de cycle de vie SharePoint pour gérer la durée de vie d'une boîte aux lettres de site. Vous pouvez, par exemple, créer une stratégie de cycle de vie dans SharePoint qui ferme automatiquement toutes les boîtes aux lettres de site au bout de six mois. Lorsque l'application du cycle de vie dans SharePoint ferme une boîte aux lettres de site, cette dernière est conservée dans SharePoint pour une période définie. La boîte aux lettres peut être ensuite réactivée par l'utilisateur de la boîte aux lettres ou par un administrateur SharePoint.

Après la période de rétention, la boîte aux lettres du site Exchange de la base de données de boîtes aux lettres aura le préfixe MDEL: ajouté au nom de boîte aux lettres pour indiquer qu'il a été marqué pour la suppression. Les boîtes aux lettres ne sont pas supprimées automatiquement d'Exchange ; vous devez les supprimer manuellement.

Gestion de la conformité

Les boîtes aux lettres de site peuvent faire partie de l'étendue eDiscovery (découverte électronique) sur place de SharePoint 2013 lorsque vous effectuez des recherches par mot-clé dans les boîtes aux lettres d'utilisateur ou les boîtes aux lettres de site. En outre, sachez que vous pouvez bloquer une boîte aux lettres de site pour des raisons juridiques.

 **Remarque :** Pour plus d'informations sur la configuration des boîtes aux lettres de site, consultez la page Configurer des boîtes aux lettres du site dans SharePoint Server 2013, à l'adresse http://go.microsoft.com/fwlink/?LinkId=290960.

Définition d'une boîte aux lettres partagée

De nombreuses organisations ont besoin que plusieurs utilisateurs accèdent à la même boîte aux lettres. Par exemple, une organisation peut fournir une adresse de messagerie telle qu'info@adatum.com sur un site Internet public. L'organisation est susceptible de vouloir que plusieurs utilisateurs surveillent la boîte aux lettres associée à l'adresse de messagerie dans le but de garantir des réponses rapides aux clients potentiels. Dans les versions précédentes d'Exchange Server, vous pouviez créer une boîte aux lettres à cet effet, puis donner à plusieurs utilisateurs l'accès à cette boîte aux lettres.

- Les boîtes aux lettres partagées sont utilisées pour fournir à plusieurs utilisateurs l'accès à une boîte aux lettres commune
- Les boîtes aux lettres partagées peuvent être créées en une seule étape dans le CAE ou dans l'environnement de ligne de commande Exchange Management Shell
- Les autorisations Accès total et Envoyer en tant que peuvent être accordées aux utilisateurs

Exchange Server 2013 simplifie le processus de création de ce type de boîte aux lettres en proposant des boîtes aux lettres partagées. Une boîte aux lettres partagées est un type particulier de boîte aux lettres d'utilisateur dans laquelle le compte d'utilisateur associé à la boîte aux lettres est un compte désactivé, et d'autres utilisateurs ont le droit d'accéder à la boîte aux lettres en question. Pour y accéder, les utilisateurs autorisés se connectent à leurs propres boîtes aux lettres, puis ouvrent une boîte aux lettres partagée en ajoutant la boîte aux lettres partagée à leur profil Outlook ou en accédant à la boîte aux lettres via Outlook Web App.

Remarque : Lorsqu'un profil Outlook d'utilisateur est configuré en mode de cache, toutes les boîtes aux lettres, pour lesquelles l'utilisateur dispose d'un accès complet, seront téléchargées et mises en mémoire cache sur l'ordinateur virtuel. Ce comportement peut être modifié de telle sorte que les boîtes aux lettres principales et les dossiers (hors courriers électroniques), tels que les dossiers Calendrier, Contacts et Tâches, soient mis en mémoire cache pour les autres boîtes aux lettres. Vous pouvez modifier le registre ou utiliser les objets de stratégie de groupe pour configurer ce paramètre. Pour plus d'informations, consultez la page http://go.microsoft.com/fwlink/?LinkId=290961.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans Exchange Server 2013, la création d'une boîte aux lettres partagée se fait en une seule étape à l'aide du CAE ou de l'environnement de ligne de commande Exchange Management Shell. Vous pouvez créer une boîte aux lettres partagée et accorder aux utilisateurs les autorisationsAccès total et Envoyer en tant au moment de sa création.

Quand vous accordez à un utilisateur l'accès total à la boîte aux lettres partagée, l'utilisateur délégué peut se connecter à la boîte aux lettres, et visualiser et gérer tous les messages de la boîte aux lettres. Toutefois, un délégué doté d'une autorisation Accès total ne peut pas envoyer de messages à partir de la boite aux lettres partagée. Pour ce faire, il doit disposer de l'autorisation Envoyer en tant que. Lorsqu'un utilisateur, doté de l'autorisation Envoyer en tant que, envoie un message à partir de la boîte aux lettres déléguée, tout message envoyé à partir de la boîte aux lettres apparaîtra comme s'il avait été envoyé par le propriétaire de la boîte aux lettres.

 **Remarque :** Vous pouvez également permettre aux utilisateurs délégués d'accéder aux boîtes aux lettres normales plutôt que de créer des boîtes aux lettres partagées. Lorsque vous configurez l'accès délégué à une boîte aux lettres normale, vous pouvez également accorder une autorisation Envoyer de la part de. Cette autorisation permet à un utilisateur délégué d'envoyer des messages de la boîte aux lettres, mais l'adresse De : d'un message envoyé par le délégué montre que ce message a été envoyé par le délégué au nom du propriétaire de la boîte aux lettres.

Démonstration : Création d'une boîte aux lettres partagée

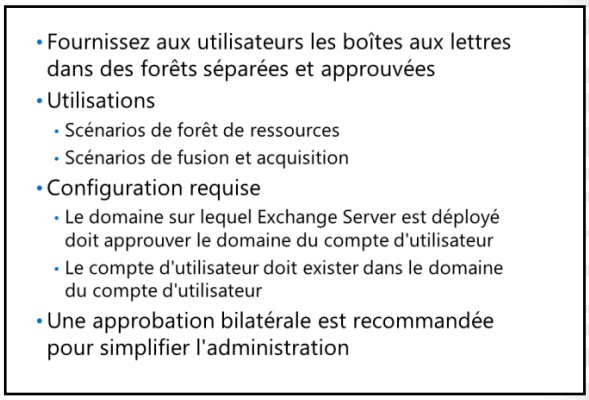
Dans cette démonstration, vous allez apprendre à configurer une boîte aux lettres partagée et accéder à la boîte aux lettres via Outlook 2013 et Outlook Web App.

Procédure de démonstration

1. Sur LON-CAS1, dans le CAE, créez une boîte aux lettres partagée avec les informations suivantes :
   - Nom complet : **Sales Information**
   - Adresse de messagerie : **salesInfo**
   - Octroyez l'autorisation d'accès complet à **Aidan Delany** et **Amr Zaki**
   - Base de données de boîtes aux lettres : **Mailbox Database 1**
2. Sur LON-CAS1, ouvrez une session sur Outlook Web App en tant qu'**Administrateur**, puis envoyez un message à la boîte aux lettres **Sales Information**.
3. Sur LON-CL1, connecté en tant qu'Aidan, basculez sur Outlook 2013 et vérifiez que le dossier Sales Information est affiché.
4. Répondez au message envoyé à la boîte aux lettres Sales Information.
5. Accédez à Outlook Web App en tant qu'Amr, et ouvrez la boîte aux lettres **Sales Information**.

Définition des boîtes aux lettres liées

Les boîtes aux lettres liées sont les boîtes aux lettres pour les utilisateurs dont les comptes principaux se situent dans une forêt séparée et approuvée. Les utilisateurs disposant d'une boîte aux lettres liée se connectent à leur domaine Active Directory local via les informations d'identification locales, lesquelles sont ensuite utilisées pour accéder à une boîte aux lettres au sein d'une organisation Exchange dans une forêt différente.



Les boîtes aux lettres liées peuvent être utiles dans les deux scénarios suivants :

- Les organisations déploient Exchange dans une forêt de ressources. Quand les organisations déploient Exchange dans un scénario de forêt de ressources, ils déploient Exchange dans une forêt Active Directory, tout en permettant d'accéder à l'organisation Exchange avec des comptes d'utilisateur situés dans une ou plusieurs forêts approuvées (appelées forêts de comptes).
- Les organisations utilisent les boîtes aux lettres liées dans un scénario de fusion ou acquisition. Dans ce scénario, les deux organisations peuvent déployer le serveur Exchange avant la fusion ou l'acquisition. Les boîtes aux lettres liées offre l'occasion de supprimer le déploiement du serveur Exchange de l'une des deux organisations. Les utilisateurs d'une des deux organisations peuvent être configurés avec les boîtes aux lettres liées dans l'autre organisation. Cela garantit que les utilisateurs des deux organisations figurent sur la même liste d'adresses globale et que les informations sur la disponibilité sont à la disposition de tous les utilisateurs.

En configurant une boîte aux lettres liée, le compte d'utilisateur qui est utilisé pour accéder à la boîte aux lettres liée n'existe pas dans la forêt dans laquelle Exchange est déployé. Lorsque vous créez la boîte aux lettres liée, un compte d'utilisateur désactivé est crée dans le domaine où Exchange est déployé et associé à la boîte aux lettres liée. Le compte d'utilisateur de la forêt de comptes dispose du contrôle total de la boîte aux lettres.

Pour implémenter les boîtes aux lettres liées, procédez comme suit :

- Configurez une approbation unilatérale dans laquelle le domaine de déploiement d'Exchange approuve le domaine dans lequel le compte d'utilisateur existe. Cela peut être une approbation externe ou une approbation de forêt. Sachez que l'approbation unilatérale est indispensable.
- Vérifiez que le compte d'utilisateur existe dans la forêt de comptes avant de créer une boîte aux lettres liée. Vous ne pouvez pas créer le compte d'utilisateur lorsque vous créez la boîte aux lettres liée.
- Outre la configuration de l'approbation unilatérale, vous devez également envisager de créer une approbation bilatérale entre les domaines. Cette dernière n'est pas obligatoire, mais le compte qui crée la boîte aux lettres liée doit être autorisé à modifier l'objet utilisateur dans la forêt de comptes. Si vous n'implémentez pas d'approbation bilatérale, vous devrez fournir les informations d'identification de l'administrateur de forêt de comptes lors de la création de la boîte aux lettres liée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Gestion d'autres destinataires Exchange

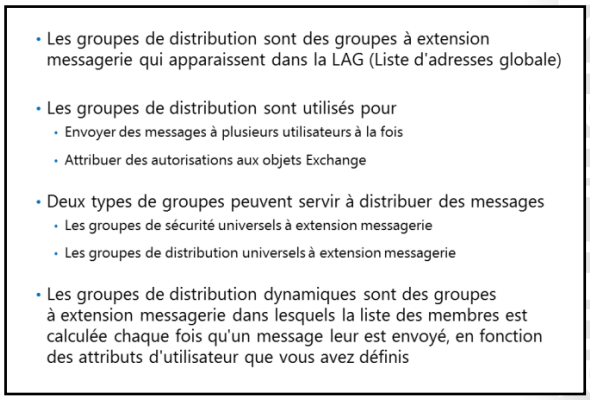
Exchange Server 2013 fournit plusieurs autres types de destinataires sans compter les différents types de boîtes aux lettres. Ces destinataires incluent les groupes de distribution, qui sont utilisés pour envoyer des courriers électroniques aux groupes de destinataires et pour attribuer des autorisations au sein d'une organisation Exchange Server, des contacts de messagerie et des utilisateurs de messagerie. Cette leçon fournit une vue d'ensemble de ces types de destinataires et décrit comment les gérer.

Objectifs de la leçon

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

- décrire les groupes de distribution ;
- créer et configurer des groupes de distribution ;
- configurer la gestion en libre-service des groupes de distribution ;
- gérer les contacts de messagerie et les utilisateurs de messagerie ;
- configurer les boîtes aux lettres de site.

Définition des groupes de distribution



Dans Exchange Server, les groupes de distribution sont des groupes à extension messagerie. Lorsque vous disposez d'un groupe à extension messagerie, Exchange Server 2013 attribue une adresse de messagerie au groupe, et le groupe par défaut est ajouté à la LAG. Vous pouvez utiliser les groupes à extension messagerie pour permettre aux utilisateurs d'envoyer des courriers électroniques à plusieurs destinataires. Les groupes de sécurité à extension messagerie vous permettent également d'attribuer des autorisations simultanément à plusieurs utilisateurs pour les objets Exchange Server, tels que les boîtes aux lettres partagées et les dossiers publics.

Dans Exchange Server 2013, vous pouvez créer deux types de groupes à extension messagerie :

- *Groupes de sécurité universels*. Outre le fait d'être utilisés comme groupe de distribution Exchange Server 2013, les groupes de sécurité universels des services de domaine Active Directory permettent d'attribuer des autorisations aux ressources du réseau.
- *Groupes de distribution universels*. Les groupes de distribution universels d'Active Directory peuvent être utilisés uniquement pour regrouper les destinataires des messages électroniques ; ils ne peuvent pas être utilisés pour accorder des autorisations d'accès aux ressources du réseau.

Groupes de distribution dynamiques

Exchange Server 2013 prend également en charge les groupes de distribution dynamiques. Les groupes de distribution dynamiques sont les objets de groupe à extension messagerie qui n'ont pas de liste de membres préconfigurée. À la place, la liste des membres des groupes de distribution dynamiques est calculée chaque fois qu'un message est envoyé au groupe.

Lorsque vous configurez une liste de distribution dynamique, vous pouvez définir l'appartenance au groupe selon divers filtres et conditions. Par exemple, vous pouvez créer une liste de distribution dynamique qui comprend tous les utilisateurs dans un bâtiment spécifique ou tous les utilisateurs dans une unité d'organisation spécifique. Lorsqu'un message électronique est envoyé à un groupe de distribution dynamique, le serveur Exchange interroge un serveur de catalogues global à la recherche de tous les destinataires de l'organisation qui correspondent aux critères définis pour ce groupe. Le serveur Exchange complète ensuite le groupe selon la requête, et remet le courrier électronique aux utilisateurs.

Démonstration : Création et configuration de groupes de distribution

Au cours de cette démonstration, vous allez apprendre à configurer divers types de groupes de distribution.

Remarque : Dans le CAE, vous ne pouvez activer la messagerie pour un groupe de sécurité ou de distribution universel existant. Pour ce faire, utilisez l'applet de commande **Enable-DistributionGroup**.

Procédure de démonstration

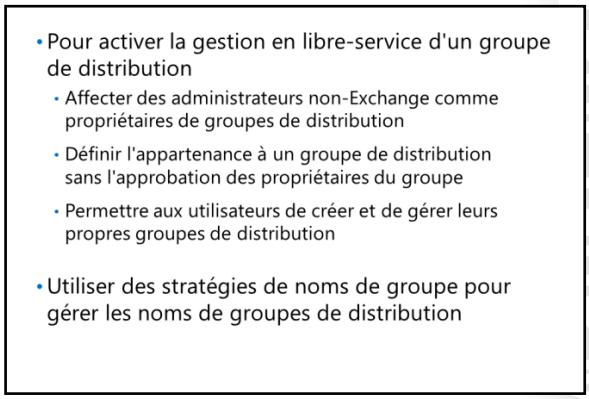
1. Sur LON-CAS1, connectez-vous au Centre d'administration Exchange en tant qu'**ADATUM\Administrateur**.
2. Créez un groupe de distribution avec les paramètres suivants :
   - Nom complet : **Sales Managers**
   - Alias : **SalesManagers**
   - Unité d'organisation : **Sales**
   - Membres : **Bonnie Kearney, Dennis Bye**
   - Choisissez si l'approbation du propriétaire du groupe est requise pour rejoindre ce dernier : **Fermé**
   - Choisir s'il est possible de quitter le groupe : **Fermé**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Créez un groupe de distribution de sécurité avec les paramètres suivants :
   - Nom complet : **IT Managers**
   - Alias : **ITManagers**
   - Unité d'organisation : **IT**
   - Membres : **April Reagan, Magnus Hedlund**
   - Choisissez si l'approbation du propriétaire du groupe est requise pour rejoindre ce dernier : **Sélectionné**
4. Configurer le groupe pour exiger la modération des messages, désigner **Amr Zaki** comme modérateur et configurer le groupe IT de sorte qu'il soit habilité à effectuer des envois au groupe sans modération.
5. Créez un groupe de distribution dynamique avec les paramètres suivants :
   - Nom complet : **Developers**
   - Alias : **Developers**
   - Unité d'organisation : **Development**
   - Propriétaire : **Les membres du groupe Administrator comprennent chaque membre du groupe Development**

Implémentation de la gestion d'un groupe de distribution en libre-service

Dans certaines organisations, la gestion des groupes de distribution peut s'avérer complexe et demander du temps. Les listes des membres de groupes de distribution doivent être mises à jour fréquemment, et il n'est pas toujours évident de savoir quels utilisateurs doivent être ajoutés aux différents groupes de distribution. Les administrateurs des unités commerciales ou les responsables de projet sont souvent les mieux placés pour déterminer qui ajouter aux groupes de distribution spécifiques. Dans certains cas, les organisations sont susceptibles d'accorder aux utilisateurs la capacité de s'ajouter eux-mêmes à certains groupes de distribution.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exchange Server 2013 offre les options suivantes pour activer la gestion des groupes de distribution en libre-service :

- Affecter des administrateurs non-Exchange comme propriétaires de groupes de distribution. Grâce à cette option, les administrateurs Exchange disposant des autorisations adéquates créent des groupes de distribution, puis attribuent d'autres utilisateurs ou groupes comme propriétaires des groupes. Les propriétaires de groupes peuvent gérer l'appartenance au groupe en accédant aux propriétés du groupe dans Outlook ou via Outlook Web App.

 **Remarque :** Dans Exchange Server 2013, vous ne pouvez ajouter que des boîtes aux lettres individuelles en tant que propriétaires d'un groupe de distribution. Dans la mise à jour cumulative 1 (CU1) d'Exchange Server 2013, vous pouvez attribuer d'autres groupes en tant que propriétaires de groupes de distribution.

- Définir l'appartenance à un groupe de distribution sans l'approbation des propriétaires du groupe. Vous pouvez configurer des groupes de distribution de façon à permettre aux utilisateurs de rejoindre automatiquement ces groupes ou à spécifier qu'une approbation est nécessaire pour rejoindre ces groupes. Les options de configuration varient selon que le groupe de distribution est un groupe de sécurité ou non.
    - Pour les groupes de distribution de sécurité, vous pouvez configurer le groupe de façon à exiger l'approbation du propriétaire pour rejoindre les groupes. Seuls les propriétaires peuvent supprimer des membres des groupes de sécurité.
    - Pour les groupes de distribution qui ne sont pas des groupes de sécurité, vous pouvez configurer l'appartenance au groupe en choisissant le paramètre Ouvert ; autrement dit, quiconque peut rejoindre ou quitter le groupe de manière automatique, sans demander l'approbation des propriétaires du groupe en question. Vous pouvez également configurer le groupe de façon à exiger l'approbation du propriétaire dans le cadre de toute demande à rejoindre le groupe. Dans ce scénario, les utilisateurs peuvent demander à rejoindre le groupe, et cela sera effectif une fois que le propriétaire aura validé la demande.
- Permettre aux utilisateurs de créer et de gérer leurs propres groupes de distribution. Vous pouvez également permettre aux utilisateurs de créer des groupes de distribution à l'aide de la page Options d'Outlook Web App. Pour permettre aux utilisateurs de créer des groupes de distribution, vous devez modifier la Stratégie d'attribution de rôle par défaut ou créer une Stratégie d'attribution de rôle et activer le rôle Mes groupes de distribution. Cette option permet aux utilisateurs de créer des groupes de distribution à extension messagerie et de gérer les groupes qu'ils possèdent.

Configuration des stratégies de noms de groupe

Si vous permettez aux utilisateurs de créer leurs propres groupes, vous êtes susceptibles de toujours vouloir conserver un certain contrôle sur les noms attribués aux groupes de distribution. Vous pouvez configurer une stratégie de noms de groupe pour gérer les noms attribués aux groupes de distribution créés par les utilisateurs. Dans la stratégie de noms de groupe, vous pouvez configurer un préfixe et un suffixe qui seront ajoutés au nom d'un groupe de distribution lorsqu'il sera créé. Vous avez également la possibilité de bloquer certains mots afin qu'ils ne soient pas utilisés. Une fois une stratégie de noms de groupe configurée, les utilisateurs fournissent le nom complet pour le groupe auquel s'applique le préfixe ou le suffixe, que vous avez défini dans la stratégie de noms de groupe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration de la gestion des groupes de distribution en libre-service

Au cours de cette démonstration, vous allez apprendre à configurer deux options différentes pour la gestion des groupes en libre-service. Vous étudierez comment créer un groupe dont la liste de membres est ouverte, et valider que les utilisateurs peuvent rejoindre ce groupe sans l'approbation du propriétaire. Vous apprendrez également à créer une stratégie de noms de groupe, et permettrez aux utilisateurs de créer et de gérer leurs propres groupes.

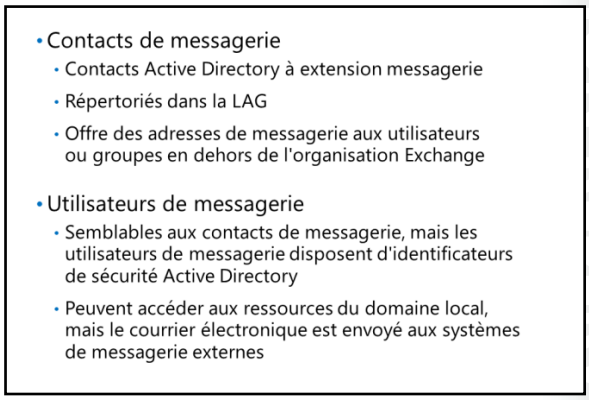
Remarque : Dans cette démonstration, vous accordez à tous les utilisateurs le droit de créer des groupes de distribution en modifiant la Stratégie d'attribution de rôles par défaut. Pour limiter le nombre d'utilisateurs habilités à créer des groupes de distribution, créez une stratégie d'attribution de rôles par défaut, qui accorde l'autorisation de créer des groupes de distribution, puis attribuez cette stratégie d'attribution de rôles aux utilisateurs sélectionnés.

Procédure de démonstration

1. Sur LON-CAS1, connectez -vous au CAE et créez un groupe de distribution intitulé **TechDiscussion** et dont le paramètre Ouvert indique que l'appartenance au groupe ne nécessite pas l'approbation de son propriétaire.
2. Dans LON-CL1, connectez-vous à Outlook Web App en tant qu'**Amr**.
3. Accédez à la page **Options d'Outlook Web App**, et vérifiez qu'Amr peut rejoindre le groupe de distribution **TechDiscussion**.
4. Sur LON-CAS1, dans le Centre d'administration Exchange, créez une stratégie de noms de groupe de distribution attribuant un suffixe **EmailDL_** et un suffixe avec l'attribut de société.
5. Activez l'option **Mes groupes de distribution** pour la **Stratégie d'attribution de rôle par défaut**.
6. Dans LON-CL1, connectez-vous à Outlook Web App en tant qu'**Aidan**.
7. Accédez à la page Options d'Outlook Web App, et créez un groupe de distribution nommé **EXAdmins**.
8. Vérifiez que la stratégie de noms de groupe est appliquée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Gestion des contacts de messagerie et des utilisateurs de messagerie



Les contacts de messagerie sont des contacts Active Directory à extension messagerie. Ces contacts contiennent des informations sur les personnes ou les organisations qui existent en dehors de votre organisation Exchange Server. Vous pouvez afficher les contacts de messagerie dans la liste d'adresses globale (LAG) ainsi que dans d'autres listes d'adresses, et vous pouvez les ajouter en tant que membres des groupes de distribution. Chaque contact dispose d'une adresse de messagerie externe, et tous les messages électroniques qui sont envoyés à un contact sont envoyés automatiquement à cette adresse.

Si plusieurs personnes de votre organisation contactent une personne externe de confiance, vous pouvez créer un contact de messagerie à partir de l'adresse de messagerie de cette personne. Cela permet aux utilisateurs Exchange Server de sélectionner cette personne à partir de la liste d'adresses globale (LAG) pour l'envoi de messages électroniques.

Utilisateurs de messagerie

Les utilisateurs de messagerie sont similaires aux contacts de messagerie. Les utilisateurs de messagerie, comme les contacts de messagerie, disposent d'adresses électroniques externes, contiennent des informations sur des personnes en dehors de votre organisation Exchange Server, et vous pouvez les afficher tous dans la liste d'adresses globale (LAG) de même que dans d'autres listes d'adresses. Cependant, à la différence des contacts de messagerie, les utilisateurs de messagerie possèdent des informations d'identification d'ouverture de session Active Directory et un identificateur de sécurité (SID) afin de leur permettre d'accéder aux ressources du réseau auxquelles ils ont l'autorisation d'accéder.

Si une personne externe à votre organisation a besoin d'accéder aux ressources de votre réseau, vous devrez créer un utilisateur de messagerie au lieu d'un contact de messagerie pour cette personne en question. Par exemple, vous pouvez créer des utilisateurs de messagerie pour les consultants temporaires qui ont besoin d'accéder à l'infrastructure du serveur mais qui utiliseront leur propre adresse électronique externe.

Dans un autre scénario, vous pouvez créer des utilisateurs de messagerie pour lesquels vous ne souhaitez pas gérer une boîte aux lettres Exchange Server. Par exemple, après une acquisition, la société acquise peut gérer sa propre infrastructure de messagerie, mais elle peut aussi avoir besoin d'accéder aux ressources de votre réseau. Pour ces utilisateurs, vous pouvez créer des utilisateurs de messagerie au lieu d'utilisateurs de boîte aux lettres.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Planification et implémentation des boîtes aux lettres de dossiers publics

Exchange Server 2013 a subi une modification considérable dans la manière d'implémenter les dossiers publics. Dans les versions antérieures d'Exchange Server, les dossiers publics étaient stockés dans une base de données de dossiers publics dédiée. Les bases de données de dossiers publics ne pouvaient pas être répliquées dans un groupe de disponibilité de base de données (DAG) ; elles avaient donc recours à la réplication des dossiers publics pour fournir un haut niveau de disponibilité et de redondance. Dans Exchange Server 2013, les dossiers publics sont désormais enregistrés dans les bases de données de boîtes aux lettres normales plutôt que dans des bases de données dédiées.

Cette leçon fournit une vue d'ensemble de la manière dont les dossiers publics sont implémentés dans Exchange Server 2013 et décrit comment créer et gérer les dossiers publics.

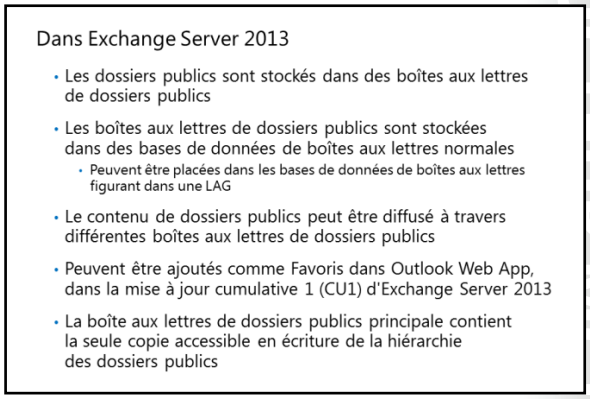
Objectifs de la leçon

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

- décrire comment les dossiers publics sont implémentés dans Exchange Server 2013 ;
- gérer les dossiers publics ;
- configurer les boîtes aux lettres de dossiers publics et les dossiers publics ;
- décrire les éléments à prendre en compte pour implémenter les dossiers publics.

Utilisation des dossiers publics dans Exchange Server 2013

Les dossiers publics étaient disponibles dans toutes les versions antérieures d'Exchange Server. De nombreuses organisations utilisent les dossiers publics comme moyen de partager les informations entre les groupes d'utilisateurs. Avec les dossiers publics, plusieurs utilisateurs peuvent accéder à un dossier partagé dans Outlook.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans Exchange Server 2013, l'architecture sous-jacente pour les dossiers publics a changé entièrement sans modifier considérablement l'expérience utilisateur en ce qui concerne les dossiers publics. Dans Exchange Server 2013 :

- Les dossiers publics sont stockés dans un type particulier de boîte aux lettres appelée boîte aux lettres de dossiers publics. Dans les versions antérieures d'Exchange Server, les dossiers publics étaient stockés dans une base de données de dossiers publics distincte. Dans Exchange Server 2013, les boîtes aux lettres de dossiers publics sont stockées dans des bases de données de boîtes aux lettres normales. La boîte aux lettres de dossiers publics stocke la hiérarchie des dossiers publics ainsi que les contenus de dossiers publics.
- Les boîtes aux lettres de dossiers publics peuvent être stockées dans des bases de données de boîtes aux lettres qui font partie d'un DAG. Dans les versions précédentes d'Exchange Server, les dossiers publics utilisaient un processus de réplication des dossiers publics pour permettre la redondance. En stockant les boîtes aux lettres de dossiers publics dans une base de données de boîtes aux lettres appartenant à un DAG, vous pouvez offrir un haut niveau de disponibilité pour le déploiement des dossiers publics à l'aide du même mécanisme que celui utilisé pour la haute disponibilité des boîtes aux lettres.
- Les dossiers publics sont diffusés à travers différentes boîtes aux lettres de dossiers publics. Dans les versions précédentes d'Exchange Server, vous pouviez répliquer le contenu des dossiers publics vers des bases de données de dossiers publics situées dans différents emplacements pour améliorer l'accès client au contenu des dossiers publics. Dans Exchange Server 2013, vous pouvez créer des dossiers publics et les stocker dans différentes boîtes aux lettres, qui peuvent se trouver sur des serveurs de boîtes aux lettres dans différents emplacements.

Remarque : Une différence importante entre la réplication des dossiers publics dans les versions précédentes d'Exchange Server et la distribution des dossiers publics sur plusieurs boîtes lettres dans Exchange Server 2013 réside dans le fait que dans Exchange Server 2013 vous ne pouvez avoir qu'une seule copie des données. Dans les versions antérieures d'Exchange Server, vous pouvez avoir plusieurs copies du contenu des dossiers publics, et la réplication des dossiers publics est un processus sur plusieurs maîtres. Dans Exchange Server 2013, vous ne pouvez enregistrer le contenu des dossiers publics que dans une boîte aux lettres, et tous les clients doivent accéder à cette boîte aux lettres pour voir ce contenu. Si vous placez la boîte aux lettres de dossiers publics dans une base de données faisant partie d'un DAG, la boîte aux lettres est hautement disponible, mais tous les clients ont encore accès à la boîte aux lettres dans la copie active de la base de données.

- Les clients peuvent accéder aux dossiers publics uniquement sur Outlook 2007 ou toute version ultérieure. Dans Exchange Server 2013, les clients Outlook Web Access ne peuvent pas accéder aux dossiers publics. Dans la mise à jour cumulative 1 (CU1) d'Exchange Server 2013, vous pouvez ajouter les dossiers publics situés sur Exchange 2013 comme Favoris dans Outlook Web App.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour implémenter les dossiers publics dans Exchange Server 2013, vous devez d'abord créer une boîte aux lettres de hiérarchie de dossiers publics principale. La boîte aux lettres de dossiers publics principale contient la seule copie accessible en écriture de la hiérarchie des dossiers publics. Une fois la boîte aux lettres de dossiers publics principale créée, vous pouvez créer des boîtes aux lettres de dossiers publics supplémentaires en tant que boîtes aux lettres de dossiers publics secondaires. Les dossiers publics secondaires contiendront les versions en lecture seule de la hiérarchie des dossiers publics.

Une fois la boîte aux lettres de dossiers publics principale créée, vous pouvez commencer à créer des dossiers publics. Par défaut, tous les dossiers publics sont créés dans la boîte aux lettres de dossiers publics principale. Si vous créez une boîte aux lettres de dossiers publics secondaire, vous pouvez créer des dossiers publics dans la boîte aux lettres de dossiers publics secondaire uniquement si vous créez le dossier public à l'aide de l'applet de commande **new-publicfolder** avec le paramètre **–mailbox**.

Gestion des dossiers publics

Une fois les boîtes aux lettres de dossiers publics et les dossiers publics créés, vous aurez peut être besoin d'effectuer plusieurs tâches de gestion supplémentaires sur les dossiers publics.

La gestion des dossiers publics comprend les points suivants

- Configuration des autorisations de dossiers publics
- Activation de la messagerie pour les dossiers publics
- Gestion des paramètres de quota et de rétention
- Contrôle des dossiers publics

Configurer les autorisations de dossiers publics

Dans Exchange Server 2013, des autorisations administratives pour gérer les dossiers publics sont activées via le contrôle d'accès basé sur un rôle (RBAC). Pour accorder aux utilisateurs l'autorisation de gérer les dossiers publics, vous devez les ajouter au groupe de rôle Gestion des dossiers publics.

De nombreuses organisations configurent également les autorisations des clients ou les droits d'accès des utilisateurs aux dossiers publics. Ces autorisations sont utilisées pour limiter les actions des utilisateurs dans les dossiers publics. Les autorisations des clients n'ont pas changé par rapport aux versions précédentes d'Exchange Server. Vous pouvez octroyer des autorisations aux utilisateurs à l'aide de rôles, tels que Propriétaire, Éditeur de publication ou Auteur. Ces rôles comprennent plusieurs types d'accès. Le rôle Éditeur de publication, par exemple, dispose des autorisations suivantes : Créer des éléments, Lire des éléments, Créer des sous-dossiers, Afficher le contenu du dossier, Modifier, Modifier tout, Supprimer, Supprimer tout. Vous pouvez également attribuer des autorisations personnalisées à l'aide d'une variété de droits d'accès.

Vous pouvez configurer les autorisations de clients dans le CAE en sélectionnant le dossier public et en cliquant sur **Gérer** sous **Autorisations d'accès aux dossiers**. En outre, vous pouvez configurer les autorisations des clients en accédant aux propriétés des dossiers publics dans Outlook, ou à l'aide des applets de commande **Add-PublicFolderClientPermission** et **Remove-PublicFolderClientPermission**.

Lorsque vous créez un dossier public, il hérite automatiquement des mêmes autorisations clients que le dossier public parent. Lorsque vous changez les autorisations sur un dossier parent, vous avez la possibilité d'appliquer à tous les sous-dossiers la modification des autorisations en question. Les autorisations par défaut attribuées aux nouveaux dossiers racines sont les suivantes : Auteur pour les utilisateurs authentifiés et Aucune pour les utilisateurs anonymes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Activer la messagerie pour les dossiers publics

L'activation de la messagerie pour un dossier public génère une adresse SMTP qui est répertoriée dans la LAG. Les utilisateurs peuvent ensuite publier les messages vers le dossier public en envoyant des messages électroniques par son intermédiaire. Lorsqu'un dossier public est doté d'une extension messagerie, vous pouvez configurer des paramètres supplémentaires sur le dossier public tel que les adresses de messagerie et les quotas de messagerie. Vous pouvez activer la messagerie pour un dossier public dans le CAE en sélectionnant le dossier public, puis en cliquant sur **Activer** sous **Paramètres de messagerie**. Vous pouvez également utiliser l'applet de commande **Enable-MailPublicFolder**.

Gérer les limites de quotas et les paramètres de rétention

Vous pouvez gérer les limites de quotas par défaut et les paramètres de rétention pour tous les dossiers publics de l'organisation à l'aide de l'applet de commande **Set-OrganizationConfig**. Vous pouvez également configurer ces paramètres dans des dossiers publics individuels à l'aide de l'applet de commande **Set-PublicFolder**.

Analyser les dossiers publics

Exchange Server 2013 fournit plusieurs applets de commande utilisables pour analyser et gérer les dossiers publics :

- **Get-PublicFolderItemStatistics**. Affiche des informations relatives aux éléments d'un dossier public spécifique. Parmi les informations figurent les éléments suivants : le sujet, la dernière date de modification, la dernière date d'accès, la date de création, les pièces jointes, la taille du message et le type d'élément.
- **Get-PublicFolderStatistics**. Affiche les informations statistiques relatives à tous les dossiers publics, tels que la taille du dossier et la dernière connexion.
- **Get-PublicFolderMailboxDiagnostics**. Affiche les informations au niveau de l'événement à propos d'une boîte aux lettres de dossiers publics. Ces informations peuvent être utilisées pour résoudre les problèmes de dossiers publics.
- **Update-PublicFolderMailbox**. Utilisé pour mettre à jour la hiérarchie des dossiers publics.

Démonstration : Création et configuration des dossiers publics

Dans cette démonstration, vous découvrirez comment créer et configurer les dossiers publics dans Exchange Server 2013. Vous apprendrez également à configurer les autorisations de dossiers publics dans le CAE.

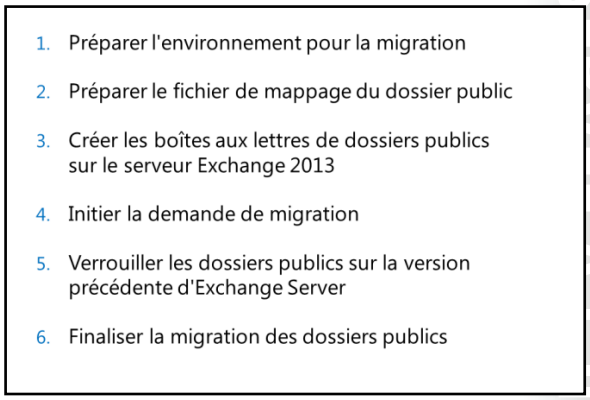
Procédure de démonstration

1. Sur LON-CAS1, dans le CAE, créez deux nouvelles boîtes aux lettres de dossiers publics **PFMBX1** et **PFMBX2**.
2. Créez un dossier public nommé **Departments**.
3. Créez un dossier public enfant au niveau du dossier public **Departments** intitulé **IT**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Ouvrez l'environnement de ligne de commande Exchange Management Shell et utilisez l'applet de commande **Get-PublicFolder** pour afficher les propriétés des dossiers publics.
5. Utilisez l'applet de commande **New-PublicFolder** pour créer le dossier public **Research** en tant que sous-dossier du dossier **Departments**, et placez le dossier public dans la boîte aux lettres **PFMBX2**.
6. Configurez le compte administrateur comme propriétaire du dossier **Departments** et de tous les sous-dossiers.

Migration des dossiers publics vers Exchange Server 2013



En raison de la nouvelle architecture des dossiers publics d'Exchange Server 2013, il est plus difficile de migrer les dossiers publics à partir de versions antérieures d'Exchange Serveur que ce n'était le cas dans les versions précédentes. Pour effectuer la migration en question, vous devez copier le contenu des dossiers publics à partir du correctif cumulatif 10 pour Exchange Server 2007 SP3 ou d'Exchange Server 2010 SP3 vers les boîtes aux lettres de dossiers publics Exchange Server 2013, puis basculer tous les accès aux dossiers publics sur le nouvel environnement. Pour vous aider à effectuer la migration, Exchange Server 2013 fournit plusieurs nouveaux applets de commande ***PublicFolderMigrationRequest**, en sus de différents scripts PowerShell. Ces applets de commande utilisent le service de réplication des boîtes aux lettres Microsoft Exchange pour exécuter la migration.

Les principales étapes d'exécution de la migration des dossiers publics à partir d'Exchange 2010 sont répertoriées ci-après. Vous pouvez utiliser les mêmes étapes pour migrer les dossiers publics à partir d'Exchange Server 2007.

1. Préparer l'environnement pour la migration. Pour préparer l'environnement, procédez comme suit :
    a. Sur le serveur Exchange Server 2010 SP3, effectuez une capture instantanée du déploiement actuel des dossiers publics. Cette capture instantanée est utilisée pour vérifier que la migration comprend les mêmes dossiers, éléments et autorisations à l'issue du processus de migration. Utilisez l'applet de commande **Get-PublicFolder**, **Get-PublicFolderStatistics** et **Get-PublicFolderClientPermission** pour réaliser cette capture instantanée.
    b. Sur le serveur Exchange Server 2010 SP3, vérifiez qu'il n'y a aucun enregistrement précédent d'une migration réussie ou en cours.
    c. Sur le serveur Exchange Server 2013, vérifiez qu'il n'y a aucune demande existante de migration des dossiers publics. Le cas échéant, supprimez-la.
    d. Assurez-vous qu'il n'existe aucun dossier public sur les serveurs Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

2. Préparer le fichier de mappage du dossier public. Cette étape comprend ce qui suit :

   a. Sur le serveur Exchange Server 2010 ou Exchange Server 2007, générez les fichiers .CSV qui répertorient l'ensemble des dossiers publics sur les versions précédentes d'Exchange Server. Pour ce faire, exécutez le script Export-PublicFolderStatistics.ps1 pour créer le fichier de mappage qui mappe le nom du dossier à la taille du dossier. Le fichier aura deux colonnes : Nom de dossier et Taille de dossier.

   b. Créer le fichier de mappage Folder-to-Mailbox. Ce fichier sera utilisé pour créer le nombre approprié de boîtes aux lettres de dossiers publics sur le serveur de boîtes aux lettres Exchange 2013. Exécutez le script **PublicFolderToMailboxMapGenerator.ps1** pour créer le fichier de mappage entre le dossier public et la boîte aux lettres.

3. Créer les boîtes aux lettres de dossiers publics sur le serveur Exchange 2013. Vérifiez que les boîtes aux lettres des dossiers publics que vous créez correspondent au nom de la boîte aux lettres cible, TargetMailbox, du fichier de mappage. Lorsque vous créez les boîtes aux lettres de dossiers publics, veillez à être en mode **HoldForMigration**.

4. Initier la demande de migration. Sur un serveur de boîtes aux lettres Exchange Server 2013, exécutez l'applet de commande **New-PublicFolderMigrationRequest** pour initier la migration. Selon le volume de données (plusieurs gigaoctets) figurant dans les dossiers publics, l'exécution de cette commande peut prendre du temps.

5. Verrouiller les dossiers publics sur les versions précédentes d'Exchange Server pour la migration finale. Jusqu'à présent, les utilisateurs ont été en mesure d'accéder aux dossiers publics pendant la migration. Au cours des étapes suivantes, les utilisateurs seront déconnectés des dossiers publics et les dossiers seront verrouillés le temps que la migration termine sa synchronisation finale. Exécutez la commande **Set-OrganizationConfig -PublicFoldersLockedForMigration:$true** sur un serveur Exchange Server 2010 SP3. Si votre organisation possède plusieurs bases de données de dossiers publics, vous devez attendre la fin de la réplication des dossiers publics pour vous assurer que toutes les bases de données de dossiers publics sont verrouillées.

6. Finaliser la migration des dossiers publics. Enfin, exécutez l'applet de commande **Set-PublicFolderMigration** et définissez l'indicateur **PreventCompletion** sur **False**. Puis reprenez la migration des dossiers publics. Exchange va maintenant exécuter une synchronisation finale des contenus des dossiers publics et définit les bases de données de dossiers publics sur les serveurs Exchange Server 2013 comme actives. À l'issue de la migration, tous les clients auront besoin d'accéder aux dossiers publics sur les serveurs Exchange Server 2013. Si vous rencontrez des problèmes avec la migration, vous pouvez restaurer la version précédente d'Exchange Server en déverrouillant les dossiers publics et en définissant la migration comme Inachevée.

 **Remarque :** Cette rubrique offre une description détaillée du processus de migration des dossiers publics depuis une version antérieure d'Exchange Server. Pour plus d'informations, consultez http://go.microsoft.com/fwlink/?LinkId=290962.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Éléments à prendre en compte pour l'implémentation des dossiers publics

- Planifier la distribution géographique des contenus et des boîtes aux lettres de dossiers publics
- Planifier les limites de taille de la boîte aux lettres de dossiers publics
- Noter que l'accès utilisateur aux dossiers publics n'a pas changé considérablement
- Placer la boîte aux lettres de dossiers publics de la hiérarchie principale dans une base de données de boîtes aux lettres dans une LAG

En raison de l'architecture entièrement nouvelle pour les dossiers publics dans Exchange Server 2013, votre processus de planification pour implémenter les dossiers publics différera considérablement du processus que vous avez utilisé avec des versions précédentes d'Exchange Server. Parmi les facteurs à prendre en considération lors de la planification du déploiement des dossiers publics figurent les éléments suivants :

- Dans les versions précédentes d'Exchange Server, les organisations avec les serveurs Exchange dans plusieurs emplacements ont souvent configuré la réplication des dossiers publics pour garantir que leur contenu était disponible dans chaque emplacement. Dans Exchange Server 2013, le contenu des dossiers publics ne peut exister que dans une seule boîte aux lettres de dossiers publics. Si votre organisation possède plusieurs sites, vous devrez prévoir l'emplacement du contenu des dossiers publics pour optimiser l'accès des utilisateurs.
- La planification de la distribution du contenu des dossiers publics peut s'avérer difficile dans les organisations possédant un important volume de données dans les dossiers publics. Exchange Server 2013 dispose d'une taille de boîte aux lettres maximale égale à 100 Go ; aussi si votre organisation possède plus de 100 Go de données dans les dossiers publics, vous devrez créer plusieurs boîtes aux lettres de dossiers publics et distribuer le contenu des dossiers publics à travers les boîtes aux lettres. Même si vous disposez de moins de 100 Go de données dans les dossiers publics, vous êtes susceptible de distribuer le contenu des dossiers publics à travers des régions géographiques, de telle sorte que le contenu se situe dans le même emplacement que les utilisateurs qui y ont accès ou de réduire la taille de la boîte aux lettres.
- De manière générale, l'accès aux dossiers publics n'a pas changé pour les utilisateurs. Les utilisateurs continueront à utiliser les clients Outlook pour accéder aux dossiers publics. S'ils ont les autorisations requises, ils seront toujours en mesure de créer des dossiers publics et de configurer les autorisations de dossiers publics dans leur client Outlook. L'unique changement considérable pour les utilisateurs de dossiers publics réside dans le fait qu'ils ne seront plus en mesure d'accéder aux dossiers publics à l'aide d'Outlook Web App. Les dossiers publics des boîtes aux lettres sont identiques aux dossiers publics des versions antérieures d'Exchange Server. Le stockage des dossiers publics est différent d'un point de vue administratif, mais ce changement demeure transparent pour les utilisateurs.
- Nous vous recommandons de localiser la boîte aux lettres de hiérarchie principale dans une base de données de boîtes aux lettres avec plusieurs copies des boîtes aux lettres dans un DAG. Si la boîte aux lettres de hiérarchie principale n'est pas disponible, les utilisateurs peuvent toujours lire le contenu des dossiers publics, mais ils ne peuvent plus apporter de modifications aux dossiers publics.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 4
Gestion des stratégies et listes d'adresses

Nombreux sont les systèmes de messagerie sur lesquels vous pourriez héberger plusieurs domaines SMTP et, par conséquent, devriez gérer les adresses de messagerie attribuées aux destinataires Exchange Server. Pour vous assurer que les destinataires ont les adresses de messagerie appropriées, vous pouvez créer et appliquer des stratégies d'adresse de messagerie.

Dans les grandes entreprises, la LAG peut contenir des milliers de destinataires. La recherche d'un destinataire spécifique dans cette liste peut s'avérer compliquée. Pour simplifier le processus de recherche des destinataires, vous pouvez configurer des listes d'adresses.

Dans cette leçon, vous allez découvrir comment configurer les stratégies d'adresse de messagerie et les listes d'adresses.

Objectifs de la leçon

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

- décrire des listes d'adresses ;
- configurer des listes d'adresses ;
- configurer des carnets d'adresses en mode hors connexion ;
- décrire des stratégies d'adresse de messagerie ;
- configurer des stratégies de carnet d'adresses ;
- décrire les stratégies d'adresse de messagerie ;
- configurer des stratégies d'adresse de messagerie.

Définition des listes d'adresses

Les listes d'adresses sont utilisées pour regrouper les objets destinataires selon une requête LDAP pour des attributs Active Directory spécifiques. Vous pouvez utiliser des listes d'adresses pour trier la liste d'adresses globale en plusieurs affichages, ce qui simplifie la recherche de destinataires. Cela est particulièrement utile pour les organisations très grandes ou très segmentées.

- Objets destinataires regroupés selon une requête LDAP pour des attributs Active Directory spécifiques
- Les listes d'adresses peuvent simplifier le processus de localisation des destinataires dans la LAG
- Les listes d'adresses par défaut comprennent les éléments suivants
  - Tous les contacts
  - Tous les groupes
  - Toutes les salles
  - Tous les utilisateurs
  - Dossiers publics
  - Liste des adresses globale par défaut

Vous pouvez configurer les listes d'adresses à l'aide de filtres de destinataire qui déterminent à qui appartiennent les objets dans chaque liste d'adresses. Les listes d'adresses sont évaluées chaque fois qu'un compte à extension messagerie est modifié pour déterminer sur quelles listes d'adresses il doit apparaître.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exemple 1

Prenons le cas d'une société qui comporte deux grandes divisions et une organisation Exchange. La première division, nommée Fourth Coffee, importe et vend des grains de café. La deuxième division, Contoso, Ltd., souscrit des polices d'assurance. En raison de la nature différente de chaque activité, les employés communiquent rarement entre eux.

Pour qu'il soit plus facile aux employés de rechercher des destinataires qui se trouvent uniquement dans leur division, vous pouvez créer deux nouvelles listes d'adresses personnalisées : l'une pour Fourth Coffee et l'autre pour Contoso, Ltd. Ces listes d'adresses personnalisées permettent aux employés qui recherchent des destinataires de leur division, de sélectionner uniquement la liste d'adresses spécifique à leur division. Toutefois, si un employé ne connaît pas exactement la division à laquelle appartient le destinataire, il peut effectuer une recherche dans la liste d'adresses globale, qui contient tous les destinataires des deux divisions.

Exemple 2

Vous pouvez utiliser des sous-catégories des listes d'adresses, appelées également listes d'adresses hiérarchiques. Par exemple, vous pouvez créer une liste d'adresses qui contient tous les destinataires à Vancouver et une autre qui contient tous destinataires de Redmond. Vous pouvez également créer une autre liste appelée Recherche et Développement dans le conteneur de liste d'adresses Vancouver, laquelle contient tous les employés qui travaillent dans le service Recherche et Développement de Vancouver. Cela permet aux employés de rechercher plus facilement les informations dont ils ont besoin.

Démonstration : Configuration de listes d'adresses

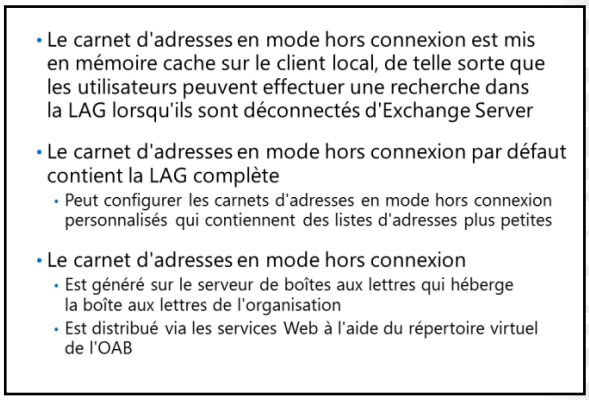
Au cours de cette démonstration, vous allez apprendre à créer et à configurer des listes d'adresses.

Procédure de démonstration

1. Sur LON-CAS1, dans le CAE, créez une liste d'adresses intitulée **AllDepartments** comprenant uniquement les utilisateurs disposant de boîtes aux lettres Exchange.
2. Créez une autre liste d'adresses enfant sous **AllDepartments** intitulée **Research** qui contient uniquement les utilisateurs possédant des boîtes aux lettres Exchange dans le service Recherche.
3. Sur LON-CL1, dans Outlook 2013, lancez un téléchargement du carnet d'adresses en mode hors connexion.
4. Vérifiez que la liste d'adresses Research figure dans la liste et contient les bons utilisateurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de carnets d'adresses en mode hors connexion



Outlook utilise le carnet d'adresses en mode hors connexion lorsque vous configurez les clients pour utiliser un profil Outlook en mode cache ou lorsque le client est en mode hors connexion. Le carnet d'adresses en mode hors connexion est mis en mémoire cache sur le client local, de telle sorte que les utilisateurs peuvent effectuer une recherche dans la LAG lorsqu'ils envoient des messages.

Le carnet d'adresses en mode hors connexion par défaut contient la LAG complète, sur laquelle figure tous les destinataires de l'organisation Exchange. Vous pouvez créer des LAG supplémentaires et les ajouter à un carnet d'adresses en mode hors connexion personnalisé.

Par défaut, le carnet d'adresses en mode hors connexion est généré sur un serveur de boîtes aux lettres uniquement une fois par jour à 17 h 00. Cela signifie que les ajouts, suppressions ou modifications apportés aux destinataires à extension messagerie ne sont validés dans le carnet d'adresses en mode hors connexion qu'une fois par jour, à moins que vous ne modifiiez la planification pour générer plus souvent le carnet d'adresses en mode hors connexion.

Le processus de génération et de distribution du carnet d'adresses en mode hors connexion comprend les composants suivants :

- Processus de *génération de carnets d'adresses en mode hors connexion*. Pour créer et mettre à jour le carnet d'adresses en mode hors connexion, le service OABGen (carnet d'adresses hors connexion) s'exécute sur le serveur de boîtes aux lettres qui héberge la boîte aux lettres de l'organisation. Le service OABGen identifie tous les destinataires qui doivent être membres du carnet d'adresses en mode hors connexion, puis crée les fichiers de carnet d'adresses en mode hors connexion dans le dossier C:\Programmes\Microsoft\Exchange Server\V15\ClientAccess\OAB.

Remarque : Vous pouvez identifier le serveur de boîtes aux lettres qui héberge la boîte aux lettres de l'organisation en exécutant la commande **Get-Mailbox -Arbitration | where {$_.PersistedCapabilities -like "*oab*"}**. La seule façon de déplacer la génération du carnet d'adresses en mode hors connexion vers un autre serveur Exchange 2013 consiste à déplacer cette boîte aux lettres vers un autre serveur de boîtes aux lettres.

- *Répertoire virtuel OAB*. Le répertoire virtuel OAB est le point de distribution de Microsoft Office Outlook 2007 et les clients récents l'utilisent pour télécharger le carnet d'adresses en mode hors connexion. Lorsque vous installez Exchange Server 2013, le répertoire virtuel OAB est créé sous le site Internet par défaut sur le serveur d'accès au client, et sous le site principal Exchange sur les serveurs de boîtes aux lettres. Par défaut, le répertoire virtuel OAB est configuré avec une URL interne. Si les clients Outlook en dehors de l'organisation ont accès à l'environnement Exchange, vous devez également configurer une URL externe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Service de découverte automatique*. Le service de découverte automatique a été introduit dans Exchange Server 2007 en tant que fonctionnalité permettant à Office® Outlook 2007 ou des clients plus récents, ainsi que certains appareils mobiles, de configurer automatiquement leur profil pour accéder automatiquement à Exchange Server. Ce service fournit la bonne URL d'OAB aux clients Outlook.
- *Distribution OAB*. Lorsque les clients ont besoin de télécharger le carnet d'adresses en mode hors connexion, le client envoie une requête au serveur d'accès au client configuré au moyen de la découverte automatique. Le serveur d'accès au client redirige ensuite via un proxy une demande sur le serveur de boîte aux lettres qui héberge les fichiers OAB. Les fichiers OAB sont alors distribués directement au client à partir du serveur de boîte aux lettres.

Éléments à prendre en compte pour la taille des carnets d'adresses en mode hors connexion

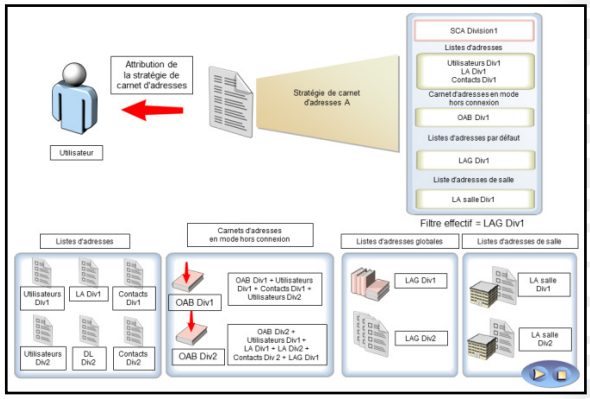
Dans les grandes organisations qui possèdent d'importants annuaires, ou dans les organisations qui ont déployé Office Outlook en mode cache, la taille des carnets d'adresses en mode hors connexion peut représenter un problème potentiel. Les tailles de carnets d'adresses en mode hors connexion peuvent aller de quelques mégaoctets (Mo) à quelques centaines de mégaoctets. Les facteurs suivants peuvent avoir une incidence sur la taille des carnets d'adresses en mode hors connexion :

- Utilisation de certificats dans une société. Plus le nombre de certificats PKI (infrastructure à clé publique) utilisés est élevé, plus grande est la taille du carnet d'adresses en mode hors connexion. Les certificats PKI vont de 1 kilo-octet (Ko) à 3 Ko. Ce sont eux qui contribuent le plus à la taille des carnets d'adresses en mode hors connexion.
- Nombre de destinataires du message Active Directory.
- Nombre de groupes de distribution Active Directory.
- Informations qu'une société ajoute à Active Directory pour chaque objet à extension messagerie ou boîte aux lettres. Par exemple, certaines organisations remplissent les propriétés d'adresse pour chaque utilisateur ; d'autres ne le font pas. La taille du carnet d'adresses en mode hors connexion augmente avec l'augmentation du nombre d'attributs.

Remarque : Les versions précédentes d'Exchange Server prenaient en charge un grand nombre de versions du carnet d'adresses en mode hors connexion. Exchange Server 2013 prend en charge uniquement OAB version 4, qui est pris en charge par Outlook 2007, Outlook 2010 et Outlook 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Définition des stratégies de carnet d'adresses



Les stratégies de carnet d'adresses peuvent limiter les informations que voient les utilisateurs dans la liste d'adresses globale (LAG) de leur organisation. Certaines organisations doivent créer des vues personnalisées de la LAG afin de limiter l'accès de certains utilisateurs. Par exemple, une grande société d'investissements peut avoir plusieurs divisions qui entrent en concurrence sur des marchés sélectionnés, et l'autorisation de la communication entre les investisseurs de chaque division est susceptible d'entrer en violation avec les lois commerciales. D'autres organisations possédant de très grandes LAG sont susceptibles de limiter la taille du carnet d'adresses en mode hors connexion pour les utilisateurs. Le fait de limiter ce que les utilisateurs peuvent visualiser dans la LAG s'appelle la segmentation de la liste d'adresses globale.

Dans Exchange Server 2013, vous pouvez utiliser des stratégies de carnet d'adresses pour configurer la segmentation de la liste d'adresses globale. Lorsque vous configurez une stratégie de carnet d'adresses, vous attribuez à la stratégie une liste d'adresses globale, un carnet d'adresses en mode hors connexion, une liste de salles et une ou plusieurs listes d'adresses. Vous pouvez ensuite attribuer la stratégie de carnet d'adresses aux utilisateurs de la boîte aux lettres, ce qui signifie que les utilisateurs ne peuvent voir que les objets de la LAG qui font partie de leur stratégie.

Remarque : Les stratégies du carnet d'adresses offrent une segmentation virtuelle de la LAG, et non une séparation légale. Autrement dit, les utilisateurs peuvent parfois voir d'autres destinataires dans l'organisation qui ne font pas partie de leur stratégie de carnet d'adresses. Par exemple, un groupe de distribution inclus dans la stratégie de carnet d'adresses peut inclure les destinataires d'autres stratégies de carnets d'adresses. Si un de ces destinataires dispose d'un message d'absence de bureau configuré, ce message sera envoyé à quiconque envoie le groupe de distribution.

Les stratégies de carnet d'adresses sont appliquées quand la boîte aux lettres de l'utilisateur se situe sur un serveur Exchange 2010 Service Pack 3 (SP3) ou Exchange Server 2013. Si vous mettez à jour la stratégie de carnet d'adresses, les clients doivent reconnecter leur boîte aux lettres avant l'application de la nouvelle stratégie. Si un client accède à la liste d'adresses globale par d'autres moyens, tels qu'une requête LDAP directe à un serveur de catalogues global, la stratégie de carnet d'adresses ne s'applique pas.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration de stratégies de carnet d'adresses

Les stratégies de carnet d'adresses contiennent les listes suivantes :

- Une LAG
- Un carnet d'adresses en mode hors connexion (OAB)
- Une liste d'adresses de salle
- Une ou plusieurs listes d'adresses

Dans cette démonstration, vous découvrirez les étapes suivantes requises pour configurer une stratégie de carnet d'adresses pour les utilisateurs du service Research au sein d'A. Datum :

- Créez une liste d'adresses globale pour le service Research.
- Créez un carnet d'adresses en mode hors connexion pour le service Research.
- Créez la stratégie de carnet d'adresses.

Remarque : Dans cette démonstration, vous utiliserez la liste d'adresses All Rooms (Toutes les salles) par défaut plutôt que de créer une liste d'adresses personnalisée.

Procédure de démonstration

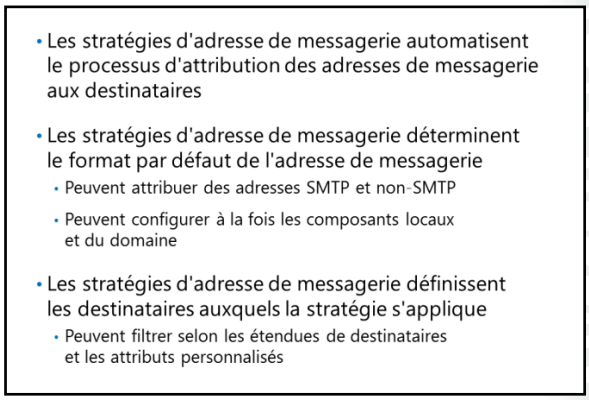
1. Sur LON-CAS1, si nécessaire, ouvrez l'environnement de ligne de commande Exchange Management Shell.
2. Utilisez les commandes suivantes pour créer la stratégie de carnet d'adresses et attribuer la stratégie à tous les utilisateurs dans l'unité d'organisation Research.

```
New-GlobalAddressList -Name ResearchGAL -RecipientFilter {(Department –eq
"Research")}
Update-GlobalAddressList -Name ResearchGAL
New-OfflineAddressBook -Name "ResearchOAB" -AddressLists "ResearchGAL"
New-AddressBookPolicy -Name ResearchABP -AddressLists \AllDepartments\Research -
OfflineAddressBook ResearchOAB -GlobalAddressList ResearchOAB -RoomList "\All Rooms"
Get-Mailbox -OrganizationalUnit Research | Set-Mailbox -AddressBookPolicy ResearchABP
```

3. Sur LON-CL1, déconnectez-vous, puis connectez-vous en tant qu'**Allie** avec le mot de passe **Pa$$w0rd**.
4. Ouvrez **Outlook 2013** et configurez le profil d'Allie.
5. Vérifiez que seule Allie peut voir les autres membres du service Research dans la LAG.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Définition des stratégies d'adresse de messagerie



Pour qu'un destinataire puisse envoyer ou recevoir des messages électroniques, il doit avoir une adresse de messagerie. Les stratégies d'adresse de messagerie génèrent les adresses de messagerie principales et secondaires pour les destinataires d'une organisation Exchange de façon à ce qu'ils puissent recevoir et envoyer des messages.

Vous devez créer un domaine accepté de sorte qu'un domaine d'une stratégie d'adresse de messagerie fonctionne correctement. Un domaine accepté est un espace de noms SMTP que vous configurez dans l'organisation Exchange, de sorte que les serveurs Exchange acceptent les messages envoyés à cet espace de noms SMTP.

Par défaut, Exchange Server contient une stratégie d'adresses de messagerie qui attribue un ou plusieurs adresses de messagerie à chaque utilisateur à extension messagerie. Cette stratégie par défaut spécifie l'alias du destinataire en tant que partie locale de l'adresse de messagerie et utilise le domaine accepté par défaut. La partie locale d'une adresse de messagerie est le nom qui précède le symbole (@). Vous pouvez toutefois configurer la manière dont les adresses de messagerie de vos destinataires s'affichent. Pour spécifier des adresses de messagerie supplémentaires pour tous les destinataires ou simplement un sous-ensemble de destinataires, vous pouvez modifier la stratégie par défaut ou créer des stratégies d'adresse de messagerie supplémentaires.

Création d'une stratégie d'adresses de messagerie

Exchange Server applique une stratégie d'adresse de messagerie au groupe de destinataires basée sur un filtre OPATH. OPATH est un langage d'interrogation conçu pour interroger les sources de données d'objet. Le filtre définit l'étendue de la recherche dans la forêt Active Directory et les attributs qui sont utilisés pour filtrer la LAG.

L'Assistant Nouvelle stratégie d'adresse de messagerie fournit une liste standard de filtres d'étendue destinataire. En voici quelques-uns :

- **Tous les types de destinataires**. Activez cette case à cocher si vous ne souhaitez pas filtrer le type de destinataire.
- **Utilisateurs avec boîtes aux lettres Exchange**. Activez cette case à cocher si vous souhaitez que votre stratégie d'adresse de messagerie s'applique aux utilisateurs qui disposent de boîtes aux lettres Exchange Server 2013, Exchange Server 2010 et Exchange Server 2007.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- **Utilisateurs de messagerie avec adresses de messagerie externes**. Activez cette case à cocher si vous voulez appliquer votre stratégie d'adresse de messagerie à des utilisateurs qui disposent d'adresses de messagerie externes. Les utilisateurs ayant des comptes de messagerie externes ont des comptes de domaine utilisateur dans les services de domaine Active Directory, mais utilisent des comptes de messagerie externes à l'organisation.
- **Boîtes aux lettres de ressources**. Activez cette case à cocher si vous voulez appliquer la stratégie d'adresse de messagerie aux boîtes aux lettres de ressources Exchange Server.
- **Contacts avec adresses de messagerie externes**. Activez cette case à cocher si vous voulez appliquer votre stratégie d'adresse de messagerie à des contacts qui disposent d'adresses de messagerie externes.
- **Groupes à extension messagerie**. Activez cette case à cocher si vous voulez appliquer la stratégie d'adresse de messagerie aux groupes de sécurité ou de distribution à extension messagerie.

Vous pouvez également configurer une règle qui peut filtrer les destinataires auxquels s'appliquera la stratégie d'adresse de messagerie. Avec cette option, vous pouvez filtrer les destinataires selon les catégories suivantes :

- **Conteneur de destinataires**. Utilisez cette catégorie pour filtrer la liste des destinataires selon l'unité d'organisation où le compte de destinataire existe.
- **État ou province**. Activez cette case à cocher si vous voulez que la stratégie d'adresse de messagerie ne comprenne que des destinataires d'états ou de provinces spécifiques.
- **Société**. Activez cette case à cocher si vous voulez que la stratégie d'adresse de messagerie ne comprenne que des destinataires de sociétés spécifiques.
- **Service**. Activez cette case à cocher si vous voulez que la stratégie d'adresse de messagerie ne comprenne que des destinataires de services spécifiques.
- **Attributs personnalisés**. Il existe 15 attributs personnalisés pour chaque destinataire. Il y a une condition distincte pour chaque attribut personnalisé. Si vous voulez que la stratégie d'adresse de messagerie inclue uniquement des destinataires qui ont une valeur spécifique définie pour un attribut personnalisé spécifique, activez la case à cocher qui correspond à cet attribut personnalisé.

Lors de la création d'une stratégie d'adresse de messagerie, vous pouvez utiliser les types d'adresse de messagerie suivants :

- *Adresse de messagerie SMTP par défaut*. Les adresses de messagerie SMTP par défaut sont des types d'adresses de messagerie couramment utilisés fournis par Exchange Server.
- *Adresse de messagerie SMTP personnalisée*. Si vous ne souhaitez pas utiliser l'une des adresses de messagerie SMTP par défaut, vous pouvez spécifier une adresse de messagerie SMTP personnalisée. Lorsque vous créez une adresse de messagerie SMTP personnalisée, vous pouvez utiliser les variables du tableau suivant pour spécifier d'autres valeurs pour la partie locale de l'adresse de messagerie.

Variable	Valeur
%g	Prénom
%i	Initiales
%s	Nom
%d	Nom complet

(*suite*)

Variable	Valeur
%m	Alias Exchange
%xs	Utilise le nombre x de lettres du nom de famille. Par exemple, si x=2, les deux premières lettres du nom de famille sont utilisées
%xg	Utilise le nombre x de lettres du prénom. Par exemple, si x=2, les deux premières lettres du prénom sont utilisées

- *Adresse de messagerie non-SMTP*. Exchange Server 2013 prend en charge un nombre de types d'adresses non SMTP, tels que X.500, X.400, Lotus Notes et Novel GroupWise.

Démonstration : Configuration de stratégies d'adresse de messagerie

Dans cette démonstration, vous découvrirez la manière de modifier la stratégie d'adresse de messagerie par défaut et de créer une stratégie d'adresse de messagerie.

Procédure de démonstration

1. Sur LON-CAS1, dans le CAE, modifiez la stratégie d'adresse de messagerie par défaut pour ajouter l'adresse de messagerie prénom.nom@adatum.com à tous les utilisateurs d'A. Datum.
2. Créez un domaine accepté pour Sales.adatum.com.
3. Créez une stratégie d'adresse de messagerie qui applique l'adresse de messagerie prénom première initiale du nom de famille @sales.adatum.com à tous les utilisateurs de l'unité d'organisation Sales.
4. Examinez les adresses de messagerie attribuées à Adam Barr et à Arlene Huff et vérifiez que les adresses de messagerie sont attribuées correctement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Gestion d'objets destinataires

Scénario

Vous êtes l'administrateur de messagerie de la société A. Datum Corporation. A. Datum a acheté une nouvelle société nommée Trey Research. Les boîtes aux lettres de Trey Research seront hébergées sur votre environnement Exchange Server 2013, mais elles doivent conserver une identité unique au sein de l'organisation. Tous les utilisateurs de Trey Research doivent utiliser le domaine SMTP TreyResearch.net pour envoyer et recevoir les e-mails. Les utilisateurs de Trey Research doivent être en mesure de visualiser uniquement les autres utilisateurs du groupe de l'entreprise.

Vous devez implémenter l'environnement de messagerie pour les utilisateurs Trey Research.

Configuration de l'atelier pratique

Durée approximative : **60 minutes**

Ordinateurs virtuels	22341B-LON-DC1 22341B-LON-CAS1 22341B-LON-MBX1 22341B-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 débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22341B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous avec les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Répétez les étapes 2 à 4 pour **22341B-LON-MBX1** et **22341B-LON-CAS1**.
6. Répétez les étapes 2 et 3 pour **22341B-LON-CL1**. N'ouvrez pas de session tant que vous n'y avez pas été invité.

Remarque : Dans certains cas, il se peut que les messages envoyés dans cet atelier pratique ne soient pas remis immédiatement. Vous pouvez noter que, lorsque vous envoyez des messages, ceux-ci demeurent dans le dossier Brouillons d'Outlook Web App. Utilisez les étapes suivantes pour dépanner le flux de messagerie si vous vous heurtez à ce problème dans cet atelier pratique ou dans d'autres ateliers pratiques :

1. Sur LON-MBX1, ouvrez l'environnement de ligne de commande Exchange Management Shell.
2. Tapez **Test-ServiceHealth**, puis appuyez sur Entrée. Vérifier que tous les services requis sont en cours d'exécution. Si tel n'est pas le cas, démarrez-les.
3. Tapez **Restart-Service MSExchangeSubmission**, puis appuyez sur Entrée.
4. Tapez **Restart-Service MSExchangeDelivery**, puis appuyez sur Entrée. Assurez-vous que le message a été remis.
5. Dans le cas contraire, tapez **Restart-Service MSExchangeTransport**, puis appuyez sur Entrée. Assurez-vous que le message a été remis.
6. Si les messages continuent à ne pas être remis, redémarrez le service **Topologie Active Directory Microsoft Exchange** à partir de la console Services. Redémarrez tous les services dépendants. Vérifiez que tous les services dont le mode de démarrage est défini sur Automatique ont démarré. Assurez-vous que le message a été remis.

Exercice 1 : Configurer les destinataires Trey Research

Scénario

Vous avez reçu un script et un fichier .csv que vous utiliserez pour créer les destinataires pour les utilisateurs Trey Research. Cependant, vous devez également configurer d'autres objets destinataires pour les utilisateurs Trey Research, tels que les groupes de distribution et les boîtes aux lettres de ressources. L'équipe du projet a demandé que vous créiez les objets destinataires suivants :

- Créez des comptes d'utilisateur et des boîtes aux lettres Active Directory à l'aide d'un script fourni par l'équipe de projet.
- Créez les boîtes aux lettres de salle et configurez les boîtes aux lettres de telle façon que seuls les utilisateurs Trey Research peuvent réserver des réunions dans les salles. Toutes les autres demandes de réunion doivent être approuvées par un administrateur Trey Research.
- Configurez une boîte aux lettres partagée pour le service des ventes de Trey Research.
- Configurez des groupes de distribution constitués de différents services de Trey Research.
- Configurez une liste de distribution dynamique comprenant les utilisateurs Trey Research et A. Datum qui travaillent sur le projet d'intégration de Trey Research. Vous avez reçu une liste des membres actuels de cette équipe, mais des modifications y seront fréquemment apportées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les tâches principales de cet exercice sont les suivantes :

1. Créer des objets Active Directory Trey Research.
2. Créer les boîtes aux lettres Trey Research.
3. Créer des groupes de distribution Trey Research.

▶ Tâche 1 : Créer des objets Active Directory Trey Research

1. Sur LON-CAS1, à partir du Gestionnaire de serveur, ouvrez le **Module Active Directory pour Windows PowerShell**.
2. Exécutez le script **TreyResearchSetup.ps1** à partir du dossier **e:\Labfiles\Mod03**.
3. Vérifiez que les unités d'organisation, les utilisateurs et les groupes Trey Research sont créés.

▶ Tâche 2 : Créer les boîtes aux lettres Trey Research

1. Sur LON-CAS1, ouvrez Exchange Management Shell et exécutez les commandes suivantes :

À	Exécuter
Créer une base de données de boîtes aux lettres pour les utilisateurs Trey Research	**New-MailboxDatabase –Name TreyResearchDB –Server LON-MBX1**
Redémarrer le service Banque d'informations Microsoft Exchange sur LON-MBX1	**Invoke-Command –ComputerName LON-MBX1 –ScriptBlock {Restart-Service msexchangeis}**
Monter la base de données	**Mount-Database –id TreyResearchDB**
Créer des boîtes aux lettres pour tous les utilisateurs Trey Research	**Get-User –OrganizationalUnit TreyResearch | Enable-Mailbox -Database TreyResearchDB**
Activer la messagerie pour tous les groupes Trey Research	**Get-Group -OrganizationalUnit TreyResearch | Enable-DistributionGroup**

2. Sur LON-CAS1, ouvrez Internet Explorer et connectez-vous à **https://LON-CAS1.adatum.com/ecp**.
3. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Créez une nouvelle boîte aux lettres de salle avec les paramètres suivants :
   - Nom de la salle : **TR_Room1**
   - Adresse de messagerie : **TR_Room1**
   - Unité d'organisation : Cliquez sur **parcourir...**, sur **TreyResearch**, puis sur **ok**
   - Emplacement : **Harrow**
   - Capacité : **20**
   - Base de données de boîtes aux lettres : **TreyResearchDB**
   - Délégués : **Charlotte Weiss**

5. Permettre à tous les utilisateurs TreyResearch de réserver des réunions sans modération en exécutant la commande **Set-CalendarProcessing –id TR_Room1 –BookinPolicy AllTreyResearch**.
6. Créez une nouvelle boîte aux lettres partagée avec les paramètres suivants :
   - Nom d'affichage : **TreyResearch Sales**
   - Adresse de messagerie : **TreyResearchSales**
   - Autorisation Accès total : **TR_Sales**
   - Base de données de boîtes aux lettres : **TreyResearchDB**

▶ Tâche 3 : Créer des groupes de distribution Trey Research

1. Sur LON-CAS1, dans le CAE, créez un groupe de distribution avec les paramètres suivants :
   - Nom d'affichage : **Trey_SalesMgrs**
   - Alias : **TreySalesMgrs**
   - Unité d'organisation : **TreyResearch/Sales**
   - Membres : **Florence Flipo**, **Sidney Higa**
   - Choisir si l'approbation du propriétaire du groupe est requise pour rejoindre ce dernier : **Fermé**
2. Choissisez s'il est possible de quitter le groupe : **Fermé**
3. Créez un autre groupe de distribution avec les paramètres suivants :
   - Nom d'affichage : **TreyResearchNews**
   - Alias : **TreyResearchNews**
   - Unité d'organisation : **TreyResearch**
   - Membres : Aucun
   - Choisir si l'approbation du propriétaire du groupe est requise pour rejoindre ce dernier : **Ouvert**
   - Choisissez s'il est possible de quitter le groupe : **Ouvert**
4. Sur LON-CAS, dans l'environnement de ligne de commande Exchange Management Shell, accédez au dossier **E:\Labfiles\Mod03** et exécutez les commandes suivantes pour configurer tous les membres de l'équipe d'intégration de TreyResearch avec un attribut personnalisé.
   - **$users=import-csv .\TreyResearchIntegrationTeam.csv**
   - **foreach ($i in $users) {set-mailbox –Identity $i.alias –CustomAttribute1 "TreyResearch Integration Project Team"}**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Sur LON-CAS1, dans le CAE, créez un groupe de distribution dynamique avec les paramètres suivants.
    - Nom d'affichage : **TreyIntegration**
    - Alias : **TreyIntegration**
    - Unité d'organisation : **TreyResearch**
    - Propriétaire : **Administrateur**
    - **Conteneur** de destinataires : **Adatum.com**
    - Attribut personnalisé 1 : **TreyResearch Integration Project Team**

Résultats : Dans cet exercice, vous avez créé des comptes de groupes et d'utilisateurs Active Directory pour Trey Research, vous avez également créé une boîte aux lettres de salles avec des autorisations personnalisées et vous avez configuré une boîte aux lettres partagée. Vous avez en outre configuré des groupes de distribution pour les utilisateurs Trey Research.

Exercice 2 : Configurez les stratégies et listes d'adresses pour Trey Research

Scénario

Votre deuxième étape pour intégrer les utilisateurs Trey Research dans l'environnement du serveur Exchange d'A. Datum consiste à créer des listes d'adresses et des stratégies requises pour garantir aux utilisateurs Trey Research qu'ils disposent de la fonctionnalité et de la séparation requises des données utilisateur. Pour ce faire, vous devez :

- Configurer TreyResearch.net en tant que domaine accepté.
- Créer une stratégie d'adresse de messagerie pour les utilisateurs Trey Research.
- Créer une liste d'adresses pour les utilisateurs Trey Research.
- Créer une stratégie de carnet d'adresses pour les utilisateurs Trey Research.
- Valider le déploiement de Trey Research.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer TreyResearch.net en tant que domaine accepté.
2. Configurer une stratégie d'adresse de messagerie pour les utilisateurs Trey Research.
3. Configurer une liste d'adresses pour les utilisateurs Trey Research.
4. Configurer une stratégie de carnet d'adresses pour les utilisateurs Trey Research.
5. Valider le déploiement.

▶ Tâche 1 : Configurer TreyResearch.net en tant que domaine accepté

- Sur LON-CAS1, dans le CAE, créez un nouveau domaine accepté appelé **TreyResearch** en utilisant le nom de domaine **TreyResearch.net**.

▶ Tâche 2 : Configurer une stratégie d'adresse de messagerie pour les utilisateurs Trey Research

- Sur LON-CAS1, dans le CAE, créez une stratégie d'adresse de messagerie nommée **Adresse de messagerie TreyResearch** qui attribue à tous les utilisateurs TreyResearch une adresse de messagerie principale se déclinant comme suit : Prénom.NomDeFamille@treyresearch.net.

▶ Tâche 3 : Configurer une liste d'adresses pour les utilisateurs Trey Research

- Sur LON-CAS1, dans le CAE, créez une nouvelle liste d'adresses nommée **TreyResearch** qui comprend tous les destinataires de l'unité d'organisation TreyResearch.

▶ Tâche 4 : Configurer une stratégie de carnet d'adresses pour les utilisateurs Trey Research

- Sur LON-CAS1, dans l'environnement de ligne de commande Exchange Management Shell, exécutez les commandes suivantes :

À	Exécuter
Créer une liste d'adresses globale comprenant uniquement les utilisateurs Trey Research.	**New-GlobalAddressList -Name TreyResearchGAL -RecipientContainer TreyResearch**
Mettre à jour la LAG Trey Research.	**Update-GlobalAddressList -id TreyResearchGAL**
Créer un carnet d'adresses en mode hors connexion pour la LAG Trey Research.	**New-OfflineAddressBook -Name "TreyResearchOAB" -AddressLists "TreyResearchGAL"**
Créer une nouvelle liste des adresses de salle pour toutes les boîtes aux lettres de ressources de l'unité d'organisation TreyResearch.	**New-AddressList -Name TreyResearchRooms –RecipientContainer TreyResearch –IncludedRecipients Resources**
Mettre à jour la liste d'adresses TreyResearchRooms.	**Update-AddressList TreyResearchRooms**
Configurer l'OAB Trey Research à distribuer via les répertoires virtuels LON-CAS1 et LON-MBX1.	**Set-OfflineAddressBook -id "TreyResearchOAB" –VirtualDirectories "LON-CAS1\oab (Default Web Site)","LON-MBX1\oab (Exchange Back End)"**
Mettre à jour le carnet d'adresses en mode hors connexion de TreyResearchOAB.	**Update-OfflineAddressBook -id "TreyResearchOAB"**
Créer une nouvelle stratégie de carnet d'adresses qui regroupe les composants de Trey Research.	**New-AddressBookPolicy -Name TreyResearchABP -AddressLists \TreyResearch -OfflineAddressBook TreyResearchOAB -GlobalAddressList TreyResearchGAL -RoomList \TreyResearchRooms**
Attribuer la stratégie de carnet d'adresses TreyResearchABP à toutes les boîtes aux lettres de l'unité d'organisation TreyResearch.	**Get-Mailbox -OrganizationalUnit TreyResearch | Set-Mailbox -AddressBookPolicy TreyResearchABP**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 5 : Valider le déploiement

1. Sur LON-CAS1, dans le CAE, vérifiez que la stratégie de carnet d'adresses **TreyResearchABP** a été attribuée à **Aaron Nicholls**.
2. Sur LON-CL1, connectez-vous en tant qu'**ADATUM\Aaron** avec le mot de passe **Pa$$w0rd**.
3. Ouvrez Outlook 2013 et configurez le profil d'Aaron.
4. Créez un message électronique.
5. Examinez les destinataires visibles dans la liste d'adresses globale. Vérifiez que seuls les destinataires de Trey Research sont disponibles.
6. Envoyez un message de test au groupe de distribution **Trey_SalesMgrs**.
7. Créez et envoyez une nouvelle demande de réunion et invitez **Cindy White** et la salle **TR_Room1** comme ressource. Vérifiez que vous pouvez réserver la salle de réunion.
8. Connectez-vous à Outlook Web App et vérifiez que vous ne pouvez pas rejoindre le groupe de distribution Trey_SalesMgrs, mais que vous pouvez rejoindre le groupe de distribution de TreyResearchNews.
9. Dans Outlook, envoyez un message au groupe **TreyIntegration**.
10. Connectez-vous à Outlook Web App en tant que **ADATUM\Aidan** à l'aide du mot de passe **Pa$$w0rd**. Vérifiez qu'Aidan a reçu le message que vous avez envoyé au groupe TreyIntegration.

Résultats : Dans cet exercice, vous avez créé une stratégie d'adresse de messagerie et une liste d'adresses pour Trey Research. Vous avez créé une stratégie de carnet d'adresses pour Trey Research et validé le déploiement.

Exercice 3 : Configurer les dossiers publics pour Trey Research

Scénario

A. Datum n'a pas implémenté les dossiers publics, mais les utilisateurs Trey Research les ont utilisés dans le passé et souhaiteraient continuer à les utiliser. Vous devez créer une infrastructure des dossiers publics pour les utilisateurs Trey Research, et vous assurer que seuls ces derniers y ont accès.

Les tâches principales de cet exercice sont les suivantes :

1. Créer la boîte aux lettres de dossiers publics.
2. Créer les dossiers publics.
3. Configurer les autorisations de dossiers publics.
4. Valider le déploiement des dossiers publics.

▶ Tâche 1 : Créer la boîte aux lettres de dossiers publics

1. Sur LON-CAS1, dans le CAE, créez une nouvelle boîte aux lettres de dossiers publics **PFMBX1**. Créez l'objet destinataire dans l'unité d'organisation **TreyResearch** et la boîte aux lettres dans la base de données de boîtes aux lettres **TreyResearchDB**.

▶ Tâche 2 : Créer les dossiers publics

1. Sur LON-CAS1, dans le CAE, créez un nouveau dossier public nommé **TreyResearch**.
2. Dans le dossier public TreyResearch, créez un sous-dossier nommé **Research**.

▶ Tâche 3 : Configurer les autorisations de dossiers publics

1. Sur LON-CAS1, dans le CAE, attribuez le groupe **TR_IT** comme propriétaire du dossier public TreyResearch et de tous ses sous-dossiers.
2. Attribuez l'autorisation d'auteur **AllTreyResearch** aux dossiers publics.

▶ Tâche 4 : Valider le déploiement des dossiers publics

1. Sur LON-CL1, dans Outlook 2013, vérifiez qu'Aaron peut accéder aux dossiers publics.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1**, **22341B-LON-MBX1** et **22341B-LON-CL1**.

Résultats : Dans cet exercice, vous avez créé des boîtes aux lettres de dossiers publics pour Trey Research et avez vérifié que les utilisateurs peuvent y accéder.

Question : Comment vérifieriez-vous que les demandes de réunion dans les boîtes aux lettres de salle sont validées manuellement avant d'être approuvées ?

Question : Comment configureriez-vous l'accès pour qu'un utilisateur puisse envoyer des messages à partir d'une autre boîte aux lettres, sans lui donner l'accès au contenu de cette boîte aux lettres ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

Si votre organisation compte un grand nombre d'utilisateurs, passez un moment à apprendre comment gérer les destinataires en utilisant l'environnement de ligne de commande Exchange Management Shell et les scripts. Cela vous permettra de gagner énormément de temps une fois que vous serez à l'aise avec l'utilisation des commandes.

Questions de contrôle des acquis

Question : Une société comporte deux grandes divisions et une organisation Exchange Server. Les employés des deux divisions communiquent rarement entre eux. Que pouvez-vous faire pour réduire le nombre de destinataires visibles par les employés de chaque division lorsqu'ils ouvrent la liste d'adresses Exchange ?

Question : Une organisation comporte un grand nombre de projets qui utilisent des groupes de distribution. La gestion des membres de groupe prend un temps considérable. Vous devez réduire le temps passé par les employés du support technique à gérer les groupes afin qu'ils puissent se consacrer à d'autres tâches. Que devez-vous faire ?

Question : Vous employez des sous-traitants qui ont besoin d'une adresse de messagerie à partir de votre société. Les sous-traitants ne doivent pas être en mesure de se connecter à votre réseau, mais vous souhaitez qu'ils apparaissent dans la LAG. La société doit permettre aux sous-traitants de recevoir ces messages dans leurs boîtes aux lettres actuelles. Que devez-vous faire ?

Problèmes réels et scénarios

Complétez ou adaptez les meilleures pratiques suivantes à vos conditions de travail :

- Définissez des conventions d'affectation de noms claires et respectez-les. Les conventions d'affectation de noms permettent d'identifier l'emplacement et le rôle des objets destinataires et aident à la fois les utilisateurs finaux et les administrateurs à localiser facilement des destinataires.
- Testez les modifications globales avant de les appliquer dans un environnement de production. Les modifications apportées aux paramètres globaux, telles que les stratégies d'adresse de messagerie, doivent être testées dans un environnement d'atelier pratique avant d'être appliquées en environnement de production. Vous éviterez ainsi des erreurs de configuration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4

Planification et déploiement des serveurs d'accès au client

Table des matières :

Vue d'ensemble du module	**4-1**
Leçon 1 : Planification du déploiement du serveur d'accès au client	**4-2**
Leçon 2 : Configuration du rôle serveur d'accès au client	**4-12**
Leçon 3 : Gestion des services d'accès au client	**4-22**
Atelier pratique : Déploiement et configuration d'un rôle serveur d'accès au client	**4-32**
Contrôle des acquis et éléments à retenir	**4-37**

Vue d'ensemble du module

Microsoft® Exchange Server 2013 permet à de nombreux clients différents d'accéder aux boîtes aux lettres des utilisateurs. Tous les clients de messagerie accèdent aux boîtes aux lettres Exchange Server via un serveur d'accès au client. En raison de l'importance de ce rôle serveur, vous devez comprendre comment le planifier, le déployer et le configurer pour prendre en charge différents types de clients. Ce module fournit des détails sur la planification et l'implémentation du rôle serveur d'accès au client dans Exchange Server 2013.

Objectifs

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

- planifier le déploiement du serveur d'accès au client ;
- configurer les rôles serveur d'accès au client ;
- gérer des services d'accès au client.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification du déploiement du serveur d'accès au client

La première étape du déploiement de l'accès au client vers les boîtes aux lettres Exchange Server consiste à planifier le déploiement et la configuration du serveur d'accès au client. Lors de la conception du déploiement, prenez en compte plusieurs facteurs, y compris la configuration matérielle et la façon dont vous allez fournir l'accès aux services activés sur le serveur d'accès au client. Cette leçon décrit la planification du déploiement d'un serveur d'accès au client.

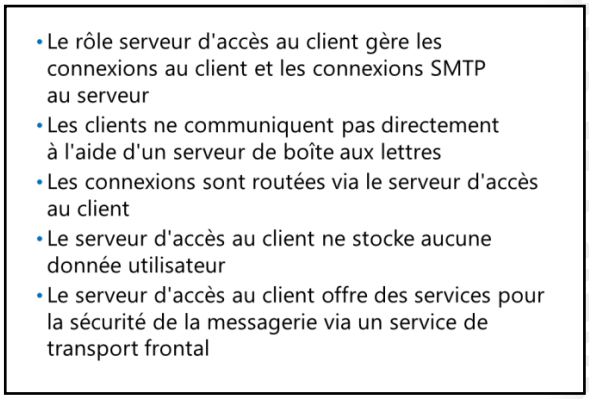
Objectifs de la leçon

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

- décrire le rôle serveur d'accès au client dans Exchange Server 2013 ;
- décrire la configuration matérielle et logicielle requise pour le serveur d'accès au client ;
- planifier le déploiement du serveur d'accès au client ;
- décrire le fonctionnement du serveur d'accès au client ;
- décrire comment les clients Outlook se connectent à leurs boîtes aux lettres ;
- décrire le fonctionnement du serveur d'accès au client avec plusieurs sites ;
- planifier la connectivité client pour le serveur d'accès au client.

Qu'est-ce que le rôle serveur d'accès au client ?

Le rôle serveur d'accès au client dans Exchange Server 2013 est l'une des deux fonctions clé pour l'infrastructure de messagerie dans son ensemble. En fait, c'est un composant obligatoire pour chaque déploiement Exchange Server. Le but principal du rôle serveur d'accès au client est d'accepter et manipuler les connexions au client et les connexions basées sur le protocole SMTP du serveur, et d'assurer ces connexions au serveur de boîtes aux lettres par l'intermédiaire d'un proxy.



Le serveur d'accès au client authentifie également les connexions au client, et fournit le contenu du rôle de serveur de boîtes aux lettres aux clients. Dans Exchange Server 2013, les clients ne peuvent pas initialiser une connexion au serveur de boîtes aux lettres directement, quel que soit le scénario. Toutes les connexions sont routées via le serveur d'accès au client, qui fournit des services Proxy, et dans la redirection du scénario de messagerie unifiée, vers le rôle serveur de boîtes aux lettres. Le serveur d'accès au client accepte les connexions SMTP d'autres serveurs SMTP sur Internet, et crée également des connexions SMTP vers les autres serveurs SMTP sur Internet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrairement à un serveur de boîtes aux lettres, le serveur d'accès au client ne stocke pas de données utilisateur ; il n'effectue pas non plus de mise en file d'attente des messages. Le serveur d'accès au client envoie et accepte des messages vers et à partir d'Internet à l'aide de son service de transport frontal, mais il n'a pas la possibilité d'accepter et de stocker des messages en vue d'une remise plus tardive. Il ne faut pas confondre le service de transport frontal avec le rôle serveur de transport Hub ou Edge des versions précédentes d'Exchange Server. Il ne faut pas non plus l'envisager comme une alternative. Il s'agit simplement d'un proxy pour les connexions client et serveur ; les véritables traitement, envoi et réception des courriers électroniques se produisent sur le rôle serveur de boîtes aux lettres.

Le serveur d'accès au client fournit également des services pour la sécurité de la messagerie. Pour les clients, il permet la communication et l'authentification basées sur SSL (Secure Sockets Layer). Le serveur d'accès au client fournit également la fonctionnalité anti-programmes malveillants et anti-courrier indésirable à mesure que le trafic SMTP le traverse. Le service de transport frontal du serveur d'accès au client ne peut pas inspecter le contenu du message, mais il bénéficie d'un accès complet à la conversation de protocole SMTP. Il peut ainsi filtrer des messages selon des connexions, des domaines, des expéditeurs et des destinataires. En outre, à la différence d'Exchange Server 2010, qui n'a pas bénéficié d'une solution intégrée anti-programmes malveillants, Exchange Server 2013 permet de configurer des options anti-programmes malveillants pour l'analyse des virus. Vous devez noter qu'aucun agent de transport pour le filtrage des connexions n'est activé par défaut pour le serveur d'accès au client dans Exchange Server 2013. Vous pouvez créer un agent de transport s'il vous en faut un.

Configuration matérielle et logicielle requise pour le serveur d'accès au client

Lorsque vous planifiez le déploiement d'un serveur d'accès au client, vous devez tenir compte des configurations matérielles et logicielles générales d'Exchange Server. Si vous choisissez de déployer un serveur d'accès au client avec le rôle serveur de boîtes aux lettres, vous devez respecter la configuration matérielle requise pour le serveur de boîtes aux lettres, car c'est un rôle plus gourmand en matière de ressources. Si vous choisissez de déployer le serveur d'accès au client sur un serveur indépendant, la même configuration logicielle requise que celle présentée dans ce cours s'applique ; toutefois, vous devez concevoir séparément le serveur d'accès au client et le matériel du serveur de boîtes aux lettres.

- La configuration matérielle et logicielle requise pour Exchange Server 2013 s'applique au serveur d'accès au client
- Le serveur d'accès au client a besoin de disques fiables
- Assurez-vous que le volume du système d'exploitation est redondant
- Si possible, fournissez plusieurs serveurs d'accès au client
- Le serveur d'accès au client nécessite une connexion réseau rapide vers les serveurs de boîte aux lettres et vers les serveurs du catalogue global

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

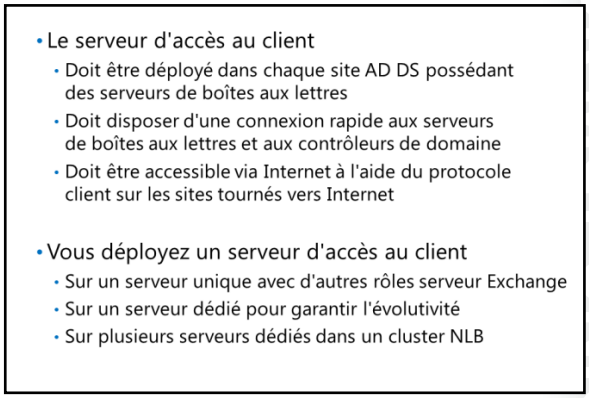
Le serveur d'accès au client ne stockant pas de données utilisateur, il n'est pas nécessaire de fournir le stockage distinct pour ce compte. Cependant, parce que ce rôle est essentiel dans une infrastructure Exchange Server, vous devez vous assurer que le disque dur du serveur d'accès au client est redondant (par exemple, en configuration en miroir). Nous vous recommandons également de déployer plusieurs serveurs d'accès au client, si possible. Si vous déployez le serveur d'accès au client sur l'ordinateur virtuel, vérifiez que ce dernier est hautement disponible.

Lorsque vous concevez la configuration du serveur d'accès au client, prenez en compte les recommandations suivantes :

- Il n'existe aucune configuration de processeur recommandée pour les serveurs d'accès au client. Cependant, nous vous recommandons d'utiliser des processeurs à 2 cœurs minimum et 12 cœurs maximum.
- La configuration de mémoire recommandée dépend du nombre de connexions clientes et de la fréquence des transactions par serveur d'accès au client. La mémoire vive (RAM) recommandée pour les serveurs d'accès au client est de 2 gigaoctets (Go) de RAM par cœur de processeur, avec un minimum de 8 Go de RAM.
- Le serveur d'accès au client n'étant pas une application gourmande en matière de disque dur, il n'est pas nécessaire d'implémenter des disques durs rapides et coûteux. Vous devez veiller à sélectionner des disques durs fiables et certifiés pour fonctionner toute la journée, en permanence.
- Le serveur d'accès au client nécessite une connexion réseau rapide aux serveurs de boîtes aux lettres et aux serveurs du catalogue global. Si le nombre de clients Microsoft Office® Outlook internes est élevé, la connexion réseau peut devenir un goulot d'étranglement. Pour réduire le goulot d'étranglement du réseau, configurez le serveur d'accès au client avec plusieurs cartes réseau de 1 gigaoctet par seconde (Go/s).
- De manière générale, il est recommandé de déployer un serveur d'accès au client pour quatre serveurs de boîtes aux lettres. Toutefois, pour des questions de redondance et d'équilibrage de charge, nous recommandons de disposer de plus d'un serveur d'accès au client.

Planification du déploiement du serveur d'accès au client

Lorsque vous planifiez le déploiement de votre serveur d'accès au client, votre système doit respecter certaines exigences pour garantir la réussite de l'installation. En outre, vous disposez de plusieurs possibilités de déploiement des serveurs d'accès au client dans les scénarios nécessitant une haute disponibilité ou lorsque plusieurs sites sont déployés.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Conditions requises pour le déploiement d'un serveur d'accès au client

Lorsque vous déployez des serveurs d'accès au client, les conditions requises suivantes doivent être remplies :

- Vous devez disposer d'au moins un serveur d'accès au client sur chaque site Active Directory où sont déployés des serveurs de boîtes aux lettres.
- Si votre forêt Active Directory® Domaine Services (AD DS) comprend plusieurs domaines, chaque site doit avoir un serveur d'accès au client pour chaque domaine contenant des serveurs de boîtes aux lettres sur ce site. Les serveurs d'accès au client doivent disposer d'une connexion réseau rapide aux serveurs de boîtes aux lettres.
- Les serveurs d'accès au client doivent disposer d'une connexion réseau rapide aux contrôleurs de domaine et aux serveurs de catalogue global.
- Si les utilisateurs doivent accéder à leurs boîtes aux lettres à partir d'Internet via le serveur d'accès au client, ce dernier doit être accessible à partir d'Internet à l'aide des protocoles HTTPS, IMAP4 ou POP3.

Remarque : Dans la mesure où le serveur qui exécute le rôle serveur d'accès au client doit être membre d'un domaine Active Directory, le déploiement du rôle serveur d'accès au client dans un réseau de périmètre n'est pas pris en charge. Au lieu de cela, utilisez un pare-feu de la couche Application pour publier les services de serveur d'accès au client sur Internet.

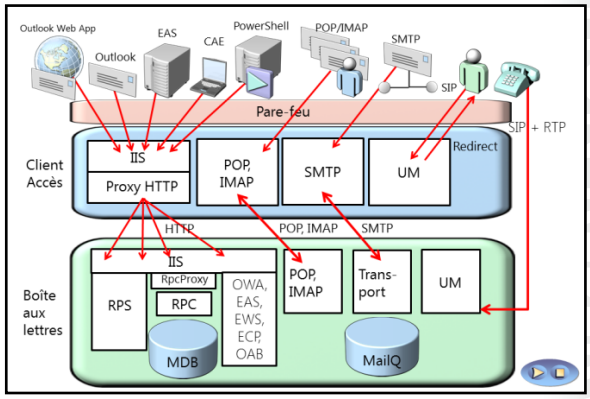
Options de déploiement d'un serveur d'accès au client

Le rôle serveur d'accès au client assure une fonction essentielle dans votre organisation Exchange Server. Les options suivantes sont disponibles quand vous déployez le rôle serveur d'accès au client :

- Il est possible de déployer le rôle serveur d'accès au client sur le même ordinateur que celui sur lequel se trouve le rôle serveur de boîtes aux lettres. L'installation de tous les rôles serveur sur un seul serveur ne fournit pas de disponibilité supplémentaire ; par ailleurs, elle ne permet qu'une évolutivité limitée.
- Il est possible de déployer le rôle serveur d'accès au client sur un serveur dédié. Ce déploiement fournit une évolutivité supplémentaire et offre des avantages en matière de performances.
- Il est possible de déployer plusieurs serveurs qui exécutent le rôle serveur d'accès au client. Pour garantir la haute disponibilité pour les serveurs d'accès au client, il est possible de déployer l'équilibrage de la charge réseau Windows (NLB) ou un programme d'équilibrage de la charge réseau matérielle afin de gérer les connexions aux serveurs d'accès au client.

Remarque : Il est possible d'installer des serveurs d'accès au client sur les serveurs de boîtes aux lettres qui appartiennent à un groupe de disponibilité de bases de données (DAG). Toutefois, le simple ajout du serveur d'accès au client à un membre du DAG ne fournit pas la haute disponibilité pour le serveur d'accès au client. Cela s'explique par le fait que le DAG utilise le clustering avec basculement, qui ne fonctionne pas avec l'équilibrage de charge Windows sur le même ordinateur. Cependant, il est possible d'utiliser un équilibrage de charge matériel pour le serveur d'accès au client dans ce scénario.

Comment fonctionne un serveur d'accès au client ?



Dans Exchange Server 2013, tous les clients de messagerie se connectent à un serveur d'accès au client lorsqu'ils accèdent à une boîte aux lettres Exchange Server. L'objet principal du serveur d'accès au client est d'accepter, authentifier et de connecter via un proxy ou de rediriger les connexions clientes, tout en traitant également le trafic des messages SMTP avec d'autres serveurs SMTP.Cependant, comparé au même rôle dans Microsoft® Exchange Server 2007 et Exchange Server 2010, le serveur d'accès au client fonctionne différemment dans Exchange Server 2013.

L'une des modifications les plus importantes est la façon dont le tableau d'accès au client communique avec les clients et le serveur de boîtes aux lettres. Dans les versions précédentes d'Exchange Server, les clients internes utilisaient l'appel de procédure distante (RPC) de l'interface de programmation d'applications de messagerie (MAPI) pour se connecter au serveur ou au serveur de boîtes aux lettres ou d'accès au client, alors que les clients externes utilisaient le RPC via le protocole HTTPS, POP3 ou IMAP4.

Dans Exchange Server 2013, MAPI via le RPC reste le protocole utilisé par Outlook. Toutefois il est désormais intégré à HTTPS par défaut, quel que soit le mode de connexion du client. La connexion du client à la boîte aux lettres se fait toujours via le serveur d'accès au client. Le serveur d'accès au client établit la connexion RPC sur HTTPS du client au serveur de boîtes aux lettres par l'intermédiaire d'un proxy.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'image suivante est un schéma qui présente le mode de fonctionnement du serveur d'accès au client.

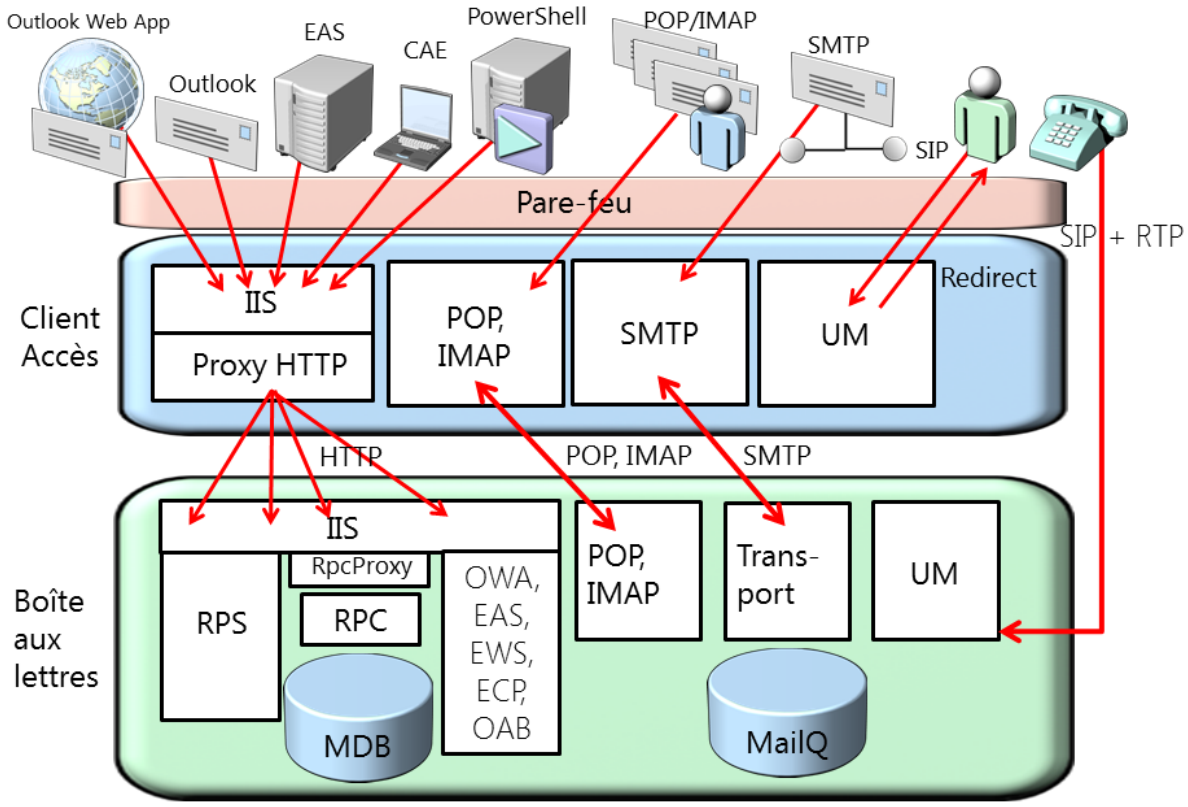


FIGURE 4.1 : COMMENT FONCTIONNE UN SERVEUR D'ACCÈS AU CLIENT ?

Remarque : Pour mieux comprendre le fonctionnement de ces connexions, vous devez comprendre les composants clés suivants qui participent à ce processus :

- MAPI. C'est l'ensemble des commandes du protocole que les clients Outlook utilisent pour interagir avec le serveur de boîtes aux lettres lorsque ce dernier accède aux boîtes aux lettres et les gère. MAPI est le langage que tous les serveurs « parlent » et il fournit l'accès client aux boîtes aux lettres. Les commandes de MAPI sont encapsulées dans le RPC.
- RPC. Il s'agit du transport par l'intermédiaire duquel les commandes MAPI sont délivrées au serveur de boîtes aux lettres.
- HTTPS. Il s'agit du protocole de transport, qui encapsule, en toute sécurité, les commandes de MAPI/RPC qui sont réparties entre les clients et les serveurs.

UTILISATEUR MCT UNIQUEMENT

Sur le serveur d'accès au client, dans Exchange Server 2010, le proxy RPC/HTTP est le composant des Services Internet (IIS) qui interrompt le trafic HTTP. Une fois le trafic HTTP interrompu, le trafic RPC est autorisé sur le reste du chemin d'accès réseau. Toutefois, lorsque le serveur d'accès au client dans Exchange Server 2013 interrompt le trafic HTTPS, il déchiffre ce dernier et inspecte les commandes MAPI/RPC. Le trafic est ensuite à nouveau chiffré avec HTTPS et envoyé au serveur de boîtes aux lettres. Ensuite, le trafic atteint le point de terminaison Proxy RPC sur les Services Internet (IIS) du serveur de boîtes aux lettres. Ce composant de point de terminaison supprime les informations d'encapsulation HTTPS, puis les commandes MAPI sont exécutées sur le serveur de boîtes aux lettres avec un RPC. En fonction des paramètres contenus dans la requête RPC, le serveur doit trouver et envoyer le bon point de terminaison sur le serveur de boîtes aux lettres lorsque le RPC client sur la connexion HTTPS atteint le serveur d'accès au client.

De la même manière que les connexions à partir des clients Outlook, POP3 et IMAP sont connectés aux services appropriés sur le rôle serveur de boîtes aux lettres par l'intermédiaire d'un proxy. Les connexions SMTP issues d'autres serveurs SMTP sont inspectées et le serveur d'accès au client les connecte au composant de transport sur le serveur de boîtes aux lettres par l'intermédiaire d'un proxy. Uniquement pour la communication de messagerie unifiée, le composant du routeur d'appel de messagerie unifiée du serveur d'accès au client redirige des clients vers le composant de messagerie unifiée sur le rôle de serveur de boîtes aux lettres.

Connexion de clients Outlook aux boîtes aux lettres

Dans Exchange Server 2007, les clients internes utilisaient le nom de domaine complet du serveur de boîtes aux lettres pour se connecter à la boîte aux lettres à l'aide d'une connexion RPC MAPI. C'était la dernière version d'Exchange Server dans laquelle les clients se connectaient directement au serveur de boîtes aux lettres. Dans Exchange Server 2010, les clients internes se déplaçaient vers le serveur d'accès au client, et utilisaient le nom de domaine complet (FQDN) du serveur d'accès au client (ou le nom du tableau d'accès au client) pour se connecter à leurs boîtes aux lettres.

- Exchange Server 2013 n'utilise plus les noms de domaine complets des serveurs ou des tableaux d'accès au client pour localiser les boîtes aux lettres des utilisateurs
- Le serveur d'accès au client utilise le GUID qui est attribué à la boîte aux lettres de l'utilisateur
- Le point de connexion est la chaîne qui constitue l'identificateur unique de la boîte aux lettres
- Le point de connexion contient le GUID de la boîte aux lettres et le nom de domaine

Sur un serveur de boîtes aux lettres, la propriété RpcClientAccessServer de chaque base de données de boîte aux lettres était renseignée à l'aide de la valeur du tableau d'accès au client. Notez que le tableau d'accès au client ne nécessitait pas forcément plusieurs serveurs ; un seul suffisait pour le créer. Cette valeur de propriété était distribuée aux clients via le processus de découverte automatique, qui configurait automatiquement le profil client dans Outlook pour se connecter au bon tableau d'accès au client et pour localiser sa boîte aux lettres.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exchange Server 2013 n'utilise plus les noms de domaine complets des serveurs ou des tableaux d'accès au client pour localiser les boîtes aux lettres des utilisateurs. À la place, le serveur d'accès au client utilise le GUID qui est attribué à la boîte aux lettres de l'utilisateur. Lorsque le client se connecte au serveur d'accès au client et demande le contenu de la boîte aux lettres, le serveur d'accès au client effectue une requête sur AD DS pour déterminer les détails de la boîte aux lettres du client en fonction du GUID de cette dernière. Ces informations intègrent des données relatives au serveur de boîtes aux lettres qui héberge celle de l'utilisateur.

Le serveur d'accès au client utilise ensuite RPC via HTTPS pour se connecter au serveur de boîtes aux lettres, puis récupère les données de l'utilisateur. En raison de cette approche, lors de la configuration d'un profil Outlook pour l'utilisateur, le nom du serveur ne sera plus Serveur d'accès au client (ou tableau de serveur d'accès au client). À la place, le point de connexion est la chaîne qui constitue l'identificateur unique de la boîte aux lettres. Elle contient le GUID de la boîte aux lettres et une partie de son nom de domaine qui est le nom de domaine principal pour l'utilisateur.

Chaque identifiant de boîte aux lettres est spécifique à un utilisateur. Ces informations identifient l'utilisateur et la boîte aux lettres. Ceci permet d'identifier efficacement la cible pour les requêtes RPC que l'utilisateur effectue dans Outlook. En outre, ces informations sont utilisées pour permettre au serveur d'accès au client de trouver à tout moment le serveur de boîte aux lettres approprié à l'utilisateur. Du point de vue d'Outlook, l'identificateur unique de boîte aux lettres est en fait le serveur de boîtes aux lettres, car il s'agit du point de terminaison pour la connexion.

Avec cette approche, un serveur d'accès au client n'est plus aussi étroitement connecté à un serveur de boîtes aux lettres spécifique que dans les versions antérieures d'Exchange Server qui utilisaient la propriété RpcClientAccessServer. Cette modification fournit une plus grande souplesse en matière de déploiement et de gestion.

En effectuant le basculement vers le RPC sur les connexions HTTPS seulement pour les clients, le serveur d'accès au client devient plus léger. Il n'est plus nécessaire que le service d'accès au client RPC soit installé. Les avantages de cette conception peuvent également être appliqués aux scénarios de tolérance aux pannes de site, car les administrateurs n'ont plus besoin de manipuler les différents espaces de noms en effectuant le basculement. Puisque le GUID de la boîte aux lettres et le Nom principal de l'utilisateur sont uniques dans toute la forêt, une connexion cliente peut être établie sans faire référence à un serveur d'accès au client spécifique.

Comment fonctionne un serveur d'accès au client avec plusieurs sites ?

Le déploiement de serveurs d'accès au client dans un environnement comprenant plusieurs sites AD DS rend plus complexe la planification de l'opération, en particulier lorsque vous prenez en compte les possibilités d'accès à Internet offertes à ces serveurs d'accès au client.

- Dans un environnement Exchange 2013 pur, un serveur d'accès au client relie toujours la connexion client au bon serveur de boîte aux lettres par l'intermédiaire d'un proxy
- Dans un environnement Exchange 2013 mixte, un serveur d'accès au client relie la connexion au serveur d'accès au client 2013 ou 2010 dans le site de destination par l'intermédiaire d'un proxy
- Les clients POP3 et IMAP4 doivent se connecter directement au serveur d'accès au client dans leur site de destination

Dans un scénario à site unique, le serveur d'accès au client communique directement avec les serveurs de boîtes aux lettres. Cependant, dans un scénario avec plusieurs sites, il peut en être autrement. Dans les versions antérieures d'Exchange Server, comme les versions 2007 ou 2010, dans un scénario avec plusieurs sites, soit Exchange Server dirigeait les clients vers un serveur d'accès au client situé dans le même site que le serveur de boîtes aux lettres, soit un serveur d'accès au client d'un site distant envoyait une requête à un serveur d'accès au client situé dans le même site que le serveur de boîtes aux lettres par l'intermédiaire d'un proxy.

Exchange Server 2013 simplifie ce processus. Lorsque le client se connecte au serveur d'accès au client dans un site et que son serveur de boîtes aux lettres est dans un autre site, le serveur d'accès au client effectue la connexion cliente au serveur de boîtes aux lettres approprié par l'intermédiaire d'un proxy, sans avoir à contacter d'abord le serveur d'accès au client situé dans le même site que le serveur de boîtes aux lettres de l'utilisateur.

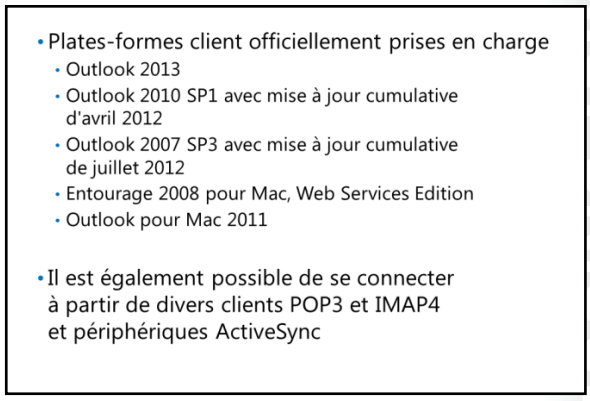
Ce processus fonctionne de la même façon dans les scénarios avec un seul point d'accès Internet ou lorsque chaque site possède son propre point d'accès Internet. La différence, c'est que dans les scénarios dans lesquels vous avez un point d'accès Internet pour chaque site qui héberge des serveurs Exchange, vous devez conserver plusieurs noms publics, un pour chaque serveur d'accès au client publié sur Internet. En outre, vous devez configurer une URL externe pour chaque serveur d'accès au client. Vous devez également vous assurer que les clients peuvent résoudre le nom de l'URL dans le système DNS (Domain Name System) et se connecter au serveur d'accès au client à l'aide du protocole approprié.

Remarque : Dans le cas d'un environnement Exchange Server mixte, il peut arriver que ce chemin de connexion ne fonctionne pas toujours de la même manière. Par exemple, dans le cas de plusieurs sites AD DS, Exchange Server 2013 étant déployé dans le site Internet alors qu'une version précédente d'Exchange Server (telle que 2007 ou 2010) est déployée dans un autre site, le serveur 2013 d'accès au client effectuera la connexion cliente au serveur d'accès au client par l'intermédiaire d'un proxy dans le site où le serveur de boîtes aux lettres de l'utilisateur réside.

En outre, l'utilisation d'un proxy ne fonctionnera pas pour des clients de messagerie POP3 ou IMAP4. Ces clients de messagerie doivent se connecter à un serveur d'accès au client sur le même site Active Directory que le serveur de boîtes aux lettres de l'utilisateur.

Planification de la connectivité client pour le serveur d'accès au client

Bien que la prise en charge de clients ait été modifiée depuis la version précédente, Exchange Server 2013 prend en charge des types de clients différents. La plus importante modification concerne le fait que Microsoft Office Outlook® 2003 n'est plus pris en charge comme logiciel client d'Exchange. En outre, les clients de courrier électronique sur les systèmes d'exploitation Mac, qui requièrent DAV (Distributed Authoring and Versioning), tels qu'Entourage 2008 pour Mac RTM et Entourage 2004, ne sont pas pris en charge.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans Exchange Server 2013, les clients suivants sont pris en charge en mode natif :

- Outlook 2013
- Outlook 2010 SP1 avec la mise à jour cumulative d'avril 2012
- Outlook 2007 SP3 avec la mise à jour cumulative de juillet 2012
- Entourage 2008 pour Mac, Web Services Edition
- Outlook pour Mac 2011

Il est également possible de se connecter au serveur d'accès au client Exchange Server 2013 à partir des applications de messagerie électronique qui utilisent les protocoles POP3 et IMAP4. Ces protocoles étant désactivés par défaut, vous devez les activer et les configurer avant de connecter des clients. Cependant, comme il n'est pas possible de bénéficier des fonctionnalités complètes d'Exchange Server avec ces protocoles, nous vous recommandons d'utiliser les clients pris en charge en mode natif répertoriés ci-dessus.

Les clients peuvent également se connecter à Exchange Server à l'aide du protocole Microsoft® Exchange ActiveSync®. Les clients qui utilisent ActiveSync sont les plates-formes principalement mobiles, telles que les clients Windows Phone 7 et ultérieurs. Les clients ActiveSync utilisant également HTTPS pour se connecter au serveur d'accès au client, aucune configuration supplémentaire n'est nécessaire côté serveur d'accès au client, sauf éventuellement celle des stratégies ActiveSync.

 **Remarque :** L'application de courrier dans Windows 8 utilise également le protocole ActiveSync pour se connecter à Exchange Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration du rôle serveur d'accès au client

Après avoir déployé un serveur d'accès au client dans votre infrastructure Exchange, vous devez configurer des options afin d'optimiser ses paramètres selon vos besoins. Vous devez configurer les espaces de noms et les certificats, ainsi que les options de sécurité et d'authentification. Le serveur d'accès au client communiquant avec les serveurs et les clients sur Internet, il est conseillé de prêter une attention particulière à ce point lors de la configuration. Dans cette leçon, vous allez apprendre à configurer le rôle serveur d'accès au client.

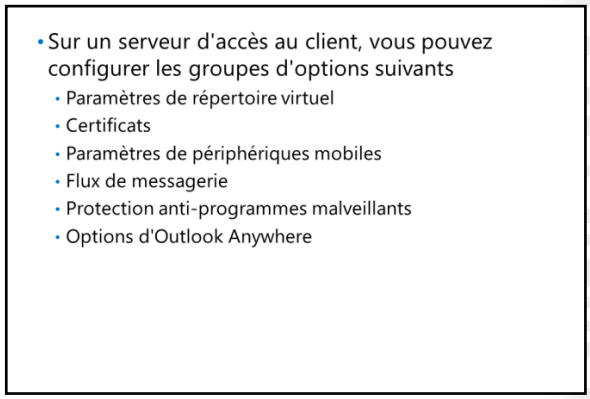
Objectifs de la leçon

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

- configurer les options du serveur d'accès au client ;
- configurer des espaces de noms sur le serveur d'accès au client ;
- configurer des certificats sur le serveur d'accès au client ;
- sécuriser le serveur d'accès au client ;
- configurer l'authentification sur le serveur d'accès au client ;
- configurer le serveur d'accès au client pour l'accès à Internet ;
- configurer l'accès aux clients POP3 et IMAP4.

Configuration des options du serveur d'accès au client

Après avoir initialement déployé un rôle serveur d'accès au client, il existe plusieurs options que vous devez configurer avant de placer le serveur d'accès au client en production. Il est possible de configurer le serveur d'accès au client à partir de l'environnement de ligne de commande Exchange Management Shell ou en utilisant le Centre d'administration Exchange (CAE). Dans le CAE, vous pouvez configurer des options dans les catégories suivantes sur le serveur d'accès au client :



- Paramètres de répertoire virtuel.
  Ces paramètres permettent de configurer chacun des répertoires virtuels que le serveur d'accès au client héberge sur IIS. Pour chaque répertoire virtuel, il est possible de configurer les paramètres et les options d'authentification générale.
- Certificats. Nous recommandons fortement aux organisations de déployer un certificat public ou publié en interne sur le serveur d'accès au client, et de remplacer les certificats auto-signés. Le volet Certificats du Centre d'administration Exchange vous permet de gérer les certificats et de créer de nouvelles demandes de certificat.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

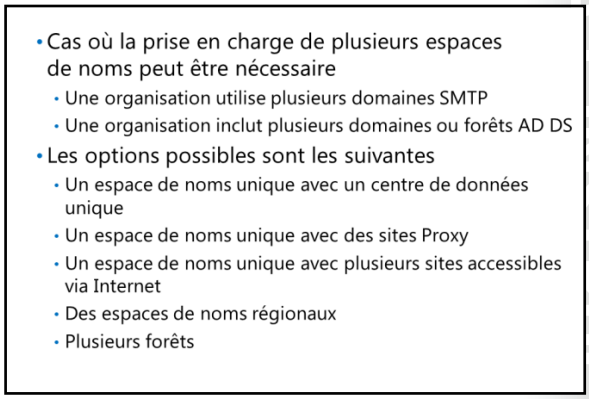
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Paramètres de périphériques mobiles. Le serveur d'accès au client gère également les options pour les appareils mobiles. Il est possible de configurer des règles d'accès aux appareils et de gérer des appareils mobiles en quarantaine. Vous pouvez également gérer des stratégies de boîtes aux lettres d'appareil mobile.
- Flux de messagerie. Les administrateurs peuvent utiliser ce nœud dans le Centre d'administration Exchange pour gérer le composant de transport qui se trouve sur le serveur d'accès au client. La gestion du composant de transport inclut la configuration des rapports de remise, des domaines acceptés et des connecteurs d'envoi et de réception.
- Protection anti-programmes malveillants. Puisque le serveur d'accès au client inclut le filtrage des programmes malveillants, le Centre d'administration Exchange permet de configurer les options de ce filtrage.
- Options d'Outlook Anywhere. Vous pouvez configurer des options pour l'authentification et les noms d'hôtes internes et externes.

Configuration d'espaces de noms sur un serveur d'accès au client

Avant de déployer Exchange Server 2013, il importe de prendre en considération l'implémentation de vos espaces de noms externes. Un espace de noms est une structure logique représentée par un nom de domaine DNS, par exemple adatum.com. Les décisions prises quant à l'espace de noms DNS ont des conséquences sur les éléments suivants :

- Configurations DNS
- Certificats numériques
- Configurations du client



Sélection d'un modèle d'espace de noms

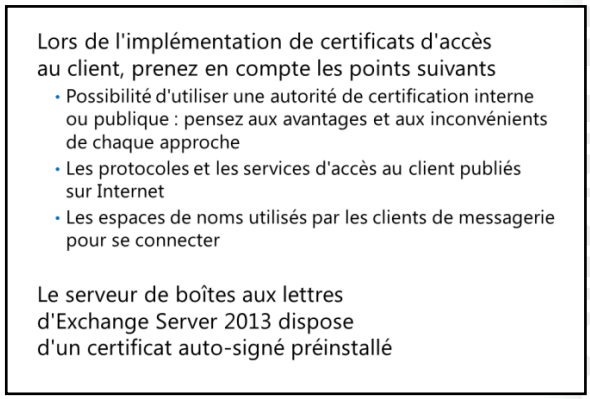
Faites coïncider vos espaces de noms avec la configuration de votre site. En particulier, pensez à implémenter un espace de noms distinct pour chaque site qui contient un serveur Internet d'accès au client. Il est possible de configurer Exchange Server 2013 en fonction d'un des modèles d'organisation suivants :

- Centre de données centralisées. Dans ce scénario, tous les serveurs Exchange sont situés dans un site physique avec un espace de noms unique, tel que mail.adatum.com. Avec ce modèle, il y a peu d'enregistrements DNS à configurer, moins de certificats à gérer, et seulement une URL pour les ordinateurs clients. Cependant, ce modèle ne prend pas en charge la tolérance aux pannes de site via l'utilisation de plusieurs centres de données.
- Espace de noms unique avec sites Proxy. Un seul site contient un serveur Internet d'accès au client. Par conséquent, ce modèle utilise un seul espace de noms. Avec ce modèle, vous devez configurer moins d'enregistrements DNS et gérer moins de certificats. De plus, les ordinateurs clients utilisent une seule URL externe. Cependant, étant donné qu'il est possible que beaucoup de sites ne contiennent pas de serveur Internet d'accès au client, de nombreux utilisateurs accéderont à leurs boîtes aux lettres en utilisant un proxy.

- Espace de noms unique et plusieurs sites. Chaque site peut avoir un serveur Internet d'accès au client, ou un seul site peut contenir les serveurs Internet d'accès au client. Dans ce modèle, les sites utilisent un espace de noms. N'oubliez pas que puisqu'il existe un espace de noms unique, il est plus facile de gérer les DNS et les certificats, et les ordinateurs clients utilisent une seule URL externe.
- Espaces de noms régionaux. Ce modèle est constitué de plusieurs sites physiques et de plusieurs espaces de noms. Par exemple, un site situé à Seattle peut avoir l'espace de noms mail.usa.adatum.com, alors qu'un site situé à Vancouver, en Colombie-Britannique, pourrait avoir l'espace de noms mail.canada.adatum.com. Ce modèle réduit les connexions par proxy, mais il y a plus d'enregistrements DNS et de certificats à gérer. En outre, vous devez configurer les ordinateurs clients avec l'URL externe appropriée.
- Plusieurs forêts. Ce modèle se compose de plusieurs forêts qui ont plusieurs espaces de noms. Une organisation qui utilise ce modèle peut être composée de deux sociétés partenaires. Les espaces de noms pourraient comprendre mail.usa.adatum.com et mail.europe.contoso.com.

Configuration de certificats sur le serveur d'accès au client

En raison de l'importance que revêt l'utilisation d'un trafic réseau sécurisé SSL entre les serveurs d'accès au client et les clients de messagerie, vous devez impérativement déployer les certificats appropriés sur les serveurs d'accès au client. Pour sécuriser toutes les connexions clientes au serveur d'accès au client, utilisez SSL.



Remarque : Par défaut, le serveur d'accès au client est configuré avec un certificat auto-signé non approuvé par les clients. Vous devez supprimer ce certificat et installer un certificat provenant d'une autorité de certification approuvée.

L'un des éléments les plus importants à prendre en compte lorsque vous envisagez d'utiliser des certificats est d'identifier la source de ces certificats. Exchange Server 2013 peut utiliser des certificats auto-signés, des certificats émis par une autorité de certification publique, ou des certificats émis par une autorité de certification privée. Chaque type de certificat a des avantages et des inconvénients, qui sont décrits ci-dessous.

L'utilisation d'une autorité de certification publique offre les avantages suivants :

- Les ordinateurs clients en interne et sur Internet approuvant déjà l'autorité de certification racine, les certificats peuvent être reliés à la racine sans aucune configuration supplémentaire.
- L'autorité de certification publique fournit des services complets de gestion des certificats et de gestion de révocation de certificats.

Le principal inconvénient concernant l'utilisation d'une autorité de certification publique est que les certificats émis par celles-ci sont plus chers que les certificats auto-signés ou que ceux émis par les autorités de certification internes.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les sociétés qui choisissent d'utiliser une autorité de certification interne pour déployer des certificats vers Exchange Server profitent des avantages suivants :

- La révocation étant gérée en interne, les certificats peuvent être révoqués de manière centralisée si une clé privée est compromise.
- En gérant votre propre autorité de certification, vous avez plus de flexibilité quant à la manière de gérer la distribution des certificats.

Les certificats émis en interne présentent également des inconvénients, notamment :

- L'implémentation d'une autorité de certification interne peut s'avérer compliquée, ce qui peut entraîner des problèmes de sécurité si l'autorité n'est pas gérée correctement.
- Bien que les certificats émis par les autorités de certification internes soient gratuits, les opérations d'implémentation et de gestion d'une autorité de certification peuvent s'avérer plus coûteuses que d'acheter des certificats auprès d'une autorité de certification publique.
- Les ordinateurs clients qui ne sont pas membres d'un domaine Active Directory interne n'approuvent pas automatiquement l'autorité de certification racine. Par conséquent, vous devez ajouter des certificats pour la racine approuvée sur les ordinateurs clients si nécessaire.

Les certificats auto-signés peuvent être déployés sans requérir d'infrastructure à clé publique (PKI). Lorsque vous installez Exchange Server 2013, un certificat auto-signé est créé automatiquement pour chaque ordinateur Exchange Server. Cependant, il n'y a aucune liste de révocation centralisée. Si la clé privée du certificat est compromise, chaque partie de confiance doit être avertie manuellement et invitée à se procurer un nouveau certificat et à ne plus utiliser le certificat existant.

Dans un environnement Exchange Server 2013, il est possible d'utiliser les certificats auto-signés pour la communication interne. Ces certificats peuvent également permettre de sécuriser les connexions clientes aux serveurs d'accès au client dans des scénarios de test ou d'évaluation. Cependant, ce certificat n'étant approuvé par aucun des ordinateurs clients, cette solution n'est pas recommandée pour un environnement de production. Vous devez plutôt envisager de vous procurer un certificat auprès d'une autorité de certification publique ou interne pour tous les serveurs d'accès au client.

Dans la plupart des cas, si les utilisateurs accèdent au serveur d'accès au client via Internet, vous devez déployer un certificat émis par une autorité de certification publique. Si seuls les ordinateurs membres du domaine interne accèdent au serveur d'accès au client, il peut être envisageable d'utiliser une autorité de certification interne ou privée. En déployant une autorité de certification d'entreprise, il est possible d'automatiser le processus de distribution et de gestion des certificats et des listes de révocation des certificats.

Remarque : Si vous planifiez d'activer le partage fédéré, vous devez obtenir, auprès d'une autorité de certification publique approuvée, un certificat pour vos serveurs d'accès au client accessibles via Internet.

Certificats sur le rôle serveur de boîtes aux lettres

Dans Exchange Server 2013, le rôle serveur de boîtes aux lettres est également fourni avec des certificats auto-signés préinstallés. Par défaut, la communication HTTP, Microsoft Exchange ActiveSync, POP3 et IMAP4 entre les serveurs de boîtes aux lettres et le serveur d'accès au client, les contrôleurs de domaine et les serveurs de catalogues globaux est chiffrée à l'aide de SSL. Toutefois, étant donné que les clients ne se connectent pas directement au serveur de boîtes aux lettres, il n'est pas accessible depuis Internet et il n'est donc pas nécessaire de remplacer ces certificats par un certificat public. Vous pouvez choisir de remplacer un certificat sur le rôle serveur de boîtes aux lettres par un certificat émis en interne, mais ce n'est pas obligatoire.

Planification des noms de certificat

Pour garantir que les clients puissent se connecter au serveur d'accès au client à l'aide de SSL sans recevoir de message d'erreur, les noms sur le certificat doivent correspondre aux noms que les clients utilisent pour se connecter au serveur. Par exemple, si vos utilisateurs se connectent au site Outlook Web App à l'aide d'une URL telle que https://mail.adatum.com/owa et qu'ils se connectent au serveur IMAP4 à l'aide d'un nom tel qu'IMAP.adatum.com, vous devez vérifier que les certificats que vous utilisez prennent en charge les deux noms de serveur. En outre, si vous activez l'accès à la découverte automatique à partir d'Internet, votre certificat doit également prendre en charge un nom tel qu'Autodiscover.adatum.com. La découverte automatique est utilisée pour configurer automatiquement Outlook et les paramètres de profil des appareils mobiles.

Il est possible d'implémenter cette configuration en utilisant les options suivantes :

- Procurez-vous un certificat distinct pour chaque protocole client qui requiert un nom unique. Cette méthode peut nécessiter plusieurs certificats pour tous les serveurs d'accès au client, et requérir plusieurs sites Web dans IIS. Il s'agit de l'option la plus complexe à configurer.
- Configurez tous les clients pour qu'ils utilisent le même nom de serveur. Par exemple, il est possible de configurer tous les clients pour qu'ils utilisent le nom du serveur mail.contoso.com et obtenir un certificat uniquement pour ce nom.
- Obtenez un certificat avec plusieurs autres noms de l'objet. La plupart des autorités de certification publiques prennent en charge l'utilisation de plusieurs noms dans l'extension d'autre nom de l'objet du certificat. Lorsque vous utilisez l'un de ces certificats, les clients peuvent se connecter au serveur d'accès au client à l'aide de chacun des noms répertoriés dans l'autre nom de l'objet.
- Utilisez un certificat avec caractères génériques. La plupart des autorités de certification publiques prennent également en charge l'utilisation de caractères génériques dans la demande de certificat. Il est par exemple possible de demander un certificat à l'aide de l'objet *.contoso.com et utiliser ce certificat pour les connexions clientes.

Tous les clients ne prennent pas en charge les certificats avec caractères génériques. Le déploiement de certificats avec caractères génériques peut poser un problème de sécurité dans de nombreuses organisations, car le certificat peut être utilisé pour tout nom de serveur dans le domaine. Si ce certificat est compromis, tous les noms d'hôte de l'organisation sont également compromis.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

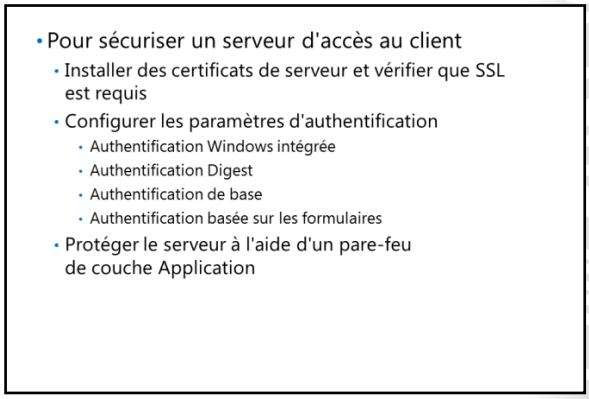
Démonstration : Création d'une demande de certificat sur un serveur d'accès au client

Procédure de démonstration

1. Ouvrez le Centre d'administration Exchange (CAE) sur LON-CAS1, puis connectez-vous en tant qu'**ADATUM\Administrateur**.
2. Cliquez sur **Certificats** dans le volet des fonctionnalités.
3. Lancez l'assistant pour créer un nouveau certificat Exchange.
4. Fournissez **mail.adatum.com** pour le nom convivial.
5. Fournissez **mail.adatum.com** comme valeur pour les services Web.
6. Suivez les champs suivants comme suit :
   a. Nom de l'organisation : **A.Datum**
   b. Nom du service : **Informatique**
   c. Nom du pays/de la région : **France**
   d. Ville/Localité : **Seattle**
   e. État/province : **WA**
7. Enregistrez la demande sur **\\lon-cas1\C$\windows\temp\certreq.req**.

Sécurisation d'un serveur d'accès au client

Dans de nombreuses organisations, le serveur d'accès au client est accessible via Internet pour les clients Outlook Anywhere, Outlook Web App ou Exchange ActiveSync. Il est par conséquent essentiel de vérifier que le serveur d'accès au client qui est connecté à Internet est sécurisé au maximum.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sécurisation des communications entre les clients et les serveurs d'accès au client

Pour chiffrer le trafic réseau entre les clients de messagerie et le serveur d'accès au client, vous devez sécuriser le trafic réseau à l'aide du protocole SSL. Pour configurer le serveur d'accès au client de sorte qu'il utilise le protocole SSL, procédez comme suit :

1. Procurez-vous un certificat de serveur et installez-le sur le serveur d'accès au client. Vérifiez que le nom du certificat correspond exactement au nom du serveur dont se serviront les utilisateurs pour accéder au serveur d'accès au client. Assurez-vous que les répertoires virtuels du serveur d'accès au client dans IIS sont configurés pour exiger SSL.
2. Sécurisez les répertoires virtuels suivants :
    - Découverte automatique
    - Panneau de configuration Exchange
    - Services Web Exchange (EWS)
    - Microsoft-Server-ActiveSync
    - Carnet d'adresses en mode hors connexion (OAB)
    - Outlook Web App (OWA)
    - Windows PowerShell

Par défaut, tous ces dossiers virtuels sont configurés pour exiger SSL, une fois que le rôle serveur d'accès au client Exchange Server est installé. Nous vous recommandons de n'effectuer aucune modification.

Configuration d'une authentification sécurisée

Exchange Server 2013 fournit plusieurs options d'authentification aux clients qui communiquent avec le serveur d'accès au client. Si plusieurs options d'authentification sont activées sur le serveur, Exchange Server 2013 négocie avec le client la méthode d'authentification la plus sécurisée qu'ils prennent tous les deux en charge.

Options d'authentification standard

Les options d'authentification standard suivantes sont disponibles sur le serveur d'accès au client :

- Authentification Windows intégrée. Il s'agit de l'option d'authentification standard la plus sécurisée. Avec l'authentification Windows intégrée, lorsque les utilisateurs ouvrent une session avec un compte de domaine, ils ne sont pas invités à entrer de nom d'utilisateur ni mot de passe. En revanche, le serveur négocie avec les packages de sécurité Windows installés sur l'ordinateur client afin d'obtenir le nom d'utilisateur et le mot de passe de l'utilisateur connecté. Les informations d'authentification non chiffrées ne sont pas transférées sur le réseau. Pour que l'authentification Windows intégrée fonctionne à partir d'un navigateur Web, l'URL du serveur d'accès au client doit être dans la zone de l'Intranet du client.
- Authentification Digest. Lorsque vous utilisez l'authentification Digest, le mot de passe est sécurisé en étant transmis sous forme de valeur de hachage sur le réseau.
- Authentification de base. Avec cette méthode, le mot de passe est transmis en texte clair sur le réseau. Par conséquent, vous devez toujours sécuriser l'authentification de base à l'aide du chiffrement SSL. L'authentification de base constitue l'option d'authentification dont la prise en charge est la plus répandue auprès des clients. L'authentification unique n'étant pas prise en charge, les informations d'identification de l'utilisateur ne sont jamais transmises automatiquement via l'authentification de base.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Authentification basée sur les formulaires

L'authentification basée sur les formulaires est disponible uniquement pour Outlook Web App et CAE. Lorsque cette option est utilisée, elle remplace les autres méthodes d'authentification. C'est l'option d'authentification par défaut pour Outlook Web App, parce qu'elle fournit une sécurité renforcée. Lorsque vous utilisez l'authentification basée sur les formulaires, Exchange Server utilise des cookies pour chiffrer les informations d'identification d'ouverture de session dans le navigateur Web de l'ordinateur client. Le suivi de l'utilisation de ces cookies permet à Exchange Server de spécifier un délai d'expiration pour les sessions inactives. L'application d'un délai d'expiration automatique aux sessions inactives est d'une grande importance, car elle permet de protéger les comptes d'utilisateurs contre les accès non autorisés si les utilisateurs s'éloignent de l'ordinateur alors que leur session est active.

Le délai s'écoulant avant l'expiration d'une session inactive varie selon le type d'ordinateur sélectionné pendant l'ouverture de session. S'il s'agit d'un ordinateur public ou partagé, la session expire après 15 minutes d'inactivité. S'il s'agit d'un ordinateur privé, la session expire après 12 heures d'inactivité.

Au lieu de créer une fenêtre publicitaire intempestive, l'authentification basée sur les formulaires crée une page Web d'ouverture de session pour Outlook Web App. Il est possible de modifier cette page en configurant l'invite d'ouverture de session (nom d'utilisateur, domaine\nom d'utilisateur ou nom principal de l'utilisateur), la langue, les graphismes et le texte. Les informations d'identification de l'utilisateur entrées dans la page de connexion Outlook Web App sont transmises en texte clair, comme pour l'authentification de base. Cependant, l'authentification basée sur les formulaires exige l'utilisation de SSL, qui chiffre les informations d'identification de l'utilisateur lorsqu'elles sont transmises sur le réseau.

L'authentification basée sur les formulaires est activée par défaut pour Outlook Web App et CAE.

Protection du serveur d'accès au client à l'aide d'un pare-feu de la couche Application

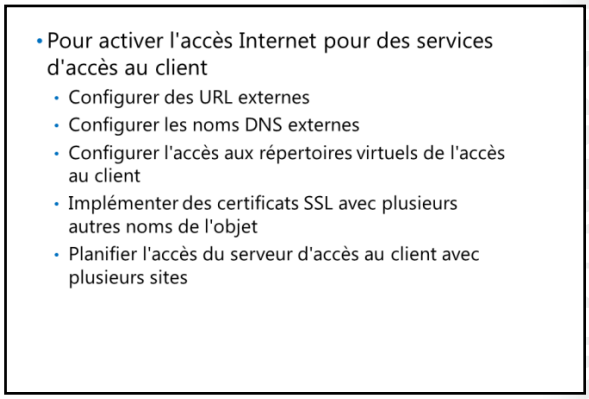
Pour offrir une couche supplémentaire de sécurité au trafic réseau et protéger le serveur d'accès au client, déployez un pare-feu au niveau de la couche Application ou un proxy inverse entre Internet et le serveur d'accès au client. Les pare-feu de couche Application fournissent les avantages suivants :

- Il est possible de configurer le pare-feu en tant que point final de la connexion SSL cliente. Le pare-feu peut ensuite déchiffrer le trafic client, appliquer le filtrage de couche Application, puis chiffrer à nouveau le trafic avant de l'envoyer au serveur d'accès au client.
- Il est possible de décharger le déchiffrement SSL vers le pare-feu. Si vous n'avez pas besoin de sécuriser toutes les connexions sur votre réseau interne, il est possible de configurer le pare-feu afin de déchiffrer le trafic SSL, sans chiffrer à nouveau avant d'envoyer le trafic au serveur d'accès au client. Cela signifie que les ressources du serveur d'accès au client ne sont pas utilisées pour exécuter les opérations de déchiffrement et de chiffrement SSL.
- Si vous utilisez Forefront Threat Management Gateway 2010 comme pare-feu de couche Application, il est possible de configurer le pare-feu pour pré-authentifier toutes les connexions clientes à l'aide de l'authentification basée sur les formulaires. Dans ce cas, seules les connexions authentifiées seront autorisées dans le réseau interne.

 **Remarque :** Threat Management Gateway 2010 n'est pas entièrement pris en charge pour la publication de services d'Exchange Server 2013. Cependant, il est possible d'utiliser l'Assistant de publication pour qu'Exchange Server 2010 publie Exchange Server 2013, mais il sera ensuite nécessaire d'effectuer des configurations manuelles supplémentaires.

Configuration du serveur d'accès au client pour l'accès Internet

Pour activer l'accès au serveur d'accès au client à partir d'Internet, procédez comme suit :



1. Configurez les URL externes pour chacune des options de client requises. Il est possible de configurer toutes les fonctionnalités Web du serveur d'accès au client avec une URL externe. Cette URL est utilisée pour accéder au site Web à partir d'emplacements externes. Par défaut, l'URL externe est vierge. Pour les serveurs d'accès au client qui font face à Internet, l'URL externe ne doit pas être configurée pour utiliser le nom publié dans le DNS (Domain Name System) pour ce site Active Directory. L'URL externe doit utiliser également le même nom que celui utilisé pour le certificat de serveur. Pour les serveurs d'accès au client qui n'auront pas de présence sur Internet, ce paramètre doit rester vierge.
2. Configurez la résolution de noms DNS externe. Pour chaque serveur d'accès au client exposé à Internet, vous devez vérifier que le nom d'hôte peut être résolu sur Internet. Pour cela, ajoutez un enregistrement d'hôte pour le serveur d'accès au client dans la zone DNS, sur le serveur DNS qui héberge la zone DNS Internet pour votre organisation. Si vous utilisez des noms d'hôte différents pour chaque serveur d'accès au client, vous devez configurer un enregistrement d'hôte pour chaque hôte.
3. Configurez l'accès aux répertoires virtuels du serveur d'accès au client. Chacune des méthodes d'accès utilise un répertoire virtuel différent. Si vous utilisez un pare-feu standard ou pare-feu de couche Application qui filtre des demandes des clients selon le répertoire virtuel, vous devez vérifier que tous les répertoires virtuels sont accessibles via le pare-feu.
4. Implémentez des certificats SSL avec plusieurs autres noms de l'objet. Si vous utilisez plusieurs noms d'hôte pour les services d'accès au client, ou si vous publiez la découverte automatique sur Internet, vérifiez que les noms du serveur obligatoires sont répertoriés dans l'extension de l'autre nom de l'objet pour les certificats SSL que vous déployez sur chaque serveur d'accès au client.
5. Planifiez l'accès du serveur d'accès au client avec plusieurs sites. Si votre organisation a plusieurs emplacements et sites Active Directory, et que vous déployez des serveurs Exchange sur chaque site, vous devez en premier lieu décider si les serveurs d'accès au client sur chaque site seront accessibles via Internet. Si vous choisissez de ne pas rendre les serveurs Exchange Server dans les sites spécifiques accessibles à partir d'Internet, vous ne devez pas configurer d'URL externe. Toutes les demandes clientes sur ce serveur peuvent servir de proxy à partir d'un serveur d'accès au client accessible via Internet. Si vous décidez de rendre le serveur d'accès au client d'un site accessible via Internet, vous devez compléter les étapes répertoriées ci-dessous pour chaque site.
    - Configurez une seule URL externe pour les serveurs d'accès au client qui sont accessibles à partir d'Internet.
    - Vérifiez que les enregistrements d'hôte pour chaque site sont ajoutés à la zone DNS appropriée.
    - Configurez les pare-feu et certificats SSL pour chaque site.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration d'accès à des clients POP3 et IMAP4

Par défaut, Exchange Server 2013 prend en charge les connexions clientes POP3 et IMAP4, mais ces services sont configurés pour démarrer manuellement. Si vous souhaitez activer l'accès utilisateur pour ces protocoles, vous devez démarrer les services et les configurer pour démarrer automatiquement. Pour ce faire, il est possible d'utiliser la console de services ou l'environnement de ligne de commande Exchange Management Shell.

Option	Description
Liaisons	Permet de configurer les adresses de serveur local
Authentification	Permet de configurer les options d'authentification
Paramètres de connexion	Permet de configurer les paramètres de connexion au serveur
Paramètres de récupération	Permet de configurer les formats de message et les paramètres de récupération du calendrier
Accès utilisateur	Permet de déterminer si un utilisateur peut utiliser le protocole

Pour utiliser l'environnement de ligne de commande Exchange Management Shell, vous devez exécuter les applets de commande suivantes sur l'ordinateur qui exécute le rôle serveur d'accès au client :

```
Set-service msExchangePOP3 -startuptype automatic
Start-service msExchangePOP3
```

Sur l'ordinateur exécutant le rôle serveur de boîtes aux lettres, vous devez exécuter les applets de commande suivants :

```
Set-service msExchangePOP34BE -startuptype automatic
Start-service msExchangePOP3BE
```

Options de configuration

Si vous choisissez d'activer l'accès POP3 ou IMAP4, il est possible de configurer les paramètres suivants :

- Liaisons. Active la configuration des adresses du serveur local qui seront utilisées pour des connexions non chiffrées, TLS ou SSL.
- Authentification. Active la configuration d'options d'authentification prises en charge. Les options prises en charge sont les suivantes : authentification de base, authentification Windows intégrée et ouverture de session sécurisée nécessitant TLS. Le paramètre par défaut est l'ouverture de session sécurisée.
- Connexion. Active la configuration de paramètres de serveur, tels que les paramètres de délais, les limites de connexion et le relais de commande ou le port cible du proxy (utilisé pour les connexions à un serveur principal Exchange Server 2003).
- Récupération. Active la configuration des formats de message utilisés pour ces protocoles, et permet de configurer comment les clients récupéreront des demandes de calendrier.
- Accès utilisateur. Sur chaque compte d'utilisateur, il est possible d'activer ou de désactiver l'accès pour les protocoles POP3 et IMAP4. Par défaut, l'accès est activé pour tous les utilisateurs.

Leçon 3
Gestion des services d'accès au client

Les serveurs d'accès au client dans Exchange Server 2013 fournissent plusieurs services pour les clients Outlook Office. Habituellement, ces services sont activés par défaut pour les clients Outlook sur le réseau interne, mais vous devrez peut-être modifier certains de ces paramètres. En outre, il est possible de mettre certains de ces services à disposition des clients Outlook qui se connectent à des serveurs Exchange en dehors du déploiement. Dans ce cas, vous devez activer ces fonctionnalités et vérifier qu'elles sont configurées correctement.

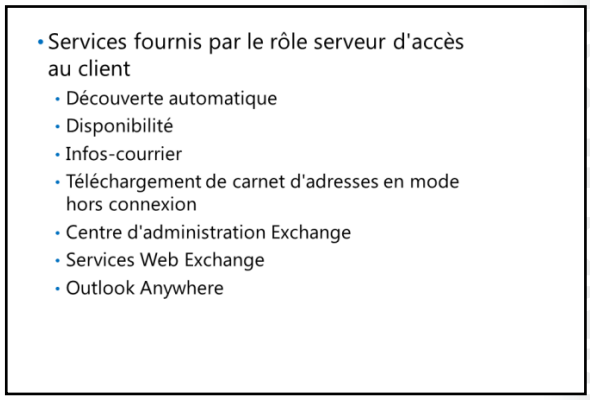
Objectifs de la leçon

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

- décrire les services fournis par le serveur d'accès au client ;
- décrire la découverte automatique ;
- configurer et gérer la découverte automatique ;
- décrire le service de disponibilité ;
- décrire les infos-courrier ;
- configurer des infos-courrier.

Services fournis par le serveur d'accès au client

Dans Exchange Server 2013, le rôle serveur d'accès au client fournit des services essentiels pour tous les clients de la messagerie, notamment les clients Outlook Office. Voici une liste des services que le rôle serveur d'accès au client fournit :

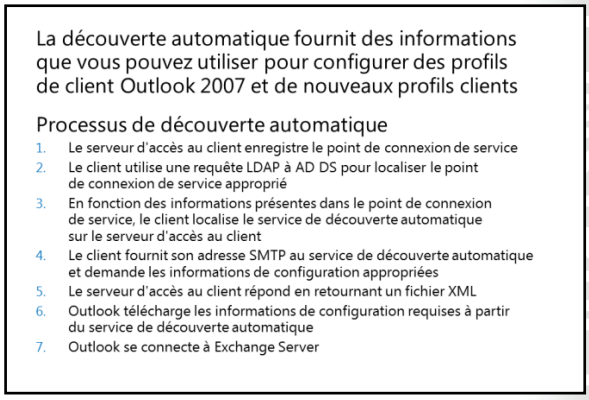


- *Découverte automatique*. Ce service configure des ordinateurs clients qui exécutent Outlook 2007 ou une version plus récente, ou des appareils mobiles pris en charge. Le processus de découverte automatique configure le profil du client Outlook, notamment le serveur de boîtes aux lettres, le service de disponibilité et les emplacements de téléchargement de carnet d'adresses en mode hors connexion (OAB).
- *Disponibilité*. Ce service est utilisé pour rendre des informations sur la disponibilité disponibles pour Outlook 2007 (et versions plus récentes) et aux clients Outlook Web App. Le service de disponibilité récupère les informations de disponibilité auprès des serveurs de boîtes aux lettres ou des dossiers publics, et présente ces informations aux clients.
- *Infos-courrier*. Cette fonctionnalité fournit des notifications aux utilisateurs concernant des problèmes potentiels liés à l'envoi d'un message, avant que celui-ci ne soit envoyé. Les infos-courrier sont prises en charge dans Outlook 2010 ou version plus récente.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *Téléchargement de carnet d'adresses en mode hors connexion*. Le serveur d'accès au client rend l'OAB disponible via un service Web. Seul les clients Microsoft Office Outlook 2007 ou version ultérieure peuvent récupérer les carnets d'adresses en mode hors connexion à partir d'un service Web.
- *CAE*. Le Centre d'administration Exchange est une interface de gestion basée sur le Web qui peut être utilisée pour gérer Exchange Server.
- *Services Web Exchange*. Les services Web Exchange permettent à des applications clientes de communiquer avec Exchange Server. Il est également possible d'accéder aux services Web Exchange par programme. Ces services permettent d'accéder à une grande partie des données accessibles via Office Outlook. Les clients des services Web Exchange peuvent intégrer des données Outlook dans des applications métier.
- *Outlook Anywhere*. Outlook Anywhere permet aux clients Outlook 2007 (ou version ultérieure) d'accéder à la boîte aux lettres utilisateur en utilisant des appels de procédure distante (RPC) encapsulés dans un paquet HTTP ou HTTPS. Cela permet d'activer l'accès sécurisé aux boîtes aux lettres utilisateur de clients situés sur Internet.

Qu'est-ce que la découverte automatique ?



Le service de découverte automatique d'Exchange Server 2013 simplifie la configuration du client dans Office Outlook 2007, 2010 et 2013. La découverte automatique fournit les informations de configuration dont Outlook a besoin pour créer un profil de configuration pour le client. Les clients Outlook peuvent également utiliser le service de découverte automatique pour réparer des paramètres de connexion Exchange Server ou si la boîte aux lettres utilisateur est déplacée vers un autre serveur. Le service de découverte automatique fournit des paramètres de profil aux clients Outlook 2007, 2010 et 2013 et aux appareils mobiles pris en charge en fonction de l'adresse de messagerie et du mot de passe de l'utilisateur.

Remarque : Fournir uniquement une adresse de messagerie et un mot de passe pour la configuration automatique avec la découverte automatique fonctionne uniquement lorsque l'adresse de messagerie de l'utilisateur est égale à son UPN. Si ce n'est pas le cas, l'utilisateur doit indiquer le nom d'utilisateur et le nom de domaine appropriés.

Lors de la création du profil, la découverte automatique fournit des informations permettant au client de localiser différents services Web, tels que le service de disponibilité, les paramètres de messagerie unifiée et les carnets d'adresses en mode hors connexion (OAB).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fonctionnement de la découverte automatique

Le client Outlook se connecte à Exchange Server 2013 de la façon suivante :

1. Lorsque vous installez le rôle serveur d'accès au client, un point de connexion de service (SCP) est automatiquement configuré dans AD DS pour le serveur d'accès au client. Le SCP aide les clients Outlook à trouver le serveur d'accès au client le plus proche de leur site AD DS. Chaque serveur d'accès au client inscrit son SCP dans AD DS. Ce SCP comprend deux informations : l'URI de découverte automatique et paramètre d'étendue du site de découverte automatique. L'identificateur de ressource uniforme (URI) de la découverte automatique et le paramètre d'étendue du site de découverte automatique. Le paramètre d'étendue du site spécifie un ou plusieurs sites AD DS pour lesquels le serveur d'accès au client spécifique est responsable. En tirant parti du paramètre d'étendue de site, il est possible d'optimiser la couverture du serveur d'accès au client si vous avez plusieurs sites AD DS avec des clients Outlook. Le SCP est utilisé uniquement par les clients joints au domaine et connectés au réseau interne. Les clients effectuent une demande LDAP (Lightweight Directory Access Protocol) à AD DS pour obtenir les informations SCP.
2. Lorsque Outlook 2007 ou une version plus récente démarre pour la première fois sur un ordinateur joint à un domaine, Outlook récupère le nom d'utilisateur ou l'adresse de messagerie et le mot de passe de l'utilisateur, et effectue ensuite la requête à AD DS pour localiser le SCP. Si l'ordinateur n'est pas joint au domaine, vous devez taper votre adresse de messagerie (ou nom d'utilisateur) et mot de passe manuellement.
3. Si Outlook s'exécute sur un ordinateur joint à un domaine, il utilise ensuite les informations du SCP pour localiser le service de découverte automatique sur un ordinateur Exchange Server 2013 sur lequel le rôle serveur d'accès au client est installé. Si vous accédez à un serveur d'accès au client Exchange de l'extérieur, ou depuis un ordinateur qui n'est pas joint à votre domaine, alors le client recherche l'hôte de découverte automatique dans DNS. Ensuite, Outlook est redirigé vers le dossier de découverte automatique sur le serveur d'accès au client, sur lequel le client effectue une demande de téléchargement des informations de configuration.
4. La demande que le client envoie au serveur d'accès au client est en fait la commande de HTTP POSTS vers le point de terminaison du serveur de découverte automatique, qui demande les informations de configuration de l'adresse SMTP que le client envoie dans la requête.
5. Le serveur d'accès au client fournit les informations de découverte automatique au client. Parmi ces informations figurent les emplacements du service Web de disponibilité, du carnet d'adresse en mode hors-connexion, du panneau de configuration Exchange, d'Outlook Web Access et de la messagerie unifiée.
6. Outlook télécharge et applique les informations de configuration requises à partir du service de découverte automatique.
7. Outlook utilise ensuite les paramètres de configuration appropriés pour se connecter à Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'emplacement où les informations de découverte automatique sont générées peut varier selon la version d'Exchange Server sur laquelle se trouve la boîte aux lettres cliente. Lorsque le client se connecte au serveur d'accès au client 2013 avec une demande de découverte automatique, soit parce que le SCP le dirige vers cet emplacement, soit parce qu'il est envoyé à l'aide de DNS, le serveur d'accès au client se comportera comme suit :

- Si la boîte aux lettres cliente est sur Exchange Server 2007, le serveur d'accès au client 2013 envoie la demande au serveur de boîtes aux lettres 2013, ce qui génère les informations de découverte automatique pour le client.
- Si la boîte aux lettres client est sur Exchange Server 2010, le serveur d'accès au client 2013 effectue la demande au serveur d'accès au client 2010 par l'intermédiaire d'un proxy et renvoie la réponse au client.

Clients et protocoles pris en charge

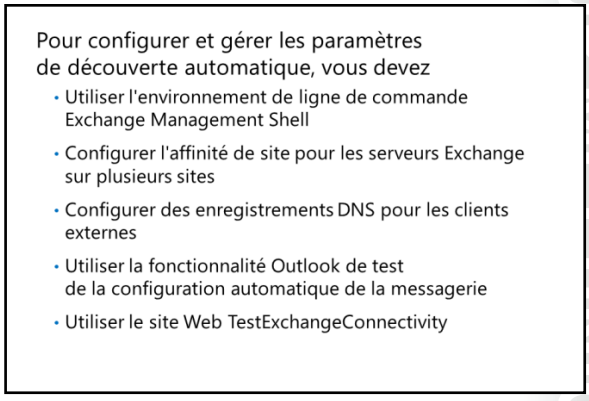
La fonction de découverte automatique prend en charge les clients et protocoles suivants :

Client	Protocole
Office Outlook	RPC sur HTTP
Outlook Anywhere	RPC sur HTTP
Exchange ActiveSync	Exchange ActiveSync sur HTTP
Entourage 2008, Web Services Edition	Services Web Exchange (HTTPS)

Remarque : Exchange Server 2013 prend en charge la découverte automatique pour les clients du service Exchange ActiveSync. Toutefois, le client du service Exchange ActiveSync doit exécuter Windows Phone 7 ou ultérieur pour prendre en charge cette fonctionnalité.

Configuration et gestion de la découverte automatique

Par défaut, les paramètres de découverte automatique pour les clients internes sont configurés automatiquement et le client Outlook 2007 ou ultérieur est configuré automatiquement pour utiliser les services appropriés. Dans certains cas, il est possible de modifier cette configuration par défaut. Pour les clients externes, vous devez configurer les paramètres DNS appropriés afin de vous assurer que ces clients peuvent localiser le serveur d'accès au client qui est accessible via Internet.



Configuration des paramètres de découverte automatique

Pour activer la découverte automatique, vous devez disposer d'au moins un serveur d'accès au client qui exécute le service de découverte automatique. Lorsque vous installez le rôle serveur d'accès au client, le répertoire virtuel de découverte automatique est créé automatiquement dans les services Internet (IIS).

Pour gérer les paramètres de découverte automatique, vous devez utiliser les applets de commande de l'environnement de ligne de commande Exchange Management Shell suivants :

- **Set-ClientAccessServer**. Configure le point de connexion du service de découverte automatique.
- **New-AutodiscoverVirtualDirectory**. Crée un répertoire virtuel de découverte automatique.
- **Remove-AutodiscoverVirtualDirectory**. Supprime un répertoire virtuel de découverte automatique.
- **Set-OutlookProvider**. Configure un fournisseur Office Outlook.
- **Get-OutlookProvider**. Localise un ou plusieurs fournisseurs Office Outlook dans le répertoire virtuel.

Généralement, vous ne devez pas modifier les paramètres de découverte automatique dans la configuration Exchange par défaut. Cependant, il existe certains scénarios où vous devrez peut-être le faire. Par exemple, si vous avez un programme d'équilibrage de la charge matérielle avec une adresse IP virtuelle pointant vers une adresse telle que mail.adatum.com, vous pouvez modifier l'URI interne pour utiliser mail.adatum.com au lieu des noms du serveur d'accès au client.

Configuration de la découverte automatique pour plusieurs sites

Si votre organisation a déployé des serveurs Exchange sur plusieurs sites Active Directory, vous devez envisager de configurer l'affinité de site pour le service de découverte automatique. Pour utiliser l'affinité de site, spécifiez les sites Active Directory préférés par les clients pour se connecter à une instance du service de découverte automatique spécifique. En général, l'affinité de site de découverte automatique est utilisée dans les scénarios où la connectivité entre tous vos sites n'est pas bonne et où vous souhaitez que les clients Outlook utilisent les services de découverte automatique sur un serveur d'accès au client vers lequel les clients ont une bonne connectivité. Dans un autre scénario, si la connectivité entre vos sites est acceptable, il peut être préférable que vos clients Outlook utilisent les services de découverte automatique sur un serveur d'accès au client dans un site local pour les clients.

Pour configurer l'affinité de site, utilisez l'applet de commande comme indiqué dans l'exemple suivant :

```
Set-ClientAccessServer -Identity "NomduServeur"
-AutodiscoverServiceInternalURI "https://VAN-EX1/autodiscover/autodiscover.xml"
-AutodiscoverSiteScope "HeadOffice"
```

Cet applet de commande configure l'URI pour que le service de découverte automatique dans le site HeadOffice utilise le serveur VAN-EX1.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de DNS pour la prise en charge de la découverte automatique

Pour que les clients externes puissent localiser les serveurs d'accès au client appropriés, vous devez configurer le DNS à l'aide des bonnes informations. Quand le client Outlook essaie de localiser le serveur d'accès au client, il tente tout d'abord de localiser les informations de point de connexion de service dans AD DS. Si le client est situé en dehors du réseau, Active Directory n'est pas disponible. Par conséquent, le client demande au DNS un nom de serveur basé sur l'adresse SMTP fournie par l'utilisateur. Office Outlook interroge le DNS sur les URL suivantes :

- https://<e-maildomain/autodiscover/autodiscover.xml
- https://autodiscover.e-maildomain/autodiscover/autodiscover.xml

Pour activer la découverte automatique, vous devez configurer un enregistrement DNS sur le serveur DNS externe utilisé par le client afin de fournir la résolution de noms pour cette demande. L'enregistrement DNS doit pointer vers un serveur d'accès au client qui est accessible depuis Internet, ou vers un serveur proxy inverse, tel que Forefront TMG, utilisé pour publier le serveur d'accès au client.

Utilisation de la fonctionnalité Tester la configuration automatique de la messagerie dans Outlook 2007 et versions ultérieures

Il est possible d'utiliser la fonctionnalité Tester la configuration automatique de la messagerie dans Outlook afin de tester si la fonctionnalité de découverte automatique fonctionne correctement. Pour réaliser ce test, maintenez la touche Ctrl enfoncée et cliquez sur l'icône d'Outlook dans la zone de notification, puis cliquez sur Configuration automatique de message électronique de test.

Il est également possible d'utiliser l'applet de commande de l'environnement de ligne de commande Exchange Management Shell TestOutlookWebServices pour tester les paramètres de découverte automatique sur un serveur d'accès au client. Pour bénéficier d'un outil très utile pour tester la fonctionnalité de découverte automatique de l'extérieur, accédez à https://www.testexchangeconnectivity.com/. Il s'agit d'un outil de test officiel de Microsoft, qu'il est possible d'utiliser pour tester la découverte automatique pour la connectivité ActiveSync et Outlook. Il peut être utilisé pour un serveur Exchange Server local, ainsi que pour tester la disponibilité des services dans Microsoft® Office 365.

Qu'est-ce que le service de disponibilité ?

Exchange Server 2013 utilise le service de disponibilité pour mettre les informations sur la disponibilité à la disposition des clients Outlook 2007 ou ultérieur, ainsi que des clients Outlook Web App. Le service de disponibilité remplace le dossier public utilisé pour stocker les informations de disponibilité dans les versions antérieures d'Exchange Server. Dans Outlook, l'Assistant Planification du composant vous permet de connaître les tranches de temps libres des participants dans leurs calendriers sans qu'ils partagent réellement leurs calendriers avec vous.

Le service de disponibilité sur un serveur d'accès au client permet d'effectuer les tâches suivantes

- Récupérer les informations de disponibilité les plus récentes pour les boîtes aux lettres dans l'organisation Exchange locale ou autre
- Afficher les heures de travail des participants
- Afficher les suggestions d'heures de réunion

- Seuls Outlook 2007 (ou version ultérieure) et Outlook Web App utilisent le service de disponibilité
- Le service de disponibilité est déployé par défaut sur tous les serveurs d'accès au client
- Le service n'a besoin d'aucune configuration par défaut

L'Assistant Planification utilise le service de disponibilité pour :

- récupérer les informations de disponibilité les plus récentes pour les boîtes aux lettres Exchange Server 2007, Exchange Server 2010 ou Exchange Server 2013 ;
- récupérer les informations de disponibilité les plus récentes provenant d'autres organisations Exchange Server 2007, Exchange Server 2010 ou Exchange Server 2013 ;
- afficher les heures de travail des participants ;
- afficher les suggestions d'heures de réunion.

Remarque : Seuls Outlook 2007 (ou version ultérieure) et Outlook Web App utilisent le service de disponibilité.

Fonctionnement du service de disponibilité

Le service de disponibilité fournit des informations de disponibilité par l'intermédiaire du processus suivant :

1. Lorsque vous démarrez l'Assistant Planification dans des clients Outlook 2007 ou version ultérieure ou dans le client Outlook Web App, le client envoie une demande à l'URL qui lui a été fournie pendant l'exécution de la découverte automatique. La demande comprend tous les utilisateurs invités, y compris les boîtes aux lettres de ressources.
2. Le service de disponibilité du serveur d'accès au client interroge Active Directory pour déterminer l'emplacement des boîtes aux lettres des utilisateurs. Pour toutes les boîtes aux lettres situées sur le même site que le serveur d'accès au client, la demande est envoyée directement au serveur de boîtes aux lettres afin de récupérer les informations de disponibilité actuelles de l'utilisateur.
3. Si la boîte aux lettres se trouve sur un autre site que celui du serveur d'accès au client, la demande est transmise au serveur de boîtes aux lettres de ce site par l'intermédiaire d'un proxy. Si un autre site exécute Exchange Server 2010, la demande est envoyée par proxy à un serveur d'accès au client 2010 sur le site où se trouve la boîte aux lettres de l'utilisateur. Le service de disponibilité combine les informations de disponibilité de tous les utilisateurs invités et les présente au client Outlook 2007 ou Outlook Web App.

Il est également possible de configurer le serveur d'accès au client pour interroger le service de disponibilité d'une autre organisation Exchange Server 2013. Il est ainsi possible de partager les informations de planification entre des organisations Exchange Server.

Déploiement du service de disponibilité

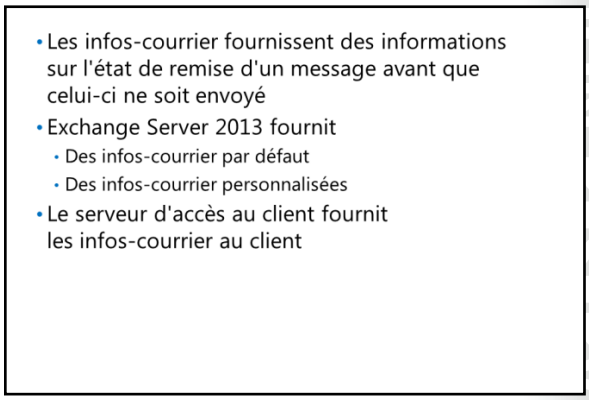
Le service de disponibilité est déployé par défaut sur tous les serveurs d'accès au client et n'a pas besoin d'être configuré, sauf dans les scénarios où vous intégrez les informations de disponibilité de plusieurs forêts.

La fonction de découverte automatique fournit l'emplacement du service de disponibilité aux clients Outlook 2007 ou ultérieur. Le service de disponibilité se trouve sur le site Web suivant : http://servername/EWS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les infos-courrier ?



Les infos-courrier sont des messages informatifs affichés à l'attention des utilisateurs avant qu'ils envoient un message. Les infos-courrier avertissent l'utilisateur d'un problème ou d'une restriction relative au message qu'il tente d'envoyer. Exchange Server 2013 analyse le message, notamment la liste des destinataires auxquels il est destiné. Si un problème potentiel est détecté, les infos-courrier avertissent les utilisateurs avant d'envoyer le message. Grâce aux informations fournies par les infos-courrier, les expéditeurs peuvent adapter le message qu'ils rédigent pour éviter des situations indésirables ou des rapports de non-remise.

Types d'infos-courrier

Exchange Server 2013 fournit plusieurs infos-courrier par défaut, notamment :

- *Boîte aux lettres pleine*. Cette info-courrier s'affiche si l'expéditeur ajoute un destinataire dont la boîte aux lettres est pleine et si l'organisation de ce dernier a implémenté une restriction empêchant la réception de message (« Prohibit Receive ») dans les boîtes aux lettres dont la taille dépasse une valeur spécifiée.
- *Réponses automatiques*. Cette info-courrier affiche les 250 premiers caractères de la réponse automatique configurée par le destinataire.
- *Destinataire restreint*. Cette info-courrier s'affiche si l'expéditeur ajoute un destinataire pour lequel des restrictions de remise sont configurées, et empêche l'envoi du message par cet expéditeur.
- *Destinataires externes*. Cette info-courrier s'affiche si l'expéditeur ajoute un destinataire qui est externe ou s'il ajoute un groupe de distribution qui contient des destinataires externes.
- *Audience étendue*. Cette info-courrier s'affiche si l'expéditeur ajoute un groupe de distribution qui comporte davantage de destinataires que la taille d'audience étendue configurée dans l'organisation de l'expéditeur. Par défaut, Exchange Server affiche cette info-courrier pour les messages destinés aux groupes de distribution qui comptent plus de 25 membres.

Il est également possible de configurer des infos-courrier personnalisées dans l'environnement de ligne de commande Exchange Management Shell. Une info-courrier personnalisée peut être attribuée à tout destinataire. Par exemple, il est possible de configurer une info-courrier personnalisée pour un destinataire qui est en congés prolongés ou pour un groupe de distribution dont tous les membres sont absents du bureau. Il est également possible de créer une info-courrier personnalisée pour un groupe de distribution, afin d'exposer l'objectif du groupe et de réduire ainsi son utilisation erronée. Lorsque vous configurez une info-courrier personnalisée, elle s'affiche lorsqu'un utilisateur rédige un message pour un destinataire spécifié.

Remarque : Les infos-courrier sont uniquement disponibles dans Outlook Web App d'Exchange Server 2010 et 2013, ou dans Microsoft Office Outlook 2010 ou version ultérieure. Les infos-courrier ne sont pas disponibles dans Outlook 2007.

Fonctionnement des infos-courrier

Les infos-courrier sont implémentées comme un service Web dans Exchange Server 2013. Lorsqu'un expéditeur rédige un message, le logiciel client effectue un appel de service Web auprès du serveur Exchange Server 2013 avec le rôle serveur d'accès au client installé, afin d'obtenir la liste d'infos-courrier. Le serveur Exchange Server 2013 répond avec la liste des infos-courrier qui s'appliquent à ce message et le logiciel client affiche les infos-courrier à l'expéditeur.

Les actions suivantes de l'expéditeur déclenchent l'évaluation ou la mise à jour des infos-courrier :

- ajout d'un destinataire ;
- ajout d'une pièce jointe ;
- réponse à l'expéditeur ou réponse à tous les expéditeurs ;
- ouverture d'un message du dossier Brouillons, qui est déjà adressé aux destinataires.

Lorsqu'une demande est lancée sur le serveur d'accès au client, celui-ci compile la liste d'infos-courrier applicables et les renvoie toutes en même temps. Ainsi, l'utilisateur voit s'afficher toutes les infos-courrier simultanément. Le serveur d'accès au client utilise le processus suivant pour compiler des infos-courrier pour un message spécifique :

1. Le client de messagerie interroge le service Web sur le serveur d'accès au client pour obtenir les infos-courrier qui s'appliquent aux destinataires dans le message.
2. Le serveur d'accès au client rassemble des données sur les infos-courrier :
    - Le serveur d'accès au client interroge AD DS et lit les données de mesures des groupes.
    - Le serveur d'accès au client interroge le serveur de boîtes aux lettres pour rassembler les infos-courrier Destinataire absent du bureau et Boîte aux lettres pleine. Si la boîte aux lettres du destinataire se trouve sur un autre site, le serveur d'accès au client demande des informations sur les infos-courrier auprès du serveur d'accès au client dans le site distant.
3. Le serveur d'accès au client renvoie les données sur les infos-courrier au client.

Remarque : Plusieurs infos-courrier sont disponibles lorsque le client Outlook est hors connexion. Pour activer cette fonctionnalité, la structure du carnet d'adresses hors connexion (OAB) a été remodelée dans Exchange Server 2013 de manière à inclure certaines informations requises par les infos-courrier. Les infos-courrier qui requièrent les informations actuelles d'Active Directory ou de la boîte aux lettres utilisateur ne fonctionnent pas lorsque le client Outlook est hors connexion. Il s'agit des infos-courrier suivantes : Destinataire externe non valide, Boîte aux lettres pleine et Destinataire absent du bureau.

Restrictions relatives aux infos-courrier

Les infos-courrier sont soumises aux restrictions suivantes :

- Lorsqu'un message est adressé à un groupe de distribution, les infos-courrier pour les destinataires individuels qui sont membres de ce groupe de distribution ne sont pas évaluées. Cependant, si l'un des membres est un destinataire externe, l'info-courrier Destinataires externes est affichée. Cette info-courrier montre à l'expéditeur le nombre de destinataires externes au groupe de distribution.
- Si le message est adressé à plus de 200 destinataires, les infos-courrier de chaque boîte aux lettres ne sont pas évaluées, pour des raisons de performance.
- Les infos-courrier personnalisées sont limités à 250 caractères.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration des infos-courrier

Procédure de démonstration

1. Dans le CAE, sur LON-CAS1, cliquez sur **destinataires** dans le volet des fonctionnalités.
2. Sélectionnez l'option de gestion des boîtes aux lettres.
3. Ouvrez les propriétés pour April Reagan.
4. Configurez les infos-courrier pour cet utilisateur avec le texte suivant : **Cette personne est en congés prolongés**.
5. Connectez-vous à Outlook Web App en tant qu'**Adatum\Don**.
6. Créez un nouveau message adressé à April et vérifiez que l'info-courrier s'affiche.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Déploiement et configuration d'un rôle serveur d'accès au client

Scénario

Vous êtes un administrateur de messagerie pour A. Datum Corporation. Votre organisation a décidé de déployer des serveurs d'accès au client afin que ces derniers soient accessibles via Internet pour divers clients de messagerie. Pour garantir un niveau de sécurité optimal du déploiement, vous devez sécuriser le serveur d'accès au client et également configurer un certificat sur le serveur qui prendra en charge les connexions des clients de messagerie. En outre, vous devez vérifier des options sur le serveur d'accès au client et configurer des infos-courrier pour certains utilisateurs.

Objectifs

- Configurer des certificats sur le serveur d'accès au client.
- Configurer les options du serveur d'accès au client.
- Configurer des infos-courrier.

Configuration de l'atelier pratique

Durée approximative : **50 minutes**

Ordinateurs virtuels	22341B-LON-DC1 22341B-LON-CAS1 22341B-LON-MBX1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22341B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Ouvrez une session en utilisant les informations d'authentification suivantes :
   a. Nom d'utilisateur : **ADATUM\Administrateur**
   b. Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22341B-LON-MBX1** et **22341B-LON-CAS1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configuration de certificats pour le serveur d'accès au client

Scénario

En tant qu'administrateur de messagerie chez A. Datum Corporation, vous avez déployé l'environnement Exchange Server et travaillez à présent à la configuration des serveurs d'accès au client. L'organisation a décidé d'utiliser un certificat émis par l'autorité de certification interne pour sécuriser toutes les connexions clientes au serveur. Vous devez activer cette configuration, puis vérifier que les clients Outlook peuvent encore se connecter au serveur.

Les tâches principales de cet exercice sont les suivantes :

1. Effectuer une demande de certificat sur Exchange Server.
2. Délivrer un certificat d'une autorité de certification interne.
3. Attribuer un certificat aux services Exchange.

▶ Tâche 1 : Effectuer une demande de certificat sur Exchange Server

1. Sur LON-CAS1, ouvrez **Internet Explorer**, tapez **https://lon-cas1.adatum.com/ecp** et appuyez sur Entrée.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Cliquez sur le nœud **serveurs**, sur **Certificats** et lancez l'Assistant pour créer une demande de certificat.
4. Fournissez **mail.adatum.com** comme nom convivial pour un certificat.
5. N'utilisez pas de certificat générique.
6. Fournissez le nom **mail.adatum.com** pour toutes les valeurs qui ne sont pas définies.
7. Assurez-vous que la demande de certificat contient les noms de domaine suivants : **mail.adatum.com**, **lon-cas1.adatum.com**, **autodiscover.adatum.com**, **LON-CAS1** et **Adatum.com**.
8. Complétez les informations supplémentaires comme suit :
   a. Nom d'organisation : **A.Datum**
   b. Nom du service : **Informatique**
   c. Nom de pays/région : **États-Unis**
   d. Ville/Localité : **Seattle**
   e. Département/région : **WA**
9. Enregistrez la demande de certificat sur **\\lon-cas1\C$\windows\temp\certreq.req**.

▶ Tâche 2 : Délivrer un certificat d'une autorité de certification interne

1. Sur LON-DC1, redémarrez le service de certificats.
2. Sur LON-CAS1, ouvrez l'**Explorateur de fichiers** et accédez à **C:\Windows\Temp**.
3. Ouvrez le fichier de demande de certificat dans le Bloc-notes et copiez tout le contenu dans le presse-papiers.
4. Connectez-vous à **http://lon-dc1.adatum.com/certsrv** en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.

5. Choisissez d'effectuer une demande de certificat avancée.
6. Collez le contenu de la demande de certificat (de l'étape 2) dans le champ approprié, et sélectionnez le modèle de **serveur Web**.
7. Enregistrez le certificat.
8. Ouvrez l'**explorateur de fichiers**, puis créez un nouveau dossier nommé **cert** sur le lecteur de C:\. Partagez le dossier et accordez l'autorisation Lecture à Tout le monde.
9. Copiez le fichier de certificat dans le dossier cert.

▶ Tâche 3 : Attribuer un certificat aux services Exchange

1. Sur LON-CAS1, ouvrez le Centre d'administration Exchange.
2. Importez le certificat Exchange **mail.adatum.com** que vous avez délivré dans la tâche 2. Importez ce certificat sur LON-CAS1.Adatum.com.
3. Attribuez le certificat au service IIS.

Résultats : À la fin de cet exercice, les stagiaires auront installé un certificat sur le serveur d'accès au client Exchange Server.

Exercice 2 : Configuration des options des services d'accès au client

Scénario

Pour préparer le serveur d'accès au client, vous devez effectuer plusieurs tâches de configuration, telles que la configuration du domaine d'accès externe et du service POP3. Le nom de domaine externe de messagerie doit être mail.adatum.com. Vous devez vérifier que les utilisateurs de POP3 peuvent se connecter en toute sécurité, que les limites de connexion doivent être appliquées et que le format de message approprié est utilisé. Vous devez également vérifier les options d'authentification des répertoires virtuels sur le serveur d'accès au client.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les options du serveur d'accès au client.
2. Vérifier les options d'authentification sur le serveur d'accès au client.

▶ Tâche 1 : Configurer les options du serveur d'accès au client

1. Dans le Centre d'administration Exchange, définissez **mail.adatum.com** comme nom de domaine externe pour LON-CAS1.
2. Ouvrez les paramètres de LON-CAS1 et définissez-les comme suit pour les utilisateurs de POP3 :
   a. Nombre maximal de connexions : **100**
   b. Nombre maximal de connexions à partir d'une seule adresse IP : **20**
   c. Nombre maximal de connexions pour un seul utilisateur : **2**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Vérifier les options d'authentification sur le serveur d'accès au client

1. Sur LON-CAS1, dans le Centre d'administration Exchange, accédez aux serveurs, puis cliquez sur les répertoires virtuels.
2. Vérifiez les options d'authentification des répertoires virtuels suivants :
   a. Autodiscover
   b. ecp
   c. PowerShell
   d. Microsoft-Server-ActiveSync
   e. OAB
3. N'effectuez aucune modification.

Résultats : À la fin de cet exercice, les stagiaires auront configuré le serveur d'accès au client.

Exercice 3 : Configuration des infos-courrier personnalisées

Scénario

Pour réduire le nombre d'utilisateurs nécessitant une assistance, A. Datum évalue l'implémentation d'infos-courrier. Vous devez configurer certains déploiements de test qui implémentent des infos-courrier et vérifier que ces dernières peuvent être activées dans plusieurs langues.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer des infos-courrier.
2. Tester les infos-courrier.

▶ Tâche 1 : Configurer des infos-courrier

1. Sur LON-CAS1, ouvrez le Centre d'administration Exchange et accédez à **Boîtes aux lettres**.
2. Sélectionnez l'objet boîte aux lettres **April Reagan**.
3. Définissez le texte d'**Info-courrier** pour April comme suit : **Info-courrier de test pour April**.
4. Ouvrez **Exchange Management Shell** et définissez une info-courrier pour Aidan en exécutant ce qui suit :

```
Set-Mailbox –Identity Aidan –Mailtip "c'est info-courrier en français"
–MailtipTranslation ("DE: Dies ist die deutsche Sprache")
```

▶ Tâche 2 : Tester les infos-courrier

1. Ouvrez Internet Explorer et tapez **https://lon-cas1.adatum.com/owa**.
2. Connectez-vous en tant qu'**ADATUM\Don** avec le mot de passe **Pa$$w0rd**.
3. Acceptez les valeurs par défaut pour le fuseau horaire et la langue.
4. Ouvrez la fenêtre Nouveau message, et tapez **April Reagan** dans la zone de texte **À**.
5. Vérifiez que l'info-courrier s'affiche.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Ouvrez la fenêtre **nouveau message** et tapez **Aidan Delaney** dans la zone de texte **À**.
7. Vérifiez que l'info-courrier apparaît en français.
8. Déconnectez-vous d'Outlook Web App et connectez-vous en tant qu'**Adatum\Amr**.
9. Sélectionnez **Deutsch (Deutschland)** comme langue d'OWA.
10. Ouvrez une fenêtre **Neue E-Mail** et tapez **Aidan Delaney** dans la zone de texte **An**.
11. Vérifiez que l'info-courrier s'affiche en allemand.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1** et **22341B-LON-MBX1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

- Si possible, rendez le serveur d'accès au client hautement disponible ou redondant.
- Fournissez un certificat public pour le serveur d'accès au client qui est exposé à Internet pour éviter des problèmes d'approbation.
- Ne placez pas le serveur d'accès au client dans le réseau de périmètre. Utilisez un pare-feu de la couche Application et un proxy inverse pour le publier en toute sécurité.
- Vérifiez que le serveur d'accès au client dispose d'une connexion rapide et fiable au serveur de boîtes aux lettres et aux contrôleurs de domaine AD DS.

Questions de contrôle des acquis

Question : Quelle est la principale différence entre un rôle serveur d'accès au client dans Exchange Server 2010 et dans Exchange Server 2013 ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 5

Planification et configuration de la connectivité pour les clients de messagerie

Table des matières :

Vue d'ensemble du module **5-1**

Leçon 1 : Connectivité client sur le serveur d'accès au client **5-2**

Leçon 2 : Configuration d'Outlook Web App **5-8**

Leçon 3 : Planification et configuration de la messagerie mobile **5-16**

Leçon 4 : Configuration de l'accès Internet sécurisé pour le serveur d'accès au client **5-26**

Atelier pratique : Planification et configuration de la connectivité pour les clients de messagerie **5-38**

Contrôle des acquis et éléments à retenir **5-46**

Vue d'ensemble du module

La planification et la configuration des connexions clientes figurent parmi les tâches les plus importantes à effectuer quand vous implémentez Microsoft® Exchange Server. Microsoft Exchange Server® 2013 prend en charge divers types de clients et de connexions à partir du Bureau, d'ordinateurs portables, et d'appareils mobiles. Il prend en charge également l'accès basé sur le Web pour de nombreux navigateurs Internet. Dans ce module, nous nous concentrons sur la planification et la configuration des services qui fournissent l'accès aux clients Microsoft Exchange. Ce module décrit en particulier Microsoft® Outlook Web App et la messagerie mobile, ainsi que l'accès sécurisé à Internet à partir du serveur d'accès au client.

Objectifs

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

- décrire les services clients fournis par Exchange Server 2013 ;
- configurer Outlook Web App ;
- planifier et configurer la messagerie mobile ;
- configurer l'accès Internet sécurisé pour le serveur d'accès au client.

Leçon 1
Connectivité client sur le serveur d'accès au client

La fonction principale du rôle serveur d'accès au client dans Exchange Server 2013 est d'accepter, d'authentifier et de connecter des clients de proxy à partir d'un réseau interne et d'Internet. Le serveur d'accès au client peut accepter, authentifier et connecter les clients de proxy en fournissant plusieurs services aux clients (comme Outlook Web App, Outlook® Anywhere et Exchange ActiveSync®). Il est indispensable de connaître ces technologies pour organiser et configurer la connectivité client.

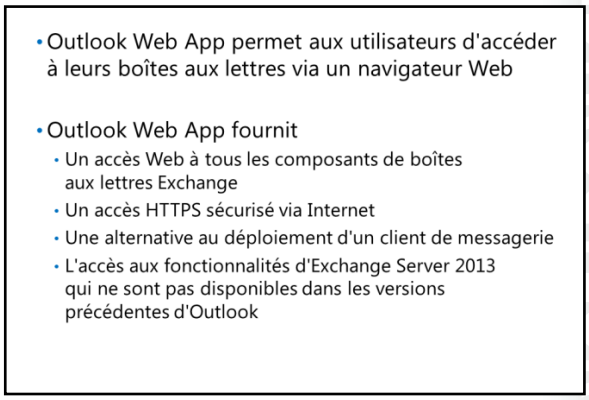
Objectifs de la leçon

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

- décrire Outlook Web App ;
- décrire Outlook Anywhere ;
- décrire Exchange ActiveSync ;
- décrire Outlook Web App Light ;
- décrire comment connecter des clients non Outlook au serveur d'accès au client.

Qu'est-ce qu'Outlook Web App ?

Outlook Web App est un service d'Exchange Server 2013 qui permet aux utilisateurs d'accéder à leur boîte aux lettres via un navigateur Web. L'ensemble des fonctionnalités disponibles dans Outlook Web App ressemble étroitement à celles de Microsoft® Outlook® 2013 et fournit des fonctionnalités qui ne sont pas disponibles dans les versions antérieures d'Outlook. Dans certains cas, par exemple, quand vous n'avez pas de client du courrier électronique installé localement, il peut être possible d'utiliser Outlook Web App au lieu d'Outlook 2010 ou 2013.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fonctionnalités d'Outlook Web App

Outlook Web App fournit la plupart des fonctionnalités disponibles lors de l'utilisation du client Outlook 2013 complet. Certaines de ces fonctionnalités permettent aux utilisateurs de réaliser les tâches suivantes :

- lire et répondre aux messages ;
- réserver des réunions et consulter le calendrier ;
- créer et modifier des contacts et des tâches ;
- lire des pièces jointes qui ont été restituées dans le contenu HTML sur le serveur ;
- configurer des paramètres personnels tels que des signatures, des messages d'absence du bureau ou des paramètres de courrier indésirable ;
- modifier les mots de passe ;
- configurer les paramètres des appareils mobiles ;
- créer et modifier des règles côté serveur ;
- accéder aux dossiers publics ;
- utiliser le protocole S/MIME (Secure/Multipurpose Internet Mail Extensions) pour signer et chiffrer des messages, et lire ces messages signés et chiffrés ;
- récupérer des éléments supprimés ;
- créer et modifier des listes de diffusion personnelles.

Outlook Web App a été repensé dans Exchange Server 2013 pour inclure des fonctionnalités telles que la conversation, la messagerie textuelle, le calendrier amélioré et le volet de personnes, l'intégration du téléphone portable, et l'affichage amélioré des conversations. Outlook Web App inclut désormais également des applications externes, telles que Bing® Maps, Rendez-vous suggérés et Éléments d'action. Ces applications s'intègrent à Outlook 2013 et Outlook Web App, et elles étendent les informations et les fonctionnalités des messages et des éléments du calendrier. En outre, Outlook Web App fournit maintenant une fonctionnalité d'accès hors connexion.

Les nouvelles fonctionnalités les plus importantes d'Outlook Web App, par rapport à Outlook Web App dans Microsoft® Exchange Server® 2010, sont notamment les suivantes :

- L'intégration d'applications Web dans l'interface Outlook Web App.
- Des améliorations ont été apportées à la fonctionnalité des personnes. Il est à présent possible de lier plusieurs entrées pour la même personne et d'afficher des informations dans une seule carte de visite. Vous pouvez également connecter le compte LinkedIn d'un utilisateur.
- Des améliorations ont été apportées au calendrier qui permettent aux utilisateurs de voir plusieurs calendriers en un ou un affichage fusionné.
- Des améliorations ont été apportées à l'interface utilisée sur les tablettes et les téléphones mobiles de type smartphone.

Dans Exchange Server 2013, ces fonctionnalités sont accessibles à partir de nombreux navigateurs Web, notamment Microsoft Internet Explorer 9.0 ou version ultérieure, Firefox, Safari et Chrome de Google.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

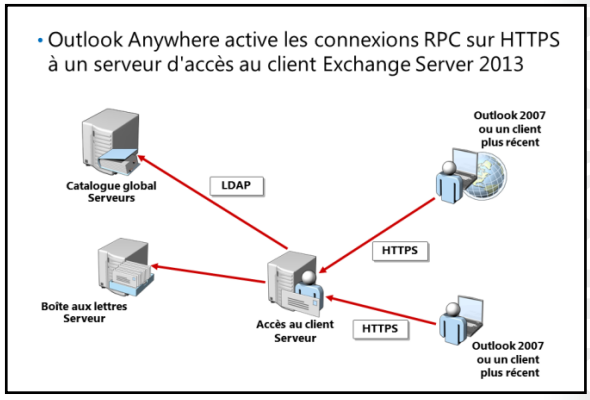
Avantages d'Outlook Web App

Outlook Web App fournit de nombreux avantages importants pour une organisation, notamment :

- L'ensemble de la communication entre le client Outlook Web App et le serveur d'accès au client est envoyé à l'aide du protocole HTTP. Vous pouvez facilement sécuriser ces informations à l'aide du protocole SSL (Secure Sockets Layer). Cela signifie que vous pouvez facilement configurer des pare-feu ou des proxys inverses pour activer l'accès Internet à Outlook Web App, car seul un port unique est requis.
- Outlook Web App ne vous oblige pas à déployer ou à configurer de client de messagerie. Tous les ordinateurs clients, y compris les ordinateurs qui exécutent Linux ou Macintosh, comportent un navigateur Web disponible. Ainsi, les utilisateurs peuvent accéder à leurs boîtes aux lettres à partir de tout client capable d'accéder à l'URL du serveur d'accès au client.
- Outlook Web App dans Exchange Server 2013 fournit également l'accès à certaines fonctionnalités qui ne sont disponibles que via Outlook Web App ou Outlook 2010 ou version ultérieure. Par exemple, des fonctionnalités telles que la boîte aux lettres d'archivage ou l'affichage des conversations sont accessibles via Outlook Web App sans déployer Outlook 2010 ou version ultérieure.

Qu'est-ce qu'Outlook Anywhere ?

Outlook Anywhere est une fonctionnalité présente dans Exchange Server depuis Exchange Server® 2003 Service Pack 2. Dans les versions plus anciennes d'Exchange Server, cette fonctionnalité était connue sous le nom de RPC sur HTTP(S).



Avec Outlook Anywhere, un client Office Outlook 2007 ou plus récent peut utiliser les RPC encapsulés dans un paquet HTTPS pour se connecter à un serveur qui exécute un serveur d'accès au client dans Exchange Server 2013. Le composant proxy RPC sur HTTP de Windows, que les clients Outlook utilisent pour se connecter, renvoie les RPCs avec une couche HTTP. Cela permet au trafic de passer via des pare-feu du réseau sans requérir d'ouverture de ports RPC.

Configuration d'Outlook Anywhere dans Exchange Server 2013

La fonctionnalité Outlook Anywhere est activée par défaut dans Exchange Server 2013. Il s'agit d'une modification par rapport aux versions précédentes d'Exchange, qui utilisaient uniquement des clients externes Outlook Anywhere. Dans Exchange Server 2013, les clients internes se connectent également à l'aide de cette méthode.

Il n'est pas nécessaire d'activer ou de déployer Outlook Anywhere, mais il doit être correctement configuré. Vous devez installer un certificat SSL approprié sur votre rôle serveur d'accès au client, et configurer le nom de DNS externe à utiliser en vous connectant à partir d'Internet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

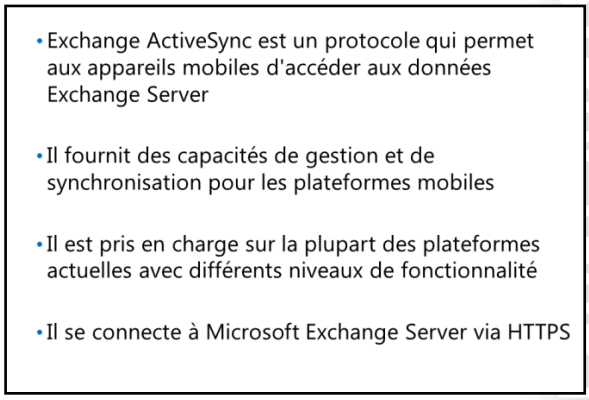
Outlook Anywhere présente plusieurs avantages, notamment :

- Les utilisateurs peuvent accéder aux serveurs Exchange à partir d'Internet de la même manière qu'à partir d'un réseau interne.
- Les mêmes URL et espace de noms peuvent être utilisés pour Outlook Anywhere, Outlook Web App et ActiveSync.
- Le même certificat est utilisé pour Outlook Anywhere, Outlook Web App et ActiveSync.
- L'utilisateur est toujours authentifié dans le client Outlook et ne peut pas accéder aux données s'il n'est pas authentifié.
- Il n'est pas nécessaire d'utiliser un réseau privé virtuel (VPN) pour accéder aux serveurs Exchange via Internet.
- Si Outlook Web App et Exchange ActiveSync sont déployés avec SSL, il est inutile d'ouvrir de port supplémentaire pour Outlook Anywhere.

Bien que la configuration d'Outlook Anywhere soit un processus assez simple, vous devez valider ses fonctionnalités avant de la mettre en production. Vous pouvez tester la connectivité des clients de bout en bout pour Outlook Anywhere et les connexions basées sur TCP à l'aide de l'applet de commande Test-OutlookConnectivity PowerShell. Vous pouvez également utiliser l'application Web Analyseur de connectivité à distance de Microsoft Exchange Server.

Qu'est-ce qu'Exchange ActiveSync ?

Exchange ActiveSync est un protocole XML qui permet aux appareils mobiles de communiquer via HTTP (ou HTTPS) avec Exchange Server. Le protocole est conçu pour la synchronisation des messages électroniques, des contacts, du calendrier, des tâches et des notes à partir d'un serveur Exchange vers un appareil mobile avec une plateforme mobile prise en charge (également appelé système d'exploitation mobile). Le protocole ActiveSync fournit également des contrôles de gestion et de stratégie d'appareil mobile. Le processus de communication Exchange ActiveSync est optimisé pour fonctionner sur des réseaux à faible bande passante et à haute latence, tels que le service GPRS (General Packet Radio Service) ou EDGE, mais il peut également tirer parti des réseaux à haut débit tels que 3G ou LTE.



Par défaut, Exchange ActiveSync est disponible pour tous les utilisateurs après l'installation d'un serveur d'accès au client. ActiveSync a évolué dans de nombreuses versions au cours des 12 dernières années. ActiveSync est implémenté dans Exchange Server 2013 et les systèmes d'exploitation mobiles Microsoft Windows® Phone 7 et Windows® Phone 8.

La connexion établie à l'aide du protocole ActiveSync ressemble beaucoup à Outlook Anywhere. Outre le type de connexion cliente, la principale différence entre Exchange ActiveSync et Outlook Anywhere est le périphérique utilisé pour afficher la messagerie électronique. Avec Outlook Anywhere, le périphérique frontal est un ordinateur portable, qui peut être membre du domaine Active Directory® Domain Services (AD DS) interne et géré en tant que tel. Avec Exchange ActiveSync, le périphérique frontal est un client mobile, qui ne peut pas être membre du domaine local.

Remarque : Windows® 8 est non seulement une plateforme mobile, mais également un système d'exploitation d'ordinateur avec une application de messagerie électronique intégrée qui utilise ActiveSync pour se connecter à Exchange Server.

Microsoft a autorisé sous licence le protocole ActiveSync pour la plupart des fournisseurs de plateformes mobiles, telles que Google, Apple et Symbian. En raison de cet accord d'octroi de licence, la majeure partie des plateformes mobiles actuelles prennent en charge ActiveSync ; cependant, toutes les plateformes ne prennent pas forcément en charge chacune de ces fonctionnalités. Chaque fournisseur de plateforme mobile peut choisir les fonctionnalités qu'il implémentera.

Qu'est-ce qu'Outlook Web App Light ?

- Outlook Web App Light est une application au sein d'Outlook Web App qui fonctionne avec d'anciens navigateurs
- Outlook Web App Light fournit ce qui suit
  - Connectivité à la boîte aux lettres utilisateur à partir de navigateurs mobiles
  - Un sous-ensemble des fonctionnalités d'Outlook Web App
  - Une authentification sécurisée

Outlook Web App Light est une version réduite d'Outlook Web App. Vous pouvez l'utiliser pour les plateformes mobiles qui ne prennent pas en charge Exchange ActiveSync ou sur lesquelles ActiveSync n'est pas activé du côté Exchange Server. Il s'agit d'un client de courrier électronique léger basé sur le Web destiné à être utilisé par les navigateurs mobiles compatibles HTML sur des appareils mobiles, tels que téléphones portables de type smartphone et des tablettes. Il utilise une interface utilisateur basée sur HTML4 très simple qui fonctionne dans la plupart des navigateurs Internet existants.

Outlook Web App Light est entièrement basé sur l'architecture Outlook Web App. Comme il fonctionne dans Outlook Web App, il utilise tous les indicateurs de partitionnement qui y existent et plusieurs sous-ensembles de paramètres Outlook Web App.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Outlook Web App Light permet aux utilisateurs d'effectuer ce qui suit :

- Accéder à la messagerie, au calendrier, aux contacts, aux tâches et à la liste des adresses globales (GAL).
- Accéder aux sous-dossiers du courrier électronique.
- Composer, répondre et envoyer des messages électroniques.
- Créer un calendrier, des contacts et des tâches.
- Traiter les demandes de réunion.
- Définir le fuseau horaire et les réponses automatiques en l'absence des utilisateurs du bureau et non disponibles pour répondre aux courriers électroniques.

Outlook Web App Light utilise les mêmes valeurs de délai d'expiration qu'Outlook Web App. Il est important de noter qu'il n'y a aucune fonctionnalité de fermeture de session dans Mobile Outlook Web App, car le système ne repose pas sur le fait que le navigateur oublie le mot de passe enregistré après la valeur de délai d'expiration par défaut.

Vous pouvez accéder à Outlook Web App Light en accédant à l'URL d'Outlook Web App avec un navigateur portable ou un navigateur qui ne prend pas en charge la version complète d'Outlook Web App.

Connecter les clients autres qu'Outlook au serveur d'accès au client

Dans certains scénarios, les clients autres qu'Outlook doivent être connectés à Exchange Server. C'est le cas dans les organisations qui utilisent un client de messagerie autre que Microsoft Office sur les ordinateurs clients. Exchange Server prend en charge les connexions clientes à partir de clients autres qu'Outlook. Les fonctionnalités obtenues ne sont pas toujours comparables.

- Les clients de courrier électronique autres qu'Outlook peuvent se connecter à Exchange Server à l'aide de ce qui suit
  - Protocole POP3
  - Protocole IMAP4
- Utilisez Outlook WebApp comme une alternative à un client de messagerie installé en local
- Pensez à utiliser l'application de messagerie Windows 8 intégrée qui se connecte à Exchange via ActiveSync

Les sociétés qui n'ont pas Outlook déployé sur les ordinateurs clients peuvent sinon utiliser Outlook Web App au lieu du logiciel client installé localement. Cela fournit une expérience utilisateur cohérente semblable à celle d'Outlook, mais pas aussi fiable. Sinon, vous pouvez également connecter les applications de messagerie existantes à Exchange à l'aide des protocoles POP3 ou IMAP4. Par défaut, dans les installations Exchange, ces protocoles sont configurés pour être démarrés manuellement, mais vous pouvez les démarrer en définissant les services correspondants sur l'état automatique. Sachez qu'Exchange Server 2013 requiert qu'une connexion POP3 soit établie via un canal sécurisé ; elle doit donc être définie dans un logiciel client de messagerie.

Si Windows 8 est déployé sur des ordinateurs clients, vous pouvez utiliser une application de courrier électronique intégrée pour vous connecter à Exchange Server à l'aide du protocole ActiveSync. Cela fournit également une bonne expérience utilisateur, bien que l'application de courrier électronique soit très simple et fournisse peu d'options.

Leçon 2
Configuration d'Outlook Web App

Outre via l'utilisation du logiciel client Outlook, la façon la plus courante d'accéder à une boîte aux lettres sur un serveur Exchange est via Outlook Web App. Outlook Web App est une application Web qui fournit une expérience cliente complète pour accéder au contenu d'une boîte aux lettres. Vous pouvez y accéder à partir des réseaux internes et externes et bénéficier de la même expérience utilisateur. Cependant, vous pouvez configurer de nombreuses options pour Outlook Web App afin de le rendre plus sécurisé et de fournir une expérience utilisateur positive.

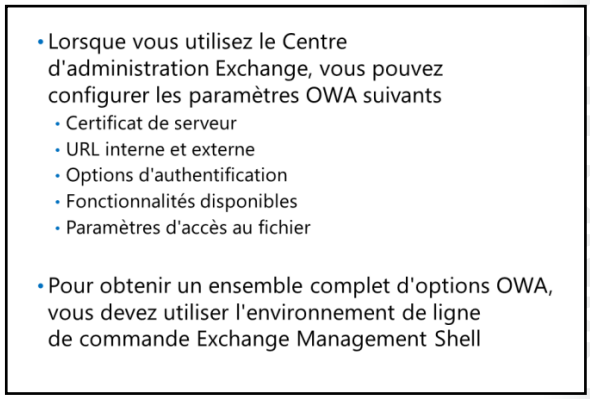
Objectifs de la leçon

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

- décrire les options de configuration d'Outlook Web App ;
- décrire la stratégie Outlook Web App ;
- configurer les options et les stratégies Outlook Web App ;
- décrire et utiliser les applications intégrées dans Outlook Web App ;
- décrire l'intégration d'Office Web Apps Server ;
- décrire l'accès hors connexion à Outlook Web App ;
- activer et utiliser l'accès hors connexion à Outlook Web App.

Options de configuration d'Outlook Web App

Bien qu'Outlook Web App soit automatiquement disponible sur les serveurs d'accès au client, vous devez le configurer afin qu'il prenne en charge les besoins spécifiques de vos utilisateurs.



Tâches de configuration d'Outlook Web App

Lorsque vous utilisez le Centre d'administration Exchange (CAE) pour configurer Outlook Web App, vous pouvez effectuer les tâches suivantes :

- Installer et configurer un certificat de serveur SSL afin d'activer le protocole SSL (Secure Sockets Layer) pour toutes les connexions clientes.
- Définir des URL internes et externes pour accéder à Outlook Web App à partir d'un réseau interne et d'Internet, respectivement.
- Définir des options d'authentification. Vous pouvez choisir parmi des authentifications de base, intégrées, Digest et basées sur les formulaires pour Outlook Web App.

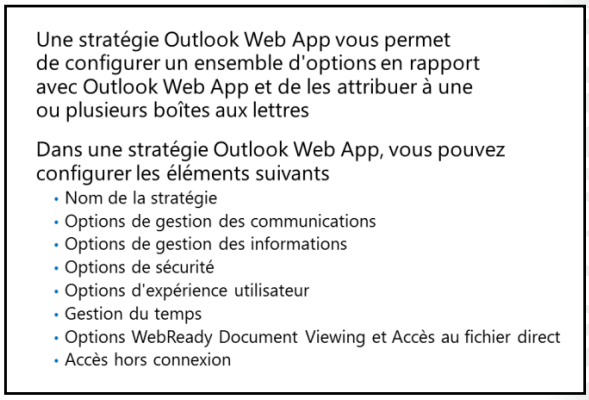
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Configurer le répertoire virtuel Outlook Web App. Lorsque vous installez le rôle serveur d'accès au client, un répertoire virtuel Outlook Web App est configuré dans le site Web des services Internet (IIS) par défaut sur le serveur d'accès au client. Dans la plupart des cas, outre pour configurer le site Web par défaut pour utiliser un certificat d'autorité de certification pour SSL et configurer des options d'authentification, vous n'aurez pas besoin de modifier de paramètres du répertoire virtuel Outlook Web App.
- Configurer les fonctionnalités disponibles dans Outlook Web App. Vous pouvez activer ou désactiver des fonctionnalités spécifiques d'Outlook Web App pour les utilisateurs d'Outlook Web App dans Exchange Server 2013. Vous pouvez le faire au niveau du répertoire virtuel Outlook Web App, auquel cas ces paramètres s'appliquent à tous les utilisateurs qui utilisent OWA. Vous pouvez éventuellement configurer les mêmes paramètres dans Outlook Web App au niveau de la stratégie, puis appliquer sélectivement la stratégie à des utilisateurs spécifiques.
- Configurer les paramètres d'accès au fichier. Vous pouvez configurer le comportement d'accès aux fichiers selon le type d'ordinateur utilisé pour accéder à Outlook Web App (privé ou public). Vous pouvez aussi forcer WebReady Document Viewing. Vous pouvez, si vous le souhaitez, utiliser l'applet de commande **set-owavirtualdirectory** de l'environnement de ligne de commande Exchange Management Shell avec les paramètres *AllowedFileTypes*, *AllowedMimeTypes*, *BlockedFileTypes*, *BlockedMIMETypes*, *ForceSaveFileTypes* et *ForceSaveMIMETypes*.
- Un ensemble complet d'options pour Outlook Web App est disponible dans l'environnement de ligne de commande Exchange Management Shell. L'applet de commande **Set-OwaVirtualDirectory** doit être utilisée pour définir les propriétés du répertoire virtuel OWA sur le serveur d'accès au client. Parmi les commutateurs courants que vous pouvez utiliser avec cette applet de commande figurent notamment :
    - *AllowedFileTypes*. Le paramètre *AllowedFileTypes* spécifie les extensions des types de fichiers que l'utilisateur peut enregistrer et afficher localement à partir d'un navigateur Web. Si des extensions identiques se trouvent dans plusieurs listes de paramètres, le paramètre le plus sécurisé remplace celui le moins sécurisé.
    - *BlockedFileTypes*. Le paramètre *BlockedFileTypes* spécifie la liste des extensions des pièces jointes qui sont bloquées. Les pièces jointes qui contiennent ces extensions proscrites ne peuvent pas être enregistrées localement ou affichées à partir d'un navigateur Web.
    - *ChangePasswordEnabled.* Le paramètre *ChangePasswordEnabled* contrôle si les utilisateurs sont autorisés à changer leur mot de passe avec l'interface OWA.
    - *LogonFormat*. Le paramètre *LogonFormat* spécifie le type de format de connexion pour Outlook Web App ou l'authentification basée sur les formulaires qui est utilisé dans la page de connexion Outlook Web App. Les attributs possibles sont FullDomain, UserName ou PrincipalName.
    - *IRMEnabled*. Le paramètre *IRMEnabled* spécifie si la fonctionnalité de gestion des droits relatifs à l'information (IRM) est activée.
    - *RedirectToOptimalOWAServer*. Quand ce paramètre est défini sur $true, Outlook Web App utilise le service de découverte pour rechercher le meilleur serveur d'accès au client à utiliser après une authentification utilisateur. Si la redirection est désactivée, OWA ne redirige pas les clients sur le serveur d'accès au client le plus efficace.
- Vous pouvez également gérer plusieurs options d'Outlook Web App dans le Centre d'administration Exchange en accédant aux fonctionnalités du répertoire virtuel Outlook Web App.

Qu'est-ce qu'une stratégie Outlook Web App ?

Une stratégie Outlook Web App permet aux administrateurs de définir le comportement d'Outlook Web App pour un ou plusieurs utilisateurs spécifiques. Une stratégie OWA est un objet qui vous permet de configurer un ensemble d'options pour Outlook Web App et d'attribuer ces options à la boîte aux lettres d'un utilisateur spécifique. Quand vous attribuez une stratégie Outlook Web App, tous les paramètres de cette stratégie sont appliqués à cet utilisateur spécifique lorsqu'il utilise l'interface Outlook Web App.



La stratégie Outlook Web App peut être configurée dans le Centre d'administration Exchange en allant dans **Autorisations**, puis en cliquant sur l'onglet **Stratégies Outlook Web App**. Quand vous cliquez sur le bouton **Nouveau**, une stratégie OWA est créée mais elle n'est pas immédiatement attribuée à une boîte aux lettres. Quand vous créez une stratégie Outlook Web App, vous pouvez spécifier les paramètres suivants :

- **Nom de la stratégie**. Entrez le nom descriptif de la stratégie.
- **Options de gestion des communications**. Spécifiez si les utilisateurs peuvent utiliser la messagerie instantanée, la messagerie textuelle, la messagerie unifiée, ActiveSync et les contacts.
- **Options de gestion des informations**. Activez ou désactivez les fonctionnalités Dossiers publics, Journalisation, Notes, Dossiers de recherche, Règles de la boîte de réception et Récupération des éléments supprimés.
- **Options de sécurité**. Configurez le filtrage du courrier indésirable et spécifiez si les utilisateurs ont la possibilité ou pas de modifier leur mot de passe dans Outlook Web App.
- **Options d'expérience utilisateur**. Définissez les options pour les thèmes d'Outlook Web App, l'expérience client étendue et la signature du courrier électronique.
- **Options de gestion du temps**. Spécifiez si les utilisateurs peuvent mettre à jour le calendrier, les tâches, les rappels et les notifications.
- **Options WebReady Document Viewing et Accès au fichier direct**. Sélectionnez les options pour les ordinateurs publics et privés.
- **Accès hors connexion**. Indiquez si Outlook Web App hors connexion (présenté ultérieurement dans cette leçon) peut être utilisé et, le cas échéant, sur quels ordinateurs (tous ou privés).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Après avoir configuré une stratégie Outlook Web App, vous devez l'attribuer à une boîte aux lettres utilisateur. Pour cela, vous devez ouvrir les propriétés de la boîte aux lettres utilisateur, en accédant à **Fonctionnalités de boîte aux lettres > Connectivité de messagerie**, puis en sélectionnant la stratégie de boîte aux lettres Outlook Web App à attribuer à l'utilisateur. Si vous souhaitez attribuer une stratégie Outlook Web App à plusieurs utilisateurs simultanément, utilisez l'applet de commande **Set-CASMailbox** de l'environnement de ligne de commande Exchange Management Shell. Par exemple, si vous souhaitez définir une stratégie appelée Stratégie des utilisateurs externes pour l'utilisateur AidanD, vous devez taper :

```
Set-CASMailbox –identity AidanD@adatum.com –OwaMailboxPolicy: "Stratégie des utilisateurs externes"
```

Démonstration : Configuration des options et des stratégies Outlook Web App

Procédure de démonstration

1. Connectez-vous au Centre d'administration Exchange (CAE) sur LON-CAS1 en tant qu'**ADATUM\Administrateur**.
2. Modifiez les paramètres d'Outlook Web App (site Web par défaut).
3. Définissez l'URL externe pour que le répertoire virtuel Outlook Web App soit **https://mail.adatum.com**.
4. Désactivez les fonctionnalités **Journalisation et thèmes** dans Outlook Web App.
5. Désactivez l'option **Accès au fichier direct** dans la section Ordinateur public ou partagé.
6. Créez une nouvelle stratégie Outlook Web App.
7. Nommez cette stratégie **Stratégie des utilisateurs externes**.
8. Désactivez les options de messagerie instantanée, les options de messagerie textuelle, les options de récupération des éléments supprimés et l'accès direct au fichier.
9. Appliquez la stratégie à l'utilisateur Adam Barr.

Applications intégrées dans Outlook Web App

Pour améliorer l'expérience utilisateur avec Outlook Web App, Microsoft a implémenté certaines applications supplémentaires dans l'interface d'OWA. L'objet de ces applications est d'identifier les besoins de l'utilisateur selon le contenu du message.

- Les applications intégrées à OWA améliorent l'expérience utilisateur en suggérant des tâches basées sur le contenu des messages
- Les applications préinstallées sont les suivantes
  - Bing Maps
  - Éléments d'action
  - Rendez-vous suggérés
  - Annuler l'abonnement
- Vous pouvez ajouter des applications à partir d'Office Store, d'une URL ou d'un fichier

Par défaut, les applications suivantes sont installées dans l'interface d'OWA :

- Bing Maps. Cette application recherche des adresses dans vos messages électroniques. Si elle trouve du texte qui ressemble à une adresse, elle affiche un onglet Bing supplémentaire avec un lien vers l'emplacement de l'adresse sur la carte, et fournit des instructions sur la façon d'y arriver. (Cette opération est limitée aux pays sélectionnés).
- Rendez-vous suggérés. Cette application recherche des expressions dans vos messages qui suggèrent ou proposent des réunions. Si elle trouve un modèle valide, elle propose de créer un rendez-vous dans votre calendrier.
- Annuler l'abonnement. Cette application est activée sur des messages à partir de flux d'abonnement, et vous permet de bloquer l'expéditeur ou d'annuler directement l'abonnement.
- Éléments d'action. Cette application recherche des suggestions de tâche possibles dans vos messages. Si une suggestion de tâche est trouvée, l'application vous crée une tâche suggérée.

Les administrateurs peuvent utiliser le Centre d'administration Exchange pour gérer les applications disponibles pour les utilisateurs de l'organisation. Dans le Centre d'administration Exchange, vous devez cliquer sur l'organisation, puis sur l'onglet **Applications**. Vous pouvez désactiver les applications par défaut et en ajouter de nouvelles, et vous pouvez choisir d'ajouter des applications à partir d'Office Store, d'une URL ou d'un fichier.

Démonstration : Utilisation d'applications dans Outlook Web App

Procédure de démonstration

1. Sur LON-CL1, ouvrez **Internet Explorer** et connectez-vous à Outlook Web App en tant qu'**administrateur**.
2. Envoyez un nouveau message électronique à Aidan Delaney avec le texte suivant :

   Are you available to meet with me tomorrow at 10:00 AM? Meeting location is Microsoft Corp, One Microsoft Way, Redmond, WA 98004. **(**Êtes-vous libre demain matin à 10 h 00 ? La réunion se déroule à Microsoft Corp One Microsoft Way, Redmond, WA 98004.).
3. Déconnectez-vous, puis connectez-vous à LON-CL1 en tant qu'**Aidan**.
4. Ouvrez Outlook 2013.
5. Cliquez sur le message de l'administrateur.
6. Vérifiez que les onglets **Bing Maps** et **Réunions suggérées** sont présents dans les messages électroniques.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que l'intégration d'Office Web Apps Server ?

Dans les versions précédentes d'Exchange Server, telles que Exchange 2010, les pièces jointes aux messages électroniques s'ouvraient à l'aide d'une application installée localement ou à l'aide de la technologie d'affichage de document WebReady (pour les formats Microsoft Office). Cette technologie permet aux utilisateurs d'ouvrir et de voir le contenu des documents Office même s'ils ne disposent pas d'un ensemble d'applications Office installé localement.

- L'intégration d'Office Web Apps Server fournit une expérience utilisateur améliorée lors de la gestion des pièces jointes aux messages électroniques
- Les applications Office Web Apps sont utilisées pour le rendu de documents
- Les utilisateurs peuvent modifier les documents en ligne
- Les applications Office Web Apps s'intègrent à l'interface Outlook Web App
- Les utilisateurs d'Exchange Online ou d'Exchange installé sur site peuvent l'utiliser
- Un serveur Office Web Apps est requis

Dans Exchange Server 2013, Outlook Web App fournit une gestion des pièces jointes améliorée. Ceci inclut la fonctionnalité avancée de visualisation et la capacité pour les utilisateurs de modifier les pièces jointes en ligne. Par exemple, si vous receviez des documents Word en tant que pièces jointes dans Exchange Server 2010, vous pouviez les voir dans la version Exchange Server 2010 d'Outlook Web App, mais vous ne pouviez pas en modifier le contenu sauf si vous aviez installé Word localement.

En intégrant Office Web Apps Server à Exchange Server 2013, les utilisateurs qui ne disposent pas d'Office installé localement peuvent maintenant ouvrir et modifier les pièces jointes à l'aide d'applications Web Office telles que Word, Excel et PowerPoint.

L'intégration d'Office Web Apps Server est possible pour tous les clients Exchange Online. Pour Exchange déployé sur site, vous devez déployer Office Web Apps Server pour permettre cela, puis intégrer votre version d'Exchange installée localement avec Office Web Apps Server. Office Web Apps Server déployé localement doit être accessible à partir d'Internet afin que les utilisateurs internes et externes d'OWA puissent l'utiliser lors de la gestion des pièces jointes.

Pour utiliser Office Web Apps Server pour afficher des pièces jointes dans Outlook Web App, vous devez spécifier l'URL d'Office Web Apps Server. Vous devez utiliser l'applet de commande **Set-OrganizationConfig** pour configurer l'URL.

Supposons par exemple qu'Office Web Apps Server soit disponible à l'emplacement suivant : https://Server1.adatum.com/hosting/discovery.

Vous devez taper l'applet de commande suivante dans l'environnement de ligne de commande Exchange Management Shell pour configurer l'intégration à un serveur Exchange Server installé localement :

```
Set-OrganizationConfig -WACDiscoveryEndPoint https://office.adatum.com/hosting/discovery
```

Vous pouvez également déterminer si les utilisateurs d'ordinateurs publics ou privés peuvent utiliser l'intégration d'Office Web Apps Server quand ils se connectent à Outlook Web App. Par exemple, si vous souhaitez activer l'intégration d'Office Web Apps Server sur les ordinateurs privés, vous pouvez utiliser l'applet de commande suivante :

```
Set-OwaVirtualDirectory "LON-CAS01\owa (Default Web Site)"
-WacViewingOnPrivateComputersEnabled $true
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Utilisation d'Outlook Web App en mode hors connexion

Dans Exchange Server 2013, Outlook Web App peut fonctionner en mode hors connexion. Cela signifie que les utilisateurs peuvent se connecter à Outlook Web App et accéder au contenu de leur boîte aux lettres même lorsqu'ils ne sont pas connectés à un serveur Exchange Server. Tout ce que l'utilisateur effectue dans la boîte aux lettres est synchronisé avec Exchange Server dès que la connexion à Exchange est rétablie. Cela fournit également une expérience améliorée pour les utilisateurs qui utilisent un réseau lent ou connecté par intermittence car il peut travailler plus rapidement.

- La fonction Outlook Web App hors connexion permet aux utilisateurs d'accéder aux données de leur boîte aux lettres même quand ils ne sont pas connectés à Exchange Server
- Outlook Web App hors connexion
  - Fonctionne avec les navigateurs sélectionnés
  - Met en cache une partie du contenu de la boîte aux lettres
  - Permet aux utilisateurs d'effectuer les tâches sélectionnées
  - Est activé par ordinateur
  - Peut être contrôlé à l'aide des stratégies OWA

Dans les versions précédentes d'Exchange Server, les utilisateurs ne pouvaient pas utiliser Outlook Web App hors connexion. La seule manière d'utiliser la messagerie en mode hors connexion était de configurer un client Outlook pour l'utiliser hors connexion. Pour cela, les utilisateurs mettaient en cache la boîte aux lettres dans un fichier .ost sur un ordinateur local. Cela a changé avec Exchange Server 2013, car il peut utiliser Outlook Web App en mode hors connexion.

Outlook Web App hors connexion est activé d'ordinateur à ordinateur. Cela signifie que l'utilisateur doit l'activer sur chaque ordinateur où il souhaite utiliser cette fonctionnalité. Nous recommandons d'activer Outlook Web App hors connexion uniquement sur les ordinateurs privés pour des raisons de sécurité, notamment car la boîte aux lettres utilisateur est stockée sur un ordinateur local dans le cache du navigateur. Internet Explorer stockera des données des boîtes aux lettres mises en cache dans **%systemdrive%\Users\%username%\AppData\Local\Microsoft\Internet Explorer\Indexed DB.** Vous pouvez également gérer ce cache à partir de l'option d'Internet Explorer appelée Cache et bases de données. Lorsque vous ouvrez les **Options** Internet Explorer, vous devez cliquer sur **Paramètres** dans l'onglet **Général**, puis sur **Caches et bases de données**. Vous pouvez alors supprimer le cache (et ainsi désactiver Outlook Web App hors connexion) ou modifier les paramètres de notification pour la taille de la mémoire cache.

Les administrateurs peuvent contrôler les utilisateurs qui peuvent utiliser Outlook Web App hors connexion en implémentant des stratégies Outlook Web App.

Les fonctionnalités fournies par Outlook Web App hors connexion sont très similaires à celles fournies par les clients téléphones qui exécutent Exchange Active Sync. Une partie du contenu de la boîte aux lettres est mise en cache localement sur l'ordinateur, exactement comme sur les smartphones.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les utilisateurs peuvent effectuer les actions suivantes tout en travaillant hors connexion dans Outlook Web App :

- Accéder aux courriers électroniques enregistrés dans la boîte de réception, les brouillons, ou d'autres dossiers (jusqu'à 15) affichés dans les trois derniers jours.
- Accéder au calendrier (allant du mois précédent jusqu'à l'année suivante).
- Accéder aux contacts.
- Envoyer des messages et des invitations du calendrier.
- Supprimer des messages.
- Recevoir des rappels actifs (pour les deux derniers mois).
- Accepter ou refuser des demandes de réunion.
- Définir des indicateurs et classer les messages par catégorie.

Outlook Web App hors connexion a certaines limitations. Par exemple, vous ne pouvez pas accéder aux archives, aux dossiers de l'équipe ou aux tâches en ligne. Vous ne pouvez pas non plus effectuer de recherche en texte intégral dans votre boîte aux lettres. Pour utiliser Outlook Web App hors connexion, vous devez utiliser Internet Explorer 10 ou version ultérieure, Google Chrome 17 ou version ultérieure, ou encore Safari 5 ou version ultérieure.

Vous pouvez utiliser l'environnement de ligne de commande Exchange Management Shell pour spécifier les ordinateurs qui seront autorisés à utiliser OWA hors connexion. Vous devez utiliser l'applet de commande **Set-OWAVirtualDirectory** avec le commutateur **AllowOfflineOn**. Le paramètre **AllowOfflineOn** spécifie les ordinateurs qui peuvent utiliser Outlook Web App en mode hors connexion. Les valeurs possibles comprennent **PrivateComputersOnly**, **NoComputers** ou **AllComputers**. La valeur est définie sur **AllComputers** par défaut. Si vous définissez la valeur sur **PrivateComputersOnly**, seuls les utilisateurs qui se connectent à Outlook Web App à l'aide de l'option **Privé** peuvent l'utiliser en mode hors connexion.

Démonstration : Activation et utilisation d'Outlook Web App en mode hors connexion

Procédure de démonstration

1. Sur LON-CL1, connectez-vous à OWA en tant qu'**Adatum\Aidan**.
2. Dans les options Outlook Web App, activez l'accès hors connexion.
3. Dans le Gestionnaire Hyper-V, déconnectez temporairement **LON-CL1** du réseau.
4. Ouvrez **Internet Explorer** sur LON-CL1 et ouvrez **https://lon-cas1.adatum.com/owa**.
5. Vérifiez que vous pouvez accéder au contenu de la boîte aux lettres.
6. Envoyez un message électronique de test à l'administrateur pendant que vous êtes hors connexion.
7. Reconnectez LON-CL1 au réseau.
8. Sur LON-CAS1, connectez-vous à OWA en tant qu'**administrateur**.
9. Vérifiez que vous avez reçu le courrier électronique envoyé par Aidan depuis Outlook Web App en mode hors connexion.

Leçon 3
Planification et configuration de la messagerie mobile

L'utilisation des téléphones mobiles de type smartphone et des tablettes pour la messagerie est devenu très populaire. De nombreux utilisateurs de téléphone mobile de type smartphone utilisent leurs appareils de manière intensive pour la messagerie, le calendrier, les tâches, etc. Avec le protocole ActiveSync, Exchange Server 2013 fournit une plateforme fiable pour connecter différents types d'appareils mobiles. Ce protocole offre non seulement des fonctionnalités pour les appareils mobiles, mais permet également aux administrateurs de sécuriser et de gérer ces périphériques.

Objectifs de la leçon

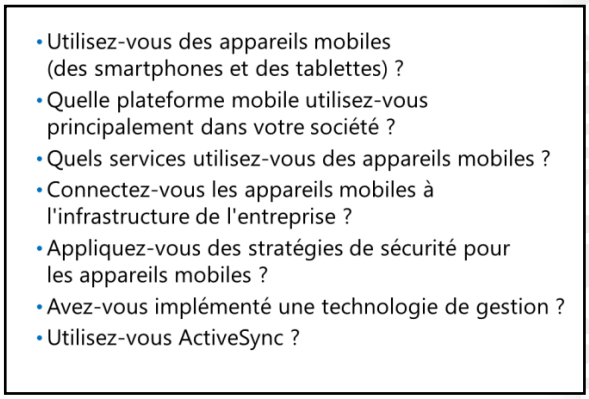
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire le fonctionnement d'Exchange ActiveSync ;
- décrire les fonctionnalités prises en charge dans Exchange ActiveSync ;
- décrire la technologie Direct Push ;
- décrire le service d'effacement à distance ;
- décrire la mise en quarantaine d'appareil mobile ;
- gérer les appareils mobiles avec des stratégies Exchange ActiveSync ;
- décrire les options pour la gestion d'appareils mobiles dans le Centre d'administration Exchange Server ;
- gérer les appareils mobiles avec Outlook Web App ;
- décrire les solutions alternatives pour la gestion d'appareil mobile.

Discussion : Utilisation des appareils mobiles dans les environnements professionnels

Cette discussion se concentre sur l'utilisation actuelle des appareils mobiles dans les environnements professionnels et les techniques de gestion et de sécurité associées. Abordez les questions suivantes :

- Utilisez-vous des appareils mobiles (des smartphones et des tablettes) dans votre environnement professionnel ?
- Quelle plateforme mobile utilisez-vous principalement dans votre société ? Sur quoi avez-vous basé votre décision pour choisir cette plateforme mobile spécifique ?
- Quels sont les services que vous utilisez sur les appareils mobiles (messagerie, calendrier, tâches et notes, par exemple) ?



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Connectez-vous les appareils mobiles à l'infrastructure de l'entreprise, ou utilisez-vous des services basés sur le cloud tels que Hotmail, Office 365 et Google Apps ?
- Appliquez-vous des stratégies de sécurité pour les appareils mobiles qui se connectent à votre environnement ?
- Avez-vous une technologie de gestion implémentée pour les appareils mobiles ?
- Utilisez-vous ActiveSync ?

Fonctionnement d'Exchange ActiveSync

La plupart des plateformes mobiles prennent désormais en charge le protocole ActiveSync pour la messagerie, le calendrier, les contacts, et les tâches. Avec le protocole ActiveSync, un appareil mobile peut se connecter de manière sécurisée à un serveur Exchange Server et en synchroniser les données. La connexion entre l'appareil mobile et Exchange Server est établie de manière sécurisée à l'aide de HTTPS. La plupart des périphériques qui prennent en charge ActiveSync peuvent également utiliser le service de découverte automatique. Ils peuvent ainsi configurer automatiquement la plupart des paramètres sur les appareils mobiles en utilisant le processus suivant :

- ActiveSync permet aux utilisateurs de synchroniser les données entre Exchange et l'appareil mobile
- Il se connecte au serveur d'accès au client via HTTPS
- Le service de découverte automatique est utilisé pour configurer les paramètres sur l'appareil
- Vous pouvez synchroniser les données de manière sélective sur l'appareil mobile
- Les données synchronisées restent sur l'appareil mobile même hors connexion

1. L'utilisateur démarre la configuration du compte Active Sync sur un appareil mobile en entrant une adresse de messagerie et un mot de passe.
2. Selon l'adresse de messagerie de l'utilisateur, l'appareil mobile se connecte au serveur DNS, et recherche l'adresse IP et l'URL du service de découverte automatique dans le domaine spécifié (s'il existe).
3. L'appareil mobile utilise une connexion HTTPS pour se connecter au répertoire virtuel du service de découverte automatique. Le service de découverte automatique établit la réponse XML selon les paramètres de synchronisation du serveur.
4. Le service de découverte automatique envoie une réponse XML via le pare-feu sur SSL. Cette réponse XML est interprétée par le périphérique portable, et les paramètres de synchronisation sont configurés automatiquement sur le téléphone mobile.

Remarque : Comme les appareils mobiles utilisent HTTPS pour se connecter à Exchange Server, chaque périphérique doit approuver l'émetteur du certificat qui est implémenté sur Exchange Server. Si vous n'utilisez pas les certificats publics pour Exchange, vous devez importer manuellement votre certificat RootCA sur l'appareil mobile. Vous pouvez importer manuellement de différentes manières selon la plateforme mobile que vous avez utilisée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Comment les clients basés sur ActiveSync se connectent-ils à Exchange Server ?

Lorsque les utilisateurs se connectent au serveur d'accès au client à l'aide d'un appareil mobile, le processus est le suivant :

1. Le client Exchange ActiveSync utilise HTTPS pour se connecter au répertoire virtuel Microsoft-Server-ActiveSync sur le serveur d'accès au client. Le serveur d'accès au client authentifie le client.
2. Si la boîte aux lettres de l'utilisateur se trouve sur un serveur de boîtes aux lettres situé dans le même site que le serveur d'accès au client, ce dernier se connecte au serveur de boîtes aux lettres de l'utilisateur et récupère les données de la boîte aux lettres. Si le serveur de boîtes aux lettres se trouve dans un autre site, le serveur d'accès au client transmet par l'intermédiaire d'un proxy la demande du client à un serveur de boîtes aux lettres situé dans le site approprié.
3. Si Exchange Active Sync est pris en charge à partir du système d'exploitation sur l'appareil mobile, il peut utiliser la technologie Direct Push pour vérifier que les messages sont remis au client mobile quand il se connecte à Exchange Server. Avec la technologie Direct Push, l'appareil mobile garde une connexion HTTPS permanente au serveur d'accès au client, ce qui entraîne une récupération instantanée des messages et un accès en temps réel au courrier électronique. Tous les systèmes d'exploitation d'appareils mobiles actuels qui prennent en charge ActiveSync, prennent également en charge la technologie Direct Push.

Lorsque le client a établi la connexion entre ActiveSync et Exchange Server, il télécharge les contacts, les éléments du calendrier, les messages électroniques et les autres éléments configurés. Sur la plupart des plateformes, vous pouvez choisir le nombre de jours du calendrier et de messages électroniques que vous synchronisez avec l'appareil. Ces données sont synchronisées avec Exchange Server de deux façons : automatiquement si Direct Push est activée, ou manuellement par l'utilisateur.



Remarque : Les données qu'un utilisateur synchronise entre Exchange Server et son appareil mobile restent sur ce dernier même lorsque la connexion à Exchange n'est pas disponible. Pour cette raison, il est très important que les appareils soient sécurisés.

Fonctionnalités prises en charge dans Exchange ActiveSync

Le protocole ActiveSync fournit de nombreuses fonctionnalités et caractéristiques. Parmi les fonctionnalités les plus importantes d'Exchange ActiveSync dans Exchange Server 2013 figurent notamment :

- La prise en charge des messages au format HTML.
- La prise en charge des indicateurs de suivi sur les messages.
- Le regroupement des messages électroniques en conversations.

- Parmi les fonctionnalités implémentées dans Exchange Server 2013 ActiveSync figurent notamment
  - La prise en charge des messages au format HTML
  - Le regroupement des messages électroniques en conversations
  - La capacité à synchroniser ou non une conversation
  - La prise en charge de la récupération rapide des messages
  - La recherche Exchange améliorée
  - La fonctionnalité de découverte automatique pour la mise en service sur les ondes
  - Direct Push
  - La prise en charge des informations sur la disponibilité
  - Les photos de la liste d'adresses globale
  - La gestion des droits relatifs à l'information (IRM)

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- La capacité à synchroniser ou non une conversation entière.
- La synchronisation des SMS avec la boîte aux lettres Exchange d'un utilisateur.
- La prise en charge de l'affichage du statut de la réponse aux messages.
- La prise en charge de la récupération rapide des messages.
- Les informations sur les participants aux réunions.
- La recherche Exchange améliorée.
- La réinitialisation PIN.
- La sécurité des appareils améliorée via des stratégies de mot de passe.
- La fonctionnalité de découverte automatique pour la mise en service sur les ondes.
- La prise en charge de la définition des réponses automatiques lorsque les utilisateurs sont en déplacement, en vacances ou absents du bureau.
- La prise en charge de la synchronisation des tâches.
- Direct Push.
- La prise en charge des informations sur la disponibilité des contacts.
- Les photos de la liste d'adresses globale. Il s'agit des images enregistrées sur un serveur Active Directory de l'utilisateur qui a envoyé le courrier électronique.
- Message Diffs. Il s'agit d'un moyen d'envoyer uniquement la nouvelle partie d'un courrier électronique et d'éviter les informations redondantes.
- La gestion des droits relatifs à l'information (IRM) sur Exchange Active Sync. Il s'agit d'une méthode permettant d'appliquer le contrôle et le chiffrement de gestion des droits numériques aux messages électroniques qui sont envoyés et reçus.

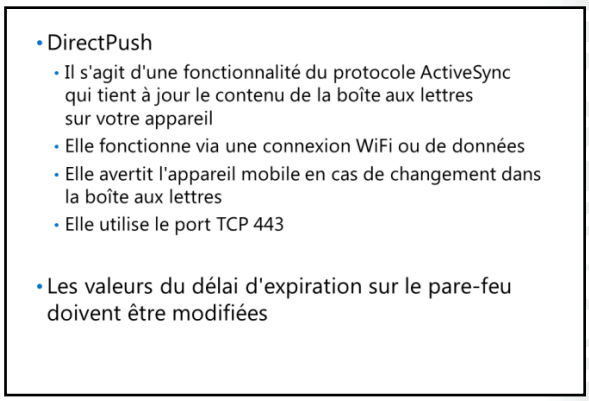
Exchange ActiveSync est fourni sous licence à de nombreux fournisseurs de système d'exploitation mobiles. Vous pouvez utiliser ActiveSync pour connecter votre appareil mobile à un appareil mobile Exchange Server, Windows Phone 7 (ou version plus récente), iOS 4 (ou versions plus récentes) et Android version 2 (et versions plus récentes). Cependant, tous les périphériques ne prennent pas en charge les mêmes fonctionnalités ActiveSync. Les fonctionnalités offertes par Exchange ActiveSync dépendent de la version du système d'exploitation exécutée sur celui-ci. Vous devez vérifier quelles fonctionnalités sont prises en charge sur votre appareil mobile.

 **Remarque :** Comme la plupart des tablettes exécutent également un système d'exploitation mobile, elles utilisent également le protocole ActiveSync pour se connecter à Exchange Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que Direct Push ?

Direct Push est une fonctionnalité intégrée à Microsoft Exchange Server 2013 qui maintient un appareil mobile à jour via une connexion cellulaire ou de réseau WiFi. Elle fournit une notification à l'appareil mobile lorsqu'un nouveau contenu est prêt à être synchronisé. Le client démarre ensuite la synchronisation pour télécharger les nouveaux éléments.



Pour établir Direct Push, procédez comme suit :

1. L'appareil mobile envoie une demande HTTPS à long terme au serveur. Cette demande est appelée « Ping ». La demande Ping laisse une connexion HTTPS ouverte avec le serveur.
2. Si de nouveaux éléments arrivent ou que des éléments sont modifiés, le serveur envoie à l'appareil une réponse qui inclut les dossiers contenant les éléments nouveaux ou modifiés. S'il n'y a aucun élément nouveau ou modifié dans les dossiers spécifiés lors de l'exécution de la demande Ping, le serveur envoie une réponse vide à l'appareil.
3. Si la réponse n'est pas vide, l'appareil mobile envoie une demande de synchronisation, puis se synchronise avec le serveur et envoie une nouvelle demande Ping. Si la réponse est vide, l'appareil mobile envoie une nouvelle demande Ping.
4. Lorsque l'utilisateur effectue une modification sur l'appareil mobile, l'appareil utilise la connexion HTTPS existante pour envoyer les mises à jour au serveur d'accès au client.

Pour permettre à Direct Push d'opérer à travers un pare-feu, vous devez ouvrir le port TCP 443. Ce port est requis pour la communication ActiveSync et il doit être ouvert entre Internet et le serveur d'accès au client.

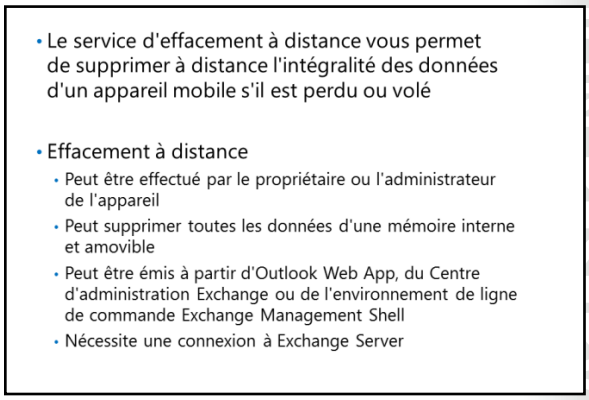
Outre l'ouverture de ports sur votre pare-feu, il est recommandé d'augmenter la valeur de délai d'expiration sur le pare-feu en faisant passer la valeur par défaut de 15 à 30 minutes pour optimiser les performances de la fonction Direct Push. La longueur maximale de la demande HTTPS est déterminée par les paramètres suivants :

- La valeur du délai d'expiration maximal définie sur les pare-feu qui contrôlent le trafic entre Internet et le serveur d'accès au client.
- Les valeurs du délai d'expiration du pare-feu qui sont définies par le fournisseur de services mobiles.
- Si la valeur du délai d'expiration est courte, l'appareil lance une nouvelle demande HTTPS plus souvent. Cela peut réduire l'autonomie de la batterie de l'appareil.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que le service d'effacement à distance ?



Lorsqu'une connexion ActiveSync est établie entre un appareil mobile et un serveur Exchange Server, l'appareil mobile enregistre une partie des données de la boîte aux lettres utilisateur. L'appareil mobile stocke également les informations d'identification du domaine de l'utilisateur, qui sont le nom d'utilisateur et mot de passe requis pour s'authentifier auprès du serveur d'accès au client. Si un appareil est perdu ou volé, ces données peuvent être compromises.

Puisque le risque de perdre un appareil mobile est particulièrement élevé, vous devez en sécuriser les données. Vous pouvez sécuriser les appareils mobiles en appliquant une stratégie ActiveSync qui définit les exigences de mot de passe pour l'appareil. Toutefois, cela n'empêche pas les données d'être compromises lorsque des appareils sont perdus ou volés.

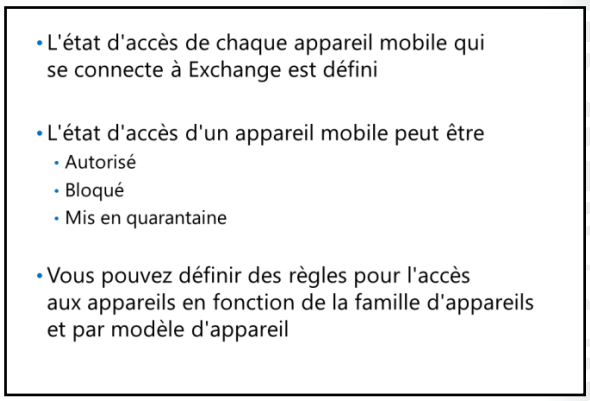
Quand un appareil est perdu ou volé, Exchange Server propose une option appelée Service d'effacement à distance. Lorsque cette commande est publiée, elle supprime toutes les données du téléphone et des cartes mémoire, et réinitialise toutes les valeurs par défaut des paramètres. La restauration des paramètres par défaut empêche tout utilisateur non-autorisé d'accéder aux données du compte ou à celles mises en cache sur l'appareil. Si vous réalisez un effacement d'appareil à distance sur un téléphone mobile en votre possession et que vous voulez conserver les données sur la carte de stockage, retirez celle-ci avant de commencer l'effacement de l'appareil à distance.

Remarque : Beaucoup de nouveaux smartphones n'ont pas de stockage amovible ; vous devez donc garder à l'esprit que le service d'effacement à distance détruira toutes leurs données.

La commande de service d'effacement à distance peut être lancée par l'utilisateur à partir d'un appareil mobile spécifique, à l'aide de l'interface Outlook Web App, ou si l'administrateur utilise le Centre d'administration Exchange ou l'environnement de ligne de commande Exchange Management Shell. Toutefois, la commande de service d'effacement à distance ne sera acceptée par l'appareil que s'il est toujours connecté à Exchange Server, par les données (3G, LTE ou service de données mobile semblable) ou par WiFi. Si la connexion est perdue (par exemple, si la carte SIM ou le module d'identité de l'abonné est supprimé ou si le compte ActiveSync est supprimé manuellement sur l'appareil), le service d'effacement à distance ne fonctionnera pas. Dans ce cas, vous devez émettre une commande de service d'effacement à distance dès que possible.

Remarque : La récupération des données est très difficile après une réinitialisation à distance. Cependant, un appareil n'est jamais aussi exempt de données résiduelles que lorsqu'il est nouveau. Il peut toujours être possible de récupérer des données d'un appareil en utilisant des outils sophistiqués.

Qu'est-ce que la mise en quarantaine d'appareil mobile ?



Microsoft Exchange Server 2013, avec la version la plus récente du protocole ActiveSync, offre de nouvelles fonctionnalités dans la zone de gestion d'appareil mobile pour les utilisateurs et les administrateurs. En tant qu'administrateur, vous pouvez créer des listes vertes, rouges et de mise en quarantaine en spécifiant les appareils mobiles qui sont autorisés à accéder à vos boîtes aux lettres Exchange. Cela vous permet d'identifier les appareils que les utilisateurs peuvent connecter à Exchange Server. Par exemple, vous pouvez spécifier que seuls les appareils qui exécutent Windows Phone 7 ou un système d'exploitation ultérieur peuvent se connecter à Exchange Server.

Cette fonction s'obtient en définissant l'état d'accès pour chaque appareil mobile qui se connecte à Exchange Server. Un état d'accès est l'état d'un appareil particulier. Vous pouvez contrôler les états d'accès d'un appareil mobile de plusieurs façons et celui-ci se comportera de manière différente à chaque état. L'état d'accès d'un appareil peut être notamment :

- Autorisé. Dans l'état d'accès Autorisé, un appareil mobile peut synchroniser via Exchange ActiveSync et se connecter à Exchange Server pour récupérer les messages électroniques et gérer les informations du calendrier, des contacts, des tâches et des notes. Cette opération se déroule tant que l'appareil est conforme aux stratégies de boîte aux lettres Exchange ActiveSync configurées. Il s'agit de l'état par défaut pour tous les appareils, car Exchange Server ne définit aucune stratégie de quarantaine.
- Bloqué. Si la règle d'accès de l'appareil spécifie qu'un appareil doit être bloqué, cet appareil ne peut pas se connecter à Exchange Server et reçoit une erreur de type HTTP 403 Refusé. Vous pouvez bloquer un appareil selon sa famille ou bloquer un modèle d'appareil spécifique. L'utilisateur recevra un message électronique d'Exchange Server lui indiquant que l'appareil mobile ne peut pas accéder à sa boîte aux lettres. Un appareil mobile peut également être bloqué car il n'applique pas les stratégies de boîte aux lettres Exchange ActiveSync.

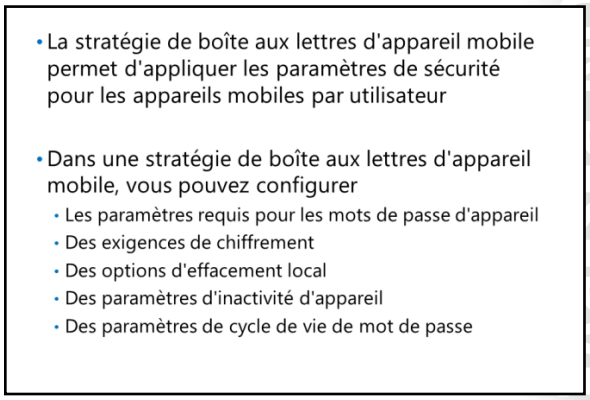
  Si c'est le cas, l'utilisateur ne peut pas recevoir de message électronique qui indique que l'appareil mobile n'a pas pu accéder à sa boîte aux lettres. Cependant, les informations à propos de l'appareil mobile affichées dans Outlook Web App indiquent qu'il est bloqué car il n'a pas pu appliquer les stratégies de boîte aux lettres Exchange ActiveSync.
- Mis en quarantaine. Lorsqu'un appareil mobile est en quarantaine, il peut se connecter à Exchange Server, mais avec un accès limité aux données. L'utilisateur peut ajouter du contenu à son calendrier, ses contacts, ses tâches et ses notes, mais le serveur ne permet pas à l'appareil de récupérer du contenu de sa boîte aux lettres. L'utilisateur recevra un message électronique unique qui lui indique que l'appareil mobile est mis en quarantaine. Ce message est reçu par l'appareil et il est également disponible dans la boîte aux lettres de l'utilisateur. Vous pouvez ajouter un texte personnalisé à ce message pour fournir des instructions aux utilisateurs dont les appareils sont mis en quarantaine. Un appareil reste en quarantaine jusqu'à ce que l'administrateur décide s'il reste bloqué ou s'il est autorisé à se connecter.

Vous pouvez créer et gérer des règles d'accès d'appareil ActiveSync en utilisant le Centre d'administration Exchange ou l'environnement de ligne de commande Exchange Management Shell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sécurisation des appareils mobiles avec les stratégies de boîte aux lettres d'appareils mobiles



Les clients mobiles, tels que les clients Exchange ActiveSync, sont difficiles à sécuriser. Dans la mesure où les appareils sont petits et portables, ils sont susceptibles d'être perdus ou volés. Par ailleurs, ils peuvent contenir des informations hautement confidentielles. Les cartes de stockage prévues pour être insérées dans les connecteurs d'extension des appareils mobiles peuvent stocker des quantités de données de plus en plus importantes. Si cette capacité de stockage est importante pour les utilisateurs d'appareils mobiles, elle aggrave les risques lorsque toutes ces données se retrouvent entre de mauvaises mains.

Les clients mobiles sont également difficiles à gérer à l'aide de stratégies centralisées, car dans certains cas, les appareils sont rarement (voire jamais) connectés au réseau interne. En outre, les appareils ne requièrent pas de comptes Active Directory ; par conséquent, vous ne pouvez pas utiliser d'objets de stratégie de groupe (GPO) pour gérer les paramètres des clients.

Implémentation d'une stratégie de boîte aux lettres d'appareil mobile

La stratégie de boîte aux lettres d'appareil mobile propose une option pour sécuriser les appareils mobiles. Lorsque vous appliquez la stratégie à un utilisateur, elle est automatiquement téléchargée sur l'appareil mobile à la prochaine connexion au serveur d'accès au client. Exchange ActiveSync vous permet de forcer les exigences en termes de mot de passe sur un appareil mobile, et de configurer plusieurs autres options de sécurité. Tous ces paramètres sont obligatoires, ce qui signifie que s'ils sont appliqués, les utilisateurs ne peuvent pas les modifier du côté client.

Les stratégies de boîte aux lettres d'appareils mobiles sont appliquées en fonction de chaque utilisateur, ce qui signifie que vous pouvez créer différentes stratégies pour différents utilisateurs. Cependant, les stratégies peuvent être appliquées uniquement au niveau pris en charge par le périphérique mobile. Les paramètres de stratégie que la plateforme mobile ne prend pas en charge côté client sont ignorés. Chaque utilisateur possède une stratégie par défaut qui n'applique aucun paramètre de sécurité. Vous pouvez créer une nouvelle stratégie et la déclarer comme stratégie par défaut afin qu'elle soit automatiquement appliquée à tous les comptes d'utilisateurs. Pour vérifier que les appareils mobiles sont parfaitement sécurisés, configurez des stratégies de boîte aux lettres d'appareils mobiles qui requièrent des mots de passe de périphérique et chiffrent les données stockées sur l'appareil mobile.

Quand vous implémentez une stratégie de boîte aux lettres d'appareil mobile, vous pouvez configurer les options suivantes :

- Il s'agit de la stratégie par défaut. Vous permet de définir une stratégie par défaut et de l'appliquer à tous les utilisateurs.
- Autoriser les appareils qui ne prennent pas entièrement en charge ces stratégies à se synchroniser. Permet aux appareils qui ne prennent pas en charge toutes les options de stratégie de se synchroniser quand même.
- Exiger un mot de passe. Vous permet de définir des exigences de mot de passe.
- Autoriser un mot de passe simple. Permet aux utilisateurs d'utiliser des mots de passe tels que 1111 ou 1234.
- Exiger un mot de passe alphanumérique. Requiert un mot de passe qui comprend à la fois des chiffres et des lettres.
- Exiger le chiffrement sur le périphérique. Requiert que le stockage sur un périphérique soit chiffré.
- Le mot de passe doit comporter les jeux de caractères suivants. Spécifie le nombre de jeux de caractères différents qu'un mot de passe doit contenir. Cette valeur est numérique. Les jeux de caractères sont des majuscules, des minuscules, des nombres et des symboles.
- Longueur minimale du mot de passe. Spécifie le nombre minimum de caractères du mot de passe.
- Nombre d'échecs de connexion avant réinitialisation de l'appareil localement. Spécifie le nombre de tentatives de saisie incorrectes de mot de passe de l'appareil avant réinitialisation. L'effacement d'appareil local est un mécanisme par lequel un téléphone mobile efface les données sans demande de la part du serveur. Le résultat d'un effacement d'appareil local est identique à celui d'un appareil distant. L'appareil retrouve son état d'usine par défaut. Quand un téléphone mobile effectue un effacement local, aucune confirmation n'est envoyée à Exchange Server.
- Demander la connexion après que le périphérique a été inactif. Spécifie la durée (en minutes) d'inactivité du périphérique après laquelle le mot de passe est requis.
- Appliquer la durée de vie de mot de passe (en jours). Spécifie la durée maximale pendant laquelle un mot de passe peut être utilisé sur le périphérique.
- Nombre de recyclages du mot de passe. Spécifie le nombre de mots de passe différents qu'un utilisateur doit utiliser avant de permettre le recyclage d'un ancien mot de passe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

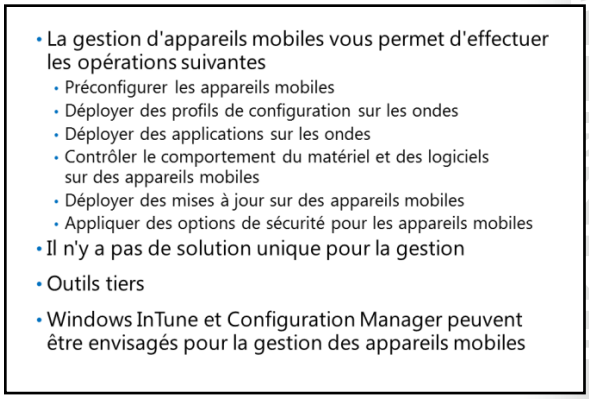
Démonstration : Vérification des options pour la gestion d'appareils mobiles dans le Centre d'administration Exchange Server

Procédure de démonstration

1. Dans le Centre d'administration Exchange, ouvrez le volet Mobile.
2. Configurez les options pour mettre en quarantaine tous les appareils jusqu'à ce que l'administrateur décide de leur accorder l'accès.
3. Configurez les options pour que l'administrateur reçoive un message dès que l'appareil est en quarantaine.
4. Configurez la nouvelle règle d'accès aux appareils avec l'option : **Mise en quarantaine – Me laisser choisir de bloquer ou d'autoriser plus tard**.

Alternatives à la gestion d'appareil mobile

Exchange Server 2013 fournit des options pour appliquer les paramètres de sécurité sur des appareils mobiles via des stratégies de boîte aux lettres d'appareil mobile. Cependant, comme il n'y a aucune option pour gérer et allouer des appareils mobiles, vous avez généralement la possibilité d'effectuer les tâches suivantes :



- Préconfigurer les appareils mobiles avec des options définies par l'entreprise.
- Déployer des profils de configuration pour les appareils mobiles sur les ondes.
- Déployer des applications pour des appareils mobiles sur les ondes.
- Contrôler le comportement du matériel et des logiciels sur des appareils mobiles.
- Déployer des mises à jour sur des appareils mobiles à partir d'un seul point d'administration.
- Appliquer des options de sécurité pour les appareils mobiles.

Actuellement, il n'y a aucun logiciel ou plateforme d'administration qui peut effectuer la gestion de chaque type de plateforme mobile. Chaque fournisseur de plateforme mobile fournit sa propre solution de gestion ou les sociétés tierces fournissent des solutions Web ou sur site pour la gestion des appareils mobiles qui sont habituellement basées sur le logiciel client déployé sur des appareils mobiles.

La seule plateforme mobile de Microsoft qui prend en charge les capacités complètes de gestion est Windows Mobile 6.5 avec Mobile Device Management Server 2008. Cependant, cette plateforme ne sera plus développée. La nouvelle version de la plateforme Windows Phone (la version 8) prend en charge plus de capacités de gestion que Windows Phone 7.

Vous pouvez également utiliser les services du cloud tels que Windows InTune pour gérer des appareils mobiles. Windows Intune se connecte à Exchange Server installé sur site et vous permet de créer des stratégies d'appareil mobile. Certaines capacités de gestion d'appareil mobile sont également intégrées dans System Center Configuration Manager.

Leçon 4

Configuration de l'accès Internet sécurisé pour le serveur d'accès au client

Exchange Server 2013 fournit l'accès aux boîtes aux lettres utilisateur à partir d'une grande variété de clients. Dans de nombreux cas, ces clients peuvent se trouver à l'extérieur du réseau d'entreprise et accéder aux boîtes aux lettres utilisateur via une connexion Internet. Étant donné que les serveurs Exchange ne peuvent pas fournir cette fonctionnalité sans être accessibles à partir d'Internet, il est important que les connexions établies à partir d'Internet soient aussi sécurisées que possible. Cette leçon décrit comment configurer l'accès sécurisé aux serveurs Exchange à partir d'Internet.

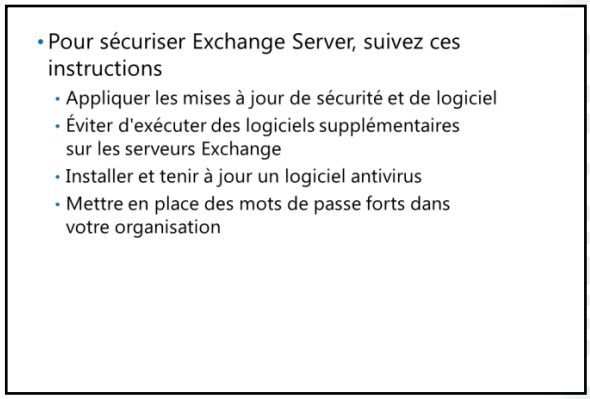
Objectifs de la leçon

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

- décrire les instructions relatives à la sécurité Exchange Server ;
- décrire les composants de l'accès Internet sécurisé ;
- déployer Exchange Server 2013 pour l'accès Internet ;
- sécuriser le trafic d'accès au client depuis Internet ;
- sécuriser les connexions SMTP (Simple Mail Transfer Protocol) à partir d'Internet ;
- décrire les avantages de l'utilisation d'un proxy inverse.

Instructions relatives à la sécurité d'Exchange Server

Grâce à sa conception, Exchange Server 2013 est sécurisé lorsque vous le déployez. Bon nombre de ses fonctionnalités, telles que les rôles serveur, l'authentification Kerberos version 5 et les certificats auto-signés, garantissent que les serveurs présentent une surface d'attaque minimale et facilitent le chiffrement de la majeure partie du trafic réseau envoyé depuis et vers des serveurs Exchange.



Pour maintenir la sécurité d'Exchange Server, les organisations doivent implémenter des processus réguliers pour surveiller et valider la configuration d'Exchange Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Appliquer les mises à jour de sécurité et de logiciel

L'une des mesures les plus essentielles pour maintenir la sécurité d'Exchange Server consiste à installer toutes les mises à jour de sécurité dès que possible après leur parution. Cela inclut à la fois les mises à jour du système d'exploitation et les mises à jour d'Exchange Server.

Avant de mettre à jour l'installation, testez le déploiement de toutes les mises à jour de logiciel sur vos serveurs Exchange. Pour ce faire, vous avez besoin d'un environnement de test qui reproduit votre environnement de production.

Éviter d'exécuter des logiciels supplémentaires sur les serveurs Exchange

Une façon de réduire la surface d'attaque d'un serveur Exchange consiste à éviter d'exécuter des logiciels inutiles sur ce serveur. Dans l'idéal, vous devez dédier le serveur Exchange aux rôles serveur Exchange. Les seuls logiciels supplémentaires que vous devez installer sont des utilitaires, tels qu'un logiciel antivirus et les outils de gestion de serveur.

Installer et tenir à jour un logiciel antivirus

Quasiment toutes les organisations déploient un logiciel antivirus pour se protéger contre le courrier électronique malveillant. Vous devez également déployer un logiciel antivirus au niveau des fichiers sur les serveurs Exchange afin de garantir que ces serveurs sont protégés contre les attaques de virus. Exchange Server 2013 est fourni avec une fonctionnalité intégrée anti-programmes malveillants. Vous pouvez utiliser cette fonctionnalité comme solution de sécurité de la messagerie.

Mettre en place des mots de passe forts dans votre organisation

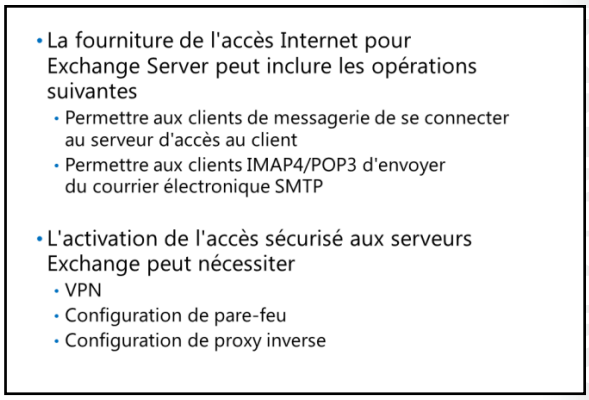
Si vous activez l'accès à distance à votre organisation Exchange Server, des intrus externes à l'organisation peuvent avoir recours à des attaques de mot de passe en force brute pour tenter de compromettre des comptes d'utilisateurs. Par conséquent, il est très important de définir et de mettre en place des stratégies de mot de passe pour tous les comptes d'utilisateurs. Cela inclut le fait d'imposer l'utilisation de mots de passe forts. Un mot de passe est fort s'il répond à plusieurs exigences de complexité qui le rendent difficile à deviner par les intrus. Ces exigences de mot de passe incluent des règles concernant la longueur du mot de passe et les catégories de caractères utilisées.

En établissant des stratégies de mot de passe fort pour votre organisation, vous pouvez contribuer à empêcher un intrus de se faire passer pour un des utilisateurs et empêcher de cette façon la perte, l'exposition ou l'altération d'informations confidentielles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Composants de l'accès Internet sécurisé

Exchange Server 2013 permet aux utilisateurs d'accéder à leurs boîtes aux lettres à partir de nombreux types de clients de messagerie différents et de quasiment n'importe où. Pour fournir un accès sécurisé pour les clients de messagerie, vous devez comprendre les types d'accès exigés par chaque type de client.



Accès client aux serveurs Exchange

La liste suivante décrit les services que les clients peuvent utiliser pour accéder aux serveurs Exchange à partir d'Internet :

- *Outlook Anywhere*. Outlook 2007 et les clients plus récents nécessitaient l'accès à l'appel de procédure distante (RPC), aux services Web Exchange (EWS) et aux répertoires virtuels de carnet d'adresses en ligne sur un serveur d'accès au client. Outlook 2010 ou les nouveaux clients nécessitent uniquement l'accès au répertoire virtuel RPC.
- *Accès au service de découverte automatique*. Le service de découverte automatique fournit une configuration automatique pour les clients Outlook et ActiveSync. Il est activé par défaut et le répertoire virtuel appelé Service de découverte automatique est créé sur le serveur d'accès au client. Le protocole requis pour le service de découverte automatique est HTTPS.
- *Microsoft Outlook Web App*. Outlook Web App fournit l'accès à Outlook Web App et aux répertoires virtuels du Panneau de configuration Exchange sur un serveur d'accès au client. Le protocole requis pour ce service est HTTPS.
- *Microsoft Exchange ActiveSync*. ActiveSync fournit l'accès au répertoire virtuel Microsoft-Server-ActiveSync sur un serveur d'accès au client et l'accès au répertoire virtuel du service de découverte automatique sur un serveur d'accès au client si le service de découverte automatique est activé. Le protocole requis pour ce service est HTTPS.
- *Internet Message Access Protocol version 4rev1 (IMAP4).* IMAP4 permet d'accéder au service IMAP4 sur un serveur d'accès au client et d'accéder au connecteur de réception SMTP avec les exigences suivantes en matière de protocole : IMAP4, SMTP (port 25 ou 587).
- *Post Office Protocol 3 (POP3)*. POP3 permet d'accéder au service POP3 sur un serveur d'accès au client, et d'accéder au connecteur de réception SMTP sur le serveur d'accès au client, ou un serveur SMTP différent avec les exigences suivantes en matière de protocole : POP3, SMTP (port 25 ou 587).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options de configuration de l'accès Internet

Plusieurs options sont disponibles pour fournir l'accès aux serveurs de transport et d'accès au client. Les options les plus courantes sont notamment les suivantes :

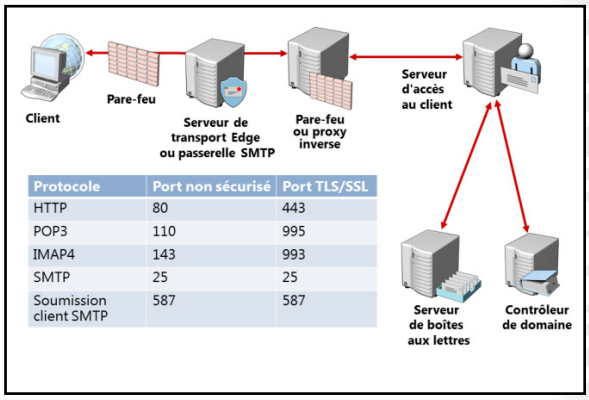
- Réseau privé virtuel (VPN). Certaines organisations exigent que tous les clients utilisent un réseau VPN pour se connecter au réseau interne. La passerelle VPN peut être un serveur de routage et d'accès distant Windows Server 2012 ou une solution tierce. En activant l'accès VPN, les utilisateurs peuvent accéder à toutes les ressources du réseau interne, y compris les serveurs Exchange. L'utilisation d'un réseau VPN ne nécessite aucune modification des clients de messagerie et les utilisateurs peuvent utiliser les mêmes noms de serveur en externe et en interne. L'implémentation d'une solution VPN simplifie également la configuration du périmètre du réseau, car vous activez uniquement une seule option pour accéder au réseau interne. Les réseaux VPN fournissent également des options de sécurité client avancées, telles que l'authentification multifacteur et la protection d'accès réseau. Toutefois, la solution VPN limite également les options dont les utilisateurs disposent pour accéder à leur courrier électronique. Ils peuvent uniquement accéder à leur courrier électronique à partir de clients capables d'établir une connexion VPN avec le réseau interne.
- Configuration de pare-feu. Quasiment toutes les organisations ont des pare-feu qui protègent leurs réseaux internes contre tout accès Internet indésirable. Vous pouvez configurer ces pare-feu pour permettre aux utilisateurs de se connecter aux répertoires virtuels et aux services requis sur le serveur d'accès au client, et pour fournir l'accès à un serveur SMTP pour les clients IMAP4 et POP3. L'implémentation d'une solution de pare-feu implique que tous les clients de messagerie soient configurés pour utiliser un nom de serveur qui est converti en adresse IP externe sur le pare-feu. Si les utilisateurs se connectent aux serveurs Exchange aussi bien depuis l'intérieur que depuis l'extérieur de l'organisation, cela peut compliquer la configuration des clients de messagerie.

  Par exemple, les utilisateurs peuvent se connecter aux serveurs Exchange depuis le réseau interne à l'aide du nom de serveur réel, mais devront peut-être utiliser un nom plus générique, tel que mail.contoso.com, lors de la connexion au serveur à partir d'Internet. Vous devrez peut-être demander aux utilisateurs d'utiliser les deux noms de serveur ou configurer la zone DNS (Domain Name System) interne pour fournir la résolution du nom en nom plus générique.

  La configuration de pare-feu pour fournir l'accès aux serveurs Exchange est facile, mais augmente les problèmes de sécurité potentiels. Les pare-feu standard peuvent filtrer le trafic réseau en fonction des ports et des adresses IP source et de destination, mais ils ne peuvent pas analyser le contenu des paquets réseau. Un pare-feu standard peut utiliser la traduction d'adresses réseau inverse, mais continue d'envoyer directement les paquets au serveur d'accès au client. Cela signifie que le trafic que le pare-feu transfère aux serveurs Exchange internes peut contenir un code malveillant qu'il n'a pas détecté.
- Configuration de proxy inverse. Comme autre solution que le pare-feu standard, vous pouvez utiliser un proxy inverse, ou un pare-feu de la couche Application, pour activer l'accès aux serveurs Exchange internes. Lorsque vous configurez un proxy inverse, il termine toutes les connexions client et analyse tous les paquets réseau pour détecter tout code malveillant. Le proxy inverse établit ensuite une nouvelle connexion au serveur d'accès au client et transfère le trafic au réseau interne. Lorsque vous utilisez un proxy inverse, vous devez configurer les clients de messagerie pour qu'ils utilisent un nom de serveur qui est converti en adresse IP externe sur le pare-feu.

Déploiement d'Exchange Server 2013 pour l'accès Internet

Lorsque vous déployez Exchange Server 2013 afin qu'il soit accessible depuis Internet, vous devez aussi déployer tous les rôles serveur sur le réseau interne. Le déploiement recommandé pour l'accès Internet à Exchange Server 2013 inclut deux pare-feu dans un scénario de pare-feu dos à dos, ce qui vous permet d'implémenter un réseau de périmètre entre les deux. Un pare-feu externe fait face à Internet et protège le réseau de périmètre. Vous devez déployer ensuite un pare-feu interne entre le réseau de périmètre et le réseau interne.



Protocole	Port non sécurisé	Port TLS/SSL
HTTP	80	443
POP3	110	995
IMAP4	143	993
SMTP	25	25
Soumission client SMTP	587	587

Remarque : Exchange Server 2013 ne fournit pas le rôle serveur de transport Edge, bien qu'il prenne en charge l'utilisation du rôle serveur de transport Edge à partir d'Exchange Server 2010. Si vous décidez d'utiliser le serveur de transport Edge à partir d'Exchange Server 2010, vous pouvez utiliser les paramètres du tableau ci-dessous. Si vous choisissez d'utiliser une passerelle SMTP tierce au lieu d'un serveur de transport Edge, quelques modifications peuvent s'avérer nécessaires.

Configuration des pare-feu externes pour l'accès Internet

Le pare-feu externe ou Internet d'une organisation protège le réseau de périmètre. Ce pare-feu peut être configuré pour accepter les paquets en fonction des ports et adresses IP source et de destination. Pour prendre en charge le déploiement d'Exchange Server, le pare-feu externe doit être configuré avec les règles de pare-feu suivantes :

Port de destination	Adresse
25	Adresse source : Toutes Adresse de destination : Serveur de transport Edge Vous devrez peut-être également configurer l'adresse IP externe du pare-feu interne comme adresse de destination si les clients POP3 et IMAP4 utilisent le port 25 pour relayer les messages via un serveur de transport Hub.
443	Adresse source : Toutes Adresse de destination : adresse IP externe du pare-feu interne

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Port de destination	Adresse
110, 995	Adresse source : Toutes Adresse de destination : adresse IP externe du pare-feu interne Uniquement requise pour l'accès POP3
143, 993	Adresse source : Toutes Adresse de destination : adresse IP externe du pare-feu interne Uniquement requise pour l'accès IMAP4
587	Adresse source : Toutes Adresse de destination : adresse IP externe du pare-feu interne Uniquement requise si les clients POP3 et IMAP4 utilisent le port de soumission du client SMTP pour envoyer le courrier électronique SMTP

Configuration des pare-feu internes pour l'accès Internet

Le pare-feu interne peut être un autre pare-feu standard ou un proxy inverse. Pour prendre en charge le déploiement d'Exchange Server, configurez le pare-feu interne avec les règles de pare-feu suivantes :

Port de destination	Adresse
25	Adresse source : Serveur de transport Edge Adresse de destination : Serveur de boîtes aux lettres Vous devrez peut-être également configurer l'adresse IP interne des hôtes externes comme adresse source si les clients POP3 et IMAP4 utilisent le port 25 pour relayer les messages via un serveur d'accès au client.
443	Adresse source : adresse IP interne du pare-feu externe Adresse de destination : serveur d'accès au client
110, 995	Adresse source : adresses IP externes Adresse de destination : serveur d'accès au client Uniquement requise pour l'accès POP3
143, 993	Adresse source : adresses IP externes Adresse de destination : serveur d'accès au client Uniquement requise pour l'accès IMAP4

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Port de destination	Adresse
587	Adresse source : adresses IP externes Adresse de destination : serveur d'accès au client Uniquement requise si les clients POP3 et IMAP4 utilisent le port de soumission du client SMTP pour envoyer le courrier électronique SMTP
50636	Adresse source : serveurs de boîtes aux lettres sur le réseau interne Adresse de destination : Serveur de transport Edge Requis pour le serveur de boîtes aux lettres afin de répliquer les informations sur les serveurs de transport Edge à l'aide d'EdgeSync
3389	Adresse source : ordinateurs d'administrateurs sur le réseau interne Adresse de destination : Serveur de transport Edge Requis si vous souhaitez utiliser le Bureau à distance pour administrer le serveur de transport Edge à distance

Les serveurs de transport Edge écoutent également les connexions Lightweight Directory Access Protocol (LDAP) non chiffrées sur le port 50389. Ce port est utilisé uniquement pour administrer l'instance Active Directory Lightweight Directory Services (AD LDS) sur le serveur de transport Edge à l'aide d'outils LDAP standard. Toutefois, ce port n'a pas à être ouvert sur le pare-feu interne.

Sécurisation du trafic d'accès au client depuis Internet

Vous devez implémenter les recommandations suivantes pour vérifier que les connexions clientes de votre organisation sont aussi sécurisées que possible :

Pour fournir l'accès au client sécurisé à partir d'Internet
- Créez et configurez un certificat de serveur
- Exigez SSL pour tous les répertoires virtuels
- Activer uniquement les méthodes d'accès au client requises
- Exigez l'authentification sécurisée
- Mettez en place la sécurité du client à distance
- Exigez TLS/SSL pour l'accès IMAP4 et POP3
- Implémentez un pare-feu de la couche Application ou proxy inverse

- Créez et configurez un certificat de serveur. Par défaut, tous les serveurs d'accès au client sont configurés avec des certificats auto-signés pendant l'installation d'Exchange Server 2013. Comme les clients n'approuvent pas ce certificat, vous devez le remplacer par un certificat d'une autorité de certification publique ou d'une autorité de certification interne. Si vous utilisez une autorité de certification d'entreprise interne, les certificats seront approuvés par les ordinateurs qui sont membres internes du domaine, mais pas par les autres ordinateurs clients.
- Exigez SSL pour tous les répertoires virtuels. Avec Exchange Server 2013, vous pouvez configurer tous les répertoires virtuels des serveurs d'accès au client pour qu'ils exigent SSL.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

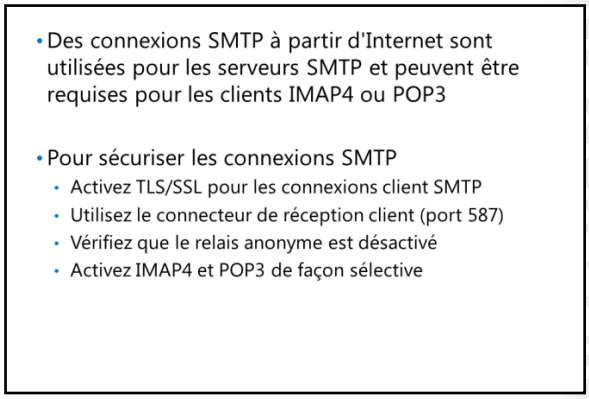
- Activez uniquement les méthodes d'accès au client requises. Vous devez uniquement autoriser l'accès aux options d'accès au client requises par votre organisation. Par exemple, si votre organisation requiert uniquement la connectivité Exchange ActiveSync et Outlook Web App à partir d'Internet, autorisez uniquement l'accès à ces répertoires virtuels via le pare-feu. Si votre organisation ne nécessite pas l'accès POP3 ou IMAP4, vous pouvez désactiver ces services sur le serveur d'accès au client et vérifier que les ports requis ne sont pas accessibles à partir d'Internet.
- Exiger l'authentification sécurisée. L'authentification basée sur les formulaires est le mécanisme d'authentification le plus sécurisé pour Outlook Web App. Les autres options d'accès au client, telles qu'Outlook Anywhere ou Exchange ActiveSync, ne peuvent pas utiliser l'authentification basée sur les formulaires et devront peut-être utiliser l'authentification de base ou l'authentification par Microsoft Windows NT LAN Manager, également appelé NTLM. Si vous configurez les répertoires virtuels pour qu'ils exigent SSL, le trafic réseau qui authentifie l'utilisateur est chiffré. Vous pouvez également implémenter l'authentification multifacteur. Par exemple, vous pouvez exiger que tous les ordinateurs clients utilisent une carte à puce ou un certificat approuvé en plus du nom d'utilisateur et du mot de passe. Vous pouvez également implémenter un mécanisme d'authentification multifacteur tiers, tel que RSA SecurID.
- Mettez en place la sécurité du client à distance. Pour garantir la sécurité de l'accès client, l'une des difficultés est que vous ne pouvez pas avoir le contrôle sur les périphériques clients que les utilisateurs utilisent pour accéder à leurs boîtes aux lettres. Par exemple, les utilisateurs peuvent utiliser leurs ordinateurs personnels ou des bornes publiques pour accéder à Outlook Web App. Si vous exigez une authentification de certificat pour les connexions client, vous pouvez limiter les clients qui peuvent accéder aux boîtes aux lettres Exchange. Plutôt que d'implémenter Outlook Web App, vous pouvez choisir d'implémenter Outlook Anywhere et de restreindre l'accès aux ordinateurs membres de votre domaine interne en implémentant l'authentification IPSec (Internet Protocol Security) basée sur les certificats pour les connexions clientes.
- Exigez TLS/SSL pour l'accès IMAP4 et POP3. Pour sécuriser les communications entre vos clients POP3 et IMAP4 et le serveur d'accès au client, configurez le serveur d'accès au client pour qu'il utilise un certificat pour ces protocoles, puis forcez tous les clients à utiliser TLS (Transport Layer Security) ou SSL pour chiffrer tout le trafic d'authentification et d'accès aux messages.
- Implémentez un pare-feu de la couche Application ou proxy inverse. Pour fournir davantage de sécurité, placez un pare-feu de la couche Application ou proxy inverse entre Internet et le serveur d'accès au client. Ce pare-feu peut déchiffrer tout le trafic réseau entre le client et le serveur d'accès au client, et il inspecte le trafic pour détecter tout code malveillant.

Remarque : L'utilisation de Microsoft® Forefront™ Threat Management Gateway 2010 (TMG) pour la publication des services Web d'Exchange Server 2013 n'est pas prise en charge par défaut, puisque TMG n'a pas d'assistant de publication pour Exchange Server 2013. Cependant, vous pouvez utiliser l'assistant de publication pour Exchange Server 2010 pour publier Exchange Server 2013. Après avoir configuré des règles de publication, vous devez manuellement modifier l'adresse de la page de fermeture de session.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Sécurisation des connexions SMTP depuis Internet

Si vous activez les connexions POP3 et IMAP4 entre Internet et vos serveurs d'accès au client, vous devez fournir un moyen par lequel ces clients peuvent envoyer du courrier électronique à l'aide de SMTP. Dans le cadre de la garantie de la sécurité de votre déploiement d'accès au client, vous devez également vérifier la connectivité SMTP sécurisée.



Connectivité SMTP pour les clients POP3 et IMAP4

Les clients peuvent utiliser POP3 et IMAP4 pour récupérer des messages des boîtes aux lettres d'utilisateur. Toutefois, ils ne peuvent pas utiliser ces connexions pour envoyer des messages. Pour permettre à ces clients d'envoyer du courrier électronique, vous devez les configurer pour qu'ils utilisent un serveur SMTP qui relaie les messages aux destinataires internes et externes.

Pour permettre aux clients POP3 et IMAP4 d'envoyer des messages, vous devez configurer un connecteur de réception SMTP pour exiger l'authentification, et accepter les connexions SMTP à partir d'Internet. En requérant l'authentification, seuls les utilisateurs avec des comptes valides dans l'organisation Exchange Server peuvent relayer des messages via le serveur.

Si vous utilisez un serveur de transport Edge ou une passerelle SMTP tierce, vous devez savoir que vous ne pouvez pas utiliser de serveur de transport Edge pour accepter les connexions SMTP authentifiées, puis l'utiliser pour relayer des messages SMTP à partir des clients POP3 et IMAP4.

Vous pouvez configurer un connecteur de réception SMTP sur un serveur de transport Edge qui utilise le port 587 et vous pouvez configurer ce connecteur de réception pour qu'il accepte les connexions authentifiées. Cependant, vous ne pouvez pas configurer le connecteur pour qu'il authentifie les connexions client à l'aide du compte Active Directory interne de l'utilisateur.

Sécurisation des connexions SMTP

Par défaut, Exchange Server 2013 fournit les connecteurs de réception suivants :

- Frontal client : fonctionne sur le port 587 et accepte les connexions sécurisées, avec TLS appliqué.
- Proxy client : fonctionne sur le port 465 et accepte les connexions à partir des serveurs d'accès au client. Ce connecteur s'exécute sur le serveur de boîtes aux lettres.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Frontal par défaut : fonctionne sur le port 25 et accepte les connexions des expéditeurs SMTP sur le port 25. C'est le point d'entrée de messagerie commun dans l'organisation.
- Nom_serveur par défaut : fonctionne sur le port 2525 et accepte les connexions à partir des serveurs de boîtes aux lettres exécutant le service de transport et des serveurs Edge (le cas échéant).
- Proxy frontal sortant : fonctionne sur le port 717 et accepte les messages d'un connecteur d'envoi sur un serveur de boîtes aux lettres, avec l'option Proxy frontal activée.

Ces connecteurs sont traités en détail dans les modules suivants. Pour sécuriser les connexions SMTP, procédez comme suit :

1. Activez TLS pour les connexions au client SMTP. Vous pouvez configurer le connecteur de réception SMTP pour exiger la sécurité TLS ou pour activer l'authentification de base uniquement après avoir lancé une session TLS. Si un certificat approuvé a été attribué au service SMTP, vous devez activer ces options, puis configurer tous les clients pour qu'ils utilisent TLS.
2. Utilisez le connecteur client frontal (port 587), et configurez deux connecteurs de réception SMTP. Le connecteur de réception frontal par défaut est configuré pour utiliser le port 25, tandis que le connecteur de réception frontal client est configuré pour utiliser le port 587. Par défaut, les deux connecteurs sont configurés pour exiger la sécurité TLS et permettre aux utilisateurs de se connecter au connecteur. Toutefois, en utilisant le connecteur de réception client, vous pouvez éviter d'utiliser le port SMTP par défaut pour les connexions client. Comme décrit dans le document RFC 2476, le port 587 a été proposé uniquement pour une utilisation à des fins d'envoi de messages à partir des clients de messagerie qui nécessitent le relais des messages.
3. Vérifiez que le relais anonyme est désactivé. Tous les connecteurs de réception doivent bloquer les relais anonymes et vous ne devez pas modifier cette option sur les connecteurs de réception qui sont accessibles à partir d'Internet. Si vous activez le relais anonyme, n'importe qui peut utiliser votre serveur pour relayer le courrier indésirable.

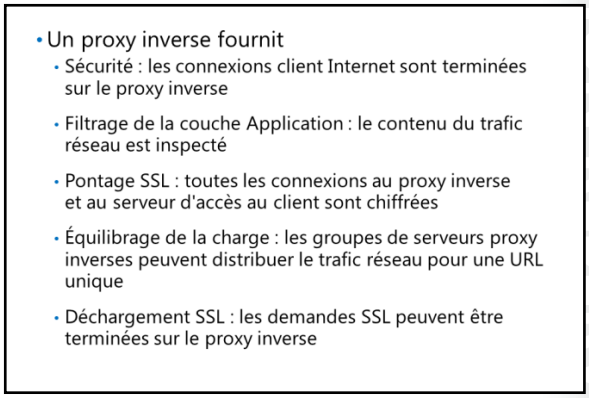
 **Remarque :** Dans certains cas, vous devrez peut-être activer le relais anonyme pour permettre aux applications internes d'envoyer du courrier électronique SMTP via le serveur Exchange. Si vous avez besoin de cette fonctionnalité, configurez des restrictions sur le connecteur de réception afin que seules les adresses IP que vous spécifiez puissent relayer les messages via le serveur.

Activez IMAP4 et POP3 de façon sélective. Si seuls quelques utilisateurs de votre organisation nécessitent l'accès POP3 et IMAP4, désactivez cette option sur toutes les autres boîtes aux lettres.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Avantages de l'utilisation d'un proxy inverse

Vous souhaiterez peut-être utiliser un serveur proxy inverse pour gérer les demandes entrantes sur un serveur d'accès au client. Un serveur proxy inverse fournit les avantages suivants par rapport à une connexion directe à un serveur d'accès au client :



- Sécurité. Le serveur proxy inverse fournit une couche protectrice supplémentaire entre le réseau et les ordinateurs externes. En effet, le serveur proxy inverse est le point de terminaison de toutes les connexions client. Le serveur proxy inverse établit ensuite une nouvelle connexion au serveur interne.
- Filtrage de la couche Application. La plupart des serveurs proxy inverses peuvent également fonctionner comme des pare-feu de la couche Application. Le filtrage de la couche Application permet au proxy d'ouvrir le paquet TCP/IP entier et d'inspecter les données d'application pour détecter les commandes et les données inacceptables. Par exemple, un filtre HTTP intercepte une communication sur le port 80 et l'inspecte pour vérifier que les commandes sont autorisées avant de transmettre la communication au serveur de destination. Les pare-feu qui sont capables de filtrer la couche Application peuvent arrêter tout code dangereux aux frontières du réseau avant qu'il ne provoque un quelconque dommage.
- Pontage SSL. Si vous devez chiffrer la communication entre le serveur proxy inverse et le serveur d'accès au client, faites-le en terminant la session SSL entre le navigateur Web et le serveur proxy inverse. Vous devez ensuite établir une nouvelle session SSL entre le serveur proxy inverse et le serveur d'accès au client. Cela protège le serveur d'accès au client contre tout accès direct à partir d'Internet, permet au serveur proxy inverse de filtrer les paquets de données avant qu'ils atteignent le serveur d'accès au client et chiffre les données tout au long du chemin entre le navigateur Web et le serveur d'accès au client.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Équilibrage de la charge. Un serveur proxy inverse peut distribuer à un groupe de serveurs le trafic destiné à une adresse URL unique. Vous implémentez automatiquement les fonctionnalités d'équilibrage de la charge Web lorsque vous publiez Outlook Web App et Outlook Anywhere. Outlook Web App sélectionne automatiquement une règle en utilisant l'équilibrage de charge basé sur les cookies. Avec l'équilibrage de charge basé sur les cookies, le serveur proxy inverse transfère toutes les demandes relatives à la même session (le même cookie unique étant fourni par le serveur dans chaque réponse) vers le même serveur. Outlook Anywhere utilise l'équilibrage de charge basé sur les protocoles IP sources. Avec l'équilibrage de charge basé sur les protocoles IP sources, le serveur proxy inverse transfère toutes les demandes provenant de la même adresse IP de client (source) vers le même serveur. Les autres services et fonctionnalités Exchange, tels qu'Exchange ActiveSync, doivent utiliser l'équilibrage de charge basé sur les cookies. Cela concerne également les services Exchange, tels que le carnet d'adresses en mode hors connexion et le service de disponibilité.
- Déchargement SSL. Au lieu de configurer le serveur d'accès au client pour fournir le chiffrement SSL, vous pouvez décharger cette fonction sur le serveur proxy inverse. Ce serveur chiffre les données qui sont envoyées entre le navigateur Web et le serveur d'accès au client, et il peut également inspecter les paquets de données et leur appliquer des filtres avant qu'ils atteignent le serveur d'accès au client. Si vous déchargez le chiffrement SSL sur un serveur proxy, les données qui sont envoyées entre le serveur proxy inverse et le serveur d'accès au client ne sont pas chiffrées, sauf si vous utilisez le pontage SSL.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et configuration de la connectivité pour les clients de messagerie

Scénario

A. Datum examine une solution de connexion cliente pour Exchange Server 2013. La société a plusieurs types de clients différents et doit rechercher une solution appropriée pour chacun, tout en restant conforme à sa stratégie de sécurité.

En tant qu'administrateur Exchange d'A. Datum, vous devez proposer et implémenter une solution pour la connectivité client. Vous devez également vérifier que les connexions Internet sont aussi sécurisées que possible.

Objectifs

- Planifier la connectivité client.
- Configurer Outlook Web App et Outlook Anywhere.
- Configurer Exchange ActiveSync.
- Publier Exchange Server 2013 via la passerelle Threat Management Gateway 2010.

Configuration de l'atelier pratique

Durée approximative : **75 minutes**

Ordinateurs virtuels	22341B-LON-DC1 22341B-LON-CAS1 22341B-LON-MBX1 22341B-LON-TMG 22341B-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 débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22341B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Ouvrez une session en utilisant les informations d'authentification suivantes :
   a. Nom d'utilisateur : **ADATUM\Administrateur**
   b. Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22341B-LON-MBX1**, **22341B-LON-CAS1**, **22341B-LON-TMG** et **22341B-LON-CL1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Planification de la connectivité des clients

Scénario

Pour activer l'accès au courrier électronique, votre organisation doit fournir des options appropriées de connectivité pour les utilisateurs qui se connectent à partir du réseau interne et d'un réseau externe (Internet). Des clients internes s'exécutent sur le système d'exploitation Windows 8. Certains clients disposent d'Outlook 2010, alors que d'autres ont Outlook 2003 ou encore aucun client Outlook. A. Datum n'envisage pas d'acheter de nouvelle licence client à ce stade.

Plusieurs utilisateurs utilisent des ordinateurs portables au bureau et à l'extérieur. Ces ordinateurs sont membres du domaine, et ils ont tous Windows 8 et Outlook 2010 installés.

La majorité des clients ont des appareils mobiles, en grande partie des téléphones portables de type smartphone et des tablettes. Ils utilisent principalement des appareils Windows Phone 7.5 et Windows Phone 8, mais un certain nombre de clients utilisent des appareils basés sur Android 4 et iOS 5. Quelques-uns ont des appareils Symbian plus anciens.

L'agent de sécurité d'A. Datum Corporation a défini les exigences de sécurité suivantes pour l'accès au courrier électronique et elles doivent être implémentées dans cette solution :

- Les clients internes doivent utiliser une connexion chiffrée au serveur de messagerie.
- Les clients externes doivent pouvoir vérifier leur courrier électronique à partir de n'importe quel ordinateur, y compris ceux situés dans les zones publiques. Cependant, ces utilisateurs ne doivent pas pouvoir télécharger de pièces jointes quand ils utilisent des ordinateurs publics.
- Pour permettre aux appareils mobiles de se connecter à votre réseau, vous devez pouvoir contrôler leurs options de sécurité et forcer les exigences de mot de passe. Il est préférable, mais pas obligatoire, que des appareils mobiles soient authentifiés à l'aide de certificats.
- Chaque utilisateur doit avoir un appareil protégé par mot de passe pour accéder à votre réseau.
- Tous les appareils qui se connectent à partir d'un réseau externe doivent avoir un certificat CA racine d'A. Datum installé dans le magasin Racine de confiance et ils doivent utiliser la sécurité SSL.
- Les administrateurs doivent pouvoir gérer des appareils mobiles. Il est préférable, mais pas obligatoire, qu'ils puissent contrôler certaines fonctionnalités de périphérique supplémentaires, comme l'utilisation du partage de données, Bluetooth, et des options d'itinérance.
- Chaque utilisateur doit pouvoir supprimer le contenu de son appareil mobile en cas de perte.

La solution que vous proposez pour la connectivité client doit répondre à toutes ces exigences.

Les tâches principales de cet exercice sont les suivantes :

1. Lisez et analysez les exigences du scénario.
2. Proposer une solution pour la connectivité client.
3. Présenter la solution à la classe.

▶ Tâche 1 : Lisez et analysez les exigences du scénario

- Lisez le scénario de l'exercice, et analysez les exigences du point de vue de la sécurité et d'une fonctionnalité. Identifiez les technologies qui devraient être utilisées.

▶ Tâche 2 : Proposer une solution pour la connectivité client

Proposez une solution pour la connectivité client pour les clients internes et externes. Utilisez les questions suivantes à titre indicatif quand vous proposez une solution :

1. Quelles plateformes clientes doivent être prises en charge pour les clients internes ?
2. Quelles plateformes clientes doivent être prises en charge pour les clients externes ?
3. Quels problèmes avez-vous avec les clients internes ?
4. Quels problèmes avez-vous avec les clients externes ?
5. Comment allez-vous répondre aux exigences en matière de chiffrement de connexion cliente ?
6. Quelle solution allez-vous proposer pour les clients internes ?
7. Quelle solution allez-vous proposer pour les clients externes ?
8. Comment allez-vous répondre aux exigences en matière de téléchargement de pièces jointes sur les ordinateurs publics ?
9. Comment allez-vous appliquer les exigences en matière de sécurité pour les appareils mobiles ?
10. Comment allez-vous déployer le certificat CA racine d'A. Datum sur les périphériques clients (les ordinateurs et les smartphones) ?
11. Existe-t-il une manière de contrôler les fonctionnalités matérielles des appareils mobiles ?
12. Pouvez-vous implémenter une authentification basée sur des certificats pour les appareils mobiles ?
13. Comment comptez-vous implémenter les exigences pour supprimer le contenu d'un appareil mobile perdu ?

▶ Tâche 3 : Présenter la solution à la classe

- Présentez la solution que vous proposez. Discutez des solutions alternatives avec les autres stagiaires et l'instructeur.

Résultats : À la fin de cet exercice, les stagiaires auront créé un plan pour la connectivité client.

Exercice 2 : Configuration d'Outlook Web App et d'Outlook Anywhere

Scénario

Dans la société A. Datum Corporation, plusieurs employés travaillent régulièrement en dehors du bureau. Ces utilisateurs doivent pouvoir consulter leur messagerie électronique sur n'importe quel ordinateur client, notamment ceux situés dans des lieux publics. Vous devez vous assurer qu'ils ne peuvent pas télécharger de pièces jointes quand ils utilisent des ordinateurs publics, et qu'ils ne peuvent pas récupérer les messages supprimés à l'aide de l'interface Outlook Web App.

Vous devez également désactiver la messagerie instantanée et les options de messagerie textuelle dans l'interface Outlook Web App. Pour cela, vous devez configurer des stratégies Outlook Web App, les appliquer aux utilisateurs qui accèdent à la messagerie à partir d'Internet, et vérifier que les paramètres ont été correctement appliqués. Ces utilisateurs seront identifiés avec un Attribut personnalisé 1 défini sur externe.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous devez également activer Outlook Anywhere pour des utilisateurs ayant des ordinateurs portables, et Outlook Web App hors connexion pour ceux qui ne disposent pas d'Outlook mais qui utilisent des ordinateurs portables.

Les tâches principales de cet exercice sont les suivantes :

1. Configuration des stratégies Outlook Web App.
2. Configuration d'Outlook Anywhere.
3. Activation et utilisation d'Outlook Web App hors connexion.

▶ Tâche 1 : Configuration des stratégies Outlook Web App

1. Sur LON-CAS1, sur l'écran d'accueil, cliquez sur **Internet Explorer**.
2. Accédez à **https://lon-cas1.adatum.com/ecp**.
3. Connectez-vous au **CAE** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Dans le CAE, dans le nœud **Autorisations**, choisissez de **créer une stratégie Outlook Web App**. Nommez cette stratégie **Stratégie des utilisateurs externes**.
5. Dans une nouvelle stratégie Outlook Web App, configurez les options pour empêcher les utilisateurs d'utiliser l'accès au fichier direct, de récupérer les éléments supprimés, et d'utiliser la messagerie instantanée et la messagerie textuelle.
6. Appliquez cette nouvelle stratégie à l'utilisateur **Adam Barr**.
7. Appliquez la nouvelle stratégie à l'utilisateur nommé **Aidan** à l'aide de l'**environnement de ligne de commande Exchange Management Shell**.
8. Utilisez le **Centre d'administration Exchange** pour affecter à l'attribut **Attribut personnalisé 1** la valeur **externe** pour les utilisateurs **Brad Sutton**, **Chad Niswonger** et **Daniel Durrer**.
9. Attribuez la **Stratégie des utilisateurs externes** à ces utilisateurs en tapant la commande suivante dans l'environnement de ligne de commande Exchange Management Shell :

   get-mailbox –filter {CustomAttribute1 –eq "external"} | Set-CASMailbox–OwaMailboxPolicy:"Stratégie des utilisateurs externes"

10. Vérifiez que la stratégie est appliquée à **Brad Sutton**, **Chad Niswonger** et **Danielle Durrer**.

▶ Tâche 2 : Configuration d'Outlook Anywhere

- Sur LON-CAS1, dans le **Centre d'administration Exchange**, configurez le nom externe afin que **Outlook Anywhere** soit **mail.adatum.com** et que l'authentification soit **NTLM**.

▶ Tâche 3 : Activation et utilisation d'Outlook Web App hors connexion

1. Sur LON-CL1, cliquez sur le Bureau, ouvrez Internet Explorer et tapez **https://lon-cas1.adatum.com/owa**, puis connectez-vous en tant qu'**ADATUM\Aidan** avec le mot de passe **Pa$$w0rd**.
2. Dans le menu **Options** d'**OWA**, sélectionnez l'option d'activation de l'accès hors connexion.
3. Ajoutez l'URL OWA aux **favoris** dans Internet Explorer.

4. Déconnectez-vous d'Outlook Web App, puis fermez Internet Explorer.
5. À l'aide de la console du Gestionnaire Hyper-V, déconnectez la carte réseau de LON-CL1 du réseau.
6. Essayez d'ouvrir OWA à partir d'Internet Explorer, et vérifiez que vous pouvez accéder au contenu de votre boîte aux lettres.
7. Envoyez un message électronique de test à l'administrateur.
8. Reconnectez LON-CL1 au réseau.
9. Vérifiez que l'administrateur a reçu le courrier électronique que vous avez envoyé lors de l'utilisation d'OWA hors connexion.

Résultats : À la fin de cet exercice, les stagiaires auront configuré Outlook Web App et Outlook Anywhere.

Exercice 3 : Configuration d'Exchange ActiveSync

Scénario

A. Datum Corporation a beaucoup d'utilisateurs qui utilisent des smartphones pour consulter leur courrier électronique. Les clients utilisent principalement des appareils Windows Phone 7.5 et Windows Phone 8, mais un certain nombre de clients utilisent des appareils Android et iOS, et certains ont des appareils Symbian plus anciens. Vous devez vous assurer que ces utilisateurs peuvent accéder à leurs boîtes aux lettres à l'aide d'Exchange ActiveSync. Vous devez également vous assurer que leurs connexions sont sécurisées et que des paramètres cohérents sont appliqués à chaque appareil. Les conditions suivantes doivent être remplies sur chaque appareil mobile :

- Un mot de passe alphanumérique doit être utilisé sur l'appareil.
- Le mot de passe doit contenir au moins deux jeux de caractères différents.
- La longueur minimale du mot de passe doit être de cinq caractères.
- Les utilisateurs peuvent taper au maximum quatre fois un mot de passe incorrect avant que le contenu de l'appareil soit effacé.
- Chaque appareil doit être verrouillé après cinq minutes d'inactivité.

Outre ces exigences, la stratégie de sécurité d'A. Datum spécifie que chaque nouvel appareil mobile qui se connecte au serveur Exchange Server de l'organisation doit être d'abord mis en quarantaine, puis autorisé ou bloqué manuellement une fois que l'administrateur Exchange a examiné la demande. Vous devez également rechercher une façon d'installer un certificat racine sur l'appareil mobile et configurer la sécurité SSL.

Les tâches principales de cet exercice sont les suivantes :

1. Planifier le déploiement d'appareil mobile.
2. Configurer les stratégies de boîte aux lettres pour les appareils mobiles.
3. Configurer les règles d'accès des appareils.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Planifier le déploiement d'appareil mobile

Conformément au scénario de l'exercice, proposez un plan pour la gestion d'appareil mobile à partir d'Exchange Server. Vous pouvez utiliser les questions suivantes à titre indicatif :

1. Sachant que de nombreuses plateformes de périphérique accéderont au serveur Exchange Server, quels sont les problèmes majeurs ?
2. Comment allez-vous faire pour que les paramètres soient cohérents sur chaque appareil mobile ?
3. Comment allez-vous implémenter les exigences en matière de mot de passe sur votre appareil mobile ?
4. Comment allez-vous implémenter les exigences en matière de mise en quarantaine ?

▶ Tâche 2 : Configurer les stratégies de boîte aux lettres pour les appareils mobiles

1. Ouvrez le Centre d'administration Exchange sur **LON-CAS1**.
2. Accédez à **Mobile** dans le volet des fonctionnalités.
3. Créez une stratégie de boîte aux lettres d'appareil mobile et nommez-la **Adatum Mobiles**.
4. Définissez la nouvelle stratégie comme stratégie par défaut.
5. Spécifiez les options suivantes dans la stratégie :
   - Exiger un mot de passe alphanumérique
   - Nombre de jeux de caractères compris dans un mot de passe : **2**
   - Longueur minimale du mot de passe : **5**
   - Nombre d'échecs de connexion avant réinitialisation du périphérique : **4**
   - Demander la connexion après que le périphérique a été inactif : **5**
6. Enregistrez la stratégie.

▶ Tâche 3 : Configurer les règles d'accès des appareils

1. Sur **LON-CAS1**, dans le Centre d'administration Exchange, accédez à **Mobile -> Accès au périphérique mobile** dans le menu.
2. Sélectionnez **Mise en quarantaine – Me laisser choisir de bloquer ou d'autoriser plus tard**.
3. Sélectionnez l'option pour que l'**administrateur reçoive un message dès que le périphérique est en quarantaine**.
4. Créez une règle d'accès de l'appareil.
5. Configurez la règle pour que tous les appareils soient mis en quarantaine quand ils se connectent pour la première fois.
6. Annulez la création de la règle d'accès des appareils.

Résultats : À la fin de cet exercice, les stagiaires auront configuré les options et les stratégies d'appareil mobile.

Exercice 4 : Publication d'Exchange Server 2013 via TMG 2010

Scénario

Après avoir configuré toutes les options de connectivité client, vous devez publier votre serveur d'accès au client sur Internet de manière sécurisée. Vous pouvez choisir Threat Management Gateway (TMG) 2010 comme solution pour effectuer cette tâche.

Les tâches principales de cet exercice sont les suivantes :

1. Publier des services Web Exchange via TMG 2010.
2. Tests de règle de publication.

▶ Tâche 1 : Publier des services Web Exchange via TMG 2010

1. Sur LON-CAS1, utilisez Windows PowerShell pour exporter le certificat webmail.adatum.com avec la clé privée. Affectez la valeur **Pa$$w0rd** au mot de passe et enregistrez le fichier **CAS1.pfx** sous **C:**
2. Sur l'ordinateur LON-TMG, importez le certificat à partir de **\\LON-CAS1\\CAS1.pfx** et enregistrez-le dans le magasin personnel de l'ordinateur.
3. Sur l'ordinateur **LON-TMG**, dans la console **Forefront TMG**, lancez l'Assistant pour publier l'accès au client Web Exchange.
4. Choisissez de publier OWA sur Exchange Server 2010.
5. Utilisez le nom public **webmail.adatum.com**.
6. Créez l'écouteur HTTPS et configurez-le pour utiliser le certificat **webmail.adatum.com**.
7. Configurez l'authentification des utilisateurs sous forme de formulaire HTML.
8. Configurez la délégation d'authentification pour qu'elle soit **de base**.
9. Sur **LON-CAS1**, configurez le répertoire virtuel OWA pour utiliser le nom externe **https://webmail.adatum.com/owa** et l'authentification **de base**.
10. Sur **LON-CAS1**, configurez le répertoire virtuel ECP pour utiliser le nom externe **https://webmail.adatum.com/ecp** et l'authentification **de base**.
11. Redémarrez **IIS** sur **LON-CAS1**.
12. Basculez vers **LON-TMG** et ouvrez les **Propriétés de la règle OWA**.
13. Sous l'onglet **Paramètres d'application**, dans le champ **URL de fermeture de session du serveur publié**, tapez **/owa/logoff.owa**. (Remarque : En effet TMG 2010 n'a pas de règle de publication pour Exchange 2013, et la page de fermeture de session dirige encore les utilisateurs vers l'ancien emplacement utilisé par Exchange Server 2010).
14. Testez la règle. Vous devez avoir des coches vertes pour ces deux URL.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Tests de règle de publication

1. Sur l'ordinateur hôte, ouvrez les paramètres de l'ordinateur **22341B-LON-CL1** et connectez-le au **Réseau privé 2**.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** sur l'ordinateur **LON-CL1**.
3. Remplacez la valeur de l'adresse IP de l'ordinateur LON-CL1 par **131.107.0.2**. Définissez la passerelle par défaut sur **131.107.0.1**. Désactivez les paramètres DNS.
4. Ouvrez le fichier d'hôtes sur **LON-CL1** à partir de l'emplacement **c:\windows\system32\drivers\etc\hosts**. Ouvrez-le avec le Bloc-notes.
5. Au bas du fichier d'hôtes, tapez **131.107.0.1** webmail.adatum.com. Enregistrez le fichier.
6. Depuis Internet Explorer, accédez à **https://webmail.adatum.com/owa**. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
7. Vérifiez que vous pouvez accéder au contenu de la boîte aux lettres. Cliquez sur **Paramètres**, puis sur **Options**. Vérifiez que vous pouvez vous connecter au Panneau de configuration Exchange.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1, 22341B-LON-MBX1, 22341B-LON-TMG** et **22341B-LON-CL1**.

Résultats : À la fin de cet exercice, les stagiaires auront publié Exchange Server 2013 via TMG 2010.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

- Configurez toujours la stratégie Outlook Web App pour les ordinateurs publics et privés.
- Utilisez OWA hors connexion uniquement sur les ordinateurs de confiance.
- Analysez les critères de sécurité pour chaque plateforme mobile avant de décider quelles plateformes vous allez prendre en charge du côté Exchange Server du système d'exploitation Windows Server® 2012.
- Configurez toujours les stratégies des appareils mobiles de sorte que le mot de passe soit requis sur un appareil.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Les utilisateurs reçoivent un avertissement en accédant à la page Outlook Web App à partir d'Internet.	
Les utilisateurs ne peuvent pas se connecter à Exchange Server avec des appareils mobiles.	

Questions de contrôle des acquis

Question : Que devez-vous utiliser pour sécuriser l'accès au serveur d'accès au client à partir d'Internet ?

Outils

- Centre d'administration Exchange
- Environnement de ligne de commande Exchange Management Shell
- Forefront Threat Management Gateway

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 6

Planification et implémentation de la haute disponibilité

Table des matières :

Vue d'ensemble du module **6-1**

Leçon 1 : Haute disponibilité dans Exchange Server 2013 **6-2**

Leçon 2 : Configuration de bases de données de boîtes aux lettres hautement disponibles **6-12**

Leçon 3 : Configuration des serveurs d'accès au client hautement disponibles **6-28**

Atelier pratique : Implémentation de la haute disponibilité **6-32**

Contrôle des acquis et éléments à retenir **6-38**

Vue d'ensemble du module

Les systèmes de messagerie sont considérés comme un outil stratégique dans la plupart des organisations. Les pannes, même de quelques heures, donnent une mauvaise image des services informatiques et peuvent faire perdre des ventes ou porter atteinte à la réputation de l'entreprise. La haute disponibilité contribue à garantir que les systèmes de messagerie basés sur Microsoft® Exchange Server 2013 peuvent survivre à la défaillance d'un serveur ou même de plusieurs serveurs. Vous pouvez implémenter la haute disponibilité pour tous les rôles serveur dans Exchange Server 2013.

Ce module décrit la technologie à haute disponibilité intégrée à Exchange Server 2013 et certains des facteurs externes qui affectent les solutions hautement disponibles.

Objectifs

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

- décrire la haute disponibilité dans Exchange Server 2013 ;
- configurer des bases de données de boîtes aux lettres hautement disponibles ;
- configurer des serveurs d'accès au client hautement disponibles.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Haute disponibilité dans Exchange Server 2013

Haute disponibilité est un terme couramment utilisé pour faire référence à une technologie ou configuration spécifique qui met en avant la disponibilité de service. Bien que de nombreuses technologies et configurations puissent mener à des configurations hautement disponibles, elles ne sont pas en elles-mêmes véritablement hautement disponibles. Une conception et une planification soigneuses doivent être exécutées pour garantir une solution hautement disponible.

Dans cette leçon, vous allez examiner la haute disponibilité et certains facteurs qui entrent dans la conception et le déploiement d'une solution hautement disponible.

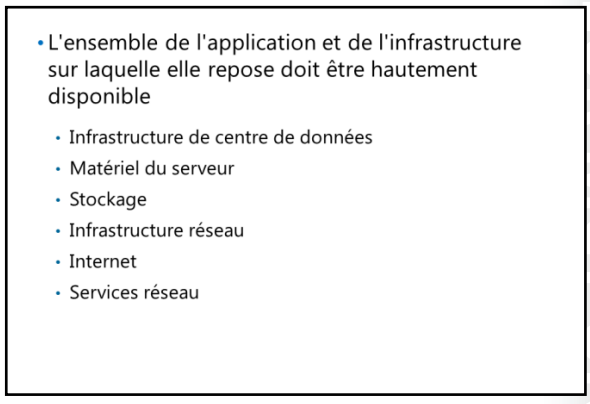
Objectifs de la leçon

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

- décrire les composants de la haute disponibilité ;
- décrire un groupe de disponibilité de base de données (DAG) ;
- expliquer comment fonctionnent les groupes de disponibilité de base de données (DAG) ;
- décrire la haute disponibilité pour les serveurs d'accès au client ;
- expliquer la haute disponibilité de transport ;
- expliquer la haute disponibilité pour les serveurs de transport Edge ;
- décrire la résilience de site ;
- présenter les technologies de haute disponibilité de virtualisation comparées aux technologies de haute disponibilité Exchange Server pour les serveurs de boîtes aux lettres.

Composants de la haute disponibilité

Lorsqu'une application comme Exchange Server 2013 requiert la haute disponibilité, vous devez prendre en compte davantage d'éléments que les composants d'application. L'ensemble de l'infrastructure et des services sur lequel l'application repose doit aussi être hautement disponible.



Vous devez prendre en compte les composants supplémentaires suivants lors de la planification de la haute disponibilité.

Infrastructure de centre de données

La salle qui abrite le serveur doit posséder une capacité d'alimentation électrique et de refroidissement suffisante et cette capacité doit également être hautement disponible. Vous pouvez rendre l'alimentation électrique hautement disponible en garantissant qu'une autre source de courant telle qu'une batterie ou un générateur est disponible en cas de panne du réseau électrique. Vous pouvez rendre la capacité de refroidissement hautement disponible en utilisant plusieurs unités de refroidissement disposant d'une capacité suffisante pour assurer le refroidissement du centre de données lorsqu'une unité tombe en panne. En cas de panne majeure, vous pouvez utiliser un autre site de centre de données.

Matériel du serveur

Pour rendre le matériel du serveur hautement disponible, celui-ci doit contenir des composants redondants. Les composants redondants peuvent être des blocs d'alimentation, des cartes réseau, des processeurs et de la mémoire. La mémoire ECC (Error-Correction Code) aide à résoudre les erreurs de mémoire mineures.

Stockage

Pour rendre le stockage hautement disponible sur un serveur unique, vous pouvez utiliser une version du système RAID (Redundant Array of Independent Disks). Ce système utilise les informations de parité pour permettre à un serveur de survivre à la perte d'un disque dur sans perdre de données. Si plusieurs serveurs sont disponibles, vous pouvez répliquer des données entre serveurs. Cela permet aux données de survivre à la perte d'un serveur complet et non uniquement d'un disque dur.

Infrastructure réseau

Pour rendre un réseau local (LAN) hautement disponible, vous devez y introduire des composants redondants. Dans un réseau local, il s'agit en général de commutateurs redondants. Même les commutateurs à prix modéré comprennent des configurations redondantes. Pour rendre la connectivité réseau d'un ordinateur individuel tolérante aux pannes, vous devez configurer des cartes d'interface réseau (NIC) redondantes sur l'ordinateur. Cette fonctionnalité est standard sur la plupart des serveurs milieu et haut de gamme. La haute disponibilité des réseaux WAN (Wide Area Network) est en général à la charge du fournisseur de services WAN. Toutefois, si vous utilisez des liens privés pour votre WAN, vous pouvez créer des chemins d'accès redondants via une liaison WAN.

Connectivité Internet

Pour rendre un accès Internet hautement disponible, vous devez avoir une connectivité Internet redondante. Dans l'idéal, vous devez utiliser deux fournisseurs de services Internet différents et deux méthodes de connectivité physique différentes. Par exemple, un des fournisseurs de services Internet peut fournir une liaison filaire et l'autre une liaison sans fil. Si vous utilisez ces méthodes, il est peu probable qu'un problème affectant un fournisseur de services Internet puisse affecter l'autre. Beaucoup de pare-feu et de routeurs peuvent utiliser une connexion pour la connectivité Internet et basculer sur une autre si le service principal tombe en panne. Pour le courrier électronique entrant, vous devez utiliser plusieurs enregistrements de ressources Exchange (MX), avec un enregistrement pointant sur l'adresse IP allouée par chaque fournisseur de services Internet.

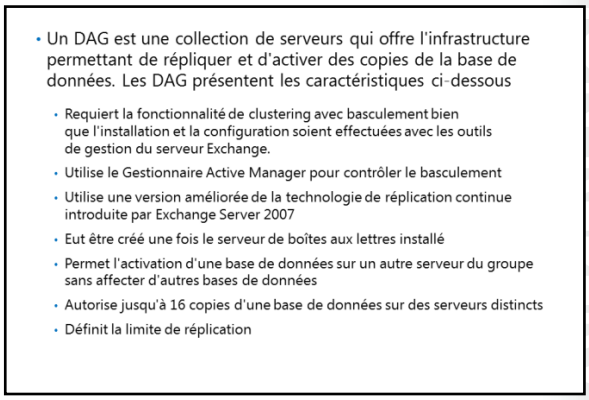
Services réseau

Le service Active Directory® Domain Services (AD DS) et le service Domain Name System (DNS) sont les deux services qui doivent être hautement disponibles pour prendre en charge les organisations Exchange Server 2013 hautement disponibles. Pour rendre les serveurs AD DS hautement disponibles, vous devez disposer de plusieurs contrôleurs de domaine et serveurs de catalogue global. Selon la taille d'un site, plusieurs contrôleurs de domaine et serveurs de catalogue global peuvent résider sur un seul site. Pour rendre les serveurs DNS internes hautement disponibles, vous devez avoir plusieurs serveurs DNS avec des informations DNS synchronisées entre eux. Par défaut, les zones DNS pour AD DS sont intégrées à Active Directory et répliquées entre tous les serveurs DNS de la forêt.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce qu'un groupe de disponibilité de base de données ?

Un groupe de disponibilité de base de données (DAG) est une collection de serveurs qui fournit l'infrastructure nécessaire pour répliquer et activer des copies de la base de données. Le DAG utilise la réplication continue pour chaque copie de base de données passive dans le DAG. Les DAG présentent les caractéristiques ci-dessous.



- Requièrent la fonctionnalité de clustering avec basculement Windows Server® 2008 R2 ou Windows Server® 2012 bien que toutes les tâches d'installation et de configuration soient effectuées avec le Centre d'administration Exchange ou l'environnement de ligne de commande Exchange Management Shell. Même si un DAG nécessite la fonctionnalité de clustering avec basculement, Exchange Server 2013 n'utilise pas le clustering avec basculement Windows pour gérer le basculement de base de données. Il utilise à la place Active Manager pour contrôler le basculement. Le clustering avec basculement Windows est utilisé pour certains scénarios de détection de panne, par exemple une panne de serveur.
- Utilisent une version améliorée de la technologie de réplication continue qui a été introduite dans Microsoft® Exchange Server 2007. Les améliorations prennent en charge les nouvelles fonctionnalités de haute disponibilité, telles que les copies de base de données et la mobilité de base de données. La réplication continue est expliquée dans la suite de cette leçon.

Remarque : Les DAG peuvent également utiliser la réplication tierce au lieu de la réplication continue.

- Vous permettent d'ajouter et de supprimer des serveurs de boîtes aux lettres à tout moment. Il n'est pas nécessaire de déterminer l'appartenance à un DAG pendant l'installation.
- Étant donné que les DAG utilisent un sous-ensemble de la fonctionnalité de clustering avec basculement Windows telle que la pulsation de cluster, Exchange Server 2013 doit être installé sur Windows® Server 2012 Datacenter Edition ou Standard Edition, ou Windows® Server 2008 R2 Enterprise Edition ou Datacenter Edition.
- Vous permettent de déplacer une base de données entre les serveurs du DAG sans affecter d'autres bases de données.
- Autorise jusqu'à 16 copies d'une base de données sur des serveurs distincts. Vous pouvez ajouter jusqu'à 16 serveurs à un DAG, ce qui vous permet de créer jusqu'à 16 copies d'une base de données. Les copies de la base de données doivent être stockées dans le même chemin d'accès sur tous les serveurs. Par exemple, si vous stockez la base de données de boîtes aux lettres 1 sur D:\Mailbox\DB\Mailbox Database 1\, sur LON-MBX01, vous devez également la stocker sur D:\Mailbox\DB\Mailbox Database 1\ sur tous les autres serveurs qui hébergent des copies de la base de données de boîtes aux lettres 1.

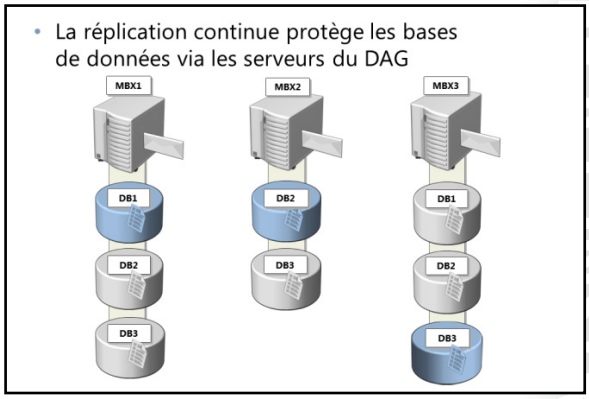
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Définit la limite de réplication, car seuls les serveurs du DAG peuvent héberger des copies de base de données. Vous ne pouvez pas répliquer d'informations de la base de données sur les serveurs de boîtes aux lettres hors du DAG.
- Vous empêchent d'ajouter un serveur Exchange 2010 à un serveur DAG Exchange 2013.

Remarque : Dans Exchange Server 2013, le concept de base d'un DAG est le même que dans Microsoft® Exchange Server 2010. Il diffère uniquement par le fait que les durées de basculement ont été réduites suite aux améliorations du code du journal des transactions et d'un point de contrôle plus approfondi sur les bases de données passives.

Présentation du fonctionnement des groupes de disponibilité de base de données

La copie active de la base de données utilise la réplication continue pour que les copies passives restent synchronisées en fonction de leur paramètre de délai d'attente. Un DAG exploite la fonctionnalité de clustering avec basculement du système d'exploitation Windows Server®. Il repose toutefois sur le composant Active Manager pour maintenir l'état de toutes les bases de données hébergées par le DAG. Voici des caractéristiques de base de données.



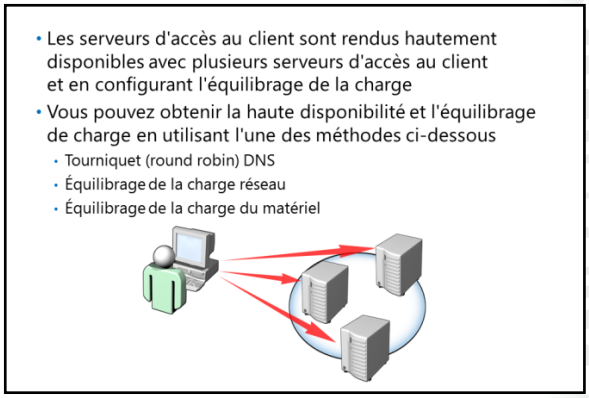
- Une base de données unique peut basculement entre les serveurs de boîtes aux lettres membres d'un DAG. Toutefois, Elle est seulement active sur un serveur à la fois.
- À un moment donné, une copie correspond soit à la source, soit à la cible de réplication, mais pas aux deux.
- Un serveur ne peut pas héberger plusieurs copies d'une base de données spécifique.
- Il n'est pas nécessaire que toutes les bases de données aient le même nombre de copies. Dans un DAG à 16 nœuds, une base de données peut avoir 16 copies, tandis qu'une autre base de données n'est pas redondante et contient uniquement la seule copie active.

Les basculements de la base de données se produisent lorsque les échecs provoquent la mise hors connexion de la base de données. Un échec d'un seul serveur ou un problème spécifique à une base de données peuvent provoquer l'échec. Une commutation se produit lorsqu'un administrateur coordonne intentionnellement le transfert d'une base de données active d'un serveur vers un autre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Présentation du fonctionnement de la haute disponibilité avec les serveurs d'accès au client

Vous configurez la haute disponibilité des serveurs d'accès au client en ajoutant au moins deux serveurs d'accès au client à votre site Active Directory. Les serveurs d'accès au client Exchange Server 2013 sont maintenant sans état. Cela signifie qu'une demande du client n'a plus besoin d'utiliser le même serveur d'accès au client et peut utiliser n'importe quel serveur. Cela vous permet d'utiliser les options ci-dessous pour distribuer la charge entre les serveurs d'accès au client.



- *Tourniquet (round robin) DNS*. Pour utiliser un tourniquet DNS, vous devez configurer un enregistrement A pour votre communication cliente et y ajouter toutes les adresses IP des serveurs d'accès au client disponibles. Si vous avez plusieurs emplacements physiques de serveurs de boîtes aux lettres, vous devez envisager d'implémenter un géoDNS pour que les serveurs clients obtiennent toujours l'adresse IP du serveur d'accès au client le plus proche. Lorsque vous prenez en considération un tourniquet DNS, vous devez tenir compte du fait que le basculement a lieu côté client. Par conséquent, le côté client doit prendre en compte l'utilisation d'un tourniquet DNS. Cette option est normalement utilisée lorsque vous ne pouvez pas utiliser l'équilibrage de charge réseau en raison d'un serveur à plusieurs rôles appartenant à un DAG, et que vous ne pouvez pas vous permettre d'avoir un équilibreur de charge matériel.
- *Équilibrage de la charge réseau*. Windows Server 2012 comporte une fonctionnalité appelée Équilibrage de la charge réseau (NLB) qui vous permet de répartir de manière égale la charge du serveur client sur les serveurs d'accès au client. Pour cela, une adresse IP virtuelle (VIP) est attribuée, en plus de l'adresse IP normale, à chaque membre du cluster NLB. La fonctionnalité d'équilibrage de la charge réseau garantit alors que le service est disponible et répondra uniquement s'il est disponible. Lorsqu'une défaillance de serveur se produira, l'adresse IP ne répondra plus et la charge sera alors répartie entre les serveurs qui fonctionnent encore correctement. Cette option assure un basculement basé sur un serveur, car le client n'utilisera que la VIP et sera connecté à un autre serveur d'accès au client automatiquement. Elle constitue une bonne solution si vous ne pouvez pas vous permettre d'avoir un équilibreur de charge matériel mais que vous souhaitez malgré tout mettre en place la haute disponibilité.
- *Équilibrage de la charge du matériel*. Tout comme un équilibrage de la charge réseau, un équilibreur de charge matériel utilise une VIP à laquelle le client envoie toutes les demandes. La différence principale entre un équilibrage de charge réseau Windows et un équilibreur de charge matériel est que vous pouvez configurer un équilibreur de charge matériel plus sophistiqué qui peut aussi être porté au-delà de la limite d'équilibrage de charge réseau Windows, soit 16 nœuds de cluster. En général, les performances sont bien meilleures avec un équilibreur de charge matériel, mais cette option comporte des coûts élevés. C'est la meilleure option pour avoir la haute disponibilité mais la plus onéreuse car elle nécessite l'achat d'un équilibreur de charge matériel.

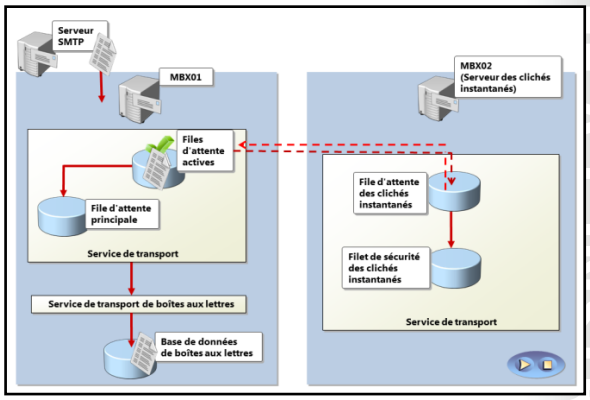
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour équilibrer la charge des serveurs d'accès au client, vous devez effectuer les tâches suivantes :

1. déployer plusieurs serveurs d'accès au client dans un site ;
2. utiliser l'équilibrage de charge réseau basée sur le matériel ou le logiciel pour créer un cluster ;
3. ajouter le nom du cluster réseau dont la charge est équilibrée dans le DNS. Par exemple, ajoutez une ressource hôte (A) pour caa1.contoso.com qui pointe vers 10.10.10.25.

Remarque : Dans Exchange Server 2010, vous deviez configurer un tableau d'accès au client dans l'environnement de ligne de commande Exchange Management Shell pour chaque site Active Directory. Dans Exchange Server 2013, cette spécification n'est plus nécessaire.

Présentation du fonctionnement de la haute disponibilité de transport



Dans Exchange Server 2013, la haute disponibilité du transport est plus qu'un simple moyen d'assurer la redondance des messages. Exchange Server 2013 tente de garantir la redondance des messages en combinant deux fonctionnalités : Redondance des clichés instantanés et Filet de sécurité (appelée Conteneur de dépôt dans Exchange Server 2010). La redondance des clichés instantanés crée une copie redondante du message sur un autre serveur avant que le message soit accepté ou reconnu. Le filet de sécurité enregistre les messages qui ont été correctement traités par le service de transport sur les serveurs de boîtes aux lettres.

Redondance des clichés instantanés

La redondance des clichés instantanés est une fonctionnalité introduite avec Exchange Server 2010 qui assure la disponibilité d'une copie d'un message si un serveur de boîtes aux lettres tombe en panne avant que les messages n'aient été soumis aux bases de données. Exchange Server 2013 améliore cette fonctionnalité en créant automatiquement une copie redondante de n'importe quel message qu'il reçoit avant d'en accuser réception correctement au serveur d'envoi SMTP.

Dans Exchange Server 2013, il n'est plus important qu'un serveur d'envoi prenne en charge la redondance des clichés instantanés car un cliché instantané est désormais créé chaque fois automatiquement. Par défaut, un cliché instantané d'un message est supprimé au bout de deux jours.

L'objectif principal de la redondance des clichés instantanés est d'avoir toujours deux copies d'un message dans une haute disponibilité limite de transport alors que le message est en transit. Cette limite est l'un des éléments ci-dessous.

- Un DAG, pour les serveurs de boîtes aux lettres membres d'un DAG. Il s'agit d'un DAG qui couvre plusieurs sites Active Directory.
- Un site Active Directory, pour les serveurs de boîtes aux lettres qui n'appartiennent pas à un DAG.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'endroit et le moment où la copie redondante du message est créée dépend de l'emplacement de provenance et destination du message. Les trois facteurs déterminants principaux sont les suivants :

- Messages reçus situés en dehors de la limite de haute disponibilité de transport.
- Messages envoyés situés en dehors de la limite de haute disponibilité de transport.
- Messages reçus du service de dépôt de transport de boîtes aux lettres d'un serveur de boîtes aux lettres dans les limites de la haute disponibilité de transport.

Remarque : La redondance des clichés instantanés ne suit jamais les messages des clichés instantanés hors des limites de la haute disponibilité de transport.

Fonctionnement de la redondance des clichés instantanés

L'exemple ci-dessous illustre le fonctionnement de la redondance des clichés instantanés dans un DAG.

1. Un serveur SMTP se connecte au service de transport sur un serveur de boîtes aux lettres sur lequel la base de données active du destinataire cible est montée et transmet un message. Lorsque le message est reçu, la session reste active.
2. Le service de transport ouvre une nouvelle session SMTP (Simple Mail Transfer Protocol) sur un service de transport situé sur un autre serveur de boîtes aux lettres dans le même DAG pour créer une copie redondante du message. Si le DAG couvre plusieurs sites Active Directory, un serveur de boîtes aux lettres situé dans un autre site Active Directory est préféré par défaut. La copie du message est le message de cliché instantané et le serveur de boîtes aux lettres qui la contient est le serveur des clichés instantanés du serveur principal. Le message existe dans une file d'attente des clichés instantanés sur le serveur des clichés instantanés.
3. Lorsque le message a été correctement transmis au serveur des clichés instantanés, le serveur accuse réception du message au serveur SMTP et ferme la connexion.

Remarque : Si le serveur de boîtes aux lettres n'est pas membre d'un DAG, tout serveur de boîtes aux lettres figurant dans le même site Active Directory sera utilisé comme serveur des clichés instantanés.

Suppression des messages des clichés instantanés

Lorsque le serveur transmet correctement le message à la base de données, le serveur met à jour l'état de suppression du message lorsque la remise est terminée. L'état de suppression est essentiellement un message qui contient la liste des messages qui sont surveillés. Un message remis correctement n'a pas besoin d'être conservé dans une file d'attente des clichés instantanés. Lorsque le serveur des clichés instantanés sait que le serveur principal a transmis correctement le message au prochain saut, le serveur des clichés instantanés déplace le message de cliché instantané de la file d'attente des clichés instantanés dans le filet de sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Fonctionnement de la récupération des messages

Lorsqu'un serveur de boîtes aux lettres a une panne due à une défaillance matérielle, chaque serveur de boîtes aux lettres qui contient des messages des clichés instantanés mis en file d'attente pour ce serveur de boîtes aux lettres assume la propriété de ces messages. Lorsque le serveur sera à nouveau en ligne, il tentera de resoumettre les messages. Tous les messages sont alors remis à nouveau à leurs destinations. Les messages sont donc remis en double. Cependant, Exchange Server détecte automatiquement les doublons et ne les rajoute pas à la base de données. Seuls les messages qui ne sont pas déjà dans la base de données seront ajoutés.

Filet de sécurité

Le filet de sécurité est une file d'attente de messages spéciale disponible dans le service de transport sur chaque serveur de boîtes aux lettres. Cette file d'attente stocke par défaut jusqu'à deux jours de messages qui ont été remis correctement à une base de données de boîtes aux lettres. Le filet de sécurité protège contre les échecs de serveur de boîtes aux lettres lorsque les journaux des transactions ont été perdus. Si une défaillance se produit et que quelques journaux des transactions ne sont pas répliqués en copie passive, vous pouvez utiliser le filet de sécurité pour remettre à nouveau les messages.

Le filet de sécurité a été amélioré dans Exchange Server 2013 comme indiqué ci-dessous.

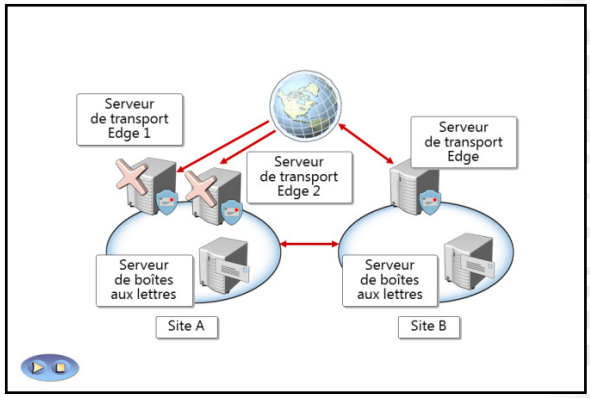
- Le filet de sécurité est désormais redondant et utilise la redondance des clichés instantanés pour fournir une file d'attente du filet de sécurité des clichés instantanés sur un autre serveur. Il n'est plus nécessaire que la redondance des clichés instantanés conserve une autre copie du message comme elle le faisait dans Exchange Server 2010. Si le filet de sécurité principal n'est pas disponible pendant plus de 12 jours, les demandes resoumises deviennent des demandes resoumises de clichés instantanés et les messages sont remis à nouveau depuis le filet de sécurité des clichés instantanés.
- Le filet de sécurité ne requiert plus de DAG. Il utilise principalement le même serveur qui est utilisé pour la redondance des clichés instantanés pour stocker une copie du filet de sécurité des clichés instantanés.

Fonctionnement du filet de sécurité

Le filet de sécurité fonctionne comme indiqué ci-dessous lorsque la redondance des clichés instantanés est terminée.

1. Le service de transport du serveur principal traite le message principal. Le service de transport de boîte aux lettres remet le message à la base de données de boîtes aux lettres. Le message est ensuite déplacé de la file d'attente dans la file d'attente principale du filet de sécurité.
2. Le serveur des clichés instantanés interroge fréquemment le serveur principal pour connaître l'état de suppression du message principal. Lorsqu'il a reçu l'état, le serveur de clichés instantanés déplace le message de la file d'attente des clichés instantanés à la file d'attente de filet de sécurité des clichés instantanés.

Présentation du fonctionnement de la haute disponibilité avec les serveurs de transport Edge



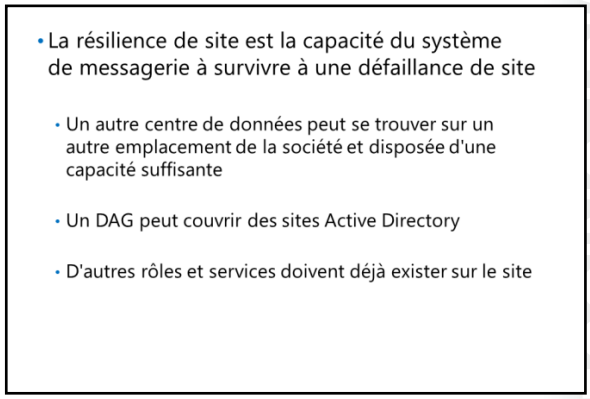
Le rôle de serveur de transport Edge n'est pas disponible dans la version finale d'Exchange Server 2013. Vous pouvez utiliser un serveur de transport Edge Exchange Server 2007 ou 2010, entièrement pris en charge. La fonctionnalité de haute disponibilité demeure la même dans Exchange Server 2013 que dans Exchange Server 2007 ou 2010.

Pour rendre le rôle serveur de transport Edge hautement disponible, vous pouvez installer un second serveur de transport Edge et configurer EdgeSync. Pour la remise des messages externes, aucune configuration supplémentaire n'est requise. Pour la réception des messages, vous devez configurer un enregistrement supplémentaire de serveur de messagerie (MX) pour le second serveur de transport Edge. Si les deux enregistrements MX ont la même priorité, les messages entrants sont réparties avec équilibrage de la charge entre les deux serveurs de transport Edge.

Pour assurer la redondance pour la remise des messages sur Internet, vous pouvez utiliser deux fournisseurs de services Internet. De nombreux pare-feu peuvent basculer vers une deuxième connexion Internet quand la connexion principale échoue. Pour recevoir des messages sur la deuxième connexion Internet, vous devez créer des enregistrements MX supplémentaires.

Si votre organisation Exchange Server a plusieurs points de contact avec Internet et plusieurs sites comportant des serveurs de transport Edge, cela n'assure pas la redondance pour les messages sortants. Les messages sont remis uniquement sur l'itinéraire le plus économique. Si les serveurs de transport Edge sur l'itinéraire le plus économique ne sont pas disponibles, les messages sont mis en file d'attente sur un serveur de boîtes aux lettres pour être remis au serveur de transport Edge. Les itinéraires de routage ne sont pas recalculés en fonction de la disponibilité.

Qu'est-ce que la résilience de site ?



La résilience de site est la capacité du système de messagerie à survivre à une défaillance de site et de continuer à fonctionner via l'utilisation d'un autre centre de données. Dans certains cas, l'autre centre de données est un site qui est dédié uniquement à la récupération d'urgence. Dans d'autres cas, l'autre centre de données peut être un autre site de société qui est en cours d'utilisation mais dispose d'une capacité suffisante pour gérer les services du site défectueux.

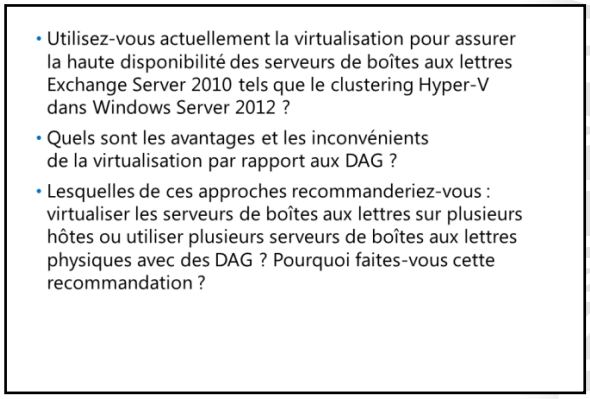
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Un DAG peut exister sur plusieurs sous-réseaux. Un DAG peut ainsi exister pour plusieurs sites Active Directory. Il s'agit d'une amélioration majeure comparée aux versions précédentes d'Exchange Server 2010, dans lesquelles vous deviez étendre un sous-réseau via une liaison WAN.

La résilience de site existe uniquement pour les serveurs de boîtes aux lettres. Tous les autres rôles serveur requis doivent déjà exister dans le site ou ils ne basculeront pas. Par exemple, les serveurs d'accès au client doivent déjà exister dans l'autre centre de données. D'autres services, par exemple DNS, les contrôleurs de domaine et les serveurs de catalogue global, doivent également être disponibles dans l'autre centre de données.

Discussion : Technologies de haute disponibilité de virtualisation comparées aux technologies de haute disponibilité Exchange pour les serveurs de boîtes aux lettres

présenter les technologies de haute disponibilité de virtualisation comparées aux technologies de haute disponibilité Exchange Server pour les serveurs de boîtes aux lettres. Menez la discussion à l'aide des questions suivantes :



- Utilisez-vous actuellement la virtualisation pour assurer la haute disponibilité des serveurs de boîtes aux lettres Exchange Server 2010 tels que le clustering Hyper-V® dans Windows Server® 2012 ?
- Quels sont les avantages et les inconvénients de la virtualisation par rapport aux DAG ?
- Lesquelles de ces approches recommanderiez-vous : virtualiser les serveurs de boîtes aux lettres sur plusieurs hôtes ou utiliser plusieurs serveurs de boîtes aux lettres physiques avec des DAG ? Pourquoi faites-vous cette recommandation ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2

Configuration de bases de données de boîtes aux lettres hautement disponibles

Historiquement, le rôle serveur de boîtes aux lettres a été le plus complexe et le composant critique dans le cadre du déploiement d'un serveur Exchange hautement disponible. Bien que cela reste vrai dans une certaine mesure, dans Exchange Server 2013 la complexité du déploiement d'un serveur de boîtes aux lettres hautement disponible est réduite. La configuration d'un DAG réduit également la probabilité que les administrateurs configureront incorrectement un cluster de serveurs de boîtes aux lettres.

Objectifs de la leçon

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

- planifier les composants logiciels et matériels pour les DAG ;
- décrire le gestionnaire Active Manager ;
- décrire la réplication continue ;
- décrire comment les groupes de disponibilité de base de données protègent les bases de données ;
- créer et configurer un DAG ;
- configurer les bases de données pour la haute disponibilité ;
- décrire des copies de base de données décalées ;
- décrire le processus de basculement ;
- décrire comment vous effectuez la surveillance et la gestion des DAG ;
- analyser l'intégrité de la réplication.

Qu'est-ce qu'un quorum ?

Le quorum maintient la logique pour qu'un cluster reconnaisse le nœud actif et les nœuds passifs. En outre, le quorum décide quel nœud passif sera activé si le nœud actif est défectueux. La configuration du quorum de cluster de basculement, telle qu'elle est utilisée par le DAG Exchange Server 2013, détermine le nombre de nœuds défectueux ou les composants de stockage et de réseau défectueux que le cluster peut supporter tout en continuant à fonctionner.

- Un quorum utilise le consensus des votants pour garantir que suffisamment de membres du cluster sont disponibles pour fournir des services
- Quorums de DAG Exchange Server 2013
  - Sont basés sur les votes dans Windows Server 2012
  - Permettent aux nœuds, partages de fichiers et disques partagés d'obtenir des votes selon le mode de quorum
  - Utilisent le nœud majoritaire avec un serveur témoin pour le quorum
    - Les DAG qui contiennent un nombre pair de serveurs de boîtes utilisent le serveur témoin
    - Les DAG qui contiennent un nombre impair de serveurs de boîtes utilisent le nœud majoritaire
- Vous pouvez avoir des nœuds non votants, si nécessaire

Un quorum empêche deux ensembles de nœuds de s'exécuter simultanément comme cluster de basculement. L'opération simultanée peut se produire lorsque des problèmes réseau empêchent un ensemble de nœuds de communiquer avec un autre ensemble de nœuds. Sans mécanisme de quorum, chaque ensemble de nœuds peut continuer à fonctionner en tant que cluster de basculement, ce qui génère une partition du cluster.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour éviter les problèmes provoqués par un fractionnement dans le cluster, les clusters de basculement utilisent un algorithme de vote afin de déterminer si le cluster a suffisamment de votes pour maintenir le quorum. Étant donné qu'un cluster donné a un jeu de nœuds et une configuration de quorum spécifiques, le cluster détermine le nombre de votes requis. Si le nombre de votes chute en dessous de la majorité, le cluster ne peut pas démarrer. Les nœuds continueront à écouter la présence d'autres nœuds, au cas où un autre nœud réapparaîtrait sur le réseau. Toutefois, un consensus doit être atteint pour que les nœuds fonctionnent sous forme de cluster.

Par exemple, si un cluster a cinq votes, il continue de fonctionner tant qu'au moins trois votes sont disponibles. Dans Exchange Server 2013, la source des votes peut être un nœud ou un partage de fichiers témoin. Lorsqu'une majorité de votes n'est pas disponible ou que seule la moitié des votes est disponible, le cluster ne démarre pas. En outre, lorsque la majorité de votes chute en dessous de la moitié des votes disponibles, Exchange Server 2013 démonte les bases de données.

Remarque : Exchange Server 2013 prend également en charge le placement d'un serveur témoin dans un autre site.

Configurations de quorum Windows Server 2012

Windows Server 2012 fournit quatre configurations de quorum : Nœud majoritaire, Nœud et partage de fichiers majoritaires, Nœud et disque majoritaires et Pas de majorité : Disque uniquement. Toutefois, Exchange Server 2013 ne prend en charge que Nœud et partage de fichiers majoritaires. Dans la configuration Nœud et partage de fichiers majoritaires, chaque nœud de cluster et un partage de fichiers désigné (également appelé serveur témoin dans Exchange Server 2013) peut voter. Le cluster fonctionne uniquement avec une majorité des votes. Ainsi, plus de la moitié des votes sont disponibles. Si un cluster actif perd la communication avec plus de la moitié de ses votes, il cesse de fonctionner.

Configuration des nœuds de cluster ne votant pas

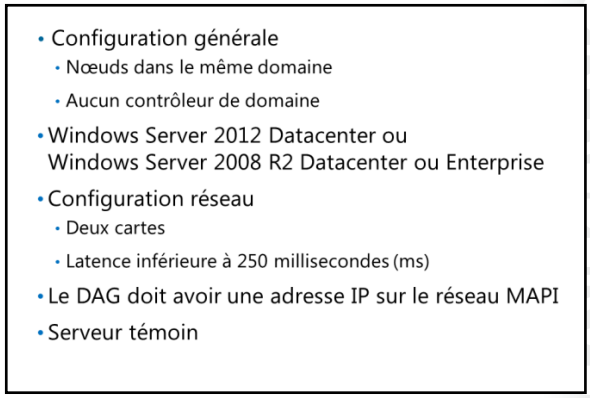
Dans Windows Server 2012, vous pouvez configurer les nœuds qui n'ont pas de vote dans le cluster pour maintenir un quorum. Vous pouvez configurer le Gestionnaire du cluster de basculement à l'aide de l'Assistant Configuration de quorum du cluster. Exchange Server 2013 prend en charge cette configuration. Toutefois, vous devez réfléchir soigneusement avant de l'utiliser.

Par exemple, examinons le scénario de résilience de site dans lequel des défaillances locales supplémentaires se produisent si le quorum est perdu. Ce scénario contient cinq membres de DAG, trois dans le site principal et deux dans le site de basculement. Si nécessaire, vous pouvez supprimer les votes des deux membres dans le site de basculement. Cette opération est possible car, si le site secondaire est défectueux, vous disposez toujours d'une défaillance supplémentaire dans votre site local avant que le cluster ne s'arrête si le quorum est perdu.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification des composants logiciels et matériels pour les groupes de disponibilité de base de données

Lorsque vous implémentez un DAG, vous devez vérifier que vous répondez à plusieurs exigences très spécifiques. Vous devez prendre en compte les exigences liées à la configuration générale, à la version du système d'exploitation, à la configuration réseau et à la configuration des DAG.



Configuration générale

Les conditions générales ci-dessous sont utilisées pour implémenter un DAG.

- Le DNS doit être implémenté avec un enregistrement d'hôte pour chaque serveur Exchange. Des mises à jour dynamiques sont préférées pour le DNS.
- Chaque serveur de boîtes aux lettres doit être un membre du même domaine. Il n'est pas possible d'avoir des serveurs de boîtes aux lettres dans différents domaines Active Directory comme membres du même DAG.
- Les serveurs de boîtes aux lettres membres d'un DAG ne peuvent pas être aussi des contrôleurs de domaine. Cette configuration n'est pas prise en charge.
- Le nom de l'ordinateur du serveur de boîtes aux lettres doit être unique et limité à 15 caractères.

Version du système d'exploitation

Tous les membres d'un DAG doivent fonctionner sur la même version de système d'exploitation. Tous les membres du DAG doivent exécuter Windows Server 2008 R2 ou Windows Server 2012. Vous ne pouvez pas combiner les deux versions de système d'exploitation dans le même DAG. La jonction avec le DAG échouera si vous tentez de joindre deux versions différentes du système d'exploitation.

Un DAG repose sur l'utilisation du clustering avec basculement dans Windows Server. Seules les versions Enterprise ou Datacenter de Microsoft® Windows Server 2008 R2 ou les versions Standard et Datacenter de Windows Server 2012 incluent le clustering avec basculement. Par conséquent, vous pouvez utiliser uniquement ces versions de système d'exploitation pour les membres de DAG.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration réseau

Les exigences ci-dessous sont liées à la configuration réseau.

- Une carte réseau est prise en charge mais il est recommandé d'utiliser deux cartes réseau. Cela permet de configurer un réseau MAPI (Messaging Application Programming Interface) et un réseau de réplication distinct.
- La latence entre les membres du DAG doit être inférieure à 500 millisecondes. Cette donnée est importante lorsque vous configurez un DAG avec des membres dans plusieurs emplacements physiques.
- Vous pouvez utiliser Internet Protocol version 6 (IPv6) uniquement si Internet Protocol version 4 (IPv4) est également configuré. Vous ne pouvez pas désactiver IPv4.
- l'Adressage Automatique d'IP Privée (APIPA) n'est pas pris en charge pour les membres du DAG.

Configuration de DAG

Outre les exigences de réseau physique et d'adressage IP pour les serveurs membres du DAG, le DAG lui-même a les exigences de configuration ci-dessous.

- Le DAG doit avoir au moins une adresse IP sur le réseau MAPI. Cette adresse peut être statique ou dynamique bien qu'une adresse IP statique soit utilisée dans la plupart des environnements.
- Si le DAG est développé sur plusieurs sous-réseaux, il doit avoir une adresse IP sur chaque sous-réseau.
- Le nom du DAG et le nom de chaque membre du DAG sont limités à 15 caractères ou moins et doivent être uniques.

Serveur témoin

Dans Windows Server 2012, le clustering avec basculement utilise le concept de quorum pour la prise de décision dans le cluster. Dans les clusters avec un disque partagé, la connectivité au disque partagé peut être utilisée pour définir les nœuds qui, potentiellement, doivent être actifs dans le cluster. Un DAG ne contient pas de disque central.

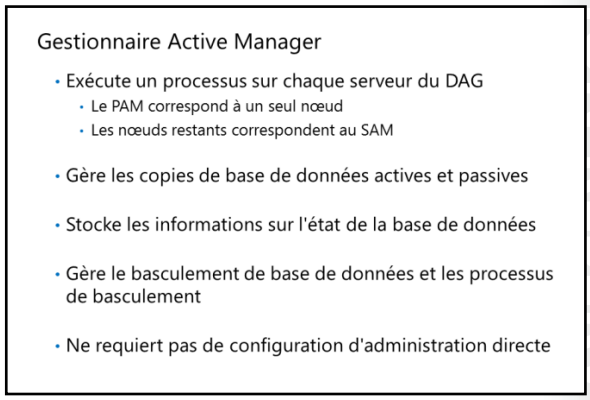
Un DAG nécessite l'utilisation d'un serveur témoin pour un nœud et un quorum de majorité de partage de fichiers. Le serveur témoin fonctionne comme membre supplémentaire du DAG pour atteindre le quorum. Toutefois, il est utilisé uniquement lorsque le DAG contient un numéro pair de membres. Le serveur témoin est un partage de fichiers situé sur un serveur qui n'est pas membre du DAG.

Le quorum correspondant à un DAG détermine les membres qui font partie des réplications ceux qui peuvent monter des bases de données. Par exemple, si un ordinateur d'un DAG perd la communication réseau, il n'appartient pas au quorum et ne peut pas monter de bases de données.

Nous vous recommandons de configurer le serveur témoin sur un serveur d'accès au client dans l'organisation Exchange Server. La charge supplémentaire sur le serveur est minimale et est déjà contrôlée par le groupe de gestion Exchange Server. Le serveur témoin n'a pas besoin d'exécuter la même version de Windows Server que les membres du DAG.

Si le serveur témoin du DAG n'est pas un serveur Exchange, vous devez ajouter le groupe de sous-système approuvé Exchange en tant que membre du groupe Administrateurs local sur le serveur témoin.

Qu'est-ce que le gestionnaire Active Manager ?



Pour gérer la réplication et l'activation de base de données de boîtes aux lettres, Exchange Server 2013 comprend un composant appelé Active Manager qui est exécuté comme une fonction du service de réplication Microsoft Exchange (MSExchangeRepl.exe). Le gestionnaire Active Manager remplace le modèle de la ressource et les fonctionnalités de gestion du basculement dans le clustering avec basculement Windows utilisés par Microsoft® Exchange Server 2003 et Exchange Server 2007. Pour simplifier l'architecture, le gestionnaire Active Manager s'exécute sur tous les serveurs de boîte aux lettres, même si le serveur ne fait pas partie d'un DAG.

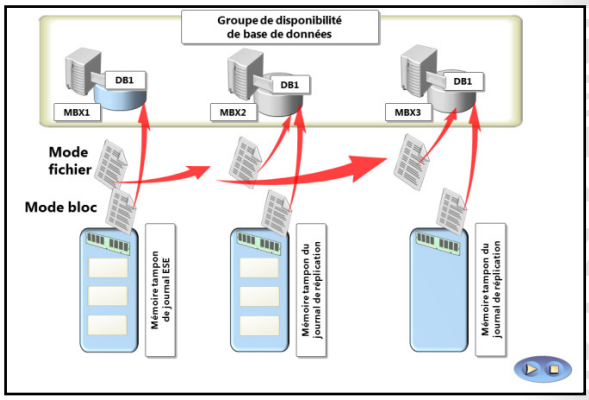
Le gestionnaire Active Manager fonctionne sur tous les membres du DAG en tant que gestionnaire Active Manager principal ou gestionnaire Active Manager de secours. Le gestionnaire Active Manager principal est le gestionnaire Active Manager du DAG qui contrôle les copies qui seront actives et celles qui seront passives. Il est chargé de traiter les notifications de modification de topologie et de réagir aux défaillances des serveurs. Le membre du DAG qui agit en tant que gestionnaire Active Manager principal est toujours le membre qui possède actuellement le groupe de clusters par défaut. Pour identifier le gestionnaire Active Manager principal, nous vous recommandons d'utiliser l'applet de commande **Get-DatabaseAvailabilityGroup <nom_DAG> -Status | Format-List Name, PrimaryActiveManager** plutôt que les outils de clustering avec basculement Windows. Si le serveur qui possède le groupe de clusters est défectueux, la fonction PAM se déplace automatiquement sur le serveur qui assume la propriété du groupe de clusters par défaut.

Le gestionnaire Active Manager de secours fonctionne comme un rôle actif et non passif. Elle fournit des informations sur le serveur qui héberge la copie active d'une base de données de boîtes aux lettres. Le gestionnaire Active Manager de secours détecte les défaillances de base de données locale et de banque d'informations Microsoft Exchange et y réagit en demandant que le gestionnaire Active Manager principal initie un basculement lorsqu'une copie est disponible. Un gestionnaire Active Manager de secours ne détermine pas de cible de basculement et ne met pas non plus à jour l'emplacement d'une base de données pour le gestionnaire Active Manager principal. Chaque gestionnaire Active Manager de secours accède à l'état de la copie de base de données active pour pouvoir rediriger les demandes de serveur d'accès au client. Le gestionnaire Active Manager principal exécute également les fonctions du rôle gestionnaire Active Manager de secours sur le système local.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que la réplication continue ?

La réplication continue a été introduite pour les serveurs de boîtes aux lettres dans Exchange Server 2007. Exchange Server 2010 a continué à utiliser la réplication continue. Depuis Exchange Server 2010 Service Pack 1 (SP1), la réplication continue comporte deux options plus disponibles : le mode fichier et le mode bloc de la réplication continue.



Réplication continue – mode Fichier

La réplication continue crée une copie de base de données passive sur un autre ordinateur Exchange Server du DAG, puis utilise l'envoi de journaux asynchrone pour gérer les copies. Le processus en mode Fichier de la réplication continue comprend les étapes indiquées ci-dessous.

1. Le rôle serveur de boîtes aux lettres avec la base de données active écrit le journal actif, puis le ferme.
2. Le service de réplication réplique le journal fermé sur les serveurs qui hébergent les bases de données passives.
3. Étant donné que toutes les copies de la base de données sont identiques, les journaux des transactions sont inspectés, puis sont relus ou appliqués aux copies de la base de données. Les bases de données demeurent synchronisées.

Dans l'amorçage Exchange Server 2013, vous n'êtes plus obligé d'utiliser la copie active comme source de l'amorçage. En outre, dans Exchange Server 2013, vous pouvez effectuer l'amorçage depuis les bases de données passives. Si une copie saine de la base de données est disponible sur un serveur, le serveur Exchange peut relire les journaux des transactions en les comparant à un jeu de données valide et commun. Vous pouvez amorcer les données avec les méthodes ci-dessous.

- Automatiquement.
- Manuellement, depuis les copies actives ou passives avec l'applet de commande **Update-MailboxDatabaseCopy**.
- Manuellement, en copiant les fichiers de base de données.

La réplication continue a lieu via des sockets TCP. Elle s'effectue comme indiqué ci-dessous.

1. Le nœud cible ou passif notifie à l'instance active les journaux de transactions qu'il attend.
2. La source répond ensuite avec les fichiers journaux des transactions demandés.
3. Une fois qu'Exchange Server 2013 a copié les fichiers journaux, il les place dans l'annuaire de l'inspecteur cible en vue de leur traitement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. L'inspection du journal vérifie que les données sont physiquement saines et inspecte l'en-tête. Si le journal réussit l'inspection, Exchange Server 2013 le place dans le répertoire des journaux cible. Si le journal ne réussit pas l'inspection, Exchange Server 2013 le demande auprès de la source jusqu'à trois fois avant d'échouer.
5. Une fois qu'Exchange Server 2013 a enregistré le journal des transactions dans le répertoire des journaux cible, la banque d'informations valide les journaux pour vérifier qu'ils sont valides, qu'aucun ne manque, et que la base de données en a besoin.

Réplication continue – mode Bloc

La réplication continue en mode Bloc a été introduite dans Exchange Server 2010 SP1. Le mode Bloc réduit l'exposition à la perte des données lors du basculement en répliquant la mémoire tampon de journal ESE (Extensible Storage Engine), qui écrit dans les copies passives de base de données parallèlement à leur écriture locale. Le mode Bloc devient actif automatiquement lorsque le mode Fichier de réplication continue est à jour avec les copies de base de données. Le processus du mode Bloc de la réplication continue se déroule comme indiqué ci-dessous.

1. Une fois en mode Bloc, tout bloc de données écrit dans la mémoire tampon de journal ESE sur le serveur Exchange qui héberge la base de données active est copié automatiquement dans la mémoire tampon de réplication, puis sur tous les serveurs qui hébergent les copies passives de la base de données active.
2. Lorsque la mémoire tampon de journal ESE est saturée, le bloc final est envoyé aux bases de données passives et un fichier journal transactionnel est écrit sur le serveur Exchange qui héberge la base de données active. La mémoire tampon de journal ESE est ensuite vidée.
3. Lorsque les serveurs Exchange hébergeant les bases de données passives reçoivent le bloc final qui remplit leur mémoire tampon de journal de réplication, ils enregistrent aussi la mémoire tampon dans un fichier journal des transactions avec la même séquence de génération du journal. Ensuite, la mémoire tampon est vidée et le processus démarre à nouveau.
4. Lorsque le serveur Exchange avec la base de données active connaît une défaillance mais que la mémoire tampon du journal de réplication n'est pas encore saturée, la mémoire tampon sur le serveur hébergeant la copie passive de la base de données est enregistrée dans un nouveau fichier journal transactionnel.

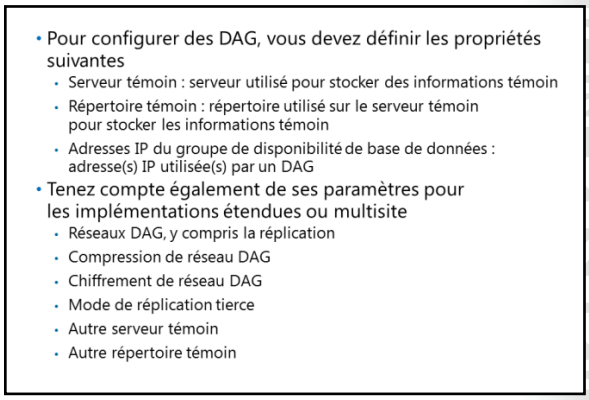
Le transport de réplication est identique que le mode Fichier soit activé ou désactivé. L'avantage du mode bloc est qu'il peut réduire les différences entre la copie active et la copie passive, tout en réduisant également les pertes de données possibles pendant un basculement et la durée d'une commutation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration d'un groupe de disponibilité de base de données

Pour configurer un DAG, vous devez comprendre les différents paramètres disponibles. Certains de ces paramètres, tels que l'adresse IP de DAG, sont requis pour chaque configuration. Vous pouvez prendre en compte d'autres paramètres, tels que les paramètres de compression de réseau, pour optimiser votre configuration DAG. Pour planifier vos DAG correctement, vous devez comprendre le rôle de chaque paramètre de configuration disponible afin de pouvoir décider si vous avez besoin de lui pour votre propre organisation Exchange.



Dans la console de gestion Exchange (EMC), les paramètres suivants sont disponibles :

- *Serveur témoin*. Le serveur que vous souhaitez utiliser comme serveur témoin. Il est recommandé d'utiliser un serveur d'accès au client situé à l'extérieur du DAG comme serveur témoin.
- *Répertoire témoin*. Le répertoire qui sera utilisé pour stocker les données témoin de partage de fichiers.
- *Autre serveur témoin*. Serveur que vous pouvez utiliser dans un autre centre de données que vous vous activerez lorsque le premier serveur témoin ne sera plus disponible.
- *Autre répertoire témoin*. Répertoire que vous utiliserez pour stocker les données témoin de partage de fichiers sur l'autre serveur témoin.
- *Adresses IP du groupe de disponibilité de base de données*. Un ou plusieurs adresses IP attribuées au DAG. Vous pouvez configurer ce paramètre en utilisant des adresses IP statiques ou en utilisant un serveur DHCP (Dynamic Host Configuration Protocol) pour obtenir une adresse IP automatiquement. Il s'agit du seul paramètre obligatoire en plus du nom du DAG, et vous devez donc configurer une adresse IP ou avoir un serveur DHCP disponible pour en extraire une. Si aucune adresse IP ne peut être extraite, le service de cluster du DAG ne démarrera pas.

Réseaux DAG

Un réseau DAG est une collection d'un ou de plusieurs sous-réseaux utilisés par le serveur Exchange pour le trafic de réplication ou MAPI. Bien que le serveur Exchange prenne en charge une carte et un chemin d'accès réseau, nous recommandons un minimum de deux réseaux DAG. Dans une configuration à deux réseaux, vous consacrez en général un réseau au trafic de réplication et l'autre au trafic MAPI.

Vous pouvez configurer la réplication dans le Centre d'administration Exchange.

Remarque : Si vous désactivez la réplication sur un réseau DAG pour le conserver pour le trafic MAPI, cela n'empêche pas automatiquement le trafic de réplication d'utiliser le réseau. Si aucun autre réseau n'est disponible, le trafic de réplication utilise automatiquement l'autre réseau DAG.

Lorsque vous implémentez un DAG sur plusieurs sites, vous devez configurer les réseaux DAG. Un DAG prend en charge plusieurs sous-réseaux sur le réseau MAPI et sur le réseau de réplication. Par conséquent, les sous-réseaux n'ont pas besoin de couvrir une liaison WAN.

Lorsque vous configurez le DAG multisite, vous devez réduire les réseaux qui sont énumérés automatiquement lorsque vous ajoutez des serveurs au DAG dans un réseau MAPI et un ou plusieurs réseaux de réplication. Toutefois, si vous configurez plusieurs réseaux, aucun routage ne peut être effectué entre le réseau MAPI et le réseau de réplication ou entre les réseaux de réplication.

Compression de réseau DAG

Les DAG intègrent une fonctionnalité de compression pour le trafic réseau. Elle est basée sur un algorithme appelé XPRESS, qui est l'implémentation Microsoft de l'algorithme LZ77. Pour configurer la compression de réseau DAG, les options suivantes sont utilisées :

- Disabled. Le trafic réseau n'est pas compressé.
- Enabled. La compression est utilisée pour la réplication et l'amorçage.
- InterSubnetOnly. Paramètre par défaut dans lequel la compression est utilisée uniquement lors de la réplication sur différents sous-réseaux dans le trafic de sous-réseau qui n'est pas compressé.
- SeedOnly. La compression est utilisée uniquement pour l'amorçage.

Vous pouvez configurer la compression de réseau DAG à l'aide de l'applet de commande suivante :

```
Set-DatabaseAvailabilityGroup <nom_DAG> - NetworkCompression <Option>
```

Chiffrement de réseau DAG

Vous pouvez configurer le chiffrement de communication de réseau DAG avec les différentes options suivantes :

- Disabled. le trafic réseau n'est pas chiffré ;
- Enabled. le trafic réseau pour la réplication et l'amorçage est toujours chiffré ;
- InterSubnetOnly. C'est le paramètre par défaut dans lequel le trafic réseau est chiffré en répliquant sur différents sous-réseaux dans le trafic de sous-réseau qui n'est pas chiffré.
- SeedOnly. Le trafic réseau est seulement chiffré pour l'amorçage.

Vous pouvez configurer le chiffrement de réseau DAG à l'aide de l'applet de commande suivante :

```
Set-DatabaseAvailabilityGroup <nom_DAG> - NetworkEncryption <Option>
```

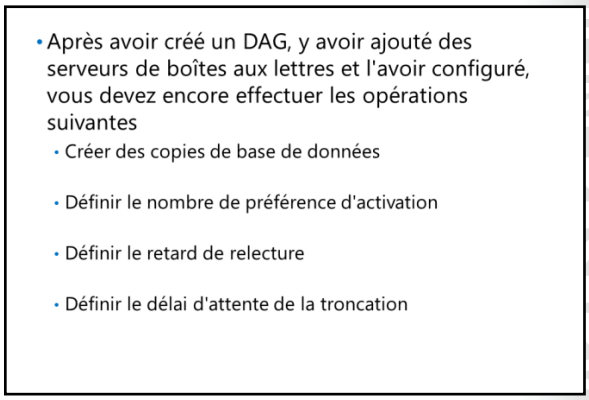
Mode de réplication tierce

Par défaut, un DAG est conçu pour utiliser la fonctionnalité de réplication continue intégrée pour répliquer les bases de données de boîtes aux lettres entre des serveurs du DAG. Si votre organisation utilise une solution de réplication de données tierce qui prend en charge l'API de réplication tierce dans Exchange Server 2013, vous pouvez également configurer le DAG pour qu'il utilise votre solution tierce au lieu de la fonctionnalité de réplication intégrée. Vous utilisez l'applet de commande **New-DatabaseAvailabilityGroup** pour configurer le DAG pour qu'il utilise une solution de réplication tierce. Elle peut uniquement être désactivée en supprimant et recréant le DAG.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration des bases de données pour la haute disponibilité

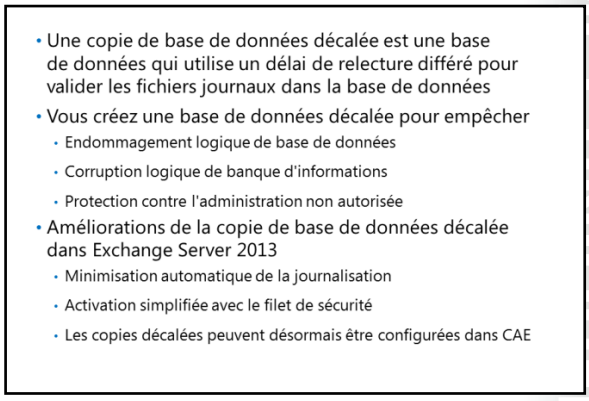


La création d'un DAG est uniquement la première étape permettant d'assurer la disponibilité de la base de données. Vous devez créer et configurer des copies supplémentaires de la base de données. Vous pouvez non seulement créer une copie de la base de données initialement, mais un administrateur peut également en créer une à tout moment. Vous pouvez répartir les copies de la base de données entre plusieurs serveurs de boîtes aux lettres de façon souple et sélective. Vous pouvez répliquer une, plusieurs ou toutes les bases de données de boîtes aux lettres sur un serveur de plusieurs façons.

Vous devez spécifier les informations ci-dessous lors de la création d'une copie de la base de données de boîtes aux lettres.

- Le nom de la base de données que vous copiez.
- Le nom du serveur de boîtes aux lettres qui hébergera la copie de la base de données.
- Un nombre de préférence d'activation. Il s'agit du numéro de séquence de la liste préférée qui représente l'ordre de préférence d'activation d'une copie de base de données après un échec ou une défaillance de la copie active.
- La durée (en minutes) du délai de relecture du journal. Il s'agit du délai de relecture qui spécifie le temps d'attente avant la validation des journaux dans la copie de la base de données. La définition de la valeur pour le délai d'attente de relecture sur 0 désactive le délai de relecture du journal.
- La durée (en minutes) du délai de troncation du journal. Il s'agit du délai d'attente de la troncation, qui spécifie le délai d'attente avant la troncation des journaux des transactions validés. La définition de la valeur pour le délai d'attente de transaction sur 0 désactive le délai de troncation du journal.

Que sont les copies de base de données décalées ?



Une copie de base de données de boîtes aux lettres décalée est une base de données qui utilise un délai de relecture différé pour valider les fichiers journaux dans la base de données. Cela vous permet de revenir à un moment donné (un maximum de 14 jours). En retardant la relecture les journaux dans une base de données, vous pouvez la récupérer à un point dans le passé.

Les copies de base de données décalées peuvent vous protéger contre des types de cas d'endommagement logique rares, notamment :

Endommagement logique de base de données

Il se produit lorsque la somme de contrôle des pages de base de données concorde mais que les données des pages sont logiquement incorrectes. Il peut se produire lorsque l'ESE tente d'écrire une page de base de données et que la pile de stockage du système d'exploitation annonce une réussite bien que les données ne soient jamais créées sur le disque ou soient écrites au mauvais endroit. Ce comportement est appelé vidage perdu. Pour éviter les vidages perdus, ESE inclut un mécanisme de détection de vidage perdu dans la base de données avec la fonctionnalité de restauration de page unique.

Corruption logique de banque d'informations

Ceci indique que des données sont ajoutées, supprimées ou modifiées de manière non acceptée par l'utilisateur et que celui-ci considère cela comme un endommagement. En général, cela provient d'une application tierce qui envoie une série d'opérations MAPI valides contre la banque d'informations. Citons par exemple une solution d'archivage endommagée qui modifie tous les éléments de message d'un utilisateur. La récupération d'élément unique ou la période de rétention fournit une protection contre ce cas, car tous les éléments modifiés sont conservés et peuvent donc être restaurés. Toutefois, en particulier lorsqu'un grand volume de données est modifié, il peut s'avérer plus facile de récupérer la base de données à un point dans le passé avant l'apparition de l'endommagement.

Protection contre l'administration non autorisée

Ceci indique que l'organisation cherche à se protéger contre des administrateurs malveillants ou non autorisés. Elle permet de se protéger principalement des administrateurs qui ajoute, modifie ou supprime intentionnellement des données du système d'une façon non appréciée des utilisateurs. Pour protéger contre cela, les copies de base de données décalées peuvent être placées sur un serveur sous contrôle administratif distinct. Les copies de base de données décalées ont été améliorées dans Exchange Server 2013 de la façon suivante :

- *Minimisation automatique de la journalisation.* Les copies décalées peuvent désormais implémenter leurs fichiers journaux dans une certaine mesure à l'aide de la minimisation automatique de la journalisation. Lorsque cette fonction est activée, les copies décalées minimisent automatiquement les fichiers journaux dans diverses situations, telles que les scénarios de mise à jour corrective de pages et d'espace disque faible. Si le système détecte que la mise à jour corrective de page est requise pour une copie décalée, les journaux reliront automatiquement dans la copie décalée pour effectuer la mise à jour corrective de page. Les copies décalées appellent également cette fonctionnalité de relecture automatique lorsqu'un seuil d'espace disque faible a été atteint et que la copie décalée a été détectée comme étant la seule copie disponible pour une période de temps spécifique. Vous pouvez activer la minimisation automatique de la journalisation pour vos bases de données décalées à l'aide de l'applet de commande suivante : **Set-DatabaseAvailabilityGroup <nom_DAG> – ReplayLagManagerEnabled $True**.
- *Activation simplifiée avec le filet de sécurité.* Les copies décalées utilisent le filet de sécurité, ce qui facilite beaucoup la récupération ou l'activation. Pour plus d'informations sur le filet de sécurité, consultez la rubrique « Comprendre le fonctionnement de la haute disponibilité de transport » plus haut dans ce module.

Vous pouvez configurer une base de données décalée dans le Centre d'administration Exchange ou dans l'environnement de ligne de commande Exchange Management Shell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Comment créer et configurer un groupe de disponibilité de base de données

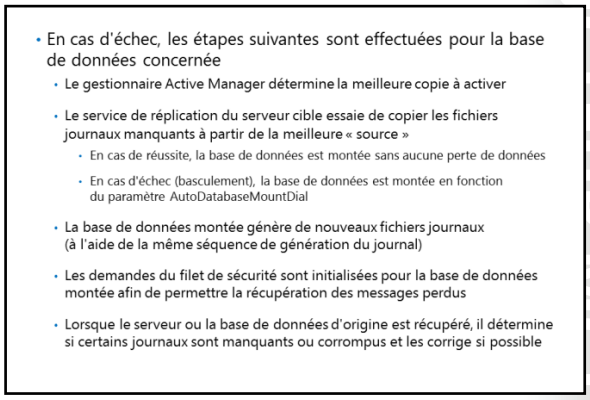
Dans cette démonstration, procédez comme il est indiqué ci-dessous.

- Préconfigurez l'objet de réseau de cluster pour un groupe de disponibilité de base de données (DAG).
- Créez un DAG.
- Ajoutez des membres à un DAG.
- Ajoutez une copie de base de données de boîtes aux lettres pour la « base de données de boîtes aux lettres 1 ».

Procédure de démonstration

1. Sur l'ordinateur LON-DC1, dans Utilisateurs et ordinateurs Active Directory, créez un objet ordinateur nommé **DAG1** et attribuez l'autorisation **Contrôle total au groupe de sous-système** approuvé Exchange et au compte d'ordinateur **LON-MBX1 (ADATUM\LON-MBX1$)**.
2. Basculez vers l'ordinateur LON-CAS1, puis ouvrez **Internet Explorer** et accédez au Centre d'administration Exchange. Créez un groupe de disponibilité de base de données nommé **DAG1**.
3. Ajoutez **LON-MBX1** et **LON-MBX2** à DAG1.
4. Ajoutez une copie de base de données sur LON-MBX2 pour la base de données de boîtes aux lettres 1.

Présentation du processus de basculement



Un basculement se produit lorsque le service à la copie de base de données active existante est compromis d'une façon ou d'une autre. Cette situation peut se produire lorsque le serveur qui héberge la base de données active est hors connexion, que quelque chose provoque le démontage de la base de données active ou que le serveur perd la connectivité réseau. Une commutation se produit lorsqu'un administrateur déplace manuellement la base de données active d'un serveur à un autre. La principale différence entre le processus de basculement et le processus de commutation est que le processus de basculement se produit automatiquement lorsque le service échoue, alors que la commutation est un processus manuel.

Pendant une commutation, vous pouvez choisir la base de données qui sera montée ou laissez le Gestionnaire Active Manager choisir la meilleure copie à monter. Lors d'un basculement, le gestionnaire Active Manager prend cette décision.

Lorsqu'un échec qui affecte la base de données active se produit, le gestionnaire Active Manager utilise plusieurs jeux de critères de sélection pour déterminer quelle copie de la base de données doit être activée. Dans Exchange Server 2013, ce processus est appelé BCSS (Best Copy and Server Selection). Le Gestionnaire Active Manager effectue les opérations ci-dessous lorsqu'il choisit la meilleure copie.

- Il crée une liste de copies de base de données qui sont des candidats potentiels pour l'activation.
- Il ignore et supprime de la liste toutes les copies de base de données qui sont inaccessibles ou sont empêchées administrativement d'être activées.
- Il trie la liste obtenue en utilisant la longueur de la file d'attente de copie comme clé primaire. Si les serveurs sont configurés avec une valeur de numérotation de montage de base de données automatique *Lossless*, le gestionnaire Active Manager trie la liste obtenue dans l'ordre croissant en utilisant la valeur ActivationPreference comme clé primaire.
- Il tente de localiser une copie de base de données de boîtes aux lettres dans la liste dont l'état est Healthy, DisconnectedAndHealthy, DisconnectedAndResynchronizing ou SeedingSource, puis évalue le potentiel d'activation de chaque copie à l'aide d'un ordre défini des critères. Ces critères comprennent diverses combinaisons de paramètres tels que l'état d'indexation du contenu, la longueur de la file d'attente et la longueur de la file d'attente de relecture. Les nouveautés intégrées à Exchange Server 2013 sont les critères supplémentaires qui mesurent l'intégrité de la pile complète de protocoles et prennent aussi en compte l'intégrité des protocoles prioritaires définie dans la sélection.
- *Basculements de base de données*. Lorsqu'une défaillance de base de données de boîtes aux lettres hautement disponible se produit, le PAM tente d'exécuter un basculement de la base de données. Avant de tenter de choisir une copie adaptée à activer, le processus ACLLs (Attempt Copy Last Logs) est exécuté. ACLL crée des RPC (Remote Procedure Calls) sur le serveur qui a hébergé la copie active de la base de données de boîtes aux lettres qui est activée. Les RPC demandent confirmation que les serveurs sont disponibles et sains et déterminent alors la valeur LogInspectorGeneration pour la copie de base de données. La dernière copie de base de données de boîtes aux lettres active est utilisée pour copier tous les fichiers journaux manquants dans la copie sélectionnée par le Gestionnaire Active Manager pour être activée.
- Une fois le processus ACLL terminé, la valeur AutoDatabaseMountDial configurée est consultée. La valeur AutoDatabaseMountDial a les trois paramètres potentiels suivants :
    - *BestAvailability*. Cette valeur permet à la base de données d'être montée automatiquement si la longueur de la file d'attente de copie, soit le nombre de journaux qui n'ont pas été répliqués sur le serveur de boîtes aux lettres cible, est inférieur ou égal à 12. Lorsque le Gestionnaire Active Manager identifie le serveur cible, Exchange Server 2013 tente de répliquer les journaux restants dans les copies passives et de monter la base de données. Il s'agit de la valeur par défaut.
    - *GoodAvailability*. Cette valeur permet à la base de données d'être montée automatiquement immédiatement après un basculement si la longueur de la file d'attente de copie est inférieure ou égale à 6. Lorsque le Gestionnaire Active Manager identifie le serveur cible, Exchange Server 2013 tente de répliquer les journaux restants dans la copie passive et de monter la base de données.
    - *Lossless*. Cette valeur ne permet pas à une base de données d'être montée automatiquement tant que tous les journaux générés sur la copie active n'ont pas été copiés dans la copie passive.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

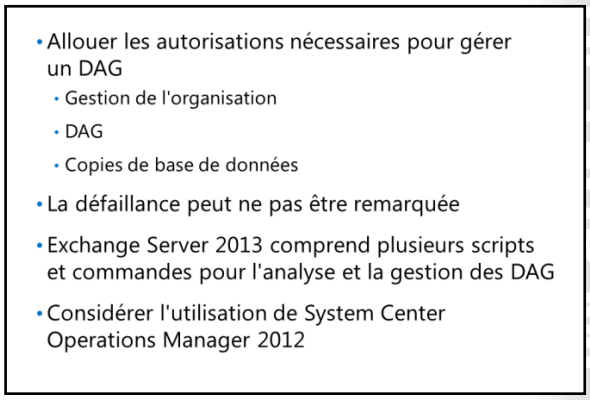
Si le nombre de journaux perdus est compris dans les limites de la valeur AutoDatabaseMountDial configurée, le gestionnaire Active Manager actif émet une demande de montage pour la banque d'informations. Si le nombre de journaux perdus n'est pas compris dans les limites de la valeur AutoDatabaseMountDial configurée, Exchange Server 2013 évalue la copie de base de données de boîtes aux lettres suivante dans la liste triée et répète l'évaluation. Si aucune base de données ne répond au paramètre AutoDatabaseMountDial configuré, un administrateur doit monter manuellement la base de données et accepter que la perte de données soit supérieure au paramètre AutoDatabaseMountDial. Vous utilisez l'applet de commande **Set-MailboxServer** pour configurer le paramètre AutoDatabaseMountDial pour tous les nœuds du DAG.

Il peut paraître illogique de répertorier le paramètre BestAvailability comme autorisant 12 journaux de transactions manquants et le paramètre GoodAvailability seulement 6. Dans ce cas, toutefois, la disponibilité fait référence à la base de données qui est montée et disponible et non à la possibilité de perdre des données. Dans la plupart des cas, la perte de données est moins acceptable que la perte de service. Vous devez décider si la base de données doit rester disponible en autorisant son montage malgré la perte de données potentielle de données ou de la laisser indisponible et d'attendre la récupération manuelle des fichiers journaux manquants.

Le Gestionnaire Active Manager se comporte différemment lorsque vous configurez un paramètre sans perte. Dans ce cas, il trie la liste obtenue dans l'ordre croissant en utilisant la valeur ActivationPreference comme clé primaire. Si vous utilisez une valeur différente de Lossless pour le paramètre AutoDatabaseMountDial, le Gestionnaire Active Manager effectue le tri en utilisant la longueur de la file d'attente de copie.

Planification, analyse et gestion d'un groupe de disponibilité de base de données

Dans les grandes organisations, la gestion du DAG est susceptible d'être limité à un groupe d'administrateurs relativement restreint. Ce groupe comprend tous les paramètres de conception qui doivent être pris en compte lors de la création et de la gestion des DAG et des copies de base de données. Vous pouvez déléguer ces autorisations à l'aide du RBAC (Role-Based Access Control). Le RBAC est le modèle d'autorisation pour Exchange Server 2013 et est expliqué plus en détail dans le module 10.



Pour créer et gérer des DAG, vous devez appartenir au groupe de rôles Gestion de l'organisation ou au rôle de gestion Groupes de disponibilité de base de données. Pour créer et gérer des copies de base de données, vous devez appartenir au groupe de rôles Gestion de l'organisation ou au rôle de gestion de copies de base de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Analyse

Un défi propre à la gestion des DAG est que, dans un système bien conçu, vous pouvez ne pas remarquer le basculement d'une base de données d'un membre du DAG à un autre. Une méthode dont vous disposez pour analyser les membres d'un DAG est d'utiliser Microsoft® System Center Operations Manager 2012 (SCOM). SCOM 2012 analyse proactivement les serveurs et peut informer les administrateurs lorsque des erreurs et des événements se produisent.

Exchange Server 2013 comporte les options suivantes pour analyser l'état d'un DAG :

- *CheckDatabaseRedundancy.ps1*. Ce script vérifie la redondance des bases de données répliquées et génère des événements si la tolérance de base de données se trouve dans un état compromis.
- *Get-MailboxDatabaseCopyStatus*. Utilisez cette applet de commande pour afficher les informations d'état d'une copie spécifique de base de données de boîtes aux lettres ou de toutes les copies d'une base de données de boîtes aux lettres sur un serveur ou dans l'organisation.
- *Test-ReplicationHealth*. Utilisez cette applet de commande pour réaliser divers tests et présenter un rapport pour différents composants de réplication.
- *CollectOverMetrics.ps1*. Ce script collecte les statistiques et informations sur les commutations et les basculements. Les données enregistrées dépendent des événements passés. Ce script inclut des mesures pour la réplication continue en mode bloc et plus de détails provenant du pipeline de réplication et de relecture. Il comporte également la création de rapports améliorée.
- *CollectReplicationMetrics.ps1*. Pendant son exécution ce script collecte des statistiques sur la réplication en temps réel.
- *Journaux d'événements*. Outre les événements contenus dans les journaux Windows, il existe également des journaux d'événements propres à Exchange Server situés dans le nœud Applications et services. Les deux journaux spécifiques qui intéressent la haute disponibilité sont les journaux HighAvailability et MailboxDatabaseFailureItems.

Exchange Server 2013 fournit les applets de commande suivantes pour la maintenance du serveur :

- **Get-ServerComponentState**. Cette applet de commande affiche tous les composants d'un serveur Exchange et l'état actuel de chaque composant.
- **Set-ServerComponentState**. Cette applet de commande effectue des commutations de serveur et met les serveurs de boîtes aux lettres hors connexion ou en ligne.

 **Remarque :** Pour obtenir des exemples sur la façon d'utiliser les outils d'analyse inclus dans Exchange Server 2013, consultez Analyse de la haute disponibilité et de la résilience de site dans le fichier d'aide d'Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Comment analyser l'intégrité de la réplication

Décrivez l'utilisation de la console de gestion Exchange et de l'environnement de ligne de commande Exchange Management Shell pour consulter les informations disponibles sur l'intégrité de la réplication de la base de données.

Au cours de cette démonstration, indiquez comment afficher le statut de la santé des copies de la base de données dans le Centre d'administration Exchange ou l'environnement de ligne de commande Exchange Management Shell.

Procédure de démonstration

1. Sur LON-CAS1, dans le Centre d'administration Exchange, montrez le volet d'informations de la base de données de boîtes aux lettres 1.
2. Ouvrez l'environnement de ligne de commande Exchange Management Shell et exécutez les applets de commande suivantes :
   - **Test-ReplicationHealth**
   - **Get-MailboxDatabaseCopyStatus –Server LON-MBX1**
3. Exécutez le script suivant :
   - **CheckDatabaseRedundancy.ps1 –MailboxDatabaseName "Base de données de boîtes aux lettres 1"**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Configuration des serveurs d'accès au client hautement disponibles

Lorsque vous prenez en considération la haute disponibilité avec Exchange Server 2013 en plus de vous concentrer sur les serveurs de boîtes aux lettres, les copies de base de données ou les groupes de disponibilité de base de données (DAG), vous devez aussi vérifier que les serveurs d'accès au client sont hautement disponibles pour vous permettre d'atteindre vos niveaux de service requis.

Objectifs de la leçon

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

- planifier les composants logiciels et matériels pour les serveurs d'accès au client hautement disponibles ;
- décrire l'équilibrage de la charge réseau (NLB) ;
- examiner les options d'implémentation de la haute disponibilité pour les serveurs d'accès au client ;
- configurer les options pour les serveurs d'accès au client hautement disponibles.

Planification des composants logiciels et matériels pour les serveurs d'accès au client hautement disponibles

Tous les clients utilisent des serveurs d'accès au client pour accéder à leurs boîtes aux lettres. Si un serveur d'accès au client est pas disponible dans un site Active Directory, les utilisateurs peuvent accéder à un serveur d'accès au client dans un autre site.

- Serveurs d'accès au client utilisés par tous les clients
- Implémenter l'équilibrage de charge pour les serveurs d'accès au client
- Les sites servant de proxy sont très importants
- Le même certificat SSL est utilisé sur tous les nœuds
- Penser aux connexions Internet redondantes pour les utilisateurs externes

Si les utilisateurs d'Internet se connectent à des serveurs d'accès au client dans un site Active Directory principal unique et que les demandes sont transmises par proxy à d'autres sites Active Directory, la défaillance des serveurs d'accès au client dans les sites principaux empêche l'accès à ces sites en proxy. Par conséquent, la haute disponibilité devient essentielle pour le site principal qui transmet les demandes par proxy.

Pour activer la haute disponibilité pour les serveurs d'accès au client, vous devez commencer par déployer plusieurs serveurs d'accès au client. Ensuite, vous devez configurer l'équilibrage de la charge réseau basé sur le matériel ou sur le logiciel (par exemple la fonctionnalité d'équilibrage de la charge réseau de Windows Server 2012). Vous pouvez également créer plusieurs enregistrements dans DNS pour vos serveurs d'accès au client et configurer un tourniquet DNS. Le tourniquet DNS vous permet de distribuer les connexions réseau sur les différents serveurs d'accès au client mais il n'assure pas l'équilibrage de charge ou le basculement automatique.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

L'équilibrage de charge répartit les demandes des clients entre les serveurs d'accès au client. Si un serveur d'accès au client devient indisponible, les demandes sont traitées par les serveurs d'accès au client restants.

Tous les serveurs d'accès au client doivent être configurés avec le même certificat numérique Secure Sockets Layer (SSL). Cela provient du fait que tous les serveurs d'accès au client utilisent le nom spécifié dans le tableau de serveur d'accès au client.

Utilisateurs Internet

Pour les utilisateurs Internet, vous devez tenir compte des connexions Internet redondantes dans votre conception. Vous pouvez avoir deux fournisseurs de services Internet (ISP) distincts et autoriser l'accès aux serveurs d'accès au client de votre organisation via ces deux fournisseurs de services Internet. Si un fournisseur de services Internet rencontre une défaillance, les utilisateurs peuvent accéder au contenu de leurs boîtes aux lettres en utilisant l'autre fournisseur de services Internet à un nom de domaine différent.

Sinon, si vous configurez chaque site Active Directory pour qu'il soit disponible directement à partir d'Internet, la défaillance d'une seule connexion Internet affecte la connectivité à un seul site Active Directory. Cela atténue les dommages provoqués par une défaillance mais n'assure pas une redondance complète.

Qu'est-ce que l'équilibrage de la charge réseau ?

L'équilibrage de la charge réseau améliore la disponibilité et l'évolutivité des applications serveur comme celles qui sont utilisées sur le serveur Web, le FTP (File Transfer Protocol), le pare-feu, le proxy, le réseau privé virtuel (VPN) et d'autres serveurs.

- L'équilibrage de la charge réseau assure une disponibilité et une évolutivité élevées pour les applications de serveur en général basées sur le Web
- NLB permet d'accéder à deux serveurs ou plus via une seule adresse IP
- NLB requiert que tous les serveurs du cluster NLB exécutent les mêmes applications de serveur avec la même configuration
- Les demandes clientes sont distribuées entre tous les serveurs disponibles du cluster NLB, selon un algorithme commun
- Tous les serveurs s'analysent mutuellement via des messages de pulsation
- Si un serveur n'envoie pas de messages de pulsation pendant cinq secondes, les autres serveurs convergent automatiquement et redistribuent les connexions clientes entre les serveurs disponibles

Un seul ordinateur exécutant Windows Server peut fournir un niveau limité de fiabilité et d'évolutivité de serveur. Avec l'équilibrage de la charge réseau, vous pouvez regrouper jusqu'à 32 ordinateurs hôtes dans un cluster NLB pour assurer l'équilibrage de charge et la redondance. Étant donné qu'un serveur appartenant à un cluster NLB peut répondre à une demande de client, les fichiers d'application et les données doivent être identiques sur tous les serveurs.

Sachez que les hôtes d'un cluster NLB ne partagent pas de données. Habituellement, cela signifie que vous utilisez un serveur principal distinct pour stocker les données ou pour autoriser la synchronisation des données sur les serveurs Web. Toutefois, cette spécification limite les applications adaptées à l'équilibrage de la charge. Parfois, ces applications sont appelées « sans état ».

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Avantages principaux de l'équilibrage de la charge réseau (NLB)

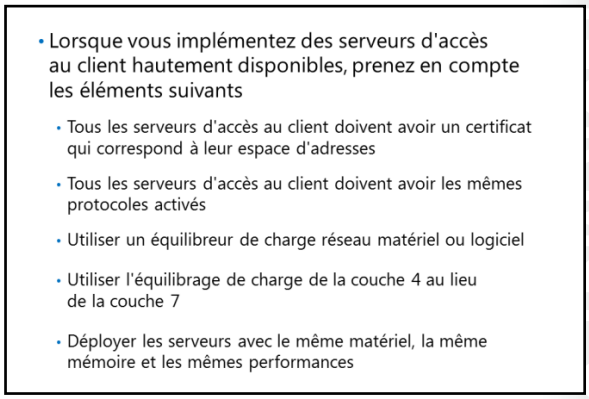
Les hôtes NLB d'un cluster communiquent parmi les autres hôtes pour offrir les avantages principaux ci-dessous.

- Évolutivité. Le NLB vous permet de faire évoluer les services réseau pour répondre aux besoins des clients. Vous pouvez ajouter de nouveaux serveurs à un cluster d'équilibrage de la charge réseau sans réécrire les applications ou reconfigurer les clients. Il n'est pas nécessaire de mettre hors connexion le cluster d'équilibrage de la charge pour ajouter de nouvelles capacités et les membres du cluster d'équilibrage de charge n'ont pas besoin d'être basés sur un matériel identique.
- Disponibilité élevée. La NLB assure un niveau élevé de disponibilité en redirigeant le trafic réseau entrant vers des hôtes du cluster actif, en cas de défaillance ou de mise hors connexion d'un hôte. Les connexions existantes à un hôte hors connexion sont interrompues, mais les services Internet restent disponibles. En général, par exemple avec les serveurs Web, les logiciels clients tentent automatiquement de rétablir la connexion qui a échoué et les clients subissent un délai de réponse de quelques secondes seulement. De nombreuses applications fonctionnent avec NLB. En général, NLB peut équilibrer la charge d'une application ou d'un service utilisant le protocole réseau TCP/IP (Transmission Control Protocol/Internet Protocol) comme protocole réseau et associé à un port TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol) spécifique.
- Performances. NLB prend en charge l'extension des performances d'un serveur en répartissant le trafic réseau entrant sur une ou plusieurs adresses IP virtuelles attribuées au cluster NLB. Les hôtes du cluster répondent simultanément aux demandes des différents clients, voire aux différentes demandes du même client. Par exemple, un navigateur Web peut obtenir chacune des images d'une page Web unique depuis différents hôtes d'un cluster NLB. Ce système accélère le traitement et raccourcit le temps de réponse aux clients.

Éléments à prendre en compte pour implémenter des serveurs d'accès au client hautement disponibles

Les éléments ci-dessous doivent être pris en compte lorsque vous implémentez des serveurs d'accès au client hautement disponibles :

- La gestion des certificats numériques est effectuée par le serveur d'accès au client. Tous les certificats numériques doivent correspondre à vos espaces de noms.
- Sachez quels protocoles doivent être gérés par vos serveurs d'accès au client. Il importe d'activer les protocoles suivants sur tous les serveurs d'accès au client :
    - Exchange ActiveSync
    - POP3
    - IMAP4
    - EWS
    - Outlook Anywhere



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Utilisez un programme d'équilibrage de charge réseau matériel ou logiciel pour obtenir une configuration haute disponibilité service qui prend en charge les services.
- Vous pouvez configurer les équilibrages de charge pour utiliser l'équilibrage de charge de la couche 4 ou 7. Lorsque vous utilisez l'équilibrage de la charge de la couche 7 et l'affinité de session, toutes les demandes entre le client et le serveur sont envoyés vers le même serveur de boîtes aux lettres. Lorsque vous utilisez l'équilibrage de la charge de la couche 4, les demandes sont distribuées sur la couche de transport. Exchange Server 2013 ne nécessite pas l'affinité de session. L'équilibrage de charge de la couche 4 sans affinité de session vous permet d'augmenter la capacité et l'utilisation de l'équilibreur de charge car le traitement n'est pas utilisé pour conserver des options d'affinité plus impliquées, telles que l'équilibrage de charge par connexion IP.
- Tentez toujours de déployer les serveurs d'accès au client avec du matériel, une mémoire et des performances similaires, afin de comprendre lorsqu'un système provoque des problèmes.

Démonstration : Configuration des options des serveurs d'accès au client hautement disponibles

Dans cette démonstration, vous allez apprendre à configurer un tourniquet DNS pour les deux serveurs d'accès au client, LON-CAS1 et LON-CAS2.

Procédure de démonstration

1. Sur l'ordinateur LON-DC1, ouvrez le **Gestionnaire DNS**.
2. Créez un nouvel hôte nommé **webmail.adatum.com** et ajoutez les adresses IP **172.16.0.21**.
3. Créez un nouvel hôte nommé **webmail.adatum.com** et ajoutez les adresses IP **172.16.0.22**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation de la haute disponibilité

Scénario

Vous êtes l'administrateur de messagerie de la société A. Datum Corporation. Vous avez terminé l'installation de base de quatre serveurs Exchange Server 2013. Vous devez maintenant terminer la configuration de façon à les rendre hautement disponibles. Pour cela, il est en général nécessaire de configurer vos bases de données de boîtes aux lettres ainsi que vos serveurs d'accès au client pour qu'ils soient hautement disponibles et de tester si le basculement automatique fonctionne.

Objectifs

Les stagiaires pourront implémenter la haute disponibilité dans l'environnement Exchange Server 2013.

Configuration de l'atelier pratique

Durée approximative : **90 minutes**

Ordinateurs virtuels	22341B-LON-DC1 22341B-LON-CAS1 22341B-LON-CAS2 22341B-LON-MBX1 22341B-LON-MBX2
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22341B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Vous devez à présent déplacer l'objet de sous-réseau actuellement associé au site de Swindon vers le site de Londres avant de démarrer les serveurs Exchange Server :
   a. Sur LON-DC1, cliquez sur **Gestionnaire de serveur**.
   b. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
   c. Dans **Sites et services Active Directory**, développez **Sites** si nécessaire, puis cliquez sur **Subnets**.
   d. Cliquez avec le bouton droit sur **172.16.0.128/25**, puis cliquez sur **Propriétés**.
   e. Dans la boîte de dialogue **Propriétés de : 172.16.0.128/25**, dans la liste **Site**, cliquez sur **London**, puis sur **OK**.
   f. Fermez **Sites et services Active Directory**.
   g. Fermez le **Gestionnaire de serveur**.
6. Répétez les étapes 2 à 4 pour les ordinateurs **22341B-LON-MBX1**, **22341B-LON-MBX2**, **22341B-LON-CAS1** et **22341B-LON-CAS2**.

Exercice 1 : Création et configuration d'un groupe de disponibilité de base de données

Scénario

Pour exécuter la configuration haute disponibilité des serveurs de boîtes aux lettres, créez un groupe de disponibilité de base de données et rendez la base de données de boîtes aux lettres 1 hautement disponible.

Les tâches principales de cet exercice sont les suivantes :

1. Préconfigurer l'objet de réseau de cluster pour un DAG.
2. Créer un DAG et y ajouter les serveurs de boîtes aux lettres.
3. Créer une copie de base de données de boîtes aux lettres.
4. Vérifier la réussite de la copie d'une base de données.
5. Interrompre et reprendre une copie de base de données.

▶ Tâche 1 : Préconfigurer l'objet de réseau de cluster pour un DAG

1. Sur LON-DC1, dans le Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Dans **Utilisateurs et ordinateurs Active Directory**, activez les **Fonctionnalités avancées**.
3. Dans le volet gauche, développez **Adatum.com** et créez un objet ordinateur nommé **DAG1** dans le conteneur **Computers**.
4. Modifiez les paramètres de sécurité de DAG1 comme indiqué ci-dessous.
   - Groupe Sous-système approuvé Exchange : **Autoriser Contrôle total**
   - LON-MBX1 (ADATUM\LON-MBX1$) : **Autoriser Contrôle total**
5. Désactivez le compte d'ordinateur **DAG1**.

▶ Tâche 2 : Créer un DAG et y ajouter les serveurs de boîtes aux lettres

1. Basculez vers LON-CAS1. Ouvrez Internet Explorer, tapez **https://lon-cas1.adatum.com/ecp**, et connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Centre d'administration Exchange, créez un groupe de disponibilité de base de données avec les paramètres suivants :
   - Nom du groupe de disponibilité de la base de données : **DAG1**
   - Serveur témoin : **LON-CAS1**
   - Répertoire témoin :. **C:\FSWDAG1**
   - Adresses IP du groupe de disponibilité de base de données : **172.16.0.33**
3. **Gérez l'appartenance au DAG** pour **DAG1**, et ajoutez les serveurs suivants :
   - **LON-MBX1**
   - **LON-MBX2**

▶ Tâche 3 : Créer une copie de base de données de boîtes aux lettres

1. Dans le Centre d'administration Exchange, cliquez sur **Bases de données**.
2. Pour la **Mailbox Database 1**, ajoutez une copie de base de données de boîtes aux lettres à **LON-MBX2**.

▶ Tâche 4 : Vérifier la réussite de la copie d'une base de données

1. Dans les onglets, cliquez sur **Actualiser**, puis patientez jusqu'à ce que le volet d'informations marque la **Mailbox Database 1\LON-MBX2** comme **Passif Sain**. Cela peut prendre plusieurs minutes et jusqu'à plusieurs heures selon la taille de la base de données.
2. Affichez les détails pour **Mailbox Database 1\LON-MBX2** et vérifiez les éléments ci-dessous.
   - État : **Sain**
   - État de l'index de contenu : **Sain**

▶ Tâche 5 : Interrompre et reprendre une copie de base de données

1. Dans le Centre d'administration Exchange, interrompez **Mailbox Database 1\LON-MBX2**.
2. Reprenez **Mailbox Database 1\LON-MBX2**. Si le bouton Reprendre n'est pas disponible, attendez, puis cliquez sur **Actualiser** plusieurs fois. Dans le volet d'informations, vérifiez que la longueur de la file d'attente de copie est égale à zéro.

Résultats : À la fin de cet exercice, les stagiaires auront préconfiguré un objet de réseau de cluster dans Active Directory, créé un DAG, ajouté deux serveurs de boîtes aux lettres au DAG et rendu une base de données hautement disponible. Les stagiaires auront aussi interrompu une copie de base de données et l'auront reprise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Déploiement des serveurs d'accès au client hautement disponibles

Scénario

Vous décidez d'implémenter l'équilibrage de la charge réseau (NLB) logicielle pour équilibrer la charge de LON-CAS1 et LON-CAS2 pour les connexions de serveur d'accès au client. Utilisez l'adresse IP 172.16.0.6 en tant qu'adresse IP virtuelle qui gère l'espace de noms mail.adatum.com pour vos connexions client-serveur. Pour atteindre cet objectif, vous devez maintenant réaliser la configuration.

Les tâches principales de cet exercice sont les suivantes :

1. Installer la fonctionnalité d'équilibrage de la charge réseau sur des serveurs d'accès au client.
2. Créer un cluster de serveurs d'accès au client à charge équilibrée.
3. Créer un enregistrement DNS pour l'adresse IP virtuelle.

▶ Tâche 1 : Installer la fonctionnalité d'équilibrage de la charge réseau sur des serveurs d'accès au client

1. Basculez vers **LON-CAS1**.
2. Dans le Gestionnaire de serveur, dans **Assistant Ajout de rôles et de fonctionnalités**, ajoutez les fonctionnalités suivantes :
   - **Équilibrage de la charge réseau**
3. Basculez vers l'ordinateur virtuel **LON-CAS2** et, dans le Gestionnaire de serveur, dans **Assistant Ajout de rôles et de fonctionnalités**, ajoutez la fonctionnalité suivante :
   - **Équilibrage de la charge réseau**

▶ Tâche 2 : Créer un cluster de serveurs d'accès au client à charge équilibrée

1. Basculez vers **LON-CAS1**, et dans le Gestionnaire de serveur, ouvrez **Gestionnaire d'équilibrage de la charge réseau**.
2. Dans le Gestionnaire d'équilibrage de la charge réseau, créez un nouveau cluster avec les paramètres ci-dessous.
   - HÔTE : **LON-CAS1**
   - Adresses IP de cluster : **172.16.0.6, Masque de sous-réseau : 255.255.0.0**
   - Nom Internet complet : **webmail.adatum.com**
3. Ajoutez l'hôte suivant pour mettre en cluster **webmail.adatum.com** :
   - **LON-CAS2**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Créer un enregistrement DNS pour l'adresse IP virtuelle

1. Basculez vers **LON-DC1**, puis dans le Gestionnaire de serveur, ouvrez **DNS**.
2. Dans le Gestionnaire DNS, sous **Adatum.com**, créez un nouvel hôte avec les paramètres suivants :
   - Nom : **Webmail**
   - Adresse IP : **172.16.0.6**

Résultats : À la fin de cet exercice, les stagiaires auront installé et configuré NLB et auront créé un enregistrement DNS pour leur adresse IP virtuelle à charge équilibrée.

Exercice 3 : Test de la configuration de la haute disponibilité

Scénario

Pour vérifier que votre configuration haute disponibilité fonctionne comme prévu, vérifiez le basculement du serveur d'accès au client et du DAG.

Les tâches principales de cet exercice sont les suivantes :

1. Simuler une défaillance sur LON-CAS1 et vérifier la fonctionnalité Microsoft® Outlook Web Access.
2. Activer LON-CAS1 et simuler une défaillance de LON-CAS2.
3. Vérifier la haute disponibilité des copies de base de données.

▶ Tâche 1 : Simuler une défaillance sur LON-CAS1 et vérifier la fonctionnalité Microsoft® Outlook Web Access

1. Basculez vers **LON-CAS1**, et dans le Gestionnaire d'équilibrage de la charge réseau, arrêtez **LON-CAS1(Ethernet)**.
2. Basculez vers **LON-DC1**, ouvrez Internet Explorer, tapez **https://webmail.adatum.com/owa** et connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Vous devez maintenant voir votre boîte de réception. Cela indique que LON-CAS2 sert actuellement de serveur d'accès au client.

▶ Tâche 2 : Activer LON-CAS1 et simuler une défaillance de LON-CAS2

1. Basculez vers l'ordinateur virtuel **LON-CAS1**, puis dans le Gestionnaire d'équilibrage de la charge réseau, démarrez **LON-CAS1(Ethernet)**.
2. Basculez vers **Ordinateur hôte**, et dans le Gestionnaire Hyper-V, arrêtez **22341B-LON-CAS2**.
3. Basculez vers l'ordinateur virtuel LON-DC1. Dans Internet Explorer, cliquez sur **Actualiser (F5)** et connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Dans Outlook Web App, vérifiez que vous pouvez accéder aux dossiers, par exemple Éléments envoyés. Cela vérifie que LON-CAS1 a assumé le rôle serveur d'accès au client pour le client.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Vérifier la haute disponibilité des copies de base de données

1. Basculez vers **LON-CAS1**, et dans le Centre d'administration Exchange, vérifiez que Mailbox Database 1\LON-MBX1 est Actif Monté et Mailbox Database 1\LON-MBX2 est Passif Sain.
2. Basculez vers **Ordinateur hôte**, et dans le Gestionnaire Hyper-V, arrêtez **22341B-LON-MBX1**.
3. Basculez vers l'ordinateur virtuel **LON-CAS1**. Dans Internet Explorer, cliquez sur **Actualiser (F5)** et, dans le Centre d'administration Exchange, vérifiez que Mailbox Database 1\LON-MBX1 marquée comme Passif ServiceDown et Mailbox Database 1\LON-MBX1 comme Actif Monté.
4. Basculez vers l'ordinateur virtuel **LON-DC1**, et dans Internet Explorer et Outlook Web App, vérifiez que vous pouvez afficher des dossiers tels que la boîte de réception et envoyer un message.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-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 les ordinateurs **22341B-LON-CAS1**, **22341B-LON-CAS2**, **22341B-LON-MBX1** et **22341B-LON-MBX2**.

 **Remarque :** Bien que certains serveurs ne soient pas en cours d'exécution, vous devez tout de même les rétablir.

Résultats : À la fin de cet exercice, les stagiaires auront testé leur configuration haute disponibilité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Votre DAG a deux serveurs de boîtes aux lettres (nœuds) et un serveur témoin. Quand perdrez-vous le quorum et ne pourrez pas monter les bases de données automatiquement ?

Méthode conseillée

Pour décider du serveur témoin à choisir pour un DAG, vous devez préférer un serveur d'accès au client à un serveur de fichiers.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Vous ne pouvez pas ajouter un serveur Exchange à un DAG.	
Lorsque vous ajoutez un serveur à un DAG, la réplication de la base de données échoue.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 7

Planification et implémentation d'une solution de récupération d'urgence

Table des matières :

Vue d'ensemble du module **7-1**

Leçon 1 : Planification de l'atténuation des risques **7-2**

Leçon 2 : Planification et implémentation de la sauvegarde d'Exchange Server 2013 **7-11**

Leçon 3 : Planification et implémentation de la récupération d'Exchange Server 2013 **7-18**

Atelier pratique : Implémentation d'une solution de récupération d'urgence pour Exchange Server 2013 **7-29**

Contrôle des acquis et éléments à retenir **7-34**

Vue d'ensemble du module

La sauvegarde régulière des données d'un serveur Exchange est une part essentielle de l'administration générale d'Exchange Server. La sauvegarde des données vous permet de restaurer les données a posteriori, soit en cas de perte ou d'altération des données, soit à la suite d'un test.

La sauvegarde d'un serveur Exchange est une tâche relativement simple, mais le régime de sauvegarde est déterminé par des facteurs tels que le matériel de sauvegarde, la durée des fenêtres de sauvegarde, et les contraintes de restauration. Les contrats de niveau de service jouent également un rôle majeur dans la détermination des régimes de sauvegarde. Si, par exemple, votre contrat de niveau de service d'Exchange Server stipule que les services d'Exchange ne doivent pas rester non opérationnels plus de deux heures lors d'un incident, votre régime de sauvegarde doit être conçu et effectué en gardant cet objectif à l'esprit.

Exchange Server 2013 comprend des fonctionnalités de sauvegarde et de restauration comme la protection des données natives Exchange que nous vous recommandons d'examiner avant d'utiliser l'approche traditionnelle de sauvegarde sur bande employée par la plupart des organisations.
Ce module présente les fonctionnalités de sauvegarde et de restauration d'Exchange Server 2013 et explique en détail les éléments à prendre en compte lors de la création d'un plan de sauvegarde.

Objectifs

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

- planifier l'atténuation des risques ;
- planifier et implémenter la sauvegarde d'Exchange Server 2013 ;
- planifier et implémenter la récupération d'Exchange Server 2013.

Leçon 1
Planification de l'atténuation des risques

L'atténuation des risques vous permet d'éviter d'avoir recours à une récupération d'urgence. Elle vous permet également de récupérer les données beaucoup plus rapidement que si vous aviez à effectuer une restauration complète du système. Exchange Server 2013 a amélioré les méthodes d'atténuation des risques disponibles pour les administrateurs, avec de nouvelles fonctionnalités telles que les groupes de disponibilité de la base de données (DAG, Database Availability Groups).

Cette leçon présente une vue d'ensemble des options disponibles dans Exchange Server 2013 vous permettant d'atténuer les effets d'un incident sans avoir à restaurer des sauvegardes. La leçon décrit également les scénarios dans lesquels les sauvegardes sont encore nécessaires.

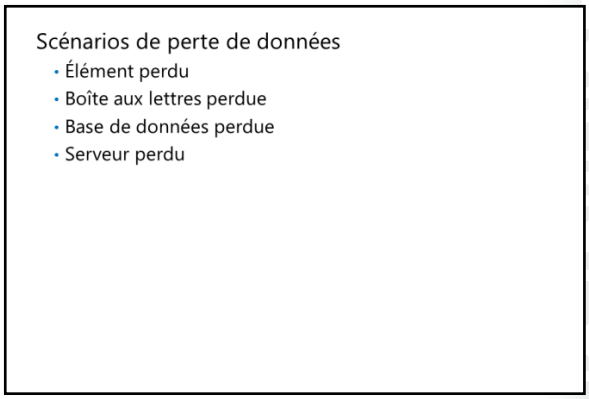
Objectifs de la leçon

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

- identifier les scénarios de perte de données ;
- répertorier les fonctionnalités d'atténuation de perte de données ;
- planifier une stratégie d'atténuation des risques ;
- expliquer les relations entre une récupération d'urgence et une haute disponibilité ;
- décrire la protection des données natives Exchange Server ;
- décrire dans quels cas la protection des données natives Exchange Server est appropriée ;
- décrire les chronologies pour la récupération d'urgence ;
- identifier les scénarios qui nécessitent une sauvegarde et une restauration.

Identifier les scénarios de perte de données

Lors de l'identification des risques, vous devez considérer tous les scénarios potentiels de perte de données qui peuvent affecter le travail des utilisateurs. Dans un environnement Exchange, les scénarios possibles de perte de données comprennent la perte d'éléments, de boîte aux lettres, de base de données et de serveur.



Élément perdu

La perte d'un élément d'une boîte aux lettres est souvent causé par la suppression de celui-ci par l'utilisateur, soit par erreur soit sciemment, et l'utilisateur se rend compte ultérieurement qu'il en a besoin. Un élément de boîte aux lettres perdu se compose en général d'un peu de données. Pourtant, cette petite quantité de données peut avoir une grande importance. Les éléments perdus sont souvent des messages électroniques ou des éléments du calendrier, et peuvent comporter des pièces jointes importantes pour l'utilisateur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Boîte aux lettres perdue

Généralement, la perte de la boîte aux lettres d'un utilisateur se produit lorsqu'elle est supprimée par l'administrateur d'Exchange. Cette situation peut se produire par erreur, mais cela arrive généralement quand un utilisateur quitte l'organisation. Dans un scénario classique, après le départ d'un utilisateur, son supérieur a besoin d'accéder à sa boîte aux lettres pour consulter les projets sur lesquels il travaillait. Cependant, la boîte aux lettres ayant déjà été supprimée par l'administrateur, le responsable ne peut plus en afficher le contenu.

Base de données perdue

La perte d'une base de données entraîne une perte de toutes les boîtes aux lettres de cette base de données. En outre, étant donné l'absence de la base de données, les utilisateurs dont les boîtes aux lettres se trouvent dans cette base de données ne peuvent plus envoyer ni recevoir de messages.

La perte d'une base de données est généralement causée par un dysfonctionnement du système, comme par exemple une défaillance du disque ou l'altération de la base de données. La récupération d'une base de données perdue est cruciale, car la panne peut affecter un grand nombre d'utilisateurs.

Serveur perdu

La perte d'un serveur occasionne la perte de toutes les bases de données se trouvant sur ce serveur. Elle est généralement causée par une défaillance du système ou de l'infrastructure. La récupération d'un serveur est cruciale, car de nombreux utilisateurs peuvent s'en trouver affectés. Si un centre de données est perdu, il est possible que plusieurs serveurs soient perdus.

Fonctionnalités d'atténuation de perte de données

Plusieurs fonctionnalités d'Exchange Server 2013 peuvent être utilisées pour vous permettre d'atténuer la perte de données. Il s'agit d'un point important car, lorsque la perte de données est atténuée, il n'est pas nécessaire d'effectuer une récupération à partir d'une sauvegarde. En général, l'utilisation de ces méthodes d'atténuation est un grain de temps, avant de tenter d'exécuter une récupération à partir d'une sauvegarde.

- L'atténuation de perte de données évite d'avoir à effectuer une récupération à partir d'une sauvegarde
- Les fonctionnalités d'atténuation de perte de données sont les suivantes
  - Récupération des éléments supprimés
  - Récupération d'élément unique
  - Blocage local
  - Rétention des boîtes aux lettres supprimées
  - Groupes de disponibilité de la base de données
  - Redondance des clichés instantanés

Récupération d'éléments supprimés

Dans les versions antérieures d'Exchange, les éléments d'un utilisateur supprimés étaient encore récupérables, tant que ces éléments n'avaient pas été vidés du conteneur de dépôt. Une suppression définitive (effectuée en pressant les touches Maj+Suppr) supprime définitivement les messages de la boîte aux lettres. Dans Exchange Server 2013, le conteneur de dépôt est remplacé par le magasin d'éléments récupérables. Si le délai de rétention par défaut n'est pas modifié, les messages sont vidés de la base de données de la boîte aux lettres après 14 jours, et des éléments du calendrier après 120 jours.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Récupération d'élément unique

Microsoft® Exchange Server 2010 a introduit la récupération d'élément unique, une nouvelle fonctionnalité qui permet de récupérer des éléments sans devoir restaurer la base de données des boîtes aux lettres à l'aide d'une sauvegarde. Cette fonctionnalité est désactivée par défaut et doit être activée pour chaque boîte aux lettres. Sans l'activation de la récupération d'élément unique, les éléments vidés du magasin d'éléments récupérables ne peuvent être récupérés qu'à l'aide de la sauvegarde de la base de données de boîtes aux lettres.

Lorsque la récupération d'élément unique est activée, tous les éléments du magasin d'éléments de récupération sont conservés et ne peuvent pas être supprimés par l'utilisateur. Sans l'activation de cette fonctionnalité, les éléments sont vidés après 14 jours, et les éléments du calendrier après 120 jours. Ces actions par défaut ne s'appliquent pas lorsque le quota d'avertissements des éléments récupérables est atteint. Dans ce cas, les éléments les plus anciens sont vidés les premiers.

Blocage local

Une autre option qui vous permet de récupérer les éléments de la boîte aux lettres d'un utilisateur est d'activer le blocage local pour l'utilisateur. Grâce à cette fonctionnalité, tous les éléments supprimés de la boîte aux lettres de l'utilisateur sont conservés dans le magasin d'éléments récupérables, et peuvent être récupérés grâce à une recherche eDiscovery dans la boîte aux lettres de l'utilisateur. Les administrateurs peuvent rechercher et récupérer les éléments bloqués. Les utilisateurs ne peuvent ni rechercher ni récupérer les éléments bloqués.

Fonctionnalités supplémentaires d'atténuation de perte de données

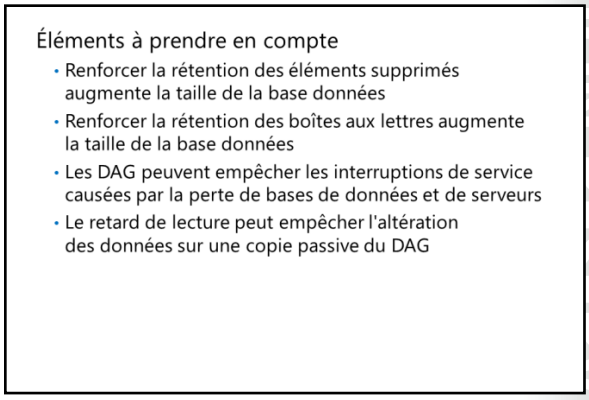
Les autres fonctionnalités d'atténuation de perte de données sont les suivantes :

- Rétention des boîtes aux lettres supprimées. Utilisez la rétention de boîte aux lettres supprimées pour les récupérer ainsi que leur contenu. Par défaut, Exchange Server 2013 conserve les boîtes aux lettres supprimées 30 jours.
- Groupe de disponibilité de base de données (Database Availability Group, DAG). Dans la plupart des scénarios, utilisez un DAG pour une récupération à partir d'un serveur ou d'une base de données perdus. Lorsqu'un serveur ou une base de données connaissent une défaillance, Exchange Server 2013 active automatiquement une copie de cette base de données sur un autre membre du DAG. Ce processus est beaucoup plus rapide qu'une restauration à partir d'une sauvegarde. Combiné avec une tolérance aux défaillances de site, un DAG atténue la perte de l'intégralité d'un centre de données.
- Redondance des clichés instantanés. Dans Exchange Server 2013, le serveur de transport fait désormais une copie de chaque message reçu avant d'envoyer un accusé de sa bonne réception au serveur d'envoi. Si Exchange Server 2013 détermine que le message d'origine a été perdu au cours du transit, la copie du message est renvoyée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification d'une stratégie d'atténuation des risques

Lors de l'implémentation d'Exchange Server 2013, la configuration par défaut suffit à de nombreuses organisations. Cependant, si vous planifiez une stratégie d'atténuation des risques, tenez compte des éléments suivants :



- augmenter la rétention d'éléments supprimés afin que les éléments soient récupérables pendant une période plus longue, mais dans la plupart des cas, la configuration par défaut de 14 jours suffit ;
- renforcer la rétention d'éléments supprimés pour les utilisateurs « essentiels ». En augmentant le délai de rétention pour les utilisateurs « essentiels », vous limitez l'augmentation de la taille de la base de données et répondez au mieux à leurs exigences ;
- activer la récupération d'élément unique pour garantir la récupération de tous les éléments. La récupération d'élément unique empêche les utilisateurs d'effectuer une suppression définitive des éléments et de les vider du magasin d'éléments récupérables. L'activation de cette option permet à un administrateur de récupérer les éléments, le cas échéant ;
- augmenter la rétention des boîtes aux lettres supprimées afin de les rendre récupérables pendant une période plus longue, bien que dans la plupart des cas, la configuration par défaut de 30 jours suffit ;
- utiliser des DAG pour permettre une redondance au niveau des serveurs et pour éviter une perte de données. Pour cela, vous devez avoir installé l'édition d'entreprise du système d'exploitation Windows Server® 2008 R2 ou l'édition Standard ou Datacenter de Windows Server® 2012 ;
- utiliser une copie retardée pour empêcher l'altération des bases de données. L'altération d'une base de données peut se produire lorsqu'une transaction est placée dans les journaux de transactions. En pareil cas, une copie retardée passive avec une configuration définie en retard de lecture peut empêcher l'altération de la copie retardée passive, car la lecture de la transaction incriminée y est empêchée.

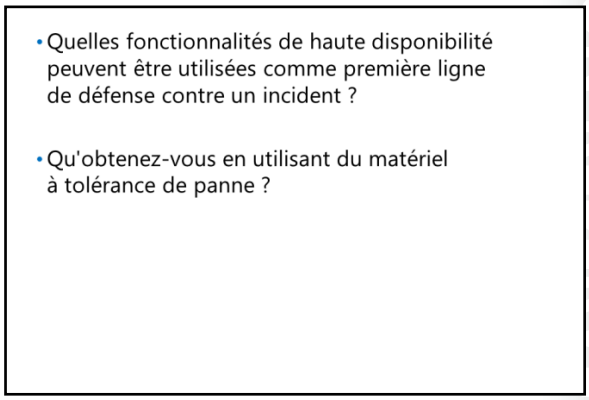
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Discussion : Quelles sont les relations entre récupération d'urgence et haute disponibilité ?

Utilisez les questions de discussion pour examiner les relations entre récupération d'urgence et haute disponibilité.

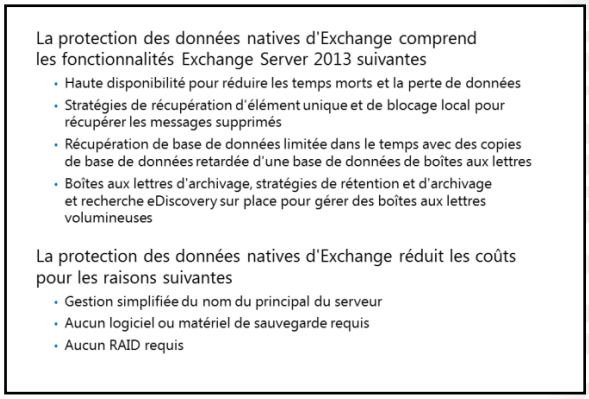
Question : Quelles fonctionnalités de haute disponibilité pouvez-vous utiliser comme première ligne de défense contre un incident ?

Question : Votre organisation accepterait-elle d'utiliser uniquement des fonctionnalités à haute disponibilité et de ne pas utiliser de sauvegardes ?



Protection des données natives Exchange Server

Exchange Server 2013 permet une intégration beaucoup plus étroite de haute disponibilité avec récupération d'urgence, en particulier si les fonctionnalités de haute disponibilité d'Exchange Server 2013 sont suffisantes pour vos impératifs de sauvegarde.



Depuis Exchange Server 2010, une nouvelle fonctionnalité appelée Protection des données natives Exchange existe. Elle permet de réduire ou de supprimer complètement vos solutions de sauvegarde traditionnelles pour les boîtes aux lettres et les serveurs Exchange. Réfléchissez soigneusement au bien fondé d'utiliser cette fonctionnalité pour répondre à vos besoins en matière de récupération d'urgence. La protection des données natives d'Exchange comprend les fonctionnalités suivantes :

- Haute disponibilité pour réduire les temps morts et la perte de données. Si les DAG d'Exchange Server 2013 constituent la méthode principale de récupération d'urgence, vous pouvez utiliser leurs fonctionnalités de haute disponibilité pour réduire les temps morts et la perte de données en cas de défaillance d'une base de données ou d'un serveur de boîte aux lettres. Les DAG vous permettent de diffuser des copies de base de données sur plusieurs centres de données ou sites Active Directory. Cela vous permet de palier aux défaillances du centre de données, et de conserver une copie hors site d'une base de données. Dans certains cas, il peut être moins coûteux de fournir plusieurs copies d'une base de données que de sauvegarder des bases de données très volumineuses.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

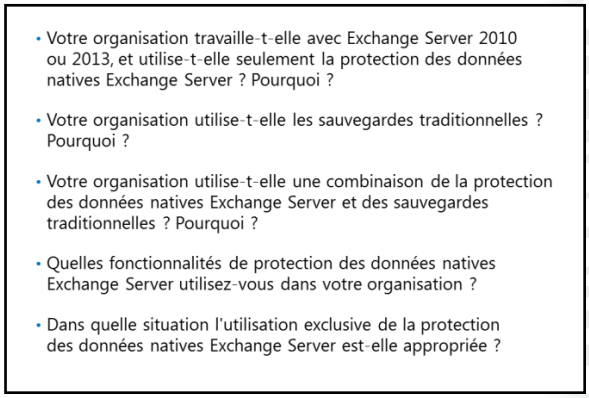
- Stratégies de récupération d'élément unique et de blocage local pour récupérer les messages supprimés. Dans Exchange Server 2013, la récupération d'élément unique garantit la conservation des éléments supprimés et modifiés en vue d'être récupérés. Ainsi, les utilisateurs ne peuvent plus les vider définitivement de leur boîte aux lettres. Le blocage local conserve les informations stockées de manière électronique, comme les messages électroniques, de sorte que les utilisateurs ne puissent pas les supprimer. Cette fonctionnalité palie le besoin d'effectuer une restauration lorsqu'un utilisateur supprime des messages d'une boîte aux lettres quand une exigence de conformité requiert l'examen de la boîte en question.
- Récupération de base de données limitée dans le temps avec des copies de base de données retardée d'une base de données de boîtes aux lettres. La configuration d'une copie de la base de données de boîtes aux lettres peut être définie pour retarder la lecture des fichiers journaux de 14 jours maximum. Ainsi, vous conservez toujours une base de données telle qu'elle était les jours précédents. En d'autres termes, si vous avez un problème avec votre base de données active actuelle, vous pouvez basculer vers la copie retardée et valider les journaux à la date ou à l'heure à laquelle la restauration est requise.
- Boîtes aux lettres d'archivage, stratégies de rétention et d'archivage et recherche eDiscovery sur place pour gérer des boîtes aux lettres volumineuses. En configurant des boîtes aux lettres d'archivage, vous pouvez proposer aux utilisateurs un emplacement de stockage pour les anciens messages. Vous pouvez également automatiser le processus de gestion de la messagerie dans les boîtes aux lettres des utilisateurs, notamment le déplacement des messages dans la boîte aux lettres d'archivage, en configurant des stratégies de rétention et d'archivage. Tous les messages sont disponibles pour l'utilisateur, et peuvent également être accessibles via la recherche dans plusieurs boîtes aux lettres.

Au cours de votre réflexion d'implémentation de ces fonctionnalités, vous devez évaluer le coût de votre infrastructure de sauvegarde actuelle, notamment le matériel, l'installation, les coûts de licence, et les frais de gestion associés à la récupération des données et à la gestion des sauvegardes. En fonction des exigences de votre organisation, il est probable que vous atteigniez un coût total de propriété d'Exchange plus bas en maintenant au moins trois copies de base de données de boîtes aux lettres plutôt qu'une seule avec sauvegardes.

Même si les déploiements hautement disponibles ne requièrent plus de sauvegardes classiques, elles peuvent encore être nécessaires dans votre organisation. L'intégration des fonctionnalités de haute disponibilité employée comme une autre solution aux sauvegardes fonctionne uniquement pour les bases de données de boîtes aux lettres. Toutefois, vous pouvez envisager d'utiliser des sauvegardes traditionnelles pour d'autres configurations d'Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

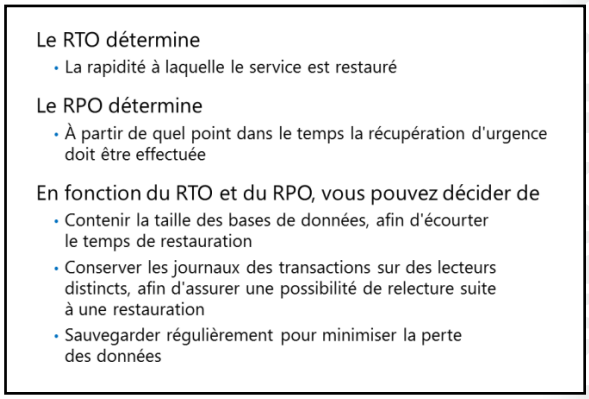
Discussion : Dans quels cas la protection des données natives Exchange Server est-elle appropriée ?



Présentez la protection des données natives Exchange Server aux les stagiaires.

- Votre organisation travaille-t-elle avec Exchange Server 2010 ou 2013, et utilise-t-elle seulement la protection des données natives Exchange Server ? Pourquoi ?
- Votre organisation utilise-t-elle les sauvegardes traditionnelles ? Pourquoi ?
- Votre organisation utilise-t-elle une combinaison de la protection des données natives Exchange Server et des sauvegardes traditionnelles ? Pourquoi ?
- Quelles fonctionnalités de protection des données natives Exchange Server utilisez-vous dans votre organisation ?
- Dans quelle situation l'utilisation exclusive de la protection des données natives Exchange Server est-elle appropriée ?

Quelles sont les chronologies pour une récupération d'urgence ?



Les échéances de la récupération d'urgence sont déterminées par le contrat de niveau de service (SLA). Chaque SLA doit inclure un objectif de temps de récupération (RTO) et un objectif de point de récupération (RPO) qui vous permettent de déterminer comment effectuer les sauvegardes et la récupération d'urgence.

Le RTO d'un service définit la vitesse à laquelle vous devriez récupérer le service. Par exemple, après la défaillance d'un serveur de boîtes aux lettres, son RTO indique que la récupération des boîtes aux lettres stockées sur ce serveur doit être effectuée dans un délai de deux heures.

Dans certains cas, il existe des RTO pour une partie des fonctionnalités. Par exemple, après la défaillance d'un serveur de boîtes aux lettres, le RTO pour l'envoi et la réception de messages est d'une heure, mais le RTO pour les données d'historique des boîtes aux lettres peut être de 12 heures.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

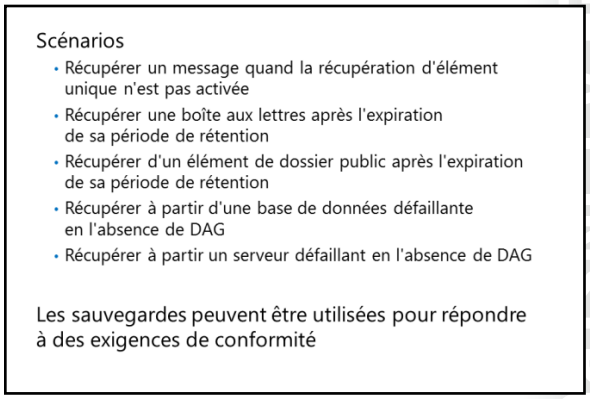
Le RPO pour un service définit une échéance avant laquelle vous devez récupérer le service. Le RPO peut stipuler que la perte de données d'un calendrier spécifique est tolérée, ou que la récupération doit être égale à un certain laps de temps. Par exemple, le RPO d'un serveur de boîtes aux lettres peut indiquer que les données des 12 dernières heures peuvent être perdues, ou qu'un serveur de boîtes aux lettres peut être récupéré à partir d'une sauvegarde ayant été effectuée à 2 h 00, le jour précédent.

Selon vos RTO et RPO de serveurs de boîtes aux lettres, vous avez la possibilité de choisir de :

- contenir la taille des bases de données, afin d'écourter le temps de récupération ;
- conserver les journaux des transactions sur des lecteurs distincts de ceux de la base de données, afin de vous assurer une possibilité de relecture suite à une restauration de base de données ;
- effectuer une sauvegarde toutes les deux ou trois heures pour minimiser la perte de données.

Scénarios pour lesquels une sauvegarde et une restauration sont requises

Après l'implémentation de l'atténuation des risques et de la haute disponibilité de perte de données des serveurs de boîtes aux lettres, il est possible que certains scénarios requièrent encore une sauvegarde et une restauration pour la récupération de données. Les scénarios de récupération de données nécessitant une sauvegarde et une restauration sont notamment :



- la récupération d'un message supprimé définitivement quand la récupération d'élément unique n'est pas activée.
  Si la récupération d'élément unique n'est pas activée sur un serveur de boîtes aux lettres, et qu'un utilisateur supprime définitivement un élément, Exchange Server 2013 supprime l'élément de la base de données sans le placer dans le magasin d'éléments récupérables ;
- la récupération d'un message après l'expiration de la période de rétention de l'élément. Même si la récupération d'élément unique est activée, Exchange Server 2013 ne conserve les éléments supprimés que pour une période spécifiée. Par défaut, cette période est de 14 jours pour les messages électroniques ;
- la récupération d'un élément de dossier public après l'expiration de la période de rétention de l'élément. Exchange Server 2013 ne conserve un élément supprimé dans un dossier public que pour une période spécifiée. Par défaut, cette période est de 14 jours ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- la récupération d'une base de données en cas de non-utilisation d'un DAG. La récupération de bases de données défaillantes doit être réalisée à partir d'une sauvegarde lorsque le serveur de boîtes aux lettres n'est pas membre d'un DAG. L'utilisation d'uniquement une copie unique dans un DAG. Il s'agit d'un scénario rare mais vous pouvez le rencontrer. Vous pouvez aussi utiliser des outils de réparation de base de données, mais, en général, il est plus rapide de restaurer une base de données à partir d'une sauvegarde que de la réparer ;
- la récupération suite à une défaillance de serveur lorsque le serveur de boîtes aux lettres n'est pas membre d'un DAG. En cas d'échec d'un serveur de boîtes aux lettres, toutes les bases de données sur ce serveur sont perdues s'il n'est pas membre d'un DAG. Vous devez récupérer le serveur à partir d'une sauvegarde.

En plus des impératifs de récupération de données, la conformité est une raison courante pour effectuer des sauvegardes. Soumises à des règlementations ou à des lois, certaines organisations se doivent de conserver une archive de leur courrier électronique pendant un certain laps de temps. Vous pouvez utiliser une sauvegarde à cet effet, mais vous devez également envisager l'utilisation d'un logiciel d'archivage non Microsoft.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Planification et implémentation de la sauvegarde d'Exchange Server 2013

Lors de la planification d'une sauvegarde d'Exchange Server 2013, tenez compte des données que vous devrez restaurer. Ne sauvegardez que les données qui doivent être restaurées. Limiter la taille de données de sauvegarde réduit la durée d'exécution d'une sauvegarde, et fournit davantage de flexibilité à votre planification de sauvegarde.

Le logiciel utilisé pour effectuer les sauvegardes peut également avec une influence sur votre processus de sauvegarde. Il existe différentes solutions non Microsoft pour sauvegarder Exchange Server 2013. Vous pouvez aussi utiliser Sauvegarde Windows Server du système d'exploitation Windows et Microsoft® System Center Data Protection Manager (Data Protection Manager).

Cette leçon présente une vue d'ensemble des conditions requises nécessaires à l'implémentation d'une solution de sauvegarde d'Exchange Server 2013.

Objectifs de la leçon

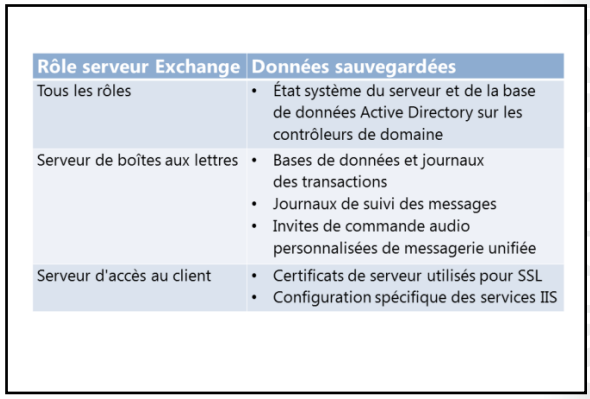
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- identifier les conditions requises de sauvegarde pour Exchange Server 2013 ;
- choisir le logiciel de sauvegarde d'Exchange Server ;
- choisir le support de sauvegarde d'Exchange Server ;
- décrire le fonctionnement de la sauvegarde du service VSS (Service de cliché instantané des volumes).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Conditions requises de sauvegarde pour Exchange Server 2013

Les conditions requises de sauvegarde pour les ordinateurs Exchange Server 2013 varient en fonction du rôle serveur Exchange installé sur l'ordinateur. Le tableau suivant répertorie les données pour lesquelles vous devez effectuer une sauvegarde pour chaque rôle serveur Exchange :



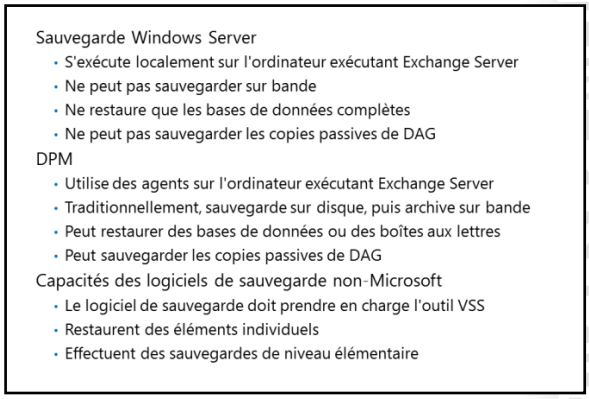
Rôle serveur Exchange	Données sauvegardées
Tous les rôles	• État système du serveur et de la base de données Active Directory sur les contrôleurs de domaine
Serveur de boîtes aux lettres	• Bases de données et journaux des transactions • Journaux de suivi des messages • Invites de commande audio personnalisées de messagerie unifiée
Serveur d'accès au client	• Certificats de serveur utilisés pour SSL • Configuration spécifique des services IIS

Rôle serveur Exchange	Données sauvegardées	Rôle
Tous les rôles	État du système du serveur et des contrôleurs de domaine Active Directory® (AD DS)	L'état du système inclut les données de configuration locale de l'ordinateur ; il s'agit d'une étape facultative, nécessaire uniquement pour la restauration d'un serveur spécifique. AD DS stocke la plupart des données de configuration Exchange Server, requises pour reconstruire le serveur à l'aide du commutateur RecoverServer.
Serveur de boîtes aux lettres	Bases de données et journaux des transactions Journaux de suivi des messages Invites de commande audio personnalisées de messagerie unifiée	Restaurer les données en cas de perte de base de données. Restaurer les informations de suivi à des fins d'analyse. Restaurer des invites audio.
Serveur d'accès au client	Certificats du serveur utilisés pour le protocole SSL (Secure Sockets Layer) Configuration spécifique des services Internet (IIS)	Restaurer le certificat du serveur sur un nouveau serveur d'accès au client. Restaurer la configuration IIS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Choix du logiciel de sauvegarde d'Exchange Server

La sauvegarde peut être effectuée en utilisant le logiciel intégré Sauvegarde Windows Server, Data Protection Manager ou un logiciel non Microsoft. Choisissez le logiciel selon les fonctionnalités dont vous avez besoin. Au minimum, utilisez un logiciel de sauvegarde qui fonctionne correctement avec Exchange Server 2013.



Le logiciel de sauvegarde choisi doit prendre en charge des sauvegardes du service VSS pour Exchange Server 2013. Une sauvegarde VSS prend une capture instantanée de la base de données plutôt qu'une diffusion en continu des données Exchange Server. Sur le serveur Exchange, l'enregistreur VSS Exchange Server déclenche la capture instantanée et rend les bases de données Exchange Server cohérentes avant la prise de la capture instantanée.

Sauvegarde Windows Server

La Sauvegarde Windows Server, fournie avec Windows Server 2008 R2 et les versions ultérieures, peut être utilisée pour sauvegarder des bases de données Exchange Server 2013 ainsi que d'autres données. Lors de l'installation d'Exchange Server 2013, la version de Sauvegarde Windows Server est mise à jour pour prendre en charge les sauvegardes d'Exchange Server 2013. Cependant, la Sauvegarde Windows Server a les limitations critiques suivantes :

- elle doit s'exécuter localement sur le serveur sur lequel se trouvent les données Exchange Server ;
- l'enregistrement est réalisé sur un disque local ou un partage réseau, et non sur une bande ;
- elle ne restaure que les bases de données complètes ;
- elle ne peut pas sauvegarder les copies passives de DAG.

DPM

DPM est une solution de sauvegarde pour les serveurs exécutant Windows Server. DPM peut sauvegarder des serveurs de base de fichier et d'impression, et des serveurs d'applications. DPM effectue tout d'abord des sauvegardes sur disque, puis peut être utilisé pour de l'archivage sur bande.

DPM offre les performances supplémentaires suivantes par rapport à Sauvegarde Windows Server :

- contrairement à Sauvegarde Windows Server, Data Protection Manager ne requiert l'installation que d'un agent sur l'ordinateur sur lequel est exécuté Exchange Server 2013. Par conséquent, Data Protection Manager peut être utilisé pour centraliser les sauvegardes de plusieurs serveurs ;
- vous pouvez restaurer des bases de données ou des boîtes aux lettres. La récupération d'une boîte aux lettres est plus facile que de restaurer une base de données dans une base de données de récupération puis d'extraire le contenu de la boîte ;
- vous pouvez enregistrer des copies passives de base de données. Cela signifie que vous pouvez sauvegarder des bases de données d'un serveur sans avoir à déterminer qu'une copie active ou passive de base de données est sur le serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Logiciel de sauvegarde non-Microsoft

La plupart des logiciels de sauvegarde non-Microsoft est semblable à DPM. Cependant, certains entre eux présentent les fonctionnalités supplémentaires suivantes :

- *Restauration d'élément individuel*. Certains logiciels de sauvegarde non-Microsoft peuvent restaurer des messages électroniques individuels directement à partir de la sauvegarde de la boîte aux lettres d'un utilisateur. Cette procédure est moins complexe que d'effectuer une récupération dans une base de données de récupération, puis d'extraire le message requis.
- *Sauvegarde de niveau élémentaire*. Les sauvegardes de niveau élémentaire sont des sauvegardes de contenu de boîte aux lettres. Pour effectuer une sauvegarde de niveau élémentaire, le logiciel de sauvegarde crée une connexion MAPI (Messaging Application Programming Interface) pour chaque boîte aux lettres qu'il sauvegarde. Cela peut être utile pour sauvegarder des boîtes aux lettres spécifiques plus fréquemment. Cependant, de manière générale, il est plus facile de séparer des boîtes aux lettres en bases de données selon différents critères de sauvegarde.

Choix du support de sauvegarde d'Exchange Server

Support	Description
Bande	Facile à transporter et durable
Disque	Augmente les performances de sauvegarde
Basé sur le réseau SAN	Sauvegarde le trafic du réseau principal et le conserve sur le réseau SAN

La sauvegarde sur bande reste une méthode de sauvegarde populaire. Les bandes sont faciles à transporter et durables. Leur capacité et leur vitesse ont augmenté de façon constante alors que les fabricants mettaient de nouveaux produits sur le marché. Si votre sauvegarde doit être effectuée sur plus d'une bande, utilisez un changeur de bandes qui alterne automatiquement plusieurs bandes au sein d'une même unité. Dans des environnements de haute capacité, vous pouvez utiliser une bibliothèque de bandes. Une bibliothèque de bandes est une armoire contenant une ou plusieurs unités de sauvegarde sur bande, dotée d'un bras de robot qui place les bandes dans les unités de sauvegarde et les retire.

Pour améliorer les performances de sauvegarde, de nombreuses organisations utilisent les sauvegardes sur disque à la place des bandes. Le stockage sur disque est souvent moins coûteux que le stockage sur bande lorsque vous utilisez des disques de grande capacité plutôt que des disques à exécution plus rapide d'interface SCSI (Small Computer System Interface).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Cependant, les sauvegardes sur disque ne sont pas aussi bien adaptées que les sauvegardes sur bande pour le stockage hors site. Les disques ont tendance à être sensibles à leur déplacement physique, et peuvent devenir peu fiables s'ils sont transportés régulièrement. Par conséquent, beaucoup d'organisations utilisent des disques comme premier niveau de sauvegarde, puis transfèrent les sauvegardes sur une bande pour un stockage hors site.

Si vos bases de données Exchange Server se trouvent sur un réseau de zone de stockage (SAN, Storage Area Network), vous pouvez utiliser des captures instantanées SAN pour réduire le trafic de sauvegarde sur le réseau principal, et maintenir le trafic de sauvegarde sur le réseau de zone de stockage. La sauvegarde est effectuée à partir de l'instantané SAN plutôt que via Exchange Server. Pour implémenter des captures instantanées SAN pour la sauvegarde d'Exchange Server, votre application de sauvegarde doit prendre en charge votre matériel spécifique SAN.

Fonctionnement d'une sauvegarde VSS

Depuis Exchange 2010, les interfaces de programmation d'applications (API) en continu du moteur de stockage extensible (ESE, Extensible storage engine) ne sont plus disponibles. Exchange ne prend plus en charge désormais que l'utilisation de sauvegardes VSS.

Exchange 2013 et la sauvegarde VSS

- L'enregistreur VSS au sein de la Banque d'informations Microsoft Exchange est déplacé vers le service de réplication Microsoft Exchange
- Désormais appelé enregistreur Microsoft Exchange
- Utilisé par les applications VSS pour Exchange pour sauvegarder et restaurer les copies actives et passives de base de données
- Pour la sauvegarde et la restauration, la Banque d'informations Microsoft Exchange et le service de réplication Microsoft Exchange sont requis et doivent s'exécuter

VSS

Le service VSS fournit l'infrastructure de sauvegarde pour Microsoft® Windows Server 2008 ou les systèmes d'exploitation plus récents, ainsi qu'un mécanisme de création de copies ponctuelles cohérentes des données appelées les clichés instantanés.

Le service VSS peut être utilisé pour plusieurs raisons, comme :

- la création de sauvegardes cohérentes de fichiers et d'applications ouverts ;
- la création des clichés instantanés pour des dossiers partagés ;
- la récupération et restauration rapides de fichiers et de données.
- la création de clichés instantanés transportables à l'aide d'un fournisseur de matériel pour la sauvegarde, le test, et les scénarios d'exploitation de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les composants suivants sont inclus dans le service VSS :

Composant	Description
Service de cliché instantané des volumes	Un service qui coordonne différents composants pour créer des clichés instantanés cohérents d'un ou plusieurs volumes.
Demandeur	Une application qui demande qu'un cliché instantané de volume soit réalisé (comme c'est le cas avec Sauvegarde Windows Server).
Enregistreur	Stocke les informations permanentes sur un ou plusieurs volumes participant à la synchronisation des clichés instantanés.
Fournisseur	Crée et gère les clichés instantanés.
Volume source	Volume qui contient des données qui deviennent des clichés instantanés.
Volume de stockage	Volume qui conserve les fichiers de stockage de clichés instantanés pour le fournisseur logiciel de copie à l'écriture du système.

Nouveauté d'Exchange Server 2013

Microsoft® Exchange Server 2007 et Exchange Server 2010 comptent deux enregistreurs VSS, un dans le service de banque d'informations Microsoft Exchange et un dans le service de réplication Microsoft Exchange. Avec Exchange Server 2013, l'enregistreur situé au sein du service de banque d'informations Microsoft Exchange est déplacé vers le service de réplication Microsoft Exchange et appelé enregistreur Microsoft Exchange. Cet enregistreur est utilisé par les applications VSS pour Exchange pour sauvegarder les copies actives et passives de base de données et les restaurer. Pour sauvegarder ou restaurer des bases de données Exchange, les deux services (service de banque d'informations Microsoft Exchange et service de réplication Microsoft Exchange) sont requis et doivent s'exécuter.

Fonctionnement de la sauvegarde VSS

Les solutions de sauvegarde qui utilisent le service VSS créent un cliché instantané du disque au début du processus de sauvegarde. Ensuite, Exchange Server crée la sauvegarde à partir du cliché instantané plutôt que du disque de travail, afin que la sauvegarde n'interrompe pas le fonctionnement normal.

Cela génère une sauvegarde d'un volume qui reflète l'état de ce volume au début de la sauvegarde, même si les données sont modifiées en cours de sauvegarde. Toutes les données de la sauvegarde présentent une cohérence interne et reflètent l'état du volume à un moment précis. Les applications et les services reçoivent une notification signalant qu'une sauvegarde est sur le point d'être exécutée. Les services et les applications, comme Exchange Server, peuvent alors se préparer pour la sauvegarde en nettoyant les structures sur disque et en vidant les caches.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Technologies prises en charge par Exchange Server 2013

Seules les sauvegardes VSS pour Exchange sont prises en charge dans Exchange Server 2013. La Sauvegarde Windows Server est étendue à l'aide d'un plug-in avec l'installation d'Exchange 2013 qui permet d'effectuer des sauvegardes VSS de données Exchange. Les applications pour Exchange suivantes peuvent être utilisées pour sauvegarder et restaurer des bases de données Exchange :

- Sauvegarde Windows Server (avec plug-in VSS)
- Data Protection Manager
- Application VSS tiers

Limitations du service VSS

Gardez à l'esprit les limitations suivantes lorsque vous utilisez le service VSS pour sauvegarder et restaurer des données Exchange :

- Avec Sauvegarde Windows Server, les volumes sauvegardés sont uniquement ceux contenant des copies actives de base de données de boîtes aux lettres ou des bases de données de boîtes aux lettres autonomes. La sauvegarde de volumes contenant des copies passives de base de données de boîtes aux lettres est impossible. Pour sauvegarder ce type de volumes, vous devez utiliser DPM ou une application VSS tiers.
- Un enregistreur VSS distinct du service de réplication Microsoft Exchange est utilisé pour sauvegarder les copies passives de base de données de boîtes aux lettres. L'enregistreur VSS du service de réplication Microsoft Exchange ne prend pas en charge la restauration de base de données. Vous pouvez sauvegarder une base de données de boîtes aux lettres passive à l'aide de DPM ou d'une application VSS tierce pour Exchange, mais il est impossible d'effectuer directement la restauration VSS d'une copie passive de base de données de boîtes aux lettres. Les étapes pour effectuer une restauration VSS sont les suivantes :
  - restaurer la base de données de boîtes aux lettres passive vers un autre emplacement ;
  - suspendre la réplication de la copie passive ;
  - copier la base de données et les fichiers journaux à partir du nouvel emplacement vers l'emplacement de la base de données passive.

Démonstration : Procédure de sauvegarde d'Exchange Server 2013

Procédure de démonstration

1. Dans le Gestionnaire de serveur, ajoutez la fonctionnalité **Sauvegarde Windows Server**.
2. Créez un dossier partagé nommé **Sauvegarde** sur LON-CAS1.
3. Dans Sauvegarde Windows Server, créez un jeu de sauvegardes pour sauvegarder l'intégralité du serveur dans **\\LON-CAS1\Sauvegarde** et exécutez la sauvegarde.
4. Vérifiez la sauvegarde dans l'Observateur d'événements.

   Question : Prévoyez-vous d'utiliser la Sauvegarde Windows Server comme solution de sauvegarde Exchange Server principale ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Planification et implémentation de la récupération d'Exchange Server 2013

Pour restaurer les serveurs et les données perdus de la façon la plus efficace, vous devez connaître les options disponibles pour récupérer des fonctionnalités et des données Exchange Server. Le processus de récupération varie selon les rôles de serveurs spécifiques. Pour s'assurer que tout le monde dans votre organisation comprend le processus de récupération, vous devez créer et gérer un plan de récupération d'urgence.

Cette leçon présente une vue d'ensemble des options disponibles pour récupérer les éléments de boîte aux lettres, les bases de données, et les serveurs Exchange.

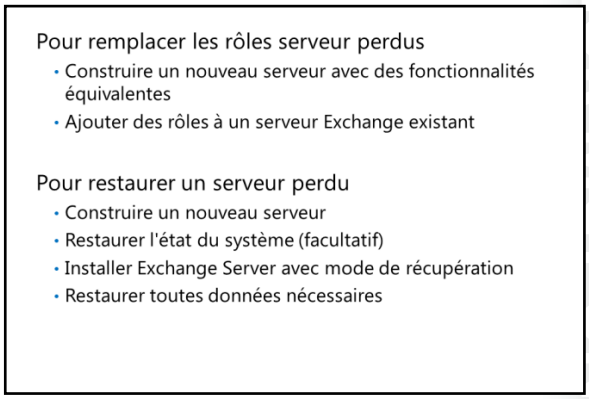
Objectifs de la leçon

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

- décrire les options pour récupérer un serveur Exchange ;
- décrire les options pour récupérer des données de boîtes aux lettres ;
- récupérer les données de boîtes aux lettres ;
- récupérer des serveurs d'accès au client ;
- récupérer la hiérarchie de dossiers publics ;
- récupérer des données à l'aide de la base de données de récupération ;
- réparer une base de données Exchange Server endommagée ;
- récupérer la base de données avec la fonctionnalité de tonalité.

Options de récupération de fonctionnalité de serveur Exchange

Vous disposez de deux options pour récupérer une fonctionnalité de serveur Exchange. Vous pouvez remplacer les rôles du serveur perdu ou récupérer le serveur perdu. Les deux options vous permettent de récupérer la fonctionnalité en intégralité.



Remplacer les rôles serveur perdus

Il est généralement plus rapide de remplacer un rôle serveur perdu que de restaurer un serveur perdu. Remplacer un rôle serveur perdu signifie que vous installez un nouveau serveur supplémentaire sur lequel se trouve le rôle perdu. Si vous utilisez un DAG, vous pouvez ajouter un nouveau serveur au DAG et créer une copie de base de données sur le serveur. Certains rôles de serveur peuvent être personnalisés et vous devrez les configurer.

Récupérer le serveur perdu

En cas d'échec d'un serveur, vous pouvez récupérer le serveur perdu pour restaurer la fonctionnalité offerte par ce serveur. Récupérer un serveur nécessite la création d'un serveur, et de joindre ce serveur au domaine avec le même nom de compte d'ordinateur. Vous pouvez restaurer l'état du système de l'ordinateur pour récupérer le nom de l'ordinateur et certaines données de configuration, telles que l'adresse IP et les certificats, mais cette méthode n'est pas le processus de récupération recommandé.

Après avoir joint le domaine, installez Exchange Server 2013 en mode de récupération. Le mode de récupération lit les informations de configuration du serveur Exchange à partir d'AD DS et installe automatiquement les rôles de serveur appropriés qui sont liés au compte d'ordinateur. Après l'installation, les informations de configuration du serveur Exchange stockées dans AD DS sont utilisées pour cet ordinateur.

 **Remarque :** Ne supprimez jamais le compte d'ordinateur d'un serveur Exchange défaillant. Auquel cas, vous ne pourrez pas récupérer la fonctionnalité du serveur Exchange pour ce serveur.

Dans quels cas récupérer un serveur perdu

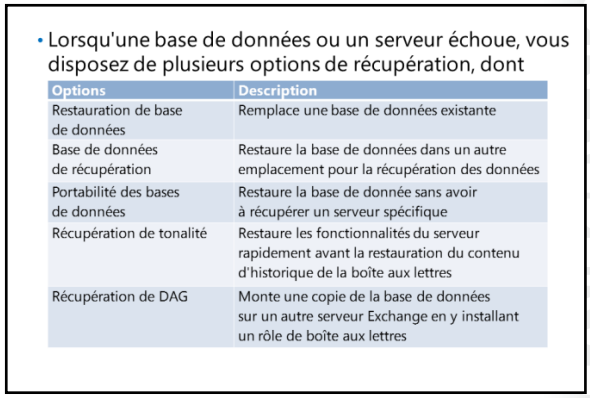
Même si remplacer un rôle serveur perdu est plus rapide et plus facile que de récupérer un serveur perdu, une récupération doit être effectuée dans les cas suivants :

- Pour éviter d'avoir à reconfigurer les pare-feu. Des serveurs accessibles Internet comme Microsoft® Outlook Web App et la technologie Microsoft® Exchange ActiveSync® sont protégés par des pare-feu et des serveurs proxy. Recréer la configuration d'origine signifie que vous n'avez pas besoin de reconfigurer les pare-feu pour le trafic direct d'un nouveau serveur. Si le serveur d'accès au client fait partie d'un tableau d'accès client, vous n'aurez pas à vous préoccuper de la reconfiguration du pare-feu, car le serveur de remplacement sera un nouveau nœud dans le tableau d'accès client existant.
- Pour récupérer des personnalisations mal documentées. Si les personnalisations d'un serveur perdu sont mal documentées, il est possible que vous ne puissiez pas répliquer la configuration. Une restauration à partir d'une sauvegarde peut être la seule solution pour récupérer la configuration.
- Pour éviter de reconfigurer des applications configurées pour utiliser un serveur spécifique. Certaines applications sont configurées pour utiliser un serveur spécifique. Par exemple, une application peut utiliser un serveur spécifique Hub Transport comme relais de messagerie. La récupération du serveur signifie qu'il n'est pas utile de reconfigurer un nouveau serveur Hub Transport avec un connecteur de réception SMTP approprié.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Options pour récupérer des données et des bases de données de boîtes aux lettres

Si une base de données est intacte, utilisez la récupération d'élément unique pour restaurer des messages individuels. Si une base de données est perdue en raison de l'altération ou de l'échec du serveur, vous devez récupérer les données stockées dans la base de données perdue. Beaucoup d'options peuvent être utilisées pour exécuter une récupération. Chaque option est appropriée selon les circonstances. La description des options disponibles est répertoriée dans le tableau suivant :



Option	Description
Restauration de base de données	Récupérer une base de données perdue suite à l'altération ou à l'échec du disque par la restauration de la base de données. Après la restauration, relisez les journaux des transactions pour remettre la base de données dans l'état dans lequel elle était juste avant qu'elle ait été perdue.
Base de données de récupération	Une base de données de récupération est une base de données montée sur un serveur de boîtes aux lettres, mais qui n'est pas accessible directement par les utilisateurs. Si vous devez récupérer des données dans une base de données, utilisez une base de données de récupération au lieu de récupérer l'intégralité de la base de données. Après avoir restauré une base de données dans la base de données de récupération, extrayez les messages ou les boîtes aux lettres à restaurer.
Portabilité des bases de données	Il n'est pas nécessaire de restaurer des bases de données sur les serveurs sur lesquels elles sont sauvegardées. Vous pouvez restaurer et monter des bases de données sur tous les serveurs de boîtes aux lettres Exchange Server 2013 de l'organisation. Cela est utile lorsqu'un des serveurs de boîtes aux lettres échoue, et que vous souhaitez récupérer la base de données sur un serveur de boîtes aux lettres opérationnel. Vous pouvez également restaurer une base de données de récupération située sur un autre serveur. Après avoir restauré une base de données sur un autre serveur, vous devez utiliser l'applet de commande **Set-Mailbox** avec le paramètre **–Database** pour lier les boîtes aux lettres au nouvel emplacement.

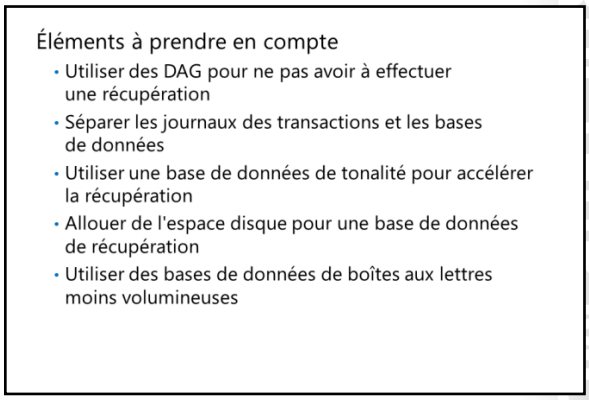
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Option	Description
Récupération de tonalité	Lorsqu'une base de données de boîtes aux lettres échoue, les utilisateurs ayant des boîtes aux lettres dans cette base de données ne peuvent plus envoyer ni recevoir de messages. Vous pouvez créer une base de données de tonalité en créant et en montant une base de données vide pour les boîtes aux lettres situées dans la base de données défaillante. Cela est une solution pour permettre aux utilisateurs d'envoyer et de recevoir des messages à nouveau rapidement. Une fois la base de données de tonalité opérationnelle, restaurez les données d'historique sur une base de données de récupération, puis fusionnez les données dans la base de données de tonalité. Si la base de données de tonalité se trouve sur un serveur différent de la base de données défaillante, utilisez l'applet de commande **Set-Mailbox** avec le paramètre **–Database** pour lier les boîtes aux lettres au nouvel emplacement.
Récupération de DAG	Effectuer une récupération de DAG signifie que vous n'avez pas besoin d'effectuer une restauration de base de données. Lorsque plusieurs copies de base de données se trouvent dans un DAG et qu'une des copies échoue, le serveur Exchange monte une autre copie de base de données et redirige les utilisateurs vers cette copie automatiquement. Pour restaurer la redondance, créez une autre copie de base de données sur un autre serveur.

Planification de la récupération de données et de bases de données de boîtes aux lettres

Lorsque vous planifiez la récupération d'un serveur de boîtes aux lettres, tenez compte des éléments suivants :

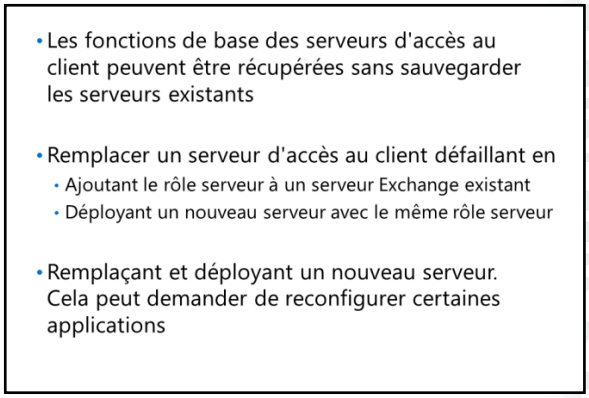


- Tout serveur dans un DAG peut héberger une copie d'une base de données de boîtes aux lettres de tout autre serveur du DAG. Lorsqu'un serveur est ajouté à un DAG, il fonctionne avec les autres serveurs dans le DAG afin d'assurer la récupération automatique suite à des défaillances qui affecteraient les bases de données de boîtes aux lettres. Ce processus est beaucoup plus rapide et plus facile que d'autres méthodes de récupération, et il améliore l'expérience de récupération pour les utilisateurs et les administrateurs.
- Placer les journaux des transactions et les bases de données sur des disques physiquement distincts si vous n'utilisez pas de DAG, et si vous devez avoir à effectuer une restauration à partir d'une sauvegarde. Cette procédure garantit la disponibilité des journaux des transactions pour une relecture en cas de perte des disques contenant la base de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Récupérer la fonctionnalité de base dès que possible si vous n'utilisez pas de DAG, et qu'un serveur ou une base de données de boîtes aux lettres échoue. Utilisez une base de données de récupération de tonalité pour permettre aux utilisateurs d'envoyer et de recevoir des messages aussi rapidement que possible. Ce processus est beaucoup plus rapide que d'attendre la restauration d'une base de données.
- Vérifier que l'espace disque disponible est suffisant pour contenir une base de données restaurée. Allouez suffisamment d'espace disque disponible pour contenir n'importe quelle base de données d'où vous devrez peut-être récupérer des données. Vous pouvez créer un numéro d'unité logique (LUN) dédié de restauration sur chaque serveur de boîtes aux lettres, ou allouer un serveur à utiliser pour les récupérations de base de données.
- Planifier l'utilisation de bases de données de boîtes aux lettres moins volumineuses. Cela est un point important lors des processus de réamorçage, lorsque des données doivent être réamorcées sur un site de récupération d'urgence ou sur un réseau étendu (WAN). Le processus peut être beaucoup plus long lorsque vous utilisez des bases de données de boîtes aux lettres plus volumineuses.

Planification de récupération de serveurs d'accès au client



Le serveur d'accès au client gère toutes les connexions clientes, en autorisant toutes les requêtes des clients et en les acheminant vers la base de données de boîtes aux lettres active appropriée. Il fournit l'authentification, ainsi que les services de redirection et proxy. En revanche, il ne contient pas une grande quantité de données d'utilisateur ou de configuration. Vous pouvez récupérer les fonctions de base des serveurs d'accès au client sans sauvegarder les serveurs existants. Les sauvegardes sont requises uniquement si vous restaurez des options de configuration supplémentaires que vous avez pu définir après l'installation.

Ajout d'un rôle serveur

Une méthode pour remplacer un serveur d'accès au client défaillant est d'ajouter le rôle serveur à un serveur Exchange existant dans le même site. Ainsi, la fonctionnalité peut être récupérée rapidement. Dans la plupart des cas, cette procédure est une solution provisoire, utilisée jusqu'à la reconstruction du serveur, ou au déploiement d'un nouveau serveur de remplacement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Déploiement d'un nouveau serveur

Vous pouvez également déployer un nouveau serveur avec le même rôle serveur pour remplacer un serveur d'accès au client défaillant. Un nouveau rôle serveur d'accès au client remplace la fonctionnalité d'un serveur d'accès au client défaillant après que toutes les configurations nécessaires sont réalisées (comme l'ajout de la configuration d'équilibrage de charge et l'importation du certificat Exchange).

Vous pouvez récupérer le serveur perdu à l'aide du commutateur RecoverServer dans Exchange Server 2013. La plupart des paramètres d'un ordinateur exécutant Exchange Serveur 2013 sont stockés dans Active Directory. Le commutateur RecoverServer reconstruit un serveur Exchange avec le même nom à l'aide des paramètres et des autres informations enregistrées dans Active Directory.

Lorsque vous remplacez un serveur d'accès au client par un nouveau, il est préférable d'effectuer des configurations supplémentaires plutôt que de reconstruire le serveur défaillant. Toutes modifications de configuration apportées aux sites Web et utilisées sur un serveur d'accès au client (par exemple, les options d'authentification) sont perdues lorsque vous remplacez un serveur d'accès au client. Pour que le rôle serveur d'accès au client retrouve à son état de configuration précédent, établissez une liste de vos modifications antérieures afin de pouvoir les appliquer sur le nouveau serveur. Lorsque vous reconstruisez un serveur, ces modifications sont restaurées à partir de la sauvegarde.

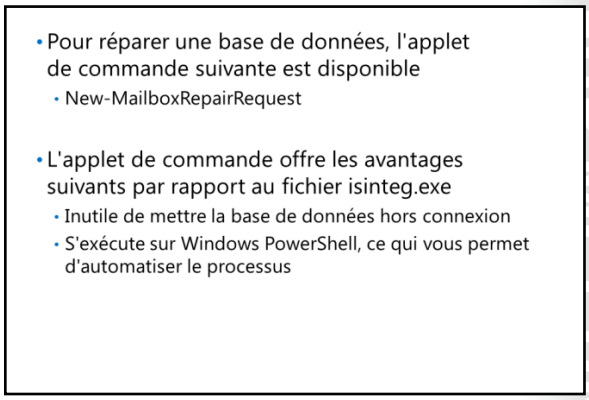
Éléments à prendre en compte pour le déploiement d'un nouveau serveur

Le déploiement d'un nouveau serveur peut vous demander de reconfigurer certaines applications. Par exemple, si vous configurez une passerelle VoIP (Voice over IP) pour communiquer avec le nom DNS ou l'adresse IP du serveur défaillant, elle doit être reconfigurée.

Si vous choisissez de ne pas reconstruire un serveur Exchange défaillant, vous devez la supprimer manuellement d'AD DS à l'aide de l'outil LDP.exe. Cet outil est un client du protocole LDAP (Lightweight Directory Access Protocol) qui permet aux utilisateurs d'exécuter des opérations sur Active Directory.

Réparation d'altération de base de données Exchange Server

Exchange Server 2013 utilise l'applet de commande **New-MailboxRepairRequest** pour détecter et réparer une boîte aux lettres ou une base de données de boîtes aux lettres endommagée tout en gardant la base de données de boîtes aux lettres en ligne. Cette applet de commande a été utilisée pour la première fois sous Exchange Server 2010 Service Pack 1 (SP1).



Remarque : Une fois le processus de réparation lancé à l'aide de ces applets de commande, vous ne pouvez arrêter le processus qu'en démontant la base de données.

Utilisez l'applet de commande **New-MailboxRepairRequest** pour détecter et résoudre les problèmes d'endommagement de boîte aux lettres et de bases de données de boîtes aux lettres. Vous pouvez exécuter cette applet de commande sur une boîte aux lettres ou sur une base de données. Pendant le processus de réparation, seule la boîte aux lettres en cours de réparation est inaccessible ; toutes les autres dans la base de données restent opérationnelles.

L'applet de commande **New-MailboxRepairRequest** détecte et résout les types d'endommagement de boîtes aux lettres suivants :

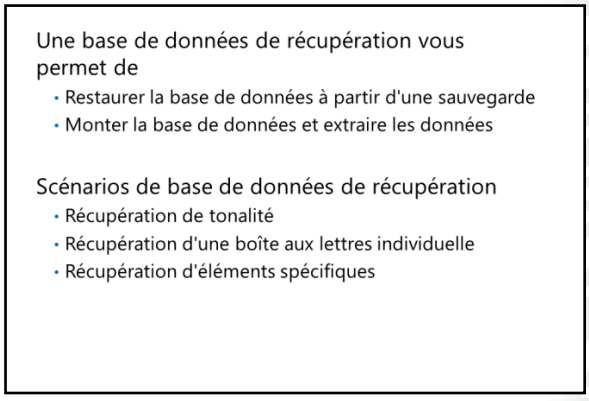
Type d'altération	Description
SearchFolder	Détecte et résout les problèmes relatifs aux dossiers de recherche endommagés.
AggregateCounts	Détecte et résout les problèmes relatifs aux nombres agrégés dans les dossiers non conformes aux valeurs correctes.
FolderView	Détecte et résout les problèmes relatifs aux vues dans les dossiers dont le contenu renvoyé n'est pas correct.
ProvisionedFolders	Détecte et résout les problèmes relatifs aux dossiers configurés qui pointent de manière incorrecte vers des dossiers parents qui ne sont pas configurés.

Par exemple, l'applet de commande suivante détecte et répare tous les éléments endommagés pour la boîte aux lettres de l'utilisatrice Christine :

```
New-MailboxRepairRequest -Mailbox Christine -CorruptionType
ProvisionedFolder,SearchFolder,AggregateCounts,Folderview
```

Processus de récupération de données à l'aide de la base de données de récupération

La base de données de récupération est une base de données récupérée pouvant coexister sur le même serveur qui héberge la base de données d'origine. Les utilisateurs ne peuvent pas y accéder directement. Seuls les administrateurs peuvent y accéder pour récupérer des éléments uniques, des dossiers, des boîtes aux lettres ou des bases de données complètes depuis la base de données de récupération.



La base de données de récupération a été utilisée pour la première fois dans Exchange Server 2010, et a remplacé le groupe de stockage de récupération des versions précédentes d'Exchange. Vous pouvez utiliser l'environnement de ligne de commande Exchange Management Shell pour créer une base de données de récupération.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Récupération de données à l'aide de la base de données de récupération

Pour récupérer des données à l'aide de la base de données de récupération, procédez comme suit :

1. Restaurez la base de données que vous souhaitez récupérer dans la structure de dossiers de la base de données de récupération.
2. Créez une base de données de récupération avec l'environnement de ligne de commande Exchange Management Shell, et configurez-la pour utiliser la base de données et les fichiers journaux de la base de données restaurée.
3. Mettez la base de données restaurée en état d'arrêt correct avec Eseutil /R.
4. Montez la base de données, et fusionnez les données de la boîte aux lettres de base de données de récupération dans la boîte aux lettres de production ou d'archivage de l'utilisateur. Vous pouvez utiliser l'applet de commande de l'environnement de ligne de commande Exchange Management Shell **New-MailboxRestoreRequest** pour effectuer cette tâche.

Dans quels cas utiliser la base de données de récupération

Vous pouvez utiliser la base de données de récupération dans les cas suivants :

- Récupération de tonalité. Lorsque vous implémentez une récupération de tonalité, vous configurez une base de données de boîtes aux lettres de tonalité sur un même serveur ou sur un autre serveur afin de fournir un accès temporaire aux services de messagerie. Vous utilisez alors la base de données de récupération pour restaurer les données temporaires dans la base de données de production une fois que vous avez récupéré la base de données d'origine à partir d'une sauvegarde.
- Récupération d'une boîte aux lettres individuelle. Vous pouvez récupérer des boîtes aux lettres individuelles en restaurant, dans la base de données de récupération, la base de données contenant cette boîte aux lettres. Vous pouvez ensuite extraire les données de la boîte aux lettres supprimée et les copier dans un dossier ou une boîte aux lettres cible de la base de données de production.
- Récupération d'éléments spécifiques. Si un message n'existe plus dans la base de données de production, vous pouvez restaurer la base de données qui contenait ce message dans la base de données de récupération. Vous pouvez ensuite extraire les données de la boîte aux lettres et les copier dans un dossier ou une boîte aux lettres cible de la base de données de production. Toutefois, dans cette situation, vous devriez aussi envisager d'utiliser la stratégie de blocage, car la récupération de la base de données peut être une opération longue.

Démonstration : Procédure de récupération de données en utilisant la base de données de récupération

Procédure de démonstration

1. Utilisez Sauvegarde Windows Server pour restaurer Exchange sur C:\Restaurer.

 **Remarque :** L'activité de sauvegarde de la démonstration précédente doit être terminée avant de poursuivre.

2. Dans l'environnement de ligne de commande Exchange Management Shell, exécutez la commande suivante pour déterminer le GUID et les emplacements de fichiers appropriés :

```
Get-MailboxDatabase –ID “Mailbox Database 1” | fl name, guid, edbfilepath,
logfolderpath
```

3. Dans l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante pour créer la base de données de récupération, puis appuyez sur Entrée.

```
New-MailboxDatabase –Recovery –Name RecoveryDB –EdbFilePath “C:\Restaurer\3c32c739-
a0ce-43bc-a299-2f56f2bcb20c\C_\Program Files\Microsoft\Exchange
Server\V15\Mailbox\Mailbox Database 1808842331\Mailbox Database 1808842331.edb” –
LogFolderPath “C:\Restaurer\GUID\C_\Program Files\Microsoft\Exchange
Server\V15\Mailbox\Mailbox Database 1808842331” –Server LON-MBX1
```

4. Redémarrez le service Banque d'informations Microsoft Exchange.

```
Restart-service msexchangeis
```

5. Dans l'environnement de ligne de commande Exchange Management Shell, accédez au dossier de la base de données de boîtes aux lettres.

```
CD “C:\Restaurer\3c32c739-a0ce-43bc-a299-2f56f2bcb20c\C_\Program
Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1808842331”
```

6. Tapez la commande suivante pour que la base de données de boîtes aux lettres restaurée soit dans un état d'arrêt correct, puis appuyez sur Entrée.

```
Eseutil /r E00 /i /d
```

7. Dans l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante pour monter la base de données de boîtes aux lettres restaurée, puis appuyez sur Entrée.

```
Mount-Database RecoveryDB
```

8. Dans l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante pour répertorier toutes les boîtes aux lettres disponibles dans la base de données de récupération, puis appuyez sur Entrée.

```
Get-MailboxStatistics –Database RecoveryDB
```

9. À l'invite de commande de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante, puis appuyez sur Entrée.

```
New-MailboxRestoreRequest –SourceDatabase RecoveryDB –SourceStoreMailbox “Tony Smith”
–TargetMailbox tony@adatum.com -SkipMerging StorageProviderForSource
```

10. À l'invite de commandes de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante, puis appuyez sur Entrée. Cette commande affiche le statut de la demande de restauration de boîte aux lettres.

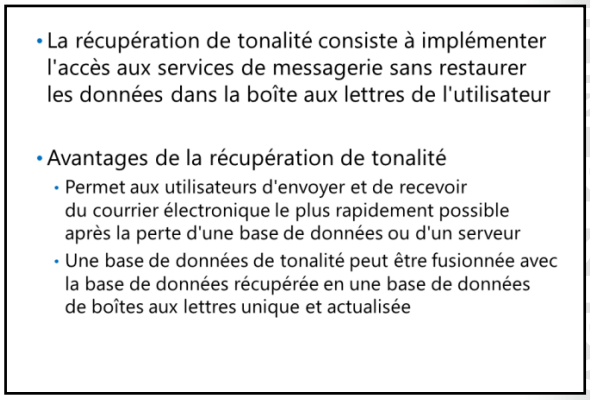
```
Get-MailboxRestoreRequest
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que la récupération de tonalité ?

La récupération de tonalité est un processus dans lequel le service de messagerie électronique est récupéré d'abord pour les utilisateurs en créant une base de données de boîtes aux lettres, appelée base de données de tonalité. La récupération des données des boîtes aux lettres a lieu lors d'une étape ultérieure. Avec la récupération de tonalité, les utilisateurs peuvent envoyer et recevoir des courriers électroniques très rapidement après une perte de serveur ou de base de données. Les utilisateurs peuvent envoyer et recevoir des messages électroniques, mais n'ont pas accès à leurs données de boîte aux lettres. Après la récupération de la base de données de boîtes aux lettres, vous pouvez fusionner le contenu de la base de données de boîtes aux lettres récupérée dans la base de données de tonalité.



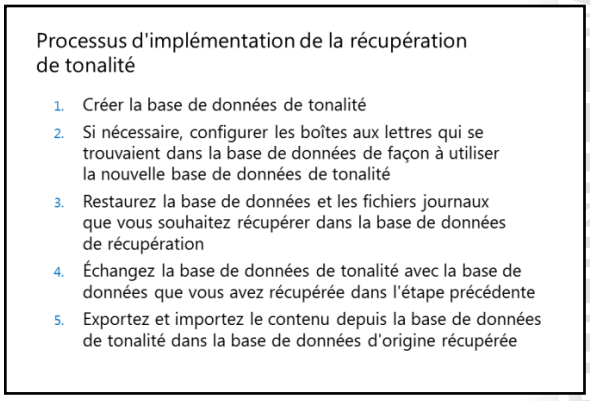
Utilisation de la récupération de tonalité

Utilisez la méthode de récupération de tonalité lorsqu'il est essentiel que les utilisateurs aient de nouveau rapidement accès aux fonctionnalités de messagerie après la perte d'un serveur ou d'une base de données de boîtes aux lettres et lorsque vous devez restaurer le plus vite possible les données d'historique à partir d'une sauvegarde. La perte peut résulter d'une panne matérielle ou de l'altération d'une base de données. Si le serveur échoue, cela demandera un temps considérable pour reconstruire le serveur et restaurer les bases de données. Si la défaillance concerne une base de données volumineuse, sa restauration à partir d'une sauvegarde pourra prendre plusieurs heures.

Si le serveur de boîtes aux lettres d'origine fonctionne toujours ou si vous en disposez d'un autre, vous pouvez restaurer les fonctionnalités de messagerie en quelques minutes en effectuant une récupération de tonalité. Elle permet une utilisation ininterrompue de la messagerie électronique pendant que vous récupérez la base de données ou le serveur défaillant.

Processus d'implémentation de la récupération de tonalité

Il existe plusieurs scénarios de récupération de tonalité, mais tous suivent les mêmes grandes étapes.



Implémentation de la récupération de tonalité

Suivez ces étapes générales pour implémenter la récupération de tonalité :

1. Créez la base de données de tonalité. Pour que les ordinateurs clients de messagerie récupèrent les fonctionnalités dans les meilleurs délais, créez une base de données de boîte aux lettres pour ces ordinateurs clients. Vous pouvez créer la base de données de tonalité de deux façons différentes :
   - Créez la base de données de tonalité sur le même serveur que celui de la base de données défaillante. Cette méthode est à privilégier si le lecteur qui contenait la base de données a connu une défaillance ou si la base de données est endommagée.
   - Créez la base de données de tonalité sur un autre serveur que celui qui héberge la base de données défaillante. Employez cette méthode pour utiliser un autre serveur plutôt que le serveur de récupération ou si le serveur d'origine connaît une défaillance.
2. Configurez les boîtes aux lettres qui se trouvaient dans la base de données défaillante de façon à utiliser la nouvelle base de données de tonalité.
3. Restaurez la base de données et les fichiers journaux que vous souhaitez récupérer dans la base de données de récupération.
4. Échangez la base de données de tonalité avec la base de données que vous avez récupérée dans l'étape précédente.
5. Exportez et importez le contenu depuis la base de données de tonalité dans la base de données d'origine récupérée.

 **Remarque :** Vous n'avez pas besoin de reconfigurer les profils Outlook avec la fonctionnalité de découverte automatique installée, car cette configuration est effectuée automatiquement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Implémentation d'une solution de récupération d'urgence pour Exchange Server 2013

Scénario

Vous êtes administrateur de messagerie chez A. Datum Corporation. Votre organisation a déployé Exchange Server 2013. Vous souhaitez maintenant vérifier que toutes les données Exchange Server sont sauvegardées et que vous pouvez restaurer non seulement l'intégralité du serveur ou de la base de données, mais aussi une boîte aux lettres ou un dossier de boîte aux lettres.

Objectifs

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

- sauvegarder Exchange Server 2013 ;
- restaurer des données Exchange Server.

Configuration de l'atelier pratique

Durée approximative : **75 minutes**

Ordinateurs virtuels	22341B-LON-DC1 22341B-LON-CAS1 22341B-LON-MBX1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

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

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le **Gestionnaire Hyper-V**, cliquez sur **22341B-LON-DC1**, et dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22341B-LON-MBX1** et **22341B-LON-CAS1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Sauvegarde d'Exchange 2013

Scénario

Vous devez créer une sauvegarde de votre base de données de boîtes aux lettres Exchange Server 2013 pour vous assurer que vous pouvez la restaurer, le cas échéant.

Les tâches principales de cet exercice sont les suivantes :

1. Remplir une boîte aux lettres avec Outlook Web App.
2. Installer Sauvegarde Windows Server.
3. Effectuer une sauvegarde d'une base de données de boîtes aux lettres à l'aide de Sauvegarde Windows Server.
4. Supprimer un message d'une boîte aux lettres.

▶ Tâche 1 : Remplir une boîte aux lettres avec Outlook Web App

1. Sur LON-CAS1, ouvrez **Internet Explorer**. Tapez **https://lon-cas1.Adatum.com/owa**.
2. Connectez-vous en tant qu'**Adatum\michael** avec le mot de passe **Pa$$w0rd**.
3. Envoyez un nouveau message électronique à Mark Bebbington dont l'objet est **Message avant de sauvegarder**, puis déconnectez-vous de Outlook Web App.
4. Reconnectez-vous en tant qu'**Adatum\mark** avec le mot de passe **Pa$$w0rd**, et vérifiez que le message est bien arrivé.
5. Déconnectez-vous d'Outlook Web App et fermez Internet Explorer.
6. Sur l'écran Accueil, ouvrez **Exchange Management Shell**, et utilisez la commande suivante pour noter le nom et le GUID de la base de données de boîtes aux lettres associée à Mark Bebbington.

```
Get-Mailbox mark@ADatum.com |fl name,database,guid
```

▶ Tâche 2 : Installer Sauvegarde Windows Server

- Sur LON-MBX1, utilisez le Gestionnaire de serveur pour installer la fonctionnalité Sauvegarde Windows Server.

▶ Tâche 3 : Effectuer une sauvegarde d'une base de données de boîtes aux lettres à l'aide de Sauvegarde Windows Server

1. Sur LON-CAS1, ouvrez l'**Explorateur de fichiers** et créez un dossier nommé **Sauvegarde** sur le lecteur C:\. Partagez ce dossier pour ADATUM\Administrateur avec des autorisations en lecture/écriture. Fermez l'Explorateur de fichiers.
2. Sur LON-MBX1, démarrez **Sauvegarde Windows Server** et effectuez une sauvegarde complète du serveur.
3. À l'emplacement de la sauvegarde, sélectionnez le dossier partagé **\\LON-CAS1\Sauvegarde**, puis sélectionnez **Ne pas hériter** sous **Contrôle d'accès**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Utilisez le compte **Administrateur** avec le mot de passe **Pa$$w0rd** comme informations d'identification.
5. Une fois la sauvegarde terminée avec succès, fermez Sauvegarde Windows Server. Cette opération peut prendre 10 à 15 minutes.

▶ Tâche 4 : Supprimer un message d'une boîte aux lettres

1. Sur LON-CAS1, ouvrez **Internet Explorer**. Tapez **https://lon-cas1.ADatum.com/owa**.
2. Connectez-vous en tant qu'**Adatum\Mark** avec le mot de passe **Pa$$w0rd**.
3. Supprimez le message reçu de Michael.
4. Videz le dossier **Éléments supprimés**, puis dans le dossier **Éléments supprimés**, videz le message dans la fenêtre récupérer les éléments supprimés.
5. Déconnectez-vous d'Outlook Web App.

Résultats : Après avoir terminé cet exercice, vous êtes parvenu à sauvegarder les bases de données de boîtes aux lettres.

Exercice 2 : Restauration de données Exchange Server 2013

Scénario

Certains utilisateurs se plaignent que certains messages sont manquants dans leur boîte aux lettres. Il vous faut donc utiliser la sauvegarde que vous avez créée pour récupérer leurs messages.

Les tâches principales de cet exercice sont les suivantes :

1. Restaurer la base de données à l'aide de la base de données Windows Server.
2. Créer une base de données de récupération à l'aide de l'environnement de ligne de commande Exchange Management Shell.
3. Récupérer une boîte aux lettres à partir de la base de données de récupération.

▶ Tâche 1 : Restaurer la base de données à l'aide de la base de données Windows Server

1. Sur LON-MBX1, ouvrez l'**Explorateur de fichiers** et créez un dossier nommé **C:\Restaurer**.
2. Ouvrez **Sauvegarde Windows Server**, et restaurez la sauvegarde située sur **\\LON-CAS1\Sauvegarde** dans l'autre emplacement **C:\Restaurer**.

▶ Tâche 2 : Créer une base de données de récupération à l'aide de l'environnement de ligne de commande Exchange Management Shell

1. Sur le serveur LON-MBX1, créez une base de données de récupération avec Exchange Management Shell en utilisant la base de données de boîtes aux lettres restaurée dans C:\Restaurer.
2. Redémarrez le service **Banque d'informations Microsoft Exchange**.
3. Dans l'environnement de ligne de commande Exchange Management Shell, passez sur le dossier qui contient la base de données récupérée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Utilisez la commande **eseutil** pour définir la base de données de boîtes aux lettres dans un état d'arrêt correct.
5. Montez la base de données restaurée.
6. Placez toutes les boîtes aux lettres sur cette base de données de boîtes aux lettres récupérée. Vérifiez que Mark Bebbington y figure.

▶ Tâche 3 : Récupérer une boîte aux lettres à partir de la base de données de récupération

1. Sur le serveur LON-MBX1, récupérez la boîte aux lettres de Mark Bebbington à l'aide de l'applet de commande **MailboxRestoreRequest**.
2. Sur LON-CAS1, ouvrez Outlook Web App et vérifiez que la boîte aux lettres et les éléments récupérés y figurent.

Résultats : Après avoir terminé cet exercice, vous aurez restauré avec succès les éléments manquants dans les boîtes aux lettres des utilisateurs.

Exercice 3 : Récupération d'urgence dans Exchange Server 2013 (facultatif)

Scénario

Suite à un dysfonctionnement du disque dur, le serveur d'accès au client Exchange Server 2013 LON-CAS2 n'est plus opérationnel. Vous devez restaurer le serveur avec le mode **/RecoverServer** de la configuration.

Les tâches principales de cet exercice sont les suivantes :

1. Installation d'Exchange Server 2013 en mode de récupération de serveur.
2. Pour préparer le module suivant.

▶ Tâche 1 : Installation d'Exchange Server 2013 en mode de récupération de serveur

1. Sur LON-DC1, réinitialisez le compte d'ordinateur de LON-CAS2 à l'aide de l'outil **Utilisateurs et ordinateurs Active Directory**.
2. Démarrez **22341B-LON-SVR1** et ouvrez une session en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Remplacez l'adresse IP pour l'ordinateur par **172.16.0.21** et l'adresse DNS par **172.16.0.10**.
4. Renommez LON-SRV1 en **LON-CAS2** et joignez le serveur au domaine Adatum.
5. Dans le Gestionnaire Hyper-V, ouvrez les paramètres de 22341B-LON-SVR1, et associez le fichier Exchange iso à partir de **D:\Program Files\Microsoft learning\22341\Drives\ ExchangeServer2013CU1.iso**.
6. Sur LON-CAS2, installez Exchange Server 20103 avec le commutateur RecoverServer.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-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 **22341B-LON-CAS1**, **22341B-LON-SVR1** et **22341B-LON-MBX1**.

Résultats : À la fin de cet exercice, vous aurez correctement récupéré LON-CAS2.

Question : De quelle fonctionnalité avez-vous besoin pour effectuer une sauvegarde locale sur un serveur Exchange 2013 sur lequel le rôle de boîte aux lettres est installé ?

Question : De quel outil avez-vous besoin pour créer une base de données de récupération dans Exchange Server 2013 ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

Complétez ou adaptez les meilleures pratiques suivantes à vos conditions de travail :

- utilisez un DAG pour protéger des bases de données de boîtes aux lettres, dès que vous en avez la possibilité ; la récupération de DAG est plus rapide et plus facile que la récupération de sauvegarde ;
- en cas de perte de base de données, utilisez une base de données de tonalité pour récupérer rapidement la fonctionnalité de base de messagerie ;
- utilisez une base de données de récupération pour récupérer des éléments spécifiques d'une sauvegarde ;
- allouez un espace disque pour une base de données de récupération lors de la conception du stockage du serveur ;
- utilisez la récupération d'élément unique pour éviter que les utilisateurs ne vident les messages avant qu'ils n'atteignent la limite de rétention d'éléments.

Questions de contrôle des acquis

Question : Quels sont les scénarios possibles de perte de données ?

Question : Quelles étapes sont requises dans un processus de récupération de données si la base de données de récupération est utilisée ?

Question : Quelle applet de commande utilisez-vous pour réparer une base de données endommagée ?

Question : Quelles sont les options dont vous disposez pour récupérer les données de boîtes aux lettres ?

Outils

- Centre d'administration Exchange
- Environnement de ligne de commande Exchange Management Shell
- Sauvegarde Windows Server

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 8

Planification et configuration du transport des messages

Table des matières :

Vue d'ensemble du module **8-1**

Leçon 1 : Vue d'ensemble du transport et du routage des messages **8-2**

Leçon 2 : Planification et configuration du transport des messages **8-22**

Leçon 3 : Gestion des règles de transport **8-31**

Atelier pratique : Planification et configuration du transport des messages **8-38**

Contrôle des acquis et éléments à retenir **8-43**

Vue d'ensemble du module

Pour implémenter le transport des messages dans Microsoft® Exchange Server 2013, vous devez tenir compte de plusieurs facteurs. Tout d'abord, il convient de comprendre les composants du transport des messages et comment Exchange Server 2013 route les messages. Vous devez également comprendre comment résoudre les problèmes liés au transport des messages. Enfin, il est important que vous sachiez configurer et appliquer des règles de transport.

Ce module décrit la planification et la configuration du transport des messages dans une organisation Exchange Server 2013.

Objectifs

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

- décrire le transport des messages dans Exchange Server 2013 ;
- planifier et configurer le transport des messages ;
- gérer des règles de transport.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Vue d'ensemble du transport et du routage des messages

Dans cette leçon, vous allez examiner le flux de messages et les composants requis par le transport des messages. Pour comprendre le flux de messages, vous devez comprendre le fonctionnement du routage des messages dans une organisation Exchange Server et le routage des messages entre sites de services de domaines Active Directory® ou à l'extérieur de l'organisation Exchange Server par Exchange Server. Exchange Server 2013 fournit plusieurs outils pour résoudre les problèmes liés à la remise de messages SMTP (Simple Mail Transfer Protocol), et cette leçon décrit comment les utiliser.

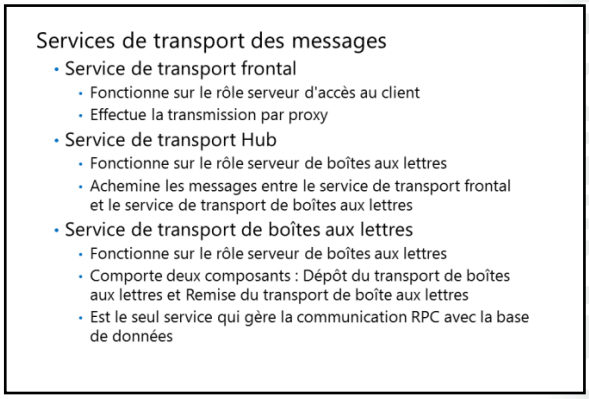
Objectifs de la leçon

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

- décrire les services de transport des messages ;
- décrire les composants du transport des messages ;
- décrire les changements de routage des messages dans Exchange Server 2013 ;
- décrire les destinations de routage et les groupes de remise ;
- décrire le routage dans le service de transport frontal ;
- décrire le routage dans le service de transport de boîtes aux lettres ;
- décrire comment modifier le flux de messages par défaut ;
- décrire et utiliser les outils de résolution des problèmes liés à la remise des messages SMTP ;
- décrire les agents de transport.

Services de transport des messages

Dans une organisation Exchange Server 2013, le transport des messages est effectué via le pipeline de transport. Le pipeline de transport représente l'ensemble des connexions, connecteurs, services, composants et files d'attente qui fonctionnent ensemble pour assurer un routage de messages adéquat.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans Exchange® Server 2007 et Exchange® Server 2010, le routage de messages était effectué par les rôles serveur Transport Hub ou Transport Edge. Dans Exchange Server 2013, les fonctionnalités de ces rôles sont réparties entre le rôle serveur d'accès au client et le rôle serveur de boîtes aux lettres. Plusieurs services fonctionnent sur le serveur d'accès au client et le serveur de boîtes aux lettres pour gérer le routage de messages pour le trafic de messagerie interne et externe.

Les services suivants participent au transport des messages :

- *Service de transport frontal*. Ce service, qui s'exécute sur le serveur d'accès au client, se comporte comme un composant proxy sans état pour l'ensemble du trafic entrant et sortant SMTP externe à l'organisation Exchange. Le service accepte les connexions SMTP d'autres serveurs SMTP sur Internet, reçoit des messages et initialise des connexions SMTP pour l'envoi de messages. Toutefois, il n'assure pas la mise en file d'attente des messages. Bien que ce service ne puisse pas inspecter le contenu des messages, il peut effectuer un filtrage sur les connexions, domaines, expéditeurs ou destinataires IP. En interne, ce service communique uniquement avec le service de transport Hub qui réside sur le rôle serveur de boîtes aux lettres.
- *Service de transport*. Ce service est quasiment identique au rôle serveur de transport Hub dans Exchange Server 2007 et Exchange Server 2010. Il fonctionne sur tous les serveurs de boîtes aux lettres d'une organisation Exchange Server 2013. Ce service gère l'ensemble du flux SMTP interne et effectue la catégorisation des messages et l'inspection du contenu. La différence majeure entre ce service et le rôle serveur de transport Hub des versions précédentes d'Exchange est que le service de transport Hub d'Exchange Server 2013 ne communique jamais directement avec les bases de données de boîtes aux lettres. Le service de transport Hub route les messages entre le service de transport frontal et le service de transport de boîtes aux lettres. Le service de transport de boîtes aux lettres communique ensuite avec la base de données de boîtes aux lettres.
- Service de transport de boîtes aux lettres. Tout comme le service de transport Hub, le service de transport de boîtes aux lettres s'exécute sur un rôle serveur de boîtes aux lettres. Il comporte les composants suivants :
    - Remise du transport de boîtes aux lettres. Ce service reçoit des messages SMTP du service de transport Hub et établit alors la connexion RPC (Remote Procedure Call) avec la base de données de boîtes à lettres pour remettre le message à la boîte aux lettres appropriée.
    - Dépôt du transport de boîtes aux lettres. Ce service fonctionne dans le sens inverse du service de remise du transport de boîtes aux lettres. Alors qu'il connecte également le RPC à la base de données de boîtes aux lettres, son rôle est de récupérer les messages pour les envoyer et non les remettre. Il envoie ensuite les messages reçus au service de transport Hub à l'aide du protocole SMTP. Contrairement au service de transport Hub, le service de transport de boîtes aux lettres ne peut pas effectuer de mise en file d'attente locale des messages.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

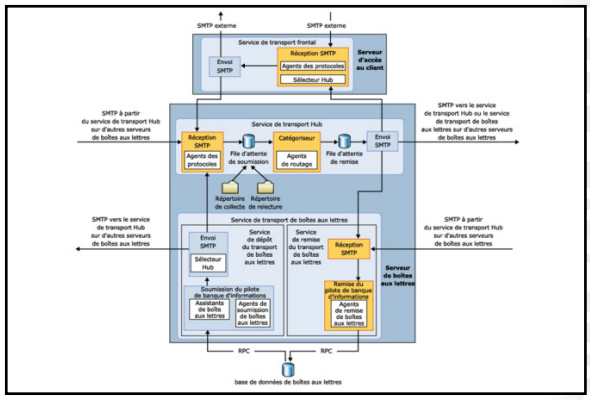
Les messages provenant d'Internet pénètrent dans le pipeline de transport Exchange via un connecteur de réception situé sur le service de transport frontal sur un serveur d'accès au client. Ensuite, les messages sont routés au service de transport Hub sur un serveur de boîtes aux lettres.

Les messages internes à l'organisation parviennent directement au service de transport Hub sur un serveur de boîtes aux lettres via le connecteur de réception, le service de transport de boîtes aux lettres ou la soumission d'agent.

Remarque : Si vous faites déployer un serveur Exchange 2010 ou un serveur de transport Edge Exchange Server 2007 sur votre réseau de périmètre, le flux de messages Internet s'effectue directement entre le service de transport Hub sur le serveur de boîtes aux lettres et le serveur de transport Edge sans passer par le transport frontal sur le serveur d'accès au client.

Composants du transport des messages

Les services de transport qui fonctionnent sur le serveur d'accès au client et le serveur de boîtes aux lettres contiennent plusieurs composants qui jouent des rôles très importants dans le routage de messages. Le schéma sur la diapositive montre ces composants, les directions de routage possibles des messages dans Exchange Server 2013 et les relations entre les composants dans le pipeline de transport.



Réception SMTP

La réception SMTP fonctionne sur le service de transport frontal mais aussi sur le service de transport Hub et le service de transport de boîtes aux lettres. Dans chaque instance, il accepte le trafic SMTP provenant de diverses sources. L'inspection du contenu du message est exécutée lorsqu'un message est reçu par le service de transport Hub. En outre, les règles de transport sont appliquées et une inspection anti-courrier indésirable et anti-programmes malveillants est exécutée. La session SMTP comprend une série d'événements qui fonctionnent ensemble dans un ordre spécifique pour valider le contenu du message avant son acceptation. Lorsqu'un message franchit le processus de réception SMTP sans être rejeté par des événements de réception ou un agent anti-courrier indésirable et anti-programmes malveillants, il est placé dans la file d'attente de soumission.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Envoi SMTP

Le processus d'envoi SMTP fonctionne dans plusieurs emplacements sur le service de transport frontal et le service de transport Hub. Le routage de messages utilise le processus d'envoi SMTP à partir du service de transport Hub et dépend de l'emplacement des destinataires des messages par rapport au serveur de boîtes aux lettres sur lequel la catégorisation s'effectue. Le message peut être routé vers les emplacements ci-dessous.

- Le service de transport de boîtes aux lettres sur le même serveur de boîtes aux lettres.
- Le service de transport de boîte aux lettres sur un serveur de boîtes aux lettres différent qui appartient au même groupe de disponibilité de base de données (DAG).
- Le service de transport Hub sur un serveur de boîtes aux lettres dans un site DAG, AD DS différent ou une forêt AD DS différente.
- Le service de transport frontal sur un serveur d'accès au client pour la remise sur Internet.

Catégoriseur

Toutes les décisions de routage sont prises pendant un processus appelé catégorisation des messages. Le catégoriseur est un composant du service de transport Hub qui classe les messages par catégorie. Le catégoriseur traite tous les messages et décide de ce qu'il doit faire de chaque message selon sa destination. Il récupère également les messages dans la file d'attente de soumission, les traite et les transfère dans la file d'attente de remise.

Chacun de ces processus est décrit ci-dessous.

- Identification et vérification des destinataires. Tous les messages doivent avoir une adresse SMTP valide à identifier.
- Bifurcation des messages entre plusieurs destinataires. L'extension des listes de distribution active l'identification de chaque destinataire appartenant à la liste de distribution. En outre, le catégoriseur traite le chemin de retour pour les notifications d'état de remise (DSN) de liste de distribution et détermine si les messages d'absence du bureau ou les réponses générées automatiquement sont envoyés à l'expéditeur initial du message.
- Détermination d'itinéraires de routage. Lors de la détermination de l'itinéraire de routage, le catégoriseur identifie la destination, laquelle doit être la boîte aux lettres d'un utilisateur, un dossier public ou un serveur d'expansion pour les groupes de distribution. Si le catégoriseur ne peut pas déterminer une destination valide, un rapport de non-remise (NDR) est généré.
- Conversion du format du contenu. Les destinataires peuvent avoir besoin de messages dans différents formats. Le catégoriseur convertit le message au format approprié pour le destinataire. Dans l'organisation Exchange, le format du destinataire est stocké dans AD DS. Les messages routés vers Internet sont envoyés au format MIME (Multipurpose Internet Mail Extensions) ou S/MIME (Secure/Multipurpose Internet Mail Extensions).
- Application de stratégies pour les messages de l'organisation. Vous pouvez utiliser des stratégies de l'organisation pour contrôler les aspects des messages, par exemple la taille des messages, les autorisations pour envoyer des messages à des utilisateurs spécifiques, le nombre de destinataires d'un message, etc.

Répertoires de collecte et de relecture

La plupart des messages entrent dans le pipeline de transport des messages via le composant de réception SMTP ou par soumission via le pilote de banque d'informations. Toutefois, les messages peuvent entrer dans le pipeline de transport des messages en étant placés dans le répertoire de collecte ou de relecture du serveur de boîtes aux lettres.

Lorsqu'un message a été placé dans le répertoire de collecte, le pilote de banque d'informations l'ajoute à la file d'attente de soumission. Le pilote de banque d'informations le supprime ensuite du répertoire de collecte. Les messages provenant du répertoire de collecte doivent être des fichiers texte conformes au format de message SMTP de base et les autorisations de lecture et d'écriture doivent être configurées.

Le répertoire de collecte permet au service de transport Hub de traiter et remettre un fichier texte formaté correctement. Cette opération peut s'avérer utile pour valider le flux de messagerie dans une organisation, relire des messages spécifiques ou renvoyer un courrier électronique récupéré dans le pipeline de transport des messages. Par ailleurs, certaines applications héritées peuvent placer des messages directement dans le répertoire de collecte pour leur remise envoi et ne pas communiquer directement avec les connecteurs de réception SMTP Exchange Server.

Voici un exemple de message en texte brut utilisant un formatage valide pour le répertoire de collecte.

```
À : mary@contoso.com
De : bob@adatum.com
Objet : objet du message
Corps du message
```

Le répertoire de relecture est utilisé pour soumettre de nouveau les messages Exchange exportés et recevoir des messages de serveurs de passerelle étrangers. Ces messages sont déjà formatés pour le répertoire de relecture. Il n'est pas vraiment utile que les administrateurs ou les applications rédigent et déposent les nouveaux fichiers de messages via le répertoire de relecture. Vous pouvez utiliser le répertoire de collecte pour créer et envoyer de nouveaux fichiers de messages.

Voici un exemple de message en texte brut utilisant un formatage valide pour le répertoire de relecture :

```
X-Receiver: <mary@contoso.com> NOTIFY=NEVER ORcpt= mary@contoso.com
X-Sender: <bob@adatum.com> BODY=7bit ENVID=12345AB auth=<someAuth>
Objet : Optional message subject
Corps du message
```

Pilote de banque d'informations

Le pilote de banque d'informations est un composant logiciel présent dans le service de transport de boîtes aux lettres des composants Dépôt du transport de boîtes aux lettres et Remise du transport de boîtes aux lettres. Le pilote de banque d'informations récupère des messages dans la boîte d'envoi de l'expéditeur, puis les envoie au composant sélecteur Hub. Il utilise également le RPC pour remettre les messages reçus dans la boîte aux lettres de l'utilisateur.

Lorsque le pilote de banque d'informations a ajouté les messages à la file d'attente de soumission, il les déplace de la boîte d'envoi de l'expéditeur dans le dossier Éléments envoyés de l'expéditeur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les messages figurant dans la boîte d'envoi sont enregistrés au format MAPI (Messaging Application Programming Interface). Le pilote de banque d'informations doit les convertir au format STNEF (Summary Transport Neutral Encapsulation Format) avant de les placer dans la file d'attente de soumission. Le pilote de banque d'informations exécute cette conversion pour vérifier que les messages ont été remis correctement indépendamment du format qui a créé les messages.
Un message encodé en TNEF (Transport Neutral Encapsulation Format) contient une version en texte brut du message et une pièce jointe binaire qui contient diverses autres parties du message initial.

Certaines fonctionnalités Microsoft Outlook® requièrent l'encodage TNEF pour être interprétées correctement par un destinataire Internet qui utilise également Outlook. Par exemple, lorsque vous envoyez un message avec des boutons de vote à un destinataire via Internet, si TNEF n'est pas activé pour ce destinataire, les boutons de vote ne seront pas reçus. Si le pilote de banque d'informations ne parvient pas à convertir le contenu, il génère un rapport de non-remise (ou notification d'échec de remise).

File d'attente de soumission

Lorsque le service de transport Microsoft Exchange démarre, le catégoriseur crée une seule file d'attente de soumission dans chaque service de transport Hub. La file d'attente de soumission stocke tous les messages sur un disque jusqu'à ce que le catégoriseur les traite avant de les remettre. Le catégoriseur ne peut pas traiter de message si le serveur de transport ne transfère pas ce message dans la file d'attente de soumission. Pendant que le catégoriseur traite un message, une copie de ce message demeure dans la file d'attente de soumission. Une fois le traitement effectué, le message est supprimé du catégoriseur et de la file d'attente de soumission.

Les messages peuvent entrer dans la file d'attente de soumission des manières indiquées ci-dessous.

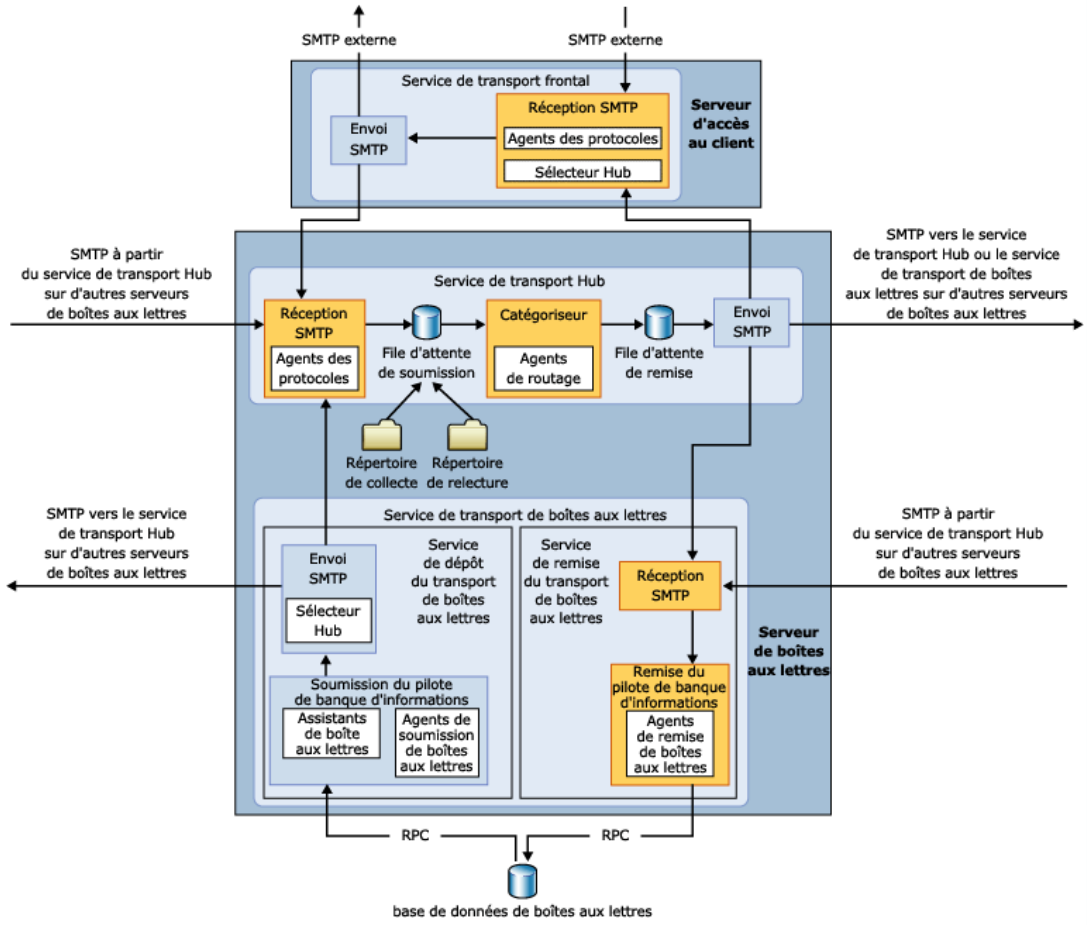
- Messages reçus par un connecteur de réception SMTP. Utilisez cette méthode pour les messages entrants en provenance d'Internet ou d'un client à l'aide du protocole POP3 (Post Office Protocol version 3) ou du protocole IMAP4 (Internet Message Access Protocol version 4).
- Messages placés dans les répertoires de collecte ou de relecture. Cette méthode est utilisée pour la résolution des problèmes et les applications héritée.
- Messages envoyés par un agent de transport, par exemple un connecteur non Microsoft, à un système de messagerie étranger.
- Messages soumis par le pilote de banque d'informations. Cette méthode est utilisée pour récupérer des messages de la boîte d'envoi de l'expéditeur.
- Nouvelle soumission des messages après un échec de remise. Le catégoriseur soumet de nouveau les messages qui ne sont pas remis à la première tentative. Vous pouvez également soumettre de nouveau les messages manuellement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

File d'attente de remise

Les files d'attente de remise contiennent les messages qu'Exchange Server n'a pas remis. Les messages figurant dans la file d'attente de remise sont envoyés au composant d'envoi SMTP et, selon leur itinéraire de remise prévu, ils peuvent être transférés à un autre serveur de boîtes aux lettres ou au composant de réception SMTP sur le même serveur de boîtes aux lettres.

Le diagramme ci-après illustre les composants et services du transport des messages dans l'infrastructure Exchange Server 2013.

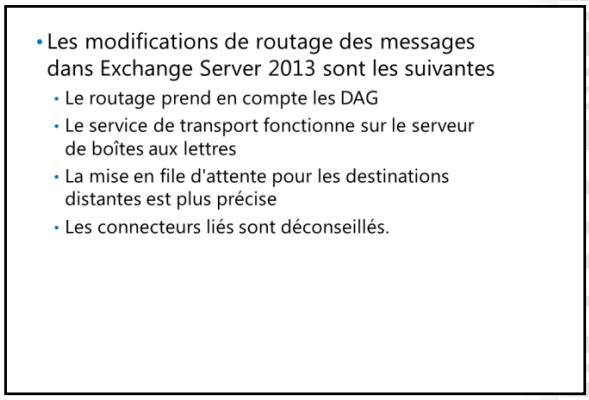


UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Modifications du routage des messages dans Exchange Server 2013

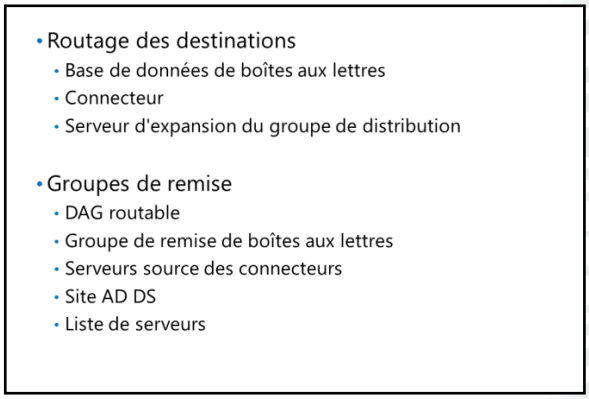
Exchange Server 2013 assure un routage de messages amélioré par rapport aux versions précédentes d'Exchange Server. Dans Exchange Server 2013, le routage de messages est intégré au serveur d'accès au client et au rôle serveur de boîtes aux lettres et est également fonctionnellement différent.



Les améliorations et changements les plus importants du routage de messages sont indiqués ci-dessous.

- Dans Exchange Server 2013 le routage utilise désormais des DAG comme limite de routage. Étant donné que chaque serveur de boîtes aux lettres héberge également des services de transport, lorsque les DAG sont implémentés, le mécanisme de routage s'aligne étroitement avec le DAG. De plus, si un DAG couvre plusieurs sites AD DS, il est beaucoup plus efficace d'utiliser le DAG comme limite de routage que comme topologie de site AD DS. Toutefois, si les DAG ne sont pas implémentés, le routage de messages s'appuie sur la topologie de site AD DS pour définir la limite de routage de messages. Le même concept est appliqué à l'interopérabilité de routage dans les versions précédentes d'Exchange Server.
- Le service de transport sur le rôle serveur de boîtes aux lettres se compose de deux services principaux : le service de transport Hub et le service de transport de boîte aux lettres. Le service de transport de boîtes aux lettres, ou pour être plus précis, ses composants Remise de transport de boîtes aux lettres et Soumission de transport de boîtes aux lettres, sont les seuls composants de transport qui interagissent directement avec la base de données de boîtes aux lettres. RPC est utilisé par le pilote de banque d'informations lors de l'envoi ou de la réception de messages vers ou depuis la base de données de boîtes aux lettres. Lorsque le serveur de boîtes aux lettres est membre d'un DAG, le service de transport de boîte aux lettres utilise uniquement RPC pour communiquer localement avec les copies actives des bases de données de boîtes aux lettres. Cela signifie que RPC n'est jamais utilisé pour la communication entre les serveurs ou les composants de transport. Ce type de communication et la communication entre le service de transport de boîtes aux lettres et le service de transport Hub sont établis si vous utilisez le protocole SMTP.
- Exchange Server 2013 utilise une mise en file d'attente plus précise pour les destinations distantes que la version précédente d'Exchange. Au lieu d'utiliser une seule file d'attente pour toutes les destinations dans un site Active Directory distant, Exchange Server 2013 met en file d'attente les messages pour les destinations spécifiques dans le site Active Directory, par exemple les différents connecteurs d'envoi.
- Dans Exchange Server 2013, les connecteurs liés sont déconseillés. Dans les versions précédentes d'Exchange, un connecteur lié était un connecteur de réception qui était lié à un connecteur d'envoi. Tous les messages reçus par le connecteur de réception étaient transmis automatiquement au connecteur d'envoi.

Routage des destinations et des groupes de remise



Chaque message envoyé a une source et une destination. La destination définitive de chaque message dans une organisation Exchange Server 2013 est appelée destination de routage. Il existe plusieurs types de destinations de routage, notamment :

- Base de données de boîtes aux lettres. Lorsqu'un message est envoyé à un utilisateur avec une boîte aux lettres sur le serveur de boîtes aux lettres dans une organisation Exchange, la destination de routage du message est la base de données de boîtes aux lettres. Cela s'applique également aux dossiers publics, lesquels sont un type de boîte aux lettres dans Exchange Server 2013.
- Connecteur. Un connecteur est utilisé comme destination de routage lorsqu'il est configuré comme connecteur d'envoi pour les messages SMTP. Un connecteur d'agent de remise ou un connecteur étranger est utilisé comme destination de routage pour les messages non SMTP.
- Serveur d'expansion du groupe de distribution. Si un groupe de distribution a un serveur d'expansion dédié, ce serveur est une destination de routage pour les messages envoyés au groupe de distribution.

Groupes de remise

Les groupes de remise sont la collection de serveurs de transport chargés de remettre les messages à une destination de routage spécifique. Chaque destination de routage a son propre groupe de remise. Les serveurs de transport d'un groupe de remise peuvent être des serveurs de boîtes aux lettres Exchange Server 2013 ou des serveurs de transport Hub Exchange Server 2010.

Dans les scénarios où la destination de routage est la base de données de boîtes aux lettres, les serveurs de transport du groupe de remise ont toujours la même version d'Exchange Server que la base de données de boîtes aux lettres. Dans les cas où la destination de routage est un connecteur ou un serveur d'expansion de groupe de distribution, les serveurs de transport peuvent être des serveurs de boîtes aux lettres Exchange Server 2013 ou des serveurs de transport Hub Exchange Server 2010.

L'itinéraire de routage de messages dépend des relations entre le serveur de transport source et le groupe de remise. Lorsque le serveur de transport source appartient au groupe de remise de destination, la destination de routage est en fait le prochain saut pour le message. Sinon, si le serveur de transport source n'appartient pas au groupe de remise de destination, le message est relayé à l'aide de l'itinéraire de routage le plus économique. Dans cet itinéraire, le message peut être relayé à d'autres serveurs de transport ou le message est relayé directement à un serveur de transport du groupe de remise de destination.

Le message peut également être remis au connecteur ou au serveur de transport du groupe de remise.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsqu'un serveur d'expansion du groupe de distribution est la destination de routage, le groupe de distribution est déjà développé avant que les messages n'atteignent le stade de catégorisation sur le serveur d'expansion du groupe de distribution. La destination de routage à partir du serveur d'expansion de groupe de distribution est toujours une base de données de boîtes aux lettres ou un connecteur.

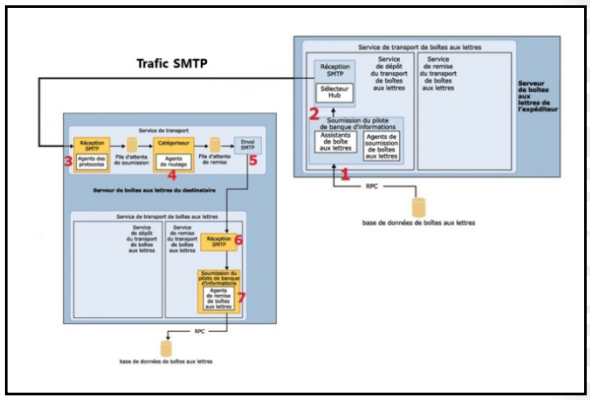
Il existe plusieurs types de groupes de remise dans Exchange Server 2013, notamment :

- *DAG routable*. Il s'agit de l'ensemble des serveurs Exchange Server 2013 qui sont membres du même DAG. Toutes les bases de données de boîtes aux lettres du DAG sont des destinations de routage pour ce groupe de remise. Lorsque le message arrive, le service de transport Hub sur le serveur de boîtes aux lettres l'accepte et le route vers le service de transport de boîtes aux lettres du serveur de boîtes aux lettres qui contient actuellement la copie active de la base de données de destination. Le service de transport de boîtes aux lettres utilise le composant Remise de transport pour remettre le message à la base de données de boîtes aux lettres. Dans ce cas, le DAG est la limite du groupe de remise.
- *Groupe de remise de boîtes aux lettres*. Il s'agit de l'ensemble des serveurs Exchange qui exécutent la même version d'Exchange Server dans un site AD DS unique qui est la limite du groupe de remise. Les bases de données de boîtes aux lettres situées sur des serveurs de boîtes aux lettres Exchange Server 2010 sont gérés par les serveurs de transport Hub Exchange Server 2010 situés dans le site AD DS. Les bases de données de boîtes aux lettres situées sur les serveurs de boîtes aux lettres Exchange Server 2013 dans le site AD DS (ceux qui n'appartiennent pas à un DAG) sont gérés par le service de transport Hub sur les serveurs de boîtes aux lettres Exchange Server 2013 dans le site AD DS. Le message est remis à l'aide de différentes techniques, en fonction de l'emplacement de la destination finale. Si le message arrive sur le serveur de boîtes aux lettres 2013, le service de transport Hub le transfère au service de transport de boîtes aux lettres avec SMTP et le service de transport de boîtes aux lettres utilise RPC pour remettre le message à la base de données. Si le message arrive sur le serveur de transport Hub Exchange Server 2010, le lecteur de magasin du transport Hub utilise RPC pour écrire le message dans la base de données de boîtes aux lettres.
- *Serveurs source des connecteurs*. Les serveurs source des connecteurs sont un ensemble combiné de serveurs de transport Hub Exchange Server 2010 et de serveurs Exchange Server 2013 désignés comme serveurs source du connecteur d'envoi, du connecteur d'agent de remise ou du connecteur étranger dans le même site AD DS ou un site AD DS différent. Le connecteur est la destination de routage. Lorsqu'un connecteur est limité en étendue à un serveur spécifique, seul ce serveur est autorisé à router des messages vers la destination définie par le connecteur.
- *Site AD DS*. Lorsque le site AD DS n'est pas la destination finale d'un message mais que le message doit passer par ce site, vous devez utiliser le site AD DS comme groupe de remise. Vous pouvez le faire si un site AD DS est désigné comme site Hub ou que le serveur Exchange Edge est abonné au site spécifique et que d'autres sites ne peuvent pas y accéder directement.
- *Liste de serveurs*. La liste de serveurs est la collection d'un ou plusieurs serveurs de transport Hub Exchange Server 2010 ou serveurs de boîtes aux lettres Exchange Server 2013 qui sont configurés comme serveurs d'expansion de groupe de distribution. Le serveur d'expansion de groupe de distribution est la destination de routage qui est gérée par ce groupe de remise.

L'appartenance au groupe de remise du serveur n'est pas exclusive. Par exemple, un serveur de boîtes aux lettres Exchange Server 2013 qui appartient à un DAG peut être aussi le serveur source d'un connecteur d'envoi étendu. Ce serveur de boîtes aux lettres appartiendrait au groupe de remise DAG routable pour les bases de données de boîtes aux lettres du DAG et aussi à un groupe de remise de serveur source de connecteur dans le connecteur d'envoi limité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Flux de messagerie dans Exchange Server 2013

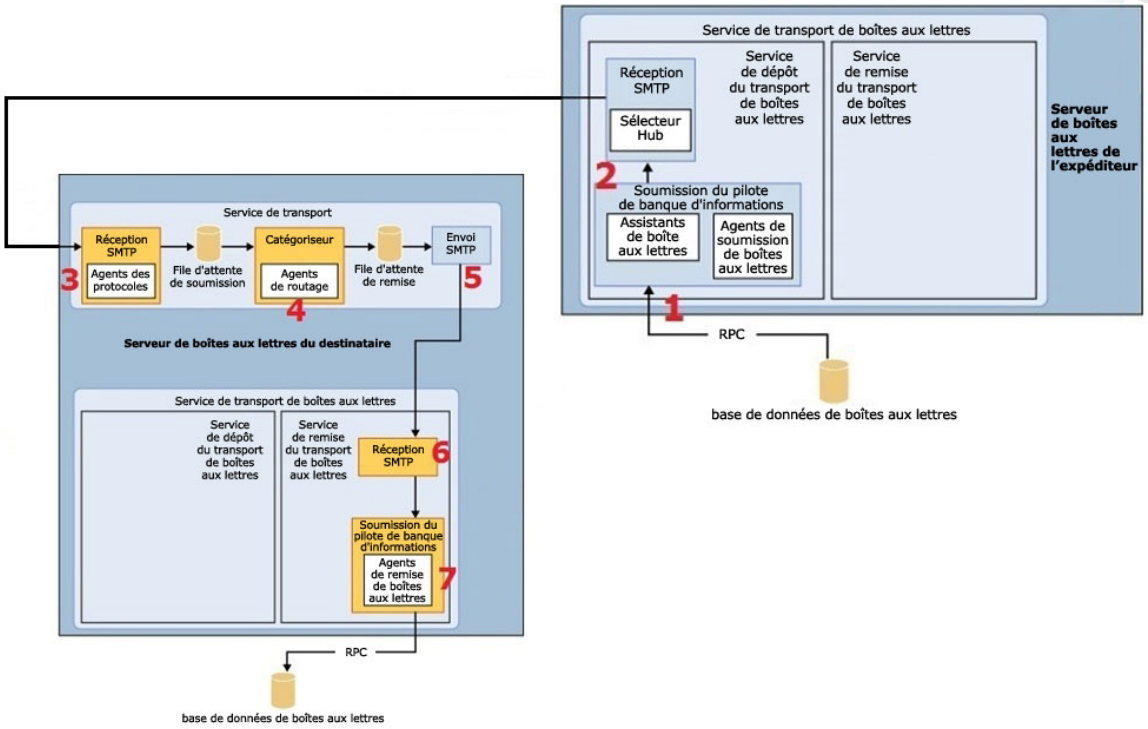


Pour mieux comprendre le fonctionnement du flux de messagerie dans Exchange Server 2013, suivez les étapes ci-après. Elles décrivent le flux de messagerie interne lorsque l'utilisateur sur le serveur de boîtes aux lettres 1 envoie un message à l'utilisateur sur le serveur de boîtes aux lettres 2 au sein de la même organisation Exchange.

1. Lorsque l'utilisateur envoie le message à partir du client Outlook, le service de dépôt de transport de boîtes aux lettres utilise le pilote de banque d'informations pour la connexion à la base de données de boîtes aux lettres via RPC et récupère le courrier électronique dans la Boîte d'envoi de l'utilisateur.
2. Une fois le message reçu dans la base de données de boîtes aux lettres, le service de dépôt de transport de boîtes aux lettres recherche le groupe de remise approprié. Dans le cas présent, il s'agit du groupe de remise de boîtes aux lettres. Le pilote de banque d'informations envoie le courrier électronique au sélecteur Hub, puis celui-ci est envoyé via SMTP au serveur approprié. Il est important de noter que, dans ce cas, le courrier électronique n'est pas transmis au service de transport sur le serveur de boîtes aux lettres de l'expéditeur. Au lieu de cela, c'est le service de dépôt de transport de boîtes aux lettres qui envoie le message directement au service de transport sur le serveur de boîtes aux lettres du destinataire. Si la destination est routable vers le groupe de disponibilité de base de données (DAG), le message est transmis directement du service de transport de boîtes aux lettres sur le serveur de boîtes aux lettres de l'expéditeur vers le service de transport de boîtes aux lettres sur le serveur de boîtes aux lettres du destinataire.
3. Le service de transport sur le serveur de boîtes aux lettres du destinataire reçoit le courrier électronique envoyé via SMTP par le service de dépôt de transport de boîtes aux lettres du serveur de boîtes aux lettres de l'expéditeur en utilisant son connecteur de réception par défaut. L'inspection du contenu est exécutée, des règles de transport sont appliquées, et une inspection anti-courrier indésirable/anti-programmes malveillants est effectuée (si cette fonction est activée). Si le message satisfait à toutes ces inspections, il est placé dans la file d'attente de soumission.
4. Le catégoriseur récupère le courrier électronique dans la file d'attente de soumission, le traite et le place dans une file d'attente de remise de la base de données de boîtes aux lettres locale.
5. Le courrier électronique est ensuite envoyé via SMTP par le service de transport au service de remise du transport de boîtes aux lettres sur le serveur de boîtes aux lettres du destinataire.
6. Le courrier électronique est reçu via SMTP par le service de remise du transport de boîtes aux lettres en provenance du service de transport :
7. Le service de remise du transport de boîtes aux lettres utilise le pilote de banque d'informations pour la connexion à la base de données de boîtes aux lettres via RPC et écrit le courrier électronique dans la base de données de boîtes aux lettres. C'est à ce stade que le destinataire reçoit le message.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

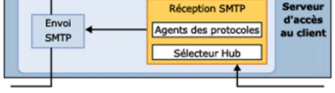
Le diagramme ci-après illustre le flux de messagerie dans Exchange 2013.



Routage dans le service de transport frontal

Le service de transport frontal s'exécute sur chaque serveur d'accès au client. Il agit comme proxy pour l'ensemble du trafic SMTP entrant et sortant pour l'organisation Exchange. Sur le plan du trafic SMTP, son rôle est semblable à celui du serveur de transport Edge dans Exchange Server 2007 ou Exchange Server 2010, mais il existe une différence notable : le serveur d'accès au client ne peut pas effectuer de mise en file d'attente des messages.

- Le service de transport frontal sert de proxy SMTP pour toutes les connexions entrantes et sortantes
- Il communique uniquement avec le service de transport Hub sur le serveur de boîtes aux lettres
- Vous pouvez utiliser les groupes de remise suivants
  - DAG routable
  - Groupe de remise de boîtes aux lettres
  - Site AD DS



Le service de transport Hub sur le serveur de boîtes aux lettres utilise le connecteur d'envoi pour communiquer avec le serveur de transport frontal. Si le paramètre **FrontEndProxyEnabled** est défini sur true, tous les messages sortants sont transmis par proxy via le service de transport frontal sur le serveur d'accès au client lorsque vous créez le connecteur d'envoi sur le serveur de boîtes aux lettres. Dans ce cas, lorsque le message est envoyé sur Internet, c'est le serveur d'accès au client qui est le composant qui envoie le message au serveur SMTP de destination.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque le message arrive en provenance d'Internet, le service de transport frontal accepte la connexion SMTP, puis tente de trouver un service de transport Hub disponible sur le serveur de boîtes aux lettres pour recevoir le message. Étant donné que le service de transport frontal ne peut pas mettre les messages en file d'attente sur lui-même, s'il ne trouve pas de service de transport Hub disponible, le service de messagerie électronique sera perçu comme indisponible par les expéditeurs externes.

Le service de transport frontal génère les tables de routage sur la base des informations issues d'AD DS et utilise des groupes de remise pour déterminer comment router les messages. Toutefois, le service de transport frontal n'est jamais considéré comme membre d'un groupe de remise, même lorsque le serveur de boîtes aux lettres et le serveur d'accès au client sont installés sur le même serveur physique. Par conséquent, le service de transport frontal communique seulement avec le service de transport Hub. En outre, les tables de routage ne contiennent pas les routes des connecteurs d'envoi. Ils contiennent à la place une liste spéciale de serveurs de boîtes aux lettres dans le site AD DS local.

Le service de routage de transport frontal trouve toujours les bases de données de boîtes aux lettres appropriées des destinataires de messages. La liste des serveurs de boîtes aux lettres que le service de transport frontal utilise est basée sur les bases de données de boîtes aux lettres des destinataires de messages. Toutefois, il est possible qu'aucun des destinataires n'ait de boîtes aux lettres. Par exemple, lorsque le destinataire est un groupe de distribution ou un utilisateur de messagerie, un serveur de boîtes aux lettres aléatoire du site local AD DS est sélectionné pour la remise.

Le service de transport frontal recherche le groupe de remise approprié pour chaque base de données de boîtes aux lettres, puis tente de trouver les informations de routage associées. Voici la liste des groupes de remise que le service de transport frontal peut utiliser :

- DAG routable.
- Groupe de remise de boîtes aux lettres.
- Site AD DS.

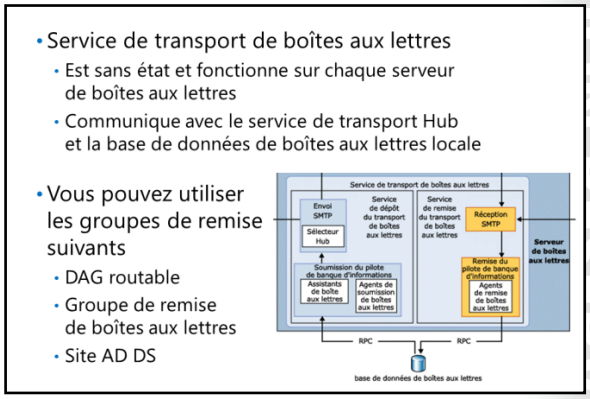
Lorsque le serveur frontal accepte le message, il consulte le nombre et le type de destinataires et effectue alors l'une des opérations ci-dessous :

- Si le message a un seul destinataire avec une boîte aux lettres, le service de transport frontal sélectionne un serveur de boîtes aux lettres dans le groupe de remise cible. Si le groupe de remise cible couvre plusieurs sites, le service de transport frontal accordera la priorité au serveur de boîtes aux lettres basé sur la proximité du site AD DS.
- Si le message a plusieurs destinataires de boîtes aux lettres, le service de transport frontal utilise les 20 premiers destinataires pour sélectionner un serveur de boîtes aux lettres dans le groupe de remise le plus proche.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Routage dans le service de transport de boîtes aux lettres

Le service de transport de boîtes aux lettres, qui s'exécute sur tous les serveurs de boîtes aux lettres dans une organisation Exchange Server 2013, se compose de deux services : le service de dépôt du transport de boîtes aux lettres et le service de remise du transport de boîtes aux lettres. Le service de transport de boîtes aux lettres est sans état et ne met pas les messages en file d'attente localement.



Comme le service de transport Hub, le service de transport de boîtes aux lettres génère les tables de routage en fonction des informations issues d'AD DS. Le service de transport de boîtes aux lettres utilise également les groupes de remise pour le routage de messages.

Le service de transport de boîtes aux lettres appartient toujours au même groupe de remise que le serveur de boîtes aux lettres et ce groupe est appelé le groupe de remise local. Ce service n'envoie également pas les messages automatiquement au service de transport Hub dans son groupe de remise local. Le service de transport de boîtes aux lettres communique uniquement avec le service de transport Hub sur les serveurs de boîtes aux lettres et avec les bases de données de boîtes aux lettres sur le serveur de boîtes aux lettres local. Il ne communique jamais avec les bases de données de boîtes aux lettres sur les autres serveurs de boîtes aux lettres.

Lorsqu'un message est envoyé depuis la boîte aux lettres de l'utilisateur, le composant Dépôt du transport du service de transport de boîtes aux lettres résout le destinataire du message dans la base de données de boîtes aux lettres appropriée, puis le composant Dépôt de transport recherche les informations de routage pour chaque base de données de boîtes aux lettres.

Les groupes de remise utilisés par le service de dépôt de transport de boîtes aux lettres sont :

- DAG routable.
- Groupe de remise de boîtes aux lettres.
- Site AD DS.

Selon le nombre et le type de destinataires du message, le service de dépôt de transport de boîtes aux lettres effectue l'une des actions suivantes :

- Si le message a un seul destinataire avec une boîte aux lettres, le service de transport de boîtes aux lettres sélectionne un serveur de boîtes aux lettres dans le groupe de remise cible. Si le groupe de remise cible couvre plusieurs sites, le service de transport frontal accorde la priorité au serveur de boîtes aux lettres en fonction de la proximité du site AD DS.
- Si le message a plusieurs destinataires de boîtes aux lettres, le service de transport de boîtes aux lettres utilise les 20 premiers destinataires pour sélectionner un serveur de boîtes aux lettres dans le groupe de remise le plus proche.
- S'il n'y a aucun destinataire de boîtes aux lettres dans le message, le service de transport de boîtes aux lettres sélectionne un serveur de boîtes aux lettres dans le groupe de remise local.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Le service de transport de boîtes aux lettres communique avec le service de transport Hub. Le message peut être accepté ou rejeté pour remise à la base de données de boîtes aux lettres locale lorsque le message est envoyé du service de transport Hub au service de transport de boîtes aux lettres. La remise du message peut être acceptée ou rejetée si le destinataire réside dans une copie active d'une base de données de boîtes aux lettres locale. Toutefois, si le destinataire ne se trouve pas dans la copie active de la base de données de boîtes aux lettres locale, le service de transport de boîtes aux lettres fournit une réponse de non-remise au service de transport Hub.

Une réponse de non-remise se produit lorsqu'une copie active de la base de données de boîtes aux lettres locale est déplacée sur un autre serveur de boîtes aux lettres et que le service de transport Hub n'a pas encore les informations mises à jour. Dans ce cas, le service de transport de boîtes aux lettres émet un rapport de non-remise (NDR) pour le service de transport Hub avec des instructions indiquant de réessayer la remise, de générer un NDR ou de rerouter le message.

Modification du flux de messages par défaut

Lorsqu'un message est remis à un groupe de remise distant, un itinéraire de routage doit être déterminé pour ce message. Un itinéraire de routage est calculé selon l'itinéraire de routage le plus économique en ajoutant le coût des liens de sites IP qui doivent être parcourus pour atteindre la destination. Si la destination est un connecteur, le coût attribué à l'espace d'adressage est ajouté au coût pour atteindre le connecteur sélectionné. Si plusieurs itinéraires de routage sont possibles, l'itinéraire de routage présentant le coût global le plus bas est utilisé.

- Vous pouvez modifier le flux de messages par défaut en effectuant les opérations suivantes
  - Configuration de sites Hub
    - Applet de commande Set-ADSite –Identity nom_site –HubSiteEnabled $true
  - Configuration des coûts de routage spécifiques à Exchange
    - Set-AdSiteLink –Identity nom_lien_sites_AD –ExchangeCost valeur
  - Configuration de serveurs d'expansion pour les groupes de distribution

Dans Exchange Server 2010, le destinataire du message était lié à un seul site AD DS spécifique. Par conséquent, il n'y avait qu'un seul itinéraire de routage économique entre la source et la destination. Toutefois, dans Exchange Server 2013, un groupe de remise peut couvrir plusieurs sites AD DS, ce qui signifie que plusieurs itinéraires de routage économiques peuvent exister vers ces différents sites AD DS. En conséquence, Exchange Server 2013 désigne un site AD DS unique dans le groupe de remise de destination comme site principal.

Dans certains cas, il est possible de modifier la configuration de routage de messages par défaut. Cela s'effectue en configurant des sites AD DS spécifiques comme sites Hub et en attribuant des coûts de routage propres à Exchange Server aux liens de sites AD DS. Les sites hub sont des sites centraux que vous définissez pour router des messages.

Par défaut, le service de transport Hub d'un site essaie de remettre des messages à un destinataire dans un autre site en établissant une connexion directe avec le service de transport Hub dans le site AD DS distant. Toutefois, vous pouvez la topologie de routage des messages par défaut de trois manières : en configurant des sites Hub, en configurant les coûts de routage propres à Exchange et en configurant des serveurs d'expansion pour les groupes de distribution.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de sites Hub

Vous pouvez configurer un ou plusieurs sites AD DS de votre organisation comme des sites Hub. En présence d'un site Hub sur l'itinéraire de routage le plus économique entre deux serveurs de boîtes aux lettres, les messages sont routés vers un serveur de boîtes aux lettres du site Hub pour être traités avant d'être relayés au serveur de destination.

Le service de transport Hub route un message via un site Hub uniquement si ce site existe le long de l'itinéraire de routage le plus économique. Le serveur de boîtes aux lettres initial commence toujours par calculer l'itinéraire le plus économique, puis vérifie si l'un des sites de l'itinéraire est un site Hub. En l'absence de site Hub sur cet itinéraire, le service de transport Hub tente une connexion directe.

Utilisez l'applet de commande suivante pour configurer un site en tant que site Hub :

```
Set-ADSite –Identity nom_site –HubSiteEnabled $true
```

Utilisez l'applet de commande suivante pour vérifier si vous avez configuré un site Hub :

```
Get-AdSite | Format-List Name,HubSiteEnabled
```

Configuration des coûts de routage spécifiques à Exchange

Vous pouvez également modifier la topologie de routage de messages par défaut en attribuant un coût propre à Exchange à un lien de sites IP Active Directory. Si vous attribuez un coût propre à Exchange au lien de sites, le service de transport Hub détermine l'itinéraire de routage le plus économique en utilisant cet attribut plutôt que le coût affecté à Active Directory, sauf si le serveur de boîtes aux lettres est un membre du DAG.

Utilisez l'applet de commande suivante pour attribuer un coût de routage propre à Exchange à un lien de sites IP Active Directory :

```
Set-AdSiteLink –Identity nom_lien_sites_AD –ExchangeCost valeur
```

Vous pouvez également attribuer une limite maximale de taille de message pour les messages envoyés entre les sites AD DS à l'aide de l'applet de commande suivante :

```
Set-AdSiteLink –Identity nom_lien_sites_AD – MaxMessageSize valeur
```

Pour vérifier si vous avez configuré correctement un coût Exchange, exécutez l'applet de commande suivante :

```
Get-AdSite | Format-List Name,HubSiteEnabled
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de serveurs d'expansion pour les groupes de distribution

Vous pouvez également modifier la topologie de routage par défaut en définissant des serveurs d'expansion pour les groupes de distribution. Par défaut, lorsqu'un message est envoyé à un groupe de distribution, le premier service de transport Hub qui reçoit le message développe la liste de distribution et détermine comment router le message à chaque destinataire de la liste. Si vous configurez un serveur d'expansion pour la liste de distribution, tous les messages envoyés à la liste de distribution sont transférés au serveur de transport Hub spécifié. Ce serveur développe ensuite la liste et distribue les messages. Par exemple, vous pouvez utiliser des serveurs d'expansion pour les groupes de distribution basés sur emplacement pour vérifier que le service de transport Hub local les résout.

Remarque : Lors du déploiement d'Exchange Server 2013, vous pouvez être amené à réviser la conception du site AD DS pour ajuster les liens de sites IP et les coûts des liens de sites afin d'optimiser la distribution ramifiée retardée au lieu de la file d'attente au point de défaillance.

Outils de résolution des problèmes liés à la remise des messages SMTP

Exchange Server 2013 comporte plusieurs outils pour résoudre les problèmes de remise de messages SMTP.

- Afficheur des files d'attente
  - Permet d'afficher et de gérer les messages non remis
- Journaux de suivi et rapports de remise
  - Permet de confirmer la remise des messages
- Enregistrement dans le journal de protocole
  - Permet de fournir des informations de niveau de protocole détaillées
- Telnet
  - Permet de vérifier si le port SMTP répond ou d'envoyer directement un courrier SMTP à un connecteur
- Site Web Analyseur de connectivité à distance
  - Permet de tester la connectivité aux services Exchange depuis Internet

Remarque : Exchange Server 2013 s'appuie sur la configuration du site AD DS pour le routage de messages. Par conséquent, pour résoudre un problème de routage de messages, vous devrez peut-être utiliser des outils AD DS pour valider ou modifier le site, le lien de sites ou les informations de sous-réseau IP, et pour vérifier la réplication AD DS. Vous pouvez utiliser l'outil Sites et services Active Directory pour afficher les sous-réseaux IP et les liens de sites.

Utilisation de l'Afficheur des files d'attente

Les messages en attente d'être traités ou remis dans Exchange Server 2013 résident dans les files d'attente de messages sur les serveurs de boîtes aux lettres Exchange Server. Toutes ces files d'attente de messages constituent un outil de diagnostic pratique pour localiser et identifier les messages qui n'ont pas été remis. Pour gérer les files d'attente, vous pouvez utiliser l'Afficheur des files d'attente d'Exchange ou l'environnement de ligne de commande Exchange Management Shell. Les fonctionnalités d'Exchange Server 2013 ont simplifié les files d'attente. Le service de transport Hub gère les files d'attente ci-dessous.

- *File d'attente de soumission*. La file d'attente de soumission contient les messages traités par le catégoriseur.
- *File d'attente de remise distante*. Il existe une file d'attente pour chaque domaine SMTP sortant vers lequel le service de transport Hub route les courriers électroniques.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- *File d'attente des messages incohérents*. La file d'attente des messages incohérents contient les messages qui pourraient provoquer un incident au niveau du serveur.
- *File d'attente de remise de boîtes aux lettres*. Il existe une file d'attente pour chaque serveur de boîtes aux lettres auquel le service de transport Hub peut remettre des messages.
- *File d'attente inaccessible*. La file d'attente inaccessible contient les messages que le service de transport Hub ne peut pas router vers la destination appropriée.

Vous pouvez afficher les files d'attente présentes sur un serveur de boîtes aux lettres en accédant à l'Afficheur des files d'attente Exchange dans la boîte à outils.

Pour gérer des files d'attente de messages à partir de l'environnement de ligne de commande Exchange Management Shell, utilisez les applets de commande suivantes :

- Get-Queue
- Get-Message

De plus, les tâches suivantes peuvent être exécutées sur les files d'attente et les messages en file d'attente à partir de l'environnement de ligne de commande Exchange Management Shell :

- Suspend-Queue et Resume-Queue
- Retry-Queue
- Suspend-Message et Resume-Message
- Remove-Message

Suivi des messages

La fonction de suivi de messages permet également de résoudre les problèmes de flux de messages. Par défaut, le suivi des messages est activé sur les serveurs de boîtes aux lettres. Ces journaux sont conservés 30 jours, la taille maximale de l'ensemble des fichiers journaux étant limitée à 250 Mo. Vous pouvez utiliser l'applet de commande **set-TransportServer** dans l'environnement de ligne de commande Exchange Management Shell pour modifier les paramètres par défaut. Si vous souhaitez explorer les journaux de suivi, vous pouvez utiliser l'applet de commande Get-MessageTrackingLog.

Dans Exchange Server 2013, vous utilisez les rapports de remise du Centre d'administration Exchange pour effectuer le suivi des messages. L'outil de suivi de messages ne fournit pas le même niveau de détail que les journaux de suivi. Par exemple, lorsque vous envoyez un message d'un serveur Exchange à un autre, tous deux situés dans le même site AD DS, les noms de serveur Exchange n'apparaissent pas dans les rapports de remise. Toutefois, les journaux de suivi fournissent ces informations.

Utilisation de l'enregistrement dans le journal de protocole

L'enregistrement dans le journal de protocole peut être configuré pour fournir des informations détaillées pour la résolution des problèmes liés au flux de messages. La fonction d'enregistrement dans le journal de protocole est activée dans les propriétés du connecteur d'envoi SMTP ou du connecteur de réception SMTP. Les fichiers journaux sont stockés dans le dossier C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\ProtocolLog.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Utilisation de Telnet

Telnet peut vérifier si le port SMTP répond, et il peut envoyer un courrier SMTP à un connecteur pour vérifier si le connecteur l'accepte. Telnet est une fonctionnalité de ligne de commande de Windows Server qui utilise la syntaxe suivante : telnet <nomserveur> SMTP ou n° du port. Vous pouvez utiliser par exemple TELNET LON-EX1 SMTP ou TELNET LON-EX1 25, qui sont fondamentalement identiques.

Site Web Analyseur de connectivité à distance

Le site Web suivant vous permet de tester la connectivité à différents services Exchange depuis Internet et les fonctionnalités de ces services : https://www.testexchangeconnectivity.com/.

Vous pouvez également tester le trafic de messagerie entrant et sortant qui utilise le protocole SMTP. Vous pouvez utiliser ce site Web pour tester un serveur Exchange local ainsi que Exchange Online dans Microsoft Office 365. Pour utiliser cet outil, vous devez entrer les informations d'identification d'un compte de travail dans le domaine Exchange que vous souhaitez tester.

 **Remarque :** Pour ne pas risquer que les informations d'identification de votre compte de travail soient utilisées et compromettent la sécurité de votre environnement de serveur Exchange, nous vous conseillons fortement de créer un compte test dans le but d'utiliser cet outil et de supprimer ce compte immédiatement après avoir exécuté le test de connectivité.

Démonstration : Comment résoudre les problèmes liés à la remise des messages SMTP

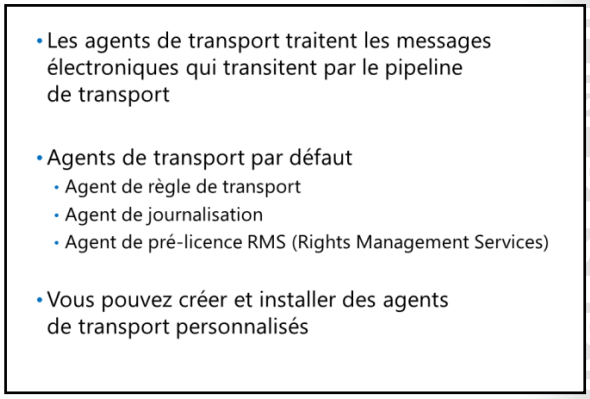
Procédure de démonstration

1. Ouvrez la fenêtre Invite de commandes.
2. Pour démarrer l'outil Telnet, à l'invite de commandes, tapez **Telnet LON-MBX1 SMTP** et essayez d'envoyer un message électronique à l'aide de Telnet.
3. Sur **LON-MBX1**, dans l'**écran d'accueil**, démarrez l'outil **Afficheur des files d'attente**.
4. Suspendez et reprenez la file d'attente **Dépôt**.
5. Fermez l'**Afficheur des files d'attente**.
6. Ouvrez **Exchange Outlook Web App** et connectez-vous en tant qu'administrateur.
7. Envoyez un message à Amr@adatum.com et un à Amr@contoso.com.
8. Ouvrez le Centre d'administration Exchange sur LON-CAS1, et dans Flux de messagerie – Rapports de remise, recherchez les messages que l'administrateur a envoyés.
9. Affichez le rapport de suivi de remise des messages.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les agents de transport ?

Les agents de transport traitent les messages électroniques qui transitent par le pipeline de transport sur les composants du service de transport. Les agents de transport personnalisés apportent des fonctionnalités supplémentaires à Exchange Server 2013, telles que des programmes anti-courrier indésirable ou des programmes antivirus, ou toute fonction de transport dont votre organisation peut avoir besoin. Vous pouvez installer des agents de transport personnalisés sur Exchange Server 2013 sous forme de composants logiciels supplémentaires.



Exchange Server 2013 comprend les agents de transport suivants qui lui permettent de fournir des fonctionnalités telles que les règles et la journalisation de transport :

- *Agent de règle de transport*. L'agent de règle de transport traite les règles de transport sur les serveurs de transport Hub. Il déclenche l'événement de transport OnRoutedMessage. Les règles de transport configurées sur les serveurs de transport Hub sont enregistrées dans AD DS, ce qui les rend donc accessibles à tous les serveurs de transport Hub de l'organisation Exchange. Cela permet à Exchange Server d'appliquer uniformément un jeu de règles unique à l'ensemble de l'organisation.
- *Agent de journalisation*. L'agent de journalisation est un agent de transport axé sur la conformité, qui traite les messages sur les serveurs de transport Hub. Il déclenche les événements de transport OnSubmittedMessage et OnRoutedMessage. Lorsque vous activez la journalisation standard sur une base de données de boîtes aux lettres, ces informations sont enregistrées dans AD DS et sont lues par l'agent de journalisation pendant le processus de journalisation des messages.
- *Agent de pré-licence RMS (Rights Management Services)*. Vous pouvez utiliser l'agent de pré-licence Active Directory Rights Management Services (AD RMS) pour certifier l'authenticité du destinataire Outlook, de sorte que le destinataire puisse ouvrir des messages sans être invité à entrer ses informations d'identification à chaque tentative. Il déclenche l'événement de transport OnRoutedMessage.

Remarque : Les agents de transport ont un accès complet à tous les messages qu'ils traitent. Exchange ne place aucune restriction sur le comportement d'un agent de transport. Par conséquent, les agents de transport qui sont instables ou contiennent des failles de sécurité peuvent affecter la stabilité et la sécurité d'Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Planification et configuration du transport des messages

La planification du transport des messages est une part importante de n'importe quel déploiement d'infrastructure Exchange. Vous devez comprendre comment gérer le flux de messagerie et comment configurer les domaines de messagerie hébergés par votre serveur Exchange. Vous devez aussi savoir comment configurer et gérer les connecteurs Envoi et réception SMTP, qui sont les composants principaux nécessaires à l'établissement du flux de messages.

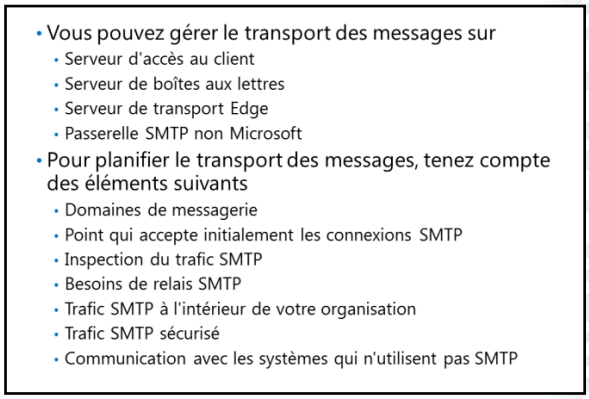
Objectifs de la leçon

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

- planifier le transport des messages Exchange ;
- décrire les paramètres de flux de messages ;
- planifier les domaines acceptés et distants ;
- créer et configurer les domaines acceptés et distants ;
- décrire les connecteurs SMTP ;
- créer et configurer les connecteurs SMTP ;
- décrire les connecteurs étrangers.

Planification du transport des messages Exchange

Avant de configurer réellement le composant de transport dans votre infrastructure Exchange Server 2013, il importe que vous planifiez soigneusement votre trafic SMTP en général et que vous identifiez les routes, les itinéraires et les points de transition pour le transport des messages.



Dans une infrastructure Exchange Server 2013, vous pouvez configurer et gérer le transport SMTP sur les éléments ci-dessous.

- Serveur d'accès au client qui héberge le service de transport frontal.
- Serveur de boîtes aux lettres, qui héberge le service de transport Hub et le service de transport de boîtes aux lettres.
- Serveur de transport Edge 2007 ou 2010, si implémenté.
- Passerelle SMTP non Microsoft, si implémentée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous devez prendre en compte les éléments ci-dessous lorsque vous planifiez le transport des messages :

- Pour quels domaines de messagerie accepterez-vous le trafic SMTP ? Vous devez identifier tous les noms de domaine de messagerie pour lesquels votre organisation acceptera des messages. Vous devez également identifier les noms de domaine pour lesquels vous accepterez et transférerez des messages.
- Quel composant accepte initialement les connexions SMTP ? Les connexions SMTP peuvent être configurées sur le serveur d'accès au client ou le serveur de transport Edge. Certains pare-feu peuvent également accepter et inspecter le trafic SMTP.
- Sur quel point implémentez-vous l'inspection du trafic SMTP pour les virus et les programmes malveillants ? Vous pouvez implémenter une solution antivirus tierce locale à cet effet ou vous pouvez utiliser la protection anti-programmes malveillants intégrée. Vous pouvez également utiliser Exchange Online Protection pour la protection anti-programmes malveillants.
- Votre réseau contient-il des hôtes qui ont besoin du relais SMTP ? Vous pouvez avoir des applications ou des services qui doivent envoyer des messages électroniques en les relayant via votre serveur Exchange. Il est très important que vous identifiiez ces services pour pouvoir configurer correctement les options de relais des messages électroniques.
- Disposez-vous de connexions fiables pour le trafic SMTP à l'intérieur de votre organisation ? Par exemple, dans certains cas, les serveurs peuvent ne pas être bien connectés et cela peut affecter le transport des messages SMTP.
- Allez-vous implémenter le trafic SMTP sécurisé avec une autre organisation ? Dans certains scénarios, vous devrez implémenter des connecteurs SMTP dédiés sécurisés avec le protocole TLS (Transport Layer Security) pour le transport des messages entre votre organisation et une autre organisation Exchange.
- Avez-vous besoin de communiquer directement avec une organisation qui n'utilise pas SMTP pour sa messagerie ?

Après avoir répondu à ces questions et fourni les détails nécessaires, vous aurez suffisamment d'informations pour configurer correctement votre structure de transport de messagerie à l'intérieur de l'organisation et également vers et depuis Internet.

Démonstration : Examen des paramètres du flux de messages

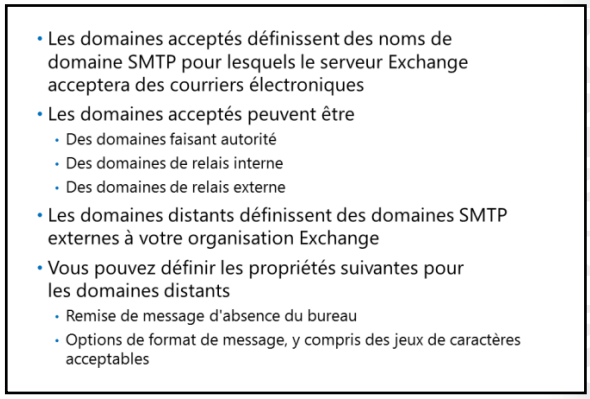
Procédure de démonstration

1. Sur LON-CAS1, basculez vers le Centre d'administration Exchange.
2. Accédez à **Flux de messagerie**.
3. Parcourez tous les onglets de la section Flux de messagerie.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification des domaines acceptés et des domaines distants

Dans le cadre du processus de configuration du transport des messages, vous devez configurer les domaines pour lesquels le serveur Exchange acceptera des messages électroniques et éventuellement configurer les utilisateurs avec d'autres adresses de messagerie.



Domaines acceptés

Les trois types de domaines ci-dessous sont disponibles lorsque vous créez un domaine accepté.

- Domaine faisant autorité. Sélectionnez cette option si les destinataires utilisant ce nom de domaine ont des boîtes aux lettres dans l'organisation Exchange Server.
- Domaine de relais interne. Sélectionnez cette option si votre serveur Exchange doit accepter les courriers électroniques mais les relayer à une autre organisation de messagerie dans une autre forêt AD DS. Dans un domaine de relais interne, les destinataires n'ont pas de boîtes aux lettres dans cette organisation Exchange mais disposent de contacts dans la liste d'adresses globale (LAG). Lorsque des messages sont envoyés aux contacts, le service de transport les transfère sur un autre serveur SMTP. Exchange Server ne génère pas de NDR pour les destinataires dont il n'est pas responsable, car il ne fait pas autorité pour le domaine de relais interne.
- Domaine de relais externe. Sélectionnez cette option si votre serveur Exchange doit accepter les courriers électroniques, mais relayez-les à un autre serveur SMTP. Dans ce scénario, le service de transport reçoit les messages adressés aux destinataires du domaine de relais externe, puis achemine ces messages vers le système de messagerie électronique du domaine de relais externe. Cette opération requiert un connecteur d'envoi du serveur de transport au domaine de relais externe.

Par défaut, seul le domaine racine de la forêt est établi comme domaine accepté. Vous devez penser à ajouter des domaines acceptés supplémentaires dans les situations ci-dessous.

- Espaces de noms supplémentaires. Si vous avez des domaines supplémentaires dans votre forêt, en particulier des arborescences supplémentaires qui représentent différents espace de noms, vous pouvez envisager d'ajouter des domaines faisant autorité pour eux. Si vous ajoutez un domaine faisant autorité pour une arborescence ou un domaine supplémentaire de votre forêt AD DS, vous devez également créer une stratégie d'adresse de messagerie pour prendre en charge le domaine.
- Fusions et acquisitions. Lorsque votre organisation acquiert une autre organisation, vous pouvez décider de configurer un domaine accepté pour faciliter le relais interne vers l'organisation acquise.
- Relais externe. Vous devez configurer un domaine accepté pour prendre en charge le relais SMTP externe. À la différence d'un relais interne sur lequel votre organisation Exchange Server achemine des messages à un serveur Exchange dans une autre forêt AD DS, un relais externe achemine des messages lorsque vous transmettez par relais à un hôte SMTP extérieur à votre organisation. Un fournisseur de services Internet (ISP) peut configurer un relais externe pour un client.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Domaines distants

Les domaines distants définissent des domaines SMTP externes à votre organisation Exchange Server. Vous pouvez créer des entrées de domaine distant pour définir les paramètres de transfert de message entre l'organisation Exchange Server 2013 et des domaines extérieurs à votre forêt de services Active Directory. Lorsque vous créez une entrée de domaine distant, vous contrôlez les types de messages envoyés à ce domaine. Vous pouvez également appliquer des stratégies de format de message et des jeux de caractères acceptables aux messages envoyés par des utilisateurs de votre organisation au domaine distant.

Les paramètres des domaines distants déterminent les paramètres de configuration globaux de l'organisation Exchange Server.

Vous pouvez créer des entrées de domaine distant pour définir les paramètres de transfert de message entre l'organisation Exchange Server 2013 et un domaine extérieur à votre forêt AD DS. Lorsque vous créez une entrée de domaine, vous fournissez un nom pour aider l'administrateur à identifier le rôle de l'entrée lorsqu'il affiche les paramètres de configuration.

Le nom de domaine est limité à 64 caractères. Vous fournissez également le nom de domaine auquel cette entrée et les paramètres associés s'appliquent. Vous pouvez insérer un caractère générique dans le nom de domaine pour inclure tous les sous-domaines. Le caractère générique doit figurer au début de l'entrée du nom de domaine. Le nom de domaine SMTP est limité à 256 caractères.

Les paramètres par défaut peuvent être adaptés à la plupart des situations, mais si vous travaillez avec une organisation partenaire, vous pouvez choisir de créer un domaine distant pour son espace de noms SMTP, puis configurer les paramètres spécifiques en conséquence. Vous pouvez également choisir de définir votre domaine Office 365 comme votre domaine distant.

Démonstration : Création et configuration des domaines acceptés et distants

Procédure de démonstration

1. Dans le Centre d'administration Exchange, accédez à **Flux de messagerie**.
2. Dans l'onglet **Domaine accepté**, créez un domaine accepté nommé **adatum.local** de type relais interne.
3. Ouvrez l'**environnement de ligne de commande Exchange Management Shell**.
4. Passez en revue la liste des domaines distants.
5. Créez un domaine distant appelé **contoso.com**.
6. Examinez tous les paramètres du domaine distant contoso.com.
7. Définissez les propriétés **AutoForwardEnabled** et **DeliveryReportEnabled** du domaine distant Contoso sur **false**.

Définition d'un connecteur SMTP ?

- Les connecteurs SMTP sont des composants Exchange Server qui prennent en charge des connexions SMTP unidirectionnelles
- Connecteurs de réception SMTP par défaut
  - <nom_serveur> par défaut (HubTransport)
  - Proxy client <nom_serveur> (HubTransport)
  - Frontal par défaut <nom_serveur> (FrontendTransport)
  - Frontal proxy sortant <nom_serveur> (FrontendTransport)
  - Frontal client <nom_serveur> (FrontendTransport)
- Aucun connecteur d'envoi SMTP n'est créé et doit être créé manuellement

Un connecteur SMTP est un composant de serveur Exchange qui prend en charge des connexions SMTP unidirectionnelles qui routent le courrier entre le service de transport Hub et le service de transport frontal ou entre les serveurs de transport Hub et Internet. Vous créez et gérez les connecteurs SMTP à partir du Centre d'administration Exchange ou de l'environnement de ligne de commande Exchange Management Shell.
Exchange Server 2013 fournit deux types de connecteurs SMTP : les connecteurs de réception SMTP et les connecteurs d'envoi SMTP. Pour permettre l'envoi ou la réception de messages via SMTP sur un serveur Exchange, au moins deux connecteurs SMTP doivent être disponibles sur ce serveur.

Que sont les connecteurs de réception SMTP ?

Exchange Server 2013 nécessite un connecteur de réception SMTP pour accepter un courrier électronique SMTP. Ce type de connecteur permet à un service de transport Exchange de recevoir des courriers électroniques de toute autre source SMTP, y compris des programmes de messagerie SMTP comme Windows Mail et des serveurs SMTP sur Internet, des serveurs de transport Edge ou d'autres serveurs SMTP Exchange Server.

Vous créez des connecteurs de réception SMTP sur chaque serveur exécutant le rôle d'accès au client ou de serveurs de boîtes aux lettres. Vous pouvez configurer plusieurs connecteurs de réception SMTP avec des paramètres différents sur un même serveur Exchange. Dans les grandes entreprises, plusieurs connecteurs de réception SMTP peuvent être utilisés sur un même serveur ou sur plusieurs serveurs. Dans les PME, seuls deux connecteurs (un connecteur d'envoi et un connecteur de réception) peuvent être utilisés pour l'ensemble de l'organisation. Par défaut, la taille maximale de message pour un nouveau connecteur de réception est égale à 35 Mo.

Vous devez configurer un port pour chaque connecteur de réception SMTP sur lequel le connecteur va recevoir des connexions, des adresses IP locales utilisées pour les connexions entrantes, ainsi qu'un sous-réseau IP distant pouvant envoyer le courrier à ce connecteur de réception SMTP. La combinaison de ces trois propriétés doit être unique pour chaque connecteur de réception SMTP de l'organisation. Lorsque vous installez Exchange Server 2013, les connecteurs de réception sont créés par défaut sur les services de transport de boîtes aux lettres et le service de transport frontal.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Connecteurs de réception par défaut sur le service de transport de boîtes aux lettres

Lorsque vous installez un rôle serveur de boîtes aux lettres, deux connecteurs de réception sont créés automatiquement. Aucun connecteur de réception supplémentaire n'est nécessaire une opération Exchange normale d'échange, et dans la plupart des cas, les connecteurs par défaut ne nécessitent pas de modification de configuration. Ces connecteurs sont les suivants :

- *<nom_serveur> par défaut*. Accepte les connexions authentifiées des serveurs de boîtes aux lettres exécutant le service de transport et des serveurs Edge. Ce connecteur a le rôle de transport Hub et accepte les connexions sur le port 2525.
- *Proxy client <nom_serveur>*. Ce connecteur accepte les connexions des serveurs frontaux. Il a le rôle de transport Hub, accepte les connexions sur le port 465 (SMTP sécurisé) et nécessite une authentification.

Connecteurs de réception par défaut sur un service de transport frontal

Pendant l'installation, les connecteurs de réception ci-dessous sont créés sur le serveur d'accès au client.

- *Frontal par défaut <nom_serveur>*. Le connecteur accepte les connexions des expéditeurs SMTP sur le port 25. C'est le point d'entrée de messagerie commun dans l'organisation Exchange. Ce connecteur accepte les connexions non authentifiées (anonymes) non et a un rôle de transport frontal.
- *Proxy frontal sortant <nom_serveur>*. Ce connecteur accepte les messages d'un connecteur d'envoi sur un serveur principal, avec le proxy frontal activé. Il accepte les connexions sur le port 717.
- *Client frontal <nom_serveur>*. Ce connecteur accepte les connexions authentifiées des clients tels que Windows Mail pour envoyer des messages électroniques. Il fonctionne sur le port 587. Ce connecteur a un rôle de transport frontal.

 **Remarque :** Dans une installation classique, aucun connecteur de réception supplémentaire n'est requis.

Que sont les connecteurs d'envoi SMTP ?

Un ordinateur Exchange Server 2013 requiert un connecteur d'envoi SMTP pour envoyer du courrier électronique SMTP et du courrier électronique à un serveur SMTP sur Internet ou à n'importe quel serveur SMTP de la même organisation Exchange Server.

Par défaut, aucun connecteur d'envoi SMTP n'est configuré sur les serveurs de boîtes aux lettres ou d'accès au client, sauf pour les connecteurs d'envoi SMTP implicites. Ces derniers sont créés dynamiquement pour communiquer avec les services de transport situés dans d'autres sites.

N'oubliez pas les relations entre le service de transport frontal sur le serveur d'accès au client et le service de transport sur les serveurs de boîtes aux lettres dans Exchange Server 2013, car les connecteurs d'envoi fonctionnent différemment dans Exchange Server 2013 que dans les versions précédentes d'Exchange Server. Vous pouvez désormais définir un connecteur d'envoi dans le service de transport sur un serveur de boîtes aux lettres pour router le courrier sortant via un serveur de transport frontal dans le site AD DS local à l'aide du paramètre **FrontEndProxyEnabled** de l'applet de commande **Set-SendConnector**. Cela vous permet de gérer comment le courrier électronique est routé depuis le service de transport.

La taille de message maximale par défaut est définie par le paramètre **MaxMessageSize**. Par défaut, la taille de message maximale pour un nouveau connecteur d'envoi est égale à 10 Mo. L'applet de commande **Set-SendConnector** fournit plus d'informations sur la façon de définir des paramètres sur un connecteur d'envoi.

En outre, le paramètre **TlsCertificateName** a été ajouté. Il authentifie le certificat local à utiliser pour les connexions sortantes et réduit le risque de certificats frauduleux.

Comment gérer les connecteurs SMTP

Vous pouvez utiliser le Centre d'administration Exchange ou l'environnement de ligne de commande Exchange Management Shell pour créer, configurer et consulter les connecteurs SMTP. Dans le Centre d'administration Exchange, les connecteurs de réception SMTP peuvent être configurés pour chaque serveur de transport Hub, tandis que les connecteurs d'envoi sont configurés dans le nœud Configuration de l'organisation. Pour gérer les connecteurs à l'aide de l'environnement de ligne de commande, utilisez les applets de commande **Set-ReceiveConnector** et **Set-SendConnector**. Si vous configurez incorrectement les connecteurs de réception SMTP, cela peut ouvrir le relais sur le serveur de messagerie. Par conséquent, vous devez tester la configuration avec soin.

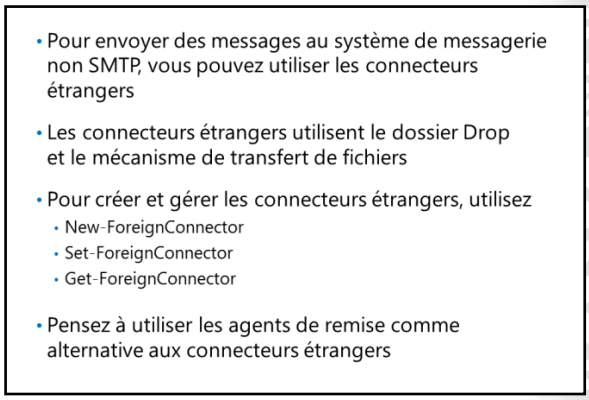
Démonstration : Comment créer et configurer les connecteurs SMTP

Procédure de démonstration

1. Utilisez l'environnement de ligne de commande Exchange Management Shell pour créer un connecteur d'**envoi** avec les propriétés suivantes :
   a. Nom : **Envoyer à Internet**
   b. Espace d'adressage : *****
   c. Source : **LON-MBX1**
2. Utilisez l'environnement de ligne de commande Exchange Management Shell pour créer un connecteur d'**envoi** avec les propriétés suivantes :
   a. Nom : **Messagerie sécurisée pour Contoso**
   b. Espace d'adressage : **contoso.com**
   c. DNSRoutingEnabled : **false**
   d. Smarthost : **172.16.0.10**
   e. Authentification : **de base**
   f. Informations d'identification : **Administrateur**, **Pa$$w0rd**
3. Utilisez le Centre d'administration Exchange pour vérifier les paramètres sur les nouveaux connecteurs d'envoi.
4. Utilisez le Centre d'administration Exchange pour créer un connecteur de **réception client** pour accepter les connexions anonymes provenant uniquement de **172.16.0.10**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les connecteurs étrangers ?



Parfois, vous devez remettre des messages électroniques à un système qui ne prend pas en charge SMTP comme mécanisme de transport. Un serveur de passerelle de télécopie en est un exemple. Dans ce scénario, vous pouvez utiliser un connecteur étranger, qui utilise le répertoire de dépôt pour envoyer des messages sortants. Le répertoire de dépôt peut être local ou partagé. Il utilise des protocoles de transfert de fichiers plutôt que SMTP comme mécanisme de transport. En sens inverse, les serveurs de passerelle étrangers peuvent envoyer des messages à l'organisation Exchange Server 2013 en utilisant le répertoire de collecte ou de relecture, comme il a été abordé précédemment dans ce module. Les fichiers de messages électroniques formatés correctement que vous copiez dans chaque répertoire sont soumis pour remise à une boîte aux lettres Exchange.

Vous pouvez créer des connecteurs étrangers sur le service de transport de boîtes aux lettres s'exécutant sur le rôle serveur de boîtes aux lettres. Vous devez utiliser l'environnement de ligne de commande Exchange Management Shell pour créer et configurer un connecteur étranger.

L'exemple ci-dessous indique comment créer un connecteur étranger.

```
New-ForeignConnector -Name "FaxGW Foreign Connector" -AddressSpaces
"X400:c=US;a=Fabrikam;P=Contoso;5" -SourceTransportServers LON-MBX1,LON-MBX2
```

Pour configurer un chemin de répertoire de dépôt pour un connecteur étranger, vous devez exécuter l'applet de commande suivante :

```
Set-ForeignConnector "Contoso Foreign Connector" -DropDirectory "C:\Drop Directory"
```

Pour vérifier une configuration d'agent étranger, vous devez exécuter l'applet de commande **Get-ForeignConnector**.

Un agent de remise peut également remettre des messages issus de votre environnement Exchange Server SMTP à un système qui n'utilise pas le protocole SMTP. Chaque agent de remise est associé à un connecteur d'agent de remise, qui met en file d'attente les messages routés vers l'agent de remise pour qu'ils soient traités et remis au périphérique ou système non SMTP.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Bien que l'architecture du connecteur étranger demeure dans Exchange Server 2013, nous vous conseillons d'utiliser des agents de remise pour acheminer les messages vers les systèmes non SMTP lorsque cela est possible. Voici les raisons principales de cette bonne pratique :

- vous pouvez utiliser la gestion de la file d'attente pour les messages ;
- il n'est pas nécessaire de gérer le transfert de fichiers vers un répertoire de dépôt ;
- vous pouvez vérifier la remise des messages.

Remarque : En général, les agents de remise sont produits par des sociétés tierces. Par défaut, Exchange Server 2013 est livré avec un seul connecteur d'agent de remise, qui est le connecteur d'agent de remise de la messagerie texte.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Gestion des règles de transport

Vous pouvez implémenter des stratégies et la conformité de messagerie en appliquant des règles de transport aux messages à mesure que les utilisateurs les envoient dans le cadre de l'organisation. En implémentant des règles de transport, vous pouvez appliquer des stratégies de messagerie et vous assurer que tous les messages électroniques envoyés au sein d'une organisation ou à des destinataires externes répondent aux exigences de conformité de votre organisation. Vous pouvez également implémenter des stratégies de gestion des droits aux messages à l'aide des règles de transport. Par exemple, vous pouvez utiliser des règles de transport pour garantir la conformité avec les stratégies de prévention des pertes de données.

Objectifs de la leçon

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

- décrire des règles de transport ;
- configurer des règles de transport ;
- planifier des règles de transport ;
- créer des règles de transport ;
- décrire les stratégies de prévention des pertes de données ;
- configurer les stratégies de prévention des pertes de données.

Que sont les règles de transport ?

Exchange Server applique les règles de transport aux messages lorsqu'ils transitent par le serveur de transport Edge ou par un service sur le serveur de boîtes aux lettres. L'agent de règle de transport applique les règles de transport sur le service de transport Hub. Les règles de transport limitent le flux des messages et la modification du contenu lorsque les messages sont en transit. Avec les règles de transport, vous pouvez :

- Les règles de transport limitent le flux des messages ou modifient le contenu des messages en transit
- Les règles de transport ont les caractéristiques suivantes
  - Elles sont stockées dans la partition de configuration AD DS
  - Elles sont appliquées par tous les serveurs de boîtes aux lettres
  - Elles servent à appliquer les exigences de conformité

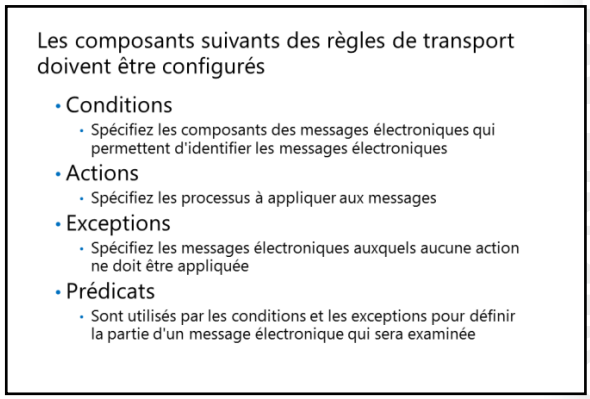
- empêcher les utilisateurs spécifiés d'échanger des courriers électroniques avec d'autres utilisateurs définis ;
- bloquer tout contenu inapproprié entrant ou sortant ;
- appliquer des restrictions basées sur les classifications de message afin de restreindre le flux d'informations confidentielles de l'organisation ;

- suivre ou journaliser les messages échangés avec certaines personnes ;
- rediriger les messages entrants ou sortants pour les examiner avant leur remise ;
- appliquer des clauses d'exclusion de responsabilité à des messages transitant par l'organisation ;
- appliquer des modèles de services AD RMS (Active Directory Rights Management Services) aux messages selon des critères de message.

Les règles de transport configurées sur un serveur de boîtes aux lettres s'appliquent automatiquement à tous les autres serveurs de boîtes aux lettres dans l'organisation. Exchange Server enregistre les règles de transport dans le conteneur de configuration dans AD DS et les réplique dans l'ensemble de la forêt AD DS pour qu'ils soient accessibles à tous les autres serveurs de boîtes aux lettres. Cela signifie qu'Exchange Server applique les mêmes règles de transport à tous les courriers électroniques échangés par les utilisateurs au sein de l'organisation.

Configuration des règles de transport

Les règles de transport sont configurées à l'aide d'un assistant similaire à celui qu'Outlook utilise pour les règles de boîtes aux lettres. Lorsque vous configurez des règles de transport, vous devez définir les éléments ci-dessous :



- *Conditions*. Les conditions de règle de transport indiquent les attributs, en-têtes, destinataires, expéditeurs ou autres parties du message électronique utilisés par Exchange Server pour identifier les messages électroniques auxquels une action de règle de transport doit être appliquée. Si les données du message électronique inspecté par la condition correspondent à la valeur de la condition, Exchange Server applique la règle si la condition ne correspond pas à une exception. Vous pouvez configurer plusieurs conditions sur une règle de transport pour réduire la portée de la règle à des critères très spécifiques. Vous pouvez également décider de ne pas appliquer les conditions, ce qui signifie que la règle de transport s'applique à tous les messages. Le nombre de conditions que vous pouvez appliquer à une règle de transport est illimité.

 **Remarque :** si vous configurez plusieurs conditions sur la même règle de transport, toutes les conditions doivent être remplies pour que la règle de transport soit appliquée à un message électronique particulier. Lorsque vous spécifiez plusieurs valeurs pour une même condition, si au moins une valeur correspond, la condition est remplie.

- *Actions*. Exchange Server applique des actions aux messages électroniques qui répondent aux conditions et pour lesquels aucune exception n'existe. Chaque action affecte les courriers électroniques de différentes manières, que ce soit pour leur réadressage ou leur suppression.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

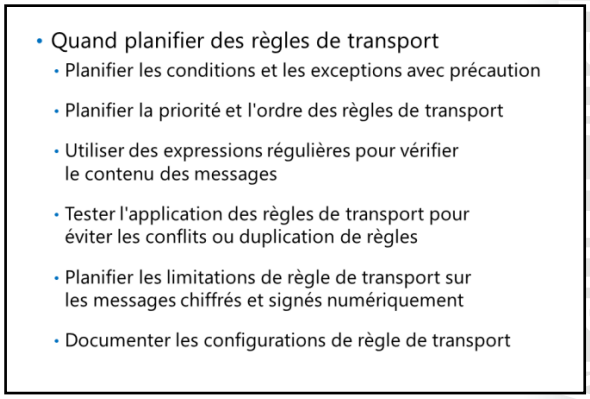
- *Exceptions*. Les exceptions déterminent les messages électroniques qui doivent être exclus d'une action. Les exceptions de règle de transport sont basées sur les mêmes prédicats que ceux utilisés pour créer des conditions de règle de transport. Les exceptions de règle de transport modifient les conditions et empêchent Exchange Server d'appliquer une action de règle de transport à un message électronique, même si le message remplit toutes les conditions de règle de transport configurées. Vous pouvez configurer plusieurs exceptions sur une règle de transport de façon à étendre les critères pour lesquels le serveur Exchange ne doit pas appliquer une action d'une règle de transport.

Remarque : Si vous configurez plusieurs exceptions sur la même règle de transport, une seule exception doit être remplie pour annuler l'action de la règle de transport. Lorsque vous spécifiez plusieurs valeurs pour une même exception, si au moins une valeur correspond, l'exception est remplie.

- *Prédicats*. Les conditions et les exceptions utilisent des prédicats pour définir la partie du courrier électronique qui est examinée par les conditions et les exceptions afin de déterminer si Exchange Server doit appliquer la règle de transport à ce message. Certains prédicats examinent les champs À : ou De : d'un message, tandis que d'autres prédicats examinent l'objet, le corps ou la taille de la pièce jointe. Pour déterminer si Exchange Server doit appliquer une règle de transport à un message, la plupart des prédicats requièrent la spécification d'une valeur à l'aide de laquelle les prédicats testent le message.

Planification des règles de transport

Les règles de transport vous fournissent la capacité presque sans limites de contrôler la messagerie dans votre organisation Exchange Server. Planifiez toujours soigneusement vos règles de transport pour vous assurer qu'elles se comportent comme prévu. Sinon, vous pourriez par erreur supprimer des messages ou en remettre à des destinataires fortuits.



Tenez compte des recommandations ci-dessous lorsque vous planifiez des règles de transport.

- Planifiez les conditions et les exceptions avec précaution. Les conditions et exceptions de règle de transport définissent les messages qui sont affectés par la règle de transport. Si vous implémentez des règles de façon incorrecte, vous pouvez involontairement modifier ou supprimer des messages.
- Planifiez la priorité et l'ordre des règles de transport. Dans de nombreux cas, vous devrez appliquer plusieurs règles de transport dans votre organisation. Si ces règles de transport comportent des conditions qui peuvent se chevaucher dans certains cas, il est très important que vous les organisiez correctement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Utilisez des expressions régulières pour vérifier le contenu des messages. Utilisez des expressions régulières pour simplifier la liste de termes lorsque vous incluez une chaîne de texte dans une condition. Vous pouvez utiliser une seule expression régulière plutôt qu'une liste de variations du même mot. Par exemple, en recherchant un modèle de numéro de téléphone, vous pouvez utiliser l'expression "\d\d\d(-|.)\d\d\d\d", qui indique un modèle à trois chiffres, ensuite un point ou un tiret, puis quatre chiffres.
- Testez l'application des règles de transport. Testez les nouvelles règles de transport pour vérifier qu'elles se comportent comme prévu. Il s'agit d'un point important car une nouvelle règle de transport pourrait être en conflit avec des règles de transport existantes.
- Planifiez les limitations de règle de transport sur les messages chiffrés et signés numériquement. L'intégration AD RMS avec Exchange Server 2013 vous permet d'implémenter les règles de transport et les stratégies de messagerie si vous utilisez la gestion des droits relatifs à l'information (IRM) AD RMS pour protéger les messages. Le chiffrement par d'autres mécanismes peut vous empêcher d'appliquer les règles de transport ou la gestion des enregistrements. Par exemple, Exchange Server peut ne pas pouvoir analyser les messages chiffrés pour rechercher la chaîne de texte spécifiée dans une règle de transport. En outre, les scanneurs antivirus ne peuvent pas analyser les messages avec des pièces jointes chiffrées.
- Pensez à récupérer la règle de transport. Les règles de transport supprimées ne sont pas récupérables facilement. Les règles de transport sont enregistrées dans AD DS et la restauration de ces règles depuis AD DS est un processus complexe. Alternativement, il est facile de recréer des règles de transport documentées, et vous pouvez exporter des règles de transport dans des fichiers de sauvegarde à l'aide de l'applet de commande **Export-TransportRuleCollection**. Toutefois, lorsque vous importez des règles de transport sur un serveur de transport Hub, le serveur remplace toutes les règles de transport existantes pour l'organisation.

Démonstration : Création des règles de transport

Procédure de démonstration

1. Sur LON-CAS1, basculez vers le Centre d'administration Exchange.
2. Accédez à **Flux de messagerie**.
3. Choisissez de **créer une nouvelle règle de transport**.
4. Configurez la règle avec les propriétés ci-dessous.
   a. Nom de la règle : **Tester la règle de transport**
   b. Condition : **Appliquer cette règle si le sujet ou le corps inclut le mot de passe**
   c. Action : **Rediriger le message à l'administrateur**
   d. **Activer cette règle maintenant**
5. Connectez-vous à **LON-CL1** en tant qu'**Aidan** et ouvrez **Outlook 2013**. Envoyez un message à Amr@adatum.com avec le texte suivant : **Mon mot de passe est Pa$$w0rd**.
6. Connectez-vous à **Outlook Web App** en tant qu'**Administrateur**.
7. Vérifiez que vous avez reçu un message électronique d'Aidan et que le message d'origine envoyé par Aidan à Amr est inclus.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Que sont les stratégies de prévention des pertes de données ?

- Les stratégies de protection contre les pertes de données appliquent des exigences de conformité pour les données stratégiques envoyées par courrier électronique
- Lorsque vous implémentez la protection contre les pertes de données, vous pouvez choisir de
  - Utiliser les modèles de protection contre les pertes de données fournis par Microsoft
  - Utiliser les fichiers de stratégie créés par un fournisseur tiers
  - Créer une stratégie personnalisée
- Les conseils de stratégie peuvent notifier aux utilisateurs qu'ils enfreignent la stratégie avant qu'ils n'envoient le courrier électronique

Dans l'environnement professionnel actuel, la messagerie est une ressource de communication essentielle. Divers types d'informations sont échangées par messagerie, et dans certains cas, des informations vitales pour l'entreprise peuvent filtrer d'une société dans un courrier électronique non protégé.

Pour éviter cela, Microsoft a implémenté des stratégies de protection des pertes de données dans Exchange Server 2013. Le rôle principal des stratégies de protection des données est d'appliquer des exigences de conformité aux données stratégiques et de gérer leur utilisation dans la messagerie sans entraver la productivité des employés. Par exemple, vous pouvez configurer une stratégie pour empêcher l'envoi de données telles que des numéros de carte de crédit, des numéros de sécurité sociale et des adresses IP dans les messages électroniques.

Remarque : La prévention des pertes de données est une fonctionnalité étendue qui nécessite une Licence d'accès client Entreprise (CAL).

Les stratégies de protection contre les pertes de données sont un ensemble de conditions qui contiennent des règles, actions et exceptions de transport. Lorsque des stratégies de protection contre les pertes de données sont appliquées, elles filtrent le trafic de messagerie pour empêcher les informations stratégiques contenues dans les courriers électroniques de sortir de la société. Les stratégies de protection contre les pertes de données sont très similaires aux règles de transport. En fait, ce sont des règles de transport avec un ensemble d'options étendu.

La différence entre les règles de transport et les stratégies de protection contre les pertes de données est une nouvelle approche consistant à classer les informations sensibles qui peuvent être incorporées au traitement du flux de messages. Elle comprend les performances de l'analyse de contenu approfondie via les correspondances de mots clés ou de dictionnaires, l'évaluation des expressions régulières et d'autres examens de contenu pour détecter le contenu qui enfreint les stratégies de l'organisation.

Vous pouvez créer des stratégies de protection contre les pertes de données dans le Centre d'administration Exchange et l'environnement de ligne de commande Exchange Management Shell. Il est possible de créer ces stratégies pour un test visant à observer les effets des stratégies. Vous pouvez aussi appliquer ces stratégies à l'ensemble du trafic de messagerie de votre organisation.

Un des avantages des stratégies de protection contre les pertes de données est que vous pouvez informer les expéditeurs de courriers électroniques qu'ils risquent de violer l'une de vos stratégies même avant qu'ils n'envoient un message. Cet avantage provient de l'utilisation des conseils en matière de stratégie de protection contre les pertes de données, qui sont très similaires aux MailTips mais sont préconfigurés pour être utilisés avec les stratégies de protection contre les pertes de données.

Microsoft fournit de nombreux modèles de stratégie de protection de pertes de données dans Exchange Server 2013. Vous pouvez également définir vos propres stratégies et règles de transport personnalisées en plus des modèles de stratégie prédéfinis fournis par Microsoft.

Il existe trois méthodes qui peuvent être appliquées lors de l'implémentation des stratégies de protection contre les pertes de données.

- Utiliser les modèles fournis par Microsoft. C'est la méthode la plus rapide pour commencer à utiliser les stratégies de protection contre les pertes de données et il n'est pas nécessaire de créer un ensemble complet de règles depuis le début. Toutefois, dans ce cas, vous devez être sûr que les exigences du modèle répondent à vos exigences de conformité. Voici quelques-uns des modèles de stratégie prédéfinis :
    - U.S. Financial Data. Aide à détecter la présence des données généralement associées à des données financières aux États-Unis. Il s'agit d'informations comme les numéros de carte de crédit, les numéros de compte et les données de carte de crédit.
    - Germany Financial Data. Aide à détecter la présence des données généralement associées à des données financières en Allemagne. Il s'agit aussi d'informations comme les numéros de carte de crédit, les numéros de compte et les données de carte de crédit.
    - U.S. Health Insurance Portability and Accountability Act (HIPAA). Aide à détecter la présence des données généralement associées à des informations de santé soumises à l'HIPAA.
    - U.S. Patriot Act. Aide à détecter la présence des données généralement soumises à l'U.S. Patriot Act.
    - U.K. Access to Medical Reports Act. Aide à détecter la présence des données généralement associées aux informations de santé au Royaume-Uni.
    - Israel Protection of Privacy Aide à détecter la présence des données généralement associées aux informations privées en Israël.
    - Saudi Arabia Anti-Cyber Crime Law. Aide à détecter la présence des données généralement associées à la loi sur les cybercrimes en Arabie Saoudite.
- Utiliser les fichiers de stratégie créés par un fournisseur de logiciels tiers. Vous pouvez importer les stratégies créées par des éditeurs de logiciels indépendants. Cela vous permet d'étendre les fonctionnalités des stratégies de protection contre les pertes de données pour mieux répondre à vos exigences de conformité. Vous pouvez importer ces stratégies à partir du fichier de stratégie.
- Créer une stratégie personnalisée. Si les stratégies prédéfinies ne correspondent pas à vos exigences, vous pouvez créer votre propre stratégie personnalisée pour vérifier vos propres données de message spécifiques et agir dessus. Pour implémenter une stratégie personnalisée de protection des pertes de données, vous devez connaître les configurations requises et les contraintes de l'environnement dans lequel la stratégie sera appliquée.

Lorsque vous créez des stratégies de protection contre les pertes de données, vous pouvez également inclure les règles qui recherchent les informations sensibles. Ces types d'informations doivent être utilisés dans vos stratégies. Les conditions que vous établissez dans une stratégie, telles que la fréquence à laquelle quelque chose est détecté avant qu'une mesure ne soit prise, peuvent être personnalisées dans vos nouvelles stratégies pour répondre à vos besoins de stratégie spécifiques.

Pour implémenter les fonctionnalités des stratégies de protection des pertes de données, il faut qu'Exchange Server 2013 soit configuré avec au moins une boîte aux lettres d'expéditeur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration des stratégies de protection contre les pertes de données

Procédure de démonstration

1. Dans le Centre d'administration Exchange, sur LON-CAS1, accédez à **Gestion de la conformité – Prévention des pertes de données**.
2. Choisissez de créer une **nouvelle stratégie DLP personnalisée**.
3. Configurez la stratégie comme il est indiqué ci-dessous.
   a. Stratégie : **Appliqué**
   b. Nom de la stratégie : **Blocs d'adresses IP**
   c. Inclure la règle : **Bloquer les messages dont le contenu est sensible**
   d. Type d'informations sensibles : **Adresse IP**
   e. Action : **Générer le rapport d'incident et l'envoyer à l'administrateur**
   f. Inclure les propriétés suivantes : **expéditeur**, **destinataire**, **objet** et **contenu correspondant**
   g. Action : **Notifier un conseil de stratégie à l'expéditeur contenant le texte « Le message est bloqué »**
4. Activer et enregistrer la stratégie.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Planification et configuration du transport des messages

Scénario

Vous êtes administrateur de messagerie chez A. Datum Corporation, qui est une grande société multinationale avec des bureaux dans plusieurs villes. Votre organisation a déployé Exchange Server 2013. Vous devez configurer Exchange Server pour envoyer des messages vers et depuis le réseau Internet. Vous devez également vous assurer que vous pouvez résoudre les problèmes liés au transport des messages, si nécessaire. À la fin, vous devez implémenter quelques règles de configuration de transport des messages conformément à la stratégie de sécurité de l'entreprise.

Objectifs

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

- configurer le transport des messages ;
- résoudre les problèmes de remise des messages ;
- configurer les règles de transport et les stratégies de prévention des pertes de données.

Configuration de l'atelier pratique

Durée approximative : **45 minutes**

Ordinateurs virtuels	22341B-LON-DC1 22341B-LON-CAS1 22341B-LON-MBX1 22341B-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 débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22341B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous avec les informations d'identification suivantes :
   a. Nom d'utilisateur : **ADATUM\Administrateur**
   b. Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22341B-LON-MBX1** et **22341B-LON-CAS1**.
6. Répétez les étapes 2 et 3 pour **22341B-LON-CL1**. Ne vous connectez pas tant que vous n'êtes pas invité à le faire.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configuration du transport des messages

Scénario

Votre organisation a déployé Exchange Server 2013 dans deux de ses sites. Toutefois, tous les messages Internet doivent transiter par le site principal. Dans le cadre de vos responsabilités professionnelles, vous devez configurer le transport des messages vers Internet et en provenance d'Internet. Vous devez également activer une application qui s'exécute sur l'hôte avec l'adresse IP 172.16.0.10 pour relayer anonymement les courriers électroniques via votre serveur Exchange.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer un connecteur d'envoi vers Internet.
2. Configurer un connecteur de réception pour accepter le relais.

▶ Tâche 1 : Configurer un connecteur d'envoi vers Internet

1. Sur LON-CAS1, ouvrez **Internet Explorer**, tapez **https://lon-cas1.adatum.com/ecp**, puis appuyez sur Entrée.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Accédez à **Flux de messagerie – Connecteurs d'envoi**.
4. Choisissez de créer un nouveau connecteur d'envoi avec les propriétés ci-dessous.
   a. Nom : **Envoi Internet**
   b. Tapez : **Internet**
   c. Résolution : **Enregistrement MX associé à un domaine de destinataire**
   d. Nom de domaine complet : *****
   e. Serveur source : **LON-MBX1**

▶ Tâche 2 : Configurer un connecteur de réception pour accepter le relais

1. Dans le Centre d'administration Exchange, choisissez de créer un **nouveau connecteur de réception**.
2. Nommez le connecteur **AppClient**.
3. Autorisez les connexions uniquement depuis l'adresse IP **172.16.0.10**.
4. Autorisez des connexions anonymes depuis cette IP.

Résultats : À la fin de cet exercice, les stagiaires auront configuré le transport des messages.

Exercice 2 : Résolution des problèmes liés à la remise de messages

Scénario

Vous avez réussi à installer Exchange Server 2013 sur deux sites. Vous devez maintenant vous assurer que le flux de messagerie fonctionne correctement.

Les tâches principales de cet exercice sont les suivantes :

1. Vérifiez que les messages provenant d'Internet peuvent être reçus.
2. Résoudre les problèmes liés au transport des messages.

▶ Tâche 1 : Vérifiez que les messages provenant d'Internet peuvent être reçus

1. Sur LON-DC1, utilisez Telnet pour vous connecter à LON-CAS1 avec le protocole SMTP.
2. Exécutez les commandes suivantes à l'invite Telnet et appuyez sur Entrée entre les commandes :
   a. **helo**
   b. **mail from: info@internet.com**
   c. **rcpt to:Aidan@adatum.com**
   d. **data**
   e. **Test depuis Internet**
   f. **.** (point)
3. Basculez vers **LON-CL1**, connectez-vous en tant qu'**Aidan** avec le mot de passe **Pa$$w0rd**, ouvrez **Outlook 2013** et vérifiez que vous avez reçu un courrier électronique de info@internet.com.
4. Répondez au message avec le texte de votre choix.

▶ Tâche 2 : Résoudre les problèmes liés au transport des messages

1. Sur LON-MBX1, ouvrez la **Exchange Toolbox**.
2. Démarrez l'**Afficheur des files d'attente**.
3. Vérifiez qu'il existe une file d'attente pour le domaine internet.com.
4. Supprimez le message de Aidan@adatum.com.
5. Basculez vers Outlook 2013 sur LON-CL1 et vérifiez qu'Aidan a reçu un rapport de non-remise (NDR).

Résultats : À la fin de cet exercice, les stagiaires auront résolu des problèmes SMTP.

Exercice 3 : Configuration des règles de transport et des stratégies de prévention des pertes de données

Scénario

Vous testez les règles de transport et les stratégies de prévention des pertes de données. Vous allez commencer par implémenter une règle de transport qui ajoute une exclusion pour chaque message envoyé depuis l'organisation A. Datum. En outre, selon la stratégie de sécurité d'entreprise, vous devrez créer une stratégie de prévention des pertes de données qui empêche les utilisateurs d'envoyer des données d'adresses IP dans des courriers électroniques.

Les tâches principales de cet exercice sont les suivantes :

1. Implémentation et test d'une règle de transport d'exclusion.
2. Créer une stratégie de prévention des pertes de données.
3. Vérifier la fonctionnalité Stratégie de prévention des pertes de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Implémentation et test d'une règle de transport d'exclusion

1. Sur LON-CAS1, dans le Centre d'administration Exchange, cliquez sur **Flux de messagerie** dans le volet des fonctionnalités.
2. Dans l'onglet **Règles**, démarrez l'assistant pour la nouvelle règle.
3. Choisissez que la règle soit appliquée chaque fois que l'expéditeur du message se trouve dans l'organisation.
4. Sélectionnez l'action correspondant au message **Ajouter une clause d'exclusion de responsabilité au message**.
5. Tapez le texte **Ceci est le texte d'exclusion de responsabilité d'Adatum** comme exclusion de responsabilité.
6. Sélectionnez renvoi à la ligne comme action de secours.
7. Configurez que l'administrateur doit être exclu de cette règle.
8. Basculez vers **LON-CL1**, puis dans Outlook 2013, envoyez un message de test à Administrateur.
9. Connectez-vous à Outlook Web App en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
10. Vérifiez que vous avez reçu le message d'Aidan et qu'il inclut l'exclusion de responsabilité.
11. Répondez à ce message.
12. Sur LON-CL1, ouvrez le message d'Administrateur et vérifiez qu'il n'y a aucune exclusion de responsabilité.

▶ Tâche 2 : Créer une stratégie de prévention des pertes de données

1. Dans le Centre d'administration Exchange, sur LON-CAS1, accédez à **Gestion de la conformité – Prévention des pertes de données**.
2. Choisissez de créer une nouvelle stratégie DLP personnalisée.
3. Configurez la stratégie comme il est indiqué ci-dessous.
   a. Stratégie : **Appliqué**
   b. Nom de la stratégie : **Blocs d'adresses IP**
   c. Inclure la règle : **Bloquer les messages dont le contenu est sensible**
   d. Appliquer cette règle si : **Le destinataire se situe dans l'organisation.**
   e. Type d'informations sensibles : **Adresse IP**
   f. Action : **Générer le rapport d'incident et l'envoyer à l' administrateur**
   g. Action : **Notifier un conseil de stratégie à l'expéditeur contenant le texte « Le message est bloqué »**.
4. Activer et enregistrer la stratégie.

▶ Tâche 3 : Vérifier la fonctionnalité Stratégie de prévention des pertes de données

1. Vérifiez que vous êtes connecté à LON-CL1 en tant qu'**Aidan**.
2. Basculez vers **Outlook 2013**.
3. Envoyez un message à amr@adatum.com avec le texte suivant : **Voici mon adresse IP : 192.168.0.100**.
4. Attendez quelques instants et vérifiez si vous recevez un message électronique indiquant que votre message précédent à Amr Zaki n'a pas été remis. Assurez-vous également que le texte « Le message est bloqué » s'affiche. Examinez le contenu du message.
5. Basculez vers **Internet Explorer**.
6. Dans Outlook Web App, assurez-vous que vous avez reçu un message électronique d'Aidan et que le message d'origine qu'Aidan a envoyé à Amr est attaché.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1, 22341B-LON-MBX1 et 22341B-LON-CL1**.

Résultats : À la fin de cet exercice, les stagiaires auront configuré des règles de transport et des stratégies de prévention de pertes de données.

Question : Que devez-vous configurer pour activer la messagerie Internet sortante à partir de chaque site d'A. Datum ?

Question : Une utilisatrice signale qu'elle a envoyé un message à un utilisateur dans une autre société il y a deux heures et que le message n'est pas arrivé. Quelle serait votre solution pour résoudre ce problème ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

- Ne pas modifier le flux de routage des messages par défaut si cela n'est pas absolument nécessaire.
- Utiliser l'Afficheur des files d'attente comme premier outil pour diagnostiquer l'échec de remise des messages.
- Comprendre la différence entre les règles de transport et les stratégies de prévention des pertes de données.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
La règle de transport n'est pas appliquée au message	

Questions de contrôle des acquis

Question : Où se trouve la fonctionnalité de transport Hub d'Exchange Server 2007 et Exchange Server 2010 dans Exchange Server 2013 ?

Outils

- Centre d'administration Exchange
- Environnement de ligne de commande Exchange Management Shell
- Afficheur des files d'attente

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 9

Planification et configuration de l'hygiène des messages

Table des matières :

Vue d'ensemble du module **9-1**

Leçon 1 : Planification de la sécurité de la messagerie **9-2**

Leçon 2 : Implémentation d'une solution antivirus pour Exchange Server 2013 **9-12**

Leçon 3 : Implémentation d'une solution anti-courrier indésirable pour Exchange Server 2013 **9-19**

Atelier pratique : Planification et configuration de la sécurité des messages **9-34**

Contrôle des acquis et éléments à retenir **9-41**

Vue d'ensemble du module

Dans un déploiement, Exchange Server 2013 est exposé à Internet 24 heures sur 24, car des messages électroniques sont couramment envoyés et reçus depuis Internet. Les utilisateurs se connectent via Internet pour accéder à leurs boîtes aux lettres, à l'aide de différents types de navigateurs Web, d'ordinateurs et de périphériques. Lorsque les utilisateurs sont ainsi exposés sur Internet, les organisations doivent planifier et déployer les solutions de sécurité qui protègent leur infrastructure Exchange. Les organisations doivent aussi vérifier que les données critiques, comme les messages électroniques, sont protégées contre les accès non autorisés en provenance d'Internet et que les serveurs le sont contre les attaques réseau et les programmes malveillants.

Objectifs

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

- planifier la sécurité de la messagerie ;
- implémenter une solution antivirus pour Exchange Server 2013 ;
- implémenter une solution anti-courrier indésirable pour Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Planification de la sécurité de la messagerie

Lorsque les administrateurs planifient le déploiement d'Exchange Server 2013, la sécurité doit faire partie de la stratégie de sécurité de l'infrastructure informatique globale de leurs organisations. Pour planifier la sécurité de la messagerie, les administrateurs doivent maîtriser Exchange Server 2013, la mise en réseau, la sécurité, le système d'exploitation Windows Server® 2012 et les services de domaine Active Directory® (AD DS).

La complexité et le coût des solutions de sécurité peuvent varier selon les exigences métier et de sécurité de l'organisation. Comme le coût est important, les administrateurs doivent veiller à inclure les chefs d'entreprise dans le processus d'approbation de la solution de sécurité optimale.

Objectifs de la leçon

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

- définir les exigences de sécurité de la messagerie ;
- planifier une solution de passerelle SMTP ;
- planifier les restrictions sur le flux de messages ;
- planifier la sécurité du connecteur SMTP ;
- planifier le routage sécurisé des messages entre les organisations partenaires ;
- planifier une sécurité de la messagerie basée sur les clients.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Définition des exigences de sécurité de la messagerie

Lorsque les administrateurs planifient la sécurité, ils doivent aligner leurs plans avec les exigences globales de sécurité de leurs organisations. Celles-ci doivent définir les types de clients qui se connecteront à Exchange Server. Elles doivent également définir comment leur infrastructure de messagerie sera protégée contre les menaces de sécurité externes ou internes.

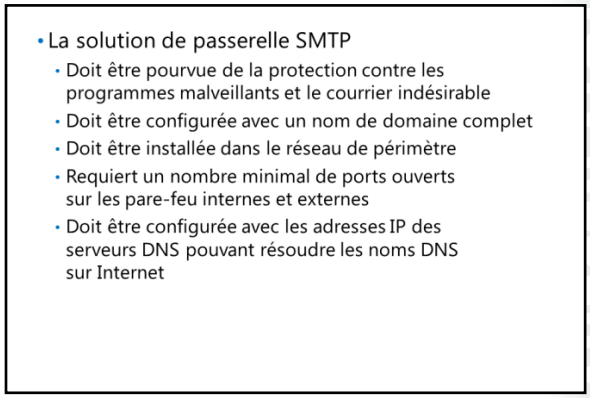
Exigences de sécurité	Technologie de protection
Exchange Server 2013	Logiciels anti-programmes malveillants, logiciels anti-courrier indésirable, autorisations de sécurité, pare-feu local
Réseau de périmètre	Pare-feu, proxy inverse, passerelle SMTP, logiciels anti-programmes malveillants, logiciels anti-courrier indésirable
Client interne	Logiciels anti-programmes malveillants, autorisations de sécurité, pare-feu local
Client externe	Logiciels anti-programmes malveillants, autorisations de sécurité, pare-feu local

La définition des exigences de sécurité pour la messagerie comprend les composants suivants :

- Exigences de sécurité pour Exchange Server. Les serveurs Exchange doivent être protégés contre les programmes malveillants et le courrier indésirable. Les organisations peuvent utiliser des solutions anti-courrier indésirable et anti-programmes malveillants sur site ou basées sur le cloud pour se protéger contre le courrier indésirable et les menaces de sécurité. En outre, sur les systèmes d'exploitation où Exchange Server 2013 est installé, le Pare-feu Windows doit être configuré avec les fonctions avancées de sécurité.
- Exigences de sécurité du périmètre. Les organisations doivent déployer les pare-feu et les périphériques ou logiciels de proxy inverse afin de protéger l'infrastructure informatique et les serveurs Exchange contre les attaques et les programmes malveillants en provenance d'Internet. En outre, vous pouvez utiliser les périphériques ou logiciels de passerelle SMTP déployés dans le réseau de périmètre. Les périphériques ou logiciels de passerelle SMTP doivent être équipés d'un logiciel anti-programmes malveillants et d'un logiciel anti-courrier indésirable.
- Exigences de sécurité des clients internes. Chaque client qui se connecte à l'infrastructure Exchange via le réseau interne de l'organisation doit être équipé d'un logiciel anti-programmes malveillants. En outre, nous recommandons que les clients internes soient équipés d'un pare-feu local activé et configuré.
- Exigences de sécurité des clients externes. Les organisations doivent déterminer les clients externes qui pourront se connecter à l'infrastructure Exchange Server. Les clients externes qui peuvent se connecter via Internet doivent également être équipés de logiciels anti-programmes malveillants et d'un pare-feu activé et configuré. Les organisations doivent également déterminer les types d'accès à accorder, tels que Microsoft Outlook® Web App, Outlook Anywhere et Microsoft Exchange ActiveSync®.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Solution de passerelle SMTP



Une solution de passerelle SMTP (Simple Mail Transfer Protocol) est un logiciel ou un périphérique déployé dans un réseau de périmètre. Si la solution de passerelle SMTP d'un réseau de périmètre s'exécute sur un système d'exploitation Windows Server, l'ordinateur ne doit pas être membre du domaine. Cette configuration rend beaucoup plus aisé et plus sécurisé le déploiement dans un réseau de périmètre, car les ordinateurs membres du domaine situés dans un réseau de périmètre doivent avoir davantage de ports ouverts sur le pare-feu pour pouvoir se connecter aux contrôleurs de domaine. Lorsque vous déployez une solution de passerelle SMTP, prenez en compte la configuration d'infrastructure requise suivante :

- La solution de passerelle SMTP doit permettre d'éviter que les messages indésirables et les programmes malveillants n'atteignent les utilisateurs de votre organisation, et ce en fournissant différents niveaux de filtre des messages indésirables et de protection contre les programmes malveillants.
- Vous devez installer une solution de passerelle SMTP sur les serveurs autonomes, ou comme périphérique. La solution de passerelle SMTP doit avoir un nom de domaine complet (FQDN) configuré. Cela est dû au fait que l'enregistrement MX du domaine SMTP de l'organisation est résolu en un nom de domaine complet de la passerelle SMTP lorsque les serveurs de messagerie externes envoient du courrier électronique à l'organisation. La passerelle SMTP doit être en mesure de communiquer sur le port 25 dans les deux directions avec le réseau interne.
- Vous devez déployer une solution de passerelle SMTP dans un réseau de périmètre. Cette configuration garantit un niveau de sécurité optimal.
- La configuration du pare-feu d'une solution de passerelle SMTP est considérablement simplifiée, car le serveur n'a pas besoin d'être membre du domaine interne. Le tableau suivant décrit les configurations de pare-feu requises.

Pare-feu	Règle du pare-feu	Explication
Externe	Autoriser l'ouverture du port TCP 25 à partir des adresses IP externes vers la solution de passerelle SMTP.	Cette règle autorise les hôtes SMTP sur Internet à envoyer du courrier électronique.
Externe	Autoriser l'ouverture du port TCP 25 vers les adresses IP externes à partir de la solution de passerelle SMTP.	Cette règle permet à la solution de passerelle SMTP d'envoyer des courriers électroniques aux hôtes SMTP sur Internet.
Externe	Autoriser l'ouverture du port TCP et UDP 53 vers les adresses IP externes à partir de la solution de passerelle SMTP.	Cette règle permet à la solution de passerelle SMTP de résoudre les noms DNS (Domain Name System) sur Internet.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

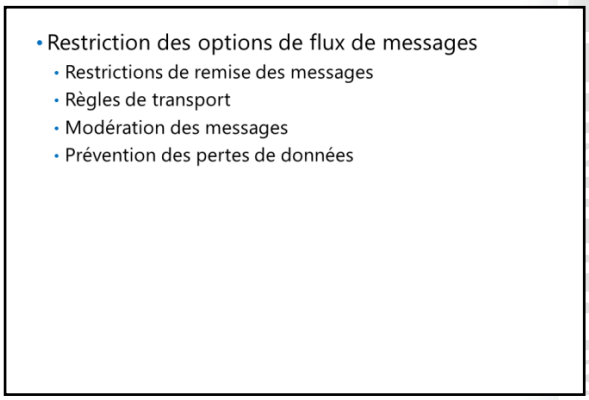
Pare-feu	Règle du pare-feu	Explication
Interne	Autoriser l'ouverture du port TCP 25 à partir de la solution de passerelle SMTP vers les serveurs d'accès au client spécifiés.	Cette règle permet à la solution de passerelle SMTP d'envoyer des messages SMTP entrants aux serveurs d'accès au client.
Interne	Autoriser l'ouverture du port TCP 25 à partir des serveurs d'accès au client vers la solution de passerelle SMTP.	Cette règle permet aux serveurs d'accès au client d'envoyer des messages SMTP entrants à la solution de passerelle SMTP.
Interne	Si la solution de passerelle SMTP est configurée pour contacter AD DS, autoriser le port spécifique requis pour un accès sécurisé entre la solution de passerelle SMTP et les contrôleurs de domaine, tel que le port LDAP (Lightweight Directory Access Protocol) 636.	Cette règle permet à AD DS de communiquer avec la solution de passerelle SMTP.
Interne	Autoriser l'ouverture du port 3389 de l'administration à distance du protocole RDP (Remote Desktop Protocol) à partir du réseau interne vers la solution de passerelle SMTP.	Cette règle est utilisée pour l'administration facultative du Bureau à distance de la solution de passerelle SMTP.

- Si la solution de passerelle SMTP achemine directement le courrier électronique vers Internet, vous devez configurer le serveur avec les adresses IP des serveurs DNS qui peuvent résoudre les noms DNS sur Internet.

Remarque : Même si un rôle serveur Edge est inclus dans Microsoft® Exchange Server 2007 et Microsoft® Exchange Server 2010, il n'est pas inclus dans Exchange Server 2013. Cependant, un environnement Exchange Server 2013 prend en charge le déploiement d'un rôle Edge Exchange Server 2010 comme solution de passerelle SMTP dans un réseau de périmètre.

Planification des restrictions du flux de messages

Chaque organisation envoie et reçoit des messages électroniques 24 heures sur 24, 7 jours sur 7. Les messages sont envoyés et reçus à partir d'Internet, et au sein de l'organisation. Pour accroître la sécurité de la messagerie, les organisations peuvent éventuellement restreindre le flux des messages, de telle sorte que certains messages ne soient pas autorisés à être envoyés à Internet et que d'autres ne soient pas envoyés au sein du réseau de l'entreprise.



La planification des restrictions du flux des messages comprend les tâches suivantes :

- Planification des restrictions de remise des messages. Les organisations peuvent décider de restreindre les personnes autorisées à envoyer des courriers électroniques aux utilisateurs ou groupes sélectionnés. Par exemple, vous pouvez configurer certains groupes de distribution dans vos organisations pour qu'ils ne reçoivent des courriers électroniques que des utilisateurs authentifiés.
- Planification des règles de transport. Les règles de transport s'appliquent lorsque les messages franchissent les composants de transport Exchange Server sur le rôle serveur de boîtes aux lettres. Les stratégies de transport peuvent limiter le flux de messages ou modifier le contenu des messages en fonction des conditions requises par votre organisation. Par exemple, vous pouvez définir des restrictions relatives aux utilisateurs qui peuvent s'envoyer des courriers électroniques ou au flux des messages en fonction du contenu. Vous pouvez également appliquer des clauses d'exclusion de responsabilité à des messages spécifiques. Vous pouvez configurer des règles de transport sur le rôle serveur de boîtes aux lettres.
- Planification de la modération des messages. Vous pouvez attribuer aux modérateurs l'autorisation d'examiner tous les messages envoyés à l'objet destinataire, comme une boîte aux lettres utilisateur ou une liste de distribution. Vous pouvez également configurer une liste d'utilisateurs qui n'a pas besoin de modération. En outre, vous pouvez configurer des notifications pour alerter les expéditeurs si leur message est approuvé ou pas.
- Planification de la prévention des pertes de données. La prévention des pertes de données (DLP) est une nouvelle fonctionnalité personnalisée d'Exchange Server 2013 qui effectue l'analyse du contenu des messages et le filtrage en utilisant les correspondances de mots clés ou de dictionnaires, l'analyse des expressions régulières et autres examens de contenu. L'objectif de la fonctionnalité est de détecter le contenu qui n'est pas conforme aux stratégies de sécurité et de conformité de l'organisation.

Planification de la sécurité du connecteur SMTP

Exchange Server 2013 offre plusieurs options de sécurisation du trafic de messagerie SMTP. Toutes ces options reposent sur des certificats permettant de chiffrer le trafic. Les méthodes suivantes de sécurisation SMTP requièrent d'implémenter l'option à la fois sur la partie source et la partie cible.

- Options de sécurité du connecteur SMTP

Protocole	Couche	Objectif
IPsec	Basé sur le réseau	Chiffre le trafic de serveur à serveur ou de client à serveur
VPN	Basé sur le réseau	Chiffre le trafic de site à site
TLS	Basé sur la session	Chiffre le trafic de serveur à serveur

- Le courrier électronique SMTP peut être davantage sécurisé via l'authentification et l'autorisation sur le connecteur SMTP

IPSec

IPsec fournit un ensemble d'extensions au protocole IP de base et vous pouvez l'utiliser pour chiffrer la communication entre serveurs. IPsec peut être utilisé pour le trafic en tunnel, ou d'égal à égal, afin de sécuriser toutes les communications IP en mode natif. Comme IPsec fonctionne sur la couche transport et est basé sur le réseau, les applications qui s'exécutent sur Exchange Server 2013 n'ont pas besoin de prendre en charge IPsec. Utilisez IPsec pour sécuriser les communications de serveur à serveur ou de client à serveur. Lorsque vous utilisez IPsec, vous n'avez pas besoin d'une autre méthode de chiffrement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

VPN

VPN opère aussi sur la couche transport et utilise fréquemment IPsec comme protocole sous-jacent. Vous pouvez utiliser VPN pour les connexions de site à site ou de client à site. Les deux fonctionnent sur la couche transport, ce qui peut être un avantage par rapport aux protocoles de la couche Application, tels que S/MIME, qui ne nécessitent pas que l'application aux deux extrémités ait connaissance du protocole.

TLS

Le protocole TLS (Transport Layer Security) est le protocole utilisé par défaut dans une organisation Exchange Server 2013 pour chiffrer la communication du serveur. Il s'agit d'un protocole standard que vous pouvez utiliser pour offrir des communications Web sécurisées sur Internet ou sur l'intranet. TLS permet aux clients d'authentifier les serveurs ou, à titre facultatif, aux serveurs d'authentifier les clients. Il offre également un canal sécurisé en chiffrant les communications. TLS est la version la plus récente du protocole SSL.

La fonctionnalité Exchange Server 2013 Sécurité du domaine utilise TLS avec l'authentification mutuelle, protocole également appelé Mutual TLS, pour fournir une authentification et un chiffrement basés sur la session. TLS standard est utilisé pour fournir la confidentialité en chiffrant les partenaires de communication, mais sans les authentifier. Il s'agit du SSL classique qui est l'implémentation HTTP de TLS.

Autres options de sécurisation du trafic SMTP

Outre les options mentionnées ci-dessus, vous pouvez également implémenter l'authentification et l'autorisation sur les connecteurs SMTP pour la sécurité. Cette méthode ne met pas en œuvre le chiffrement du trafic, mais peut empêcher les utilisateurs non autorisés d'envoyer des messages SMTP aux utilisateurs de votre organisation ou de transmettre les messages SMTP vers Internet. L'authentification et l'autorisation peuvent être configurées à partir de la connexion utilisateur, des adresses IP ou des plages IP.

Planification du routage sécurisé des messages entre les organisations partenaires

Vous pouvez configurer Exchange Server 2013 afin d'utiliser TLS pour assurer la sécurité de la messagerie SMTP. Dans la majorité des cas, vous ne pouvez pas utiliser le protocole TLS lors de l'envoi ou de la réception de courriers électroniques, car les serveurs SMTP ne sont pas configurés pour utiliser TLS. Toutefois, si vous imposez le protocole TLS pour tout le courrier électronique SMTP échangé entre votre organisation et d'autres organisations spécifiques, vous pouvez garantir un niveau de sécurité élevé pour la messagerie SMTP.

- Utilisez Mutual TLS avec les partenaires commerciaux pour activer les chemins de messages sécurisés sur Internet
- Pour configurer Mutual TLS
  - Générer une demande de certificat pour les certificats TLS
  - Importer et activer le certificat sur le serveur de boîtes aux lettres
  - Configurer la sécurité du domaine sortant
  - Configurer la sécurité du domaine entrant

Sécurisation d'un connecteur à une organisation partenaire

Pour sécuriser le connecteur à une organisation partenaire, vous devez configurer Mutual TLS, où chaque serveur vérifie l'identité de l'autre serveur en validant le certificat fourni par l'autre serveur. Il est ainsi facile pour les administrateurs de gérer des chemins de messages sécurisés entre les domaines via Internet. En d'autres termes, toutes les connexions entre les organisations partenaires sont authentifiées et tous les messages sont chiffrés au cours de leur transit sur Internet.

TLS avec authentification mutuelle diffère de TLS dans son implémentation habituelle. En général, lors de l'implémentation de TLS, le client vérifie la connexion sécurisée au serveur souhaité en validant le certificat du serveur reçu au cours de la négociation TLS. Avec Mutual TLS, chaque serveur vérifie la connexion auprès de l'autre serveur en validant un certificat fourni par ce dernier.

La sécurisation du connecteur à une organisation partenaire fonctionne d'une manière semblable à l'établissement d'une connexion TLS à un connecteur de réception SMTP. Toutefois, lorsque Mutual TLS est utilisé, l'expéditeur et le destinataire s'authentifient mutuellement avant d'envoyer les données. Le message prend l'itinéraire suivant d'une organisation à l'autre :

1. Le composant de transport du serveur de boîtes aux lettres de l'expéditeur initialise une session Mutual TLS avec le composant de transport du serveur de boîtes aux lettres cible en échangeant et en vérifiant les certificats. La session est uniquement établie lorsque les connecteurs d'envoi et de réception SMTP identifient tous les deux le domaine d'émission. Vous devez définir les informations de domaine côté envoi en utilisant l'applet de commande **Set-TransportConfig -TLSSendDomainSecureList <nom du domaine>**. Du côté de la réception, utilisez l'applet de commande **Set-TransportConfig - TLSReceiveDomainSecureList <nom du domaine>** pour définir les informations de domaine.
2. La communication SMTP est chiffrée et transférée au serveur de boîte aux lettres cible.
3. Le message est marqué comme sécurisé ; il s'affiche comme tel dans Outlook 2007 ou version ultérieure, et dans Outlook Web App.

Pour sécuriser le connecteur à une organisation partenaire, vous devez exécuter la procédure suivante :

1. Sur le serveur de boîtes aux lettres, générez une demande de certificat pour les certificats TLS. Vous pouvez demander le certificat auprès d'une autorité de certification privée, interne ou commerciale. Le serveur SMTP de l'organisation partenaire doit approuver le certificat. Lorsque vous effectuez une demande de certificat, vérifiez qu'elle inclut le nom de domaine pour tous les domaines SMTP internes de votre organisation.
2. Importez et activez le certificat sur le serveur de boîtes aux lettres. Après avoir demandé le certificat, vous devez l'importer sur le serveur de boîtes aux lettres, puis autoriser qu'il soit utilisé par les connecteurs SMTP qui permettent d'envoyer et de recevoir les messages de domaines sécurisés.
3. Configurez la sécurité du connecteur sortant. Pour configurer la sécurité du connecteur sortant, utilisez les applets de commande de l'environnement de ligne de commande Exchange Management Shell afin de spécifier les domaines auxquels vous enverrez les messages de domaines sécurisés, puis configurez le connecteur d'envoi SMTP pour utiliser les messages de domaines sécurisés.

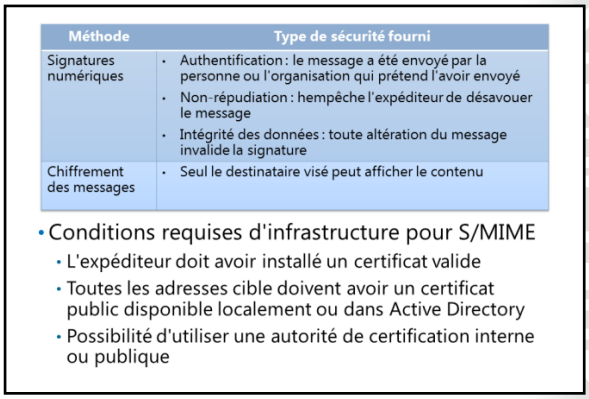
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Configurez la sécurité du connecteur entrant. Pour configurer la sécurité du connecteur entrant, utilisez les applets de commande de l'environnement de ligne de commande Exchange Management Shell pour indiquer les domaines dont vous recevrez les messages de domaines sécurisés, puis configurez le connecteur de réception SMTP pour utiliser les messages de domaines sécurisés.
5. Demandez au partenaire de configurer la sécurité du connecteur. La sécurité du connecteur doit être configurée des deux côtés, côté envoi et côté réception. Cela signifie que vous devez aussi contacter l'administrateur de votre partenaire pour configurer votre domaine pour la sécurité du connecteur.
6. Testez le flux de messages. Enfin, envoyez un message au partenaire et vice-versa pour vérifier que la sécurité du domaine fonctionne correctement.

Remarque : Lors de l'installation du rôle serveur de boîtes aux lettres, un certificat auto-signé est délivré au serveur. Aucun autre ordinateur n'approuve ce certificat. Lorsque vous exigez que l'organisation partenaire approuve le certificat, vous devez acquérir un certificat auprès d'une autorité de certification commerciale. Si vous ne souhaitez pas acheter un certificat auprès d'une autorité de certification commerciale, vous pouvez créer une approbation inter-forêts ou importer un certificat d'autorité de certification du magasin des autorités de certification racines approuvées des deux côtés.

Planification de la sécurité de la messagerie client

S/MIME est une solution de messagerie client permettant de sécuriser la messagerie SMTP. Avec S/MIME, chaque ordinateur client doit avoir un certificat et l'utilisateur est chargé de signer ou chiffrer chaque courrier électronique.



Sécurisation du courrier électronique par S/MIME

S/MIME sécurise les courriers électroniques à l'aide des options suivantes :

- Signatures numériques. Lorsqu'un utilisateur choisit d'ajouter une signature numérique à un message, la clé privée de l'expéditeur calcule et chiffre la valeur de hachage du message, puis ajoute cette valeur de hachage chiffrée au message sous forme de signature numérique. Le certificat et la clé publique de l'utilisateur sont envoyés au destinataire. Lorsque le destinataire reçoit le message, la clé publique de l'expéditeur déchiffre la valeur de hachage et la vérifie par rapport au message. Les signatures numériques garantissent les éléments suivants :
- Authentification. Si la clé publique peut déchiffrer la valeur de hachage jointe au message, le destinataire sait que le message provient de la personne ou de l'organisation qui a effectivement envoyé le message.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Non-répudiation. Seule la clé privée associée à la clé publique peut être utilisée pour chiffrer la valeur de hachage. Par conséquent, un message signé numériquement permet d'empêcher que son expéditeur ne le renie.
- Intégrité des données. Si la valeur de hachage est encore valide lorsque le destinataire la reçoit, toute modification d'un message invalide la signature numérique.
- Chiffrement des messages. Lorsqu'un utilisateur choisit de chiffrer un message à l'aide de S/MIME, le client de messagerie génère une clé de session symétrique unique et chiffre la totalité du message à l'aide de cette clé de session. La clé de session est ensuite chiffrée à l'aide de la clé publique du destinataire et la clé de session chiffrée est associée au message chiffré lors de l'envoi. Lorsque le message est reçu par le destinataire, la clé privée du destinataire le déchiffre.

  Le chiffrement des messages améliore la confidentialité. Vous ne pouvez déchiffrer un message qu'avec la clé privée associée à la clé publique utilisée pour son chiffrement. Par conséquent, seul le destinataire visé peut afficher le contenu.

Quand utiliser S/MIME ?

Lors de la configuration de S/MIME, tenez compte des éléments suivants :

- Un certificat client est requis sur chaque ordinateur qui envoie le courrier électronique sécurisé. La distribution de certificats clients à des utilisateurs non initiés à cette technologie augmente considérablement la charge de travail administratif.
- Un expéditeur doit obtenir l'accès à la clé publique du destinataire avant que l'expéditeur ne puisse envoyer un message électronique chiffré. Pour ce faire, généralement, un courrier électronique signé numériquement est envoyé.
- S/MIME est un modèle de sécurité basé sur l'utilisateur ; par conséquent, il appartient à l'utilisateur de signer ou chiffrer le message. Les utilisateurs peuvent oublier ou ne pas identifier les courriers électroniques à sécuriser.
- Les certificats doivent être sauvegardés. En cas de perte d'un message, l'utilisateur ne pourra pas déchiffrer les messages qui ont été chiffrés avec la clé publique associée au certificat.
- Les messages ne peuvent pas être analysés pour établir la conformité aux stratégies et la présence de virus ou de courriers indésirables, car les messages qui entrent dans l'organisation ou la quittent sont chiffrés. Les messages restent chiffrés dans la boîte aux lettres de l'utilisateur.

Pour créer un canal sécurisé, les administrateurs de messagerie des deux organisations doivent se mettre d'accord sur toutes les autres solutions. S/MIME reste l'option la plus réalisable si les utilisateurs doivent envoyer du courrier électronique sécurisé à des destinataires de différentes organisations.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration du routage sécurisé des messages entre les organisations partenaires

Procédure de démonstration

1. Sur LON-CAS1, ouvrez le Centre d'administration Exchange (CAE) à l'adresse **https://LON-CAS1.adatum.com/ecp**, puis connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Accédez à **Flux de messagerie – Connecteurs d'envoi**.
3. Créez un connecteur d'envoi dédié au domaine **contoso.com**. Cliquez sur le type de connecteur **Partenaire**. Sélectionnez **LON-MBX1** comme serveur source et sélectionnez l'option Proxy via le serveur d'accès au client.
4. Créez un connecteur de réception dédié au domaine **contoso.com**.
5. Cliquez sur le type de connecteur **Partenaire**, puis configurez le connecteur pour accepter le courrier électronique uniquement en provenance de **172.16.0.101**.
6. Sur LON-CAS1, dans l'environnement de ligne de commande Exchange Management Shell, tapez : **Set-TransportConfig –TLSSendDomainSecureList adatum.com**, puis appuyez sur **Entrée**.
7. Sur LON-CAS1, dans l'environnement de ligne de commande Exchange Management Shell, tapez : **Set-TransportConfig –TLSReceiveDomainSecureList contoso.com**, puis appuyez sur **Entrée**.

 **Remarque :** Les étapes décrites dans cette démonstration doivent également être effectuées dans l'organisation partenaire Contoso. Contoso doit créer un connecteur d'envoi partenaire pour le domaine **adatum.com**, créer un connecteur de réception pour **adatum.com** et configurer la sécurité TLS pour le protocole SMTP avec le domaine **adatum.com**.

Leçon 2
Implémentation d'une solution antivirus pour Exchange Server 2013

Le courrier électronique est l'un des moyens les plus courants de propager un virus d'une organisation à une autre. L'une des principales tâches de protection de votre organisation Exchange Server consiste à s'assurer que tous les messages infectés sont bloqués au périmètre de l'environnement de messagerie, mais aussi au sein du réseau de l'entreprise.

Exchange Server 2013 présente une fonctionnalité intégrée pour la protection anti-programmes malveillants. Cette fonctionnalité peut être utilisée comme solution autonome ou être couplée avec la solution cloud de Microsoft appelée Exchange Online Protection. Elle peut aussi être remplacée par une solution antivirus tierce.

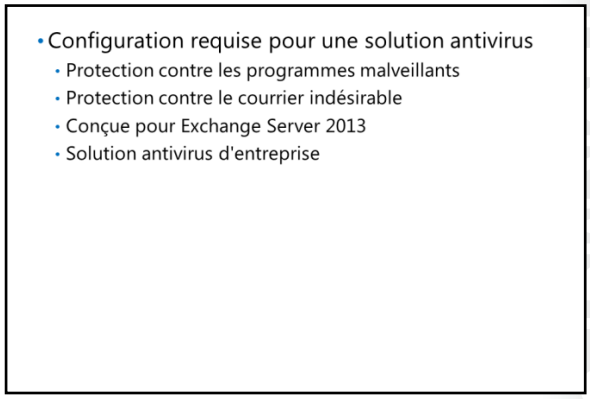
Objectifs de la leçon

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

- décrire la configuration requise des solutions antivirus ;
- décrire les options pour implémenter une solution antivirus dans Exchange Server 2013 ;
- configurer les fonctionnalités de solution antivirus dans Exchange Server 2013 ;
- décrire Exchange Online Protection ;
- décrire les options de déploiement pour la protection en ligne ;
- définir les meilleures pratiques de déploiement d'une solution antivirus.

Vue d'ensemble de la configuration requise des solutions antivirus

Les organisations doivent évaluer et planifier leur solution antivirus au niveau de l'entreprise. Elles doivent vérifier que leur infrastructure informatique est protégée contre toute menace, que celle-ci provienne d'Internet ou de leur réseau d'entreprise interne. Pour protéger avec succès leur environnement Exchange Server, les organisations doivent aussi protéger tous les autres logiciels, tels que ceux des ordinateurs clients et serveurs Windows, Microsoft® SQL Server et Microsoft® SharePoint® Server.



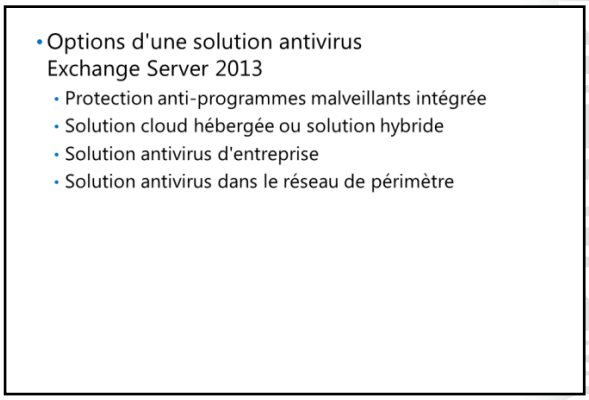
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lors de la planification d'une solution antivirus, les organisations doivent prendre en compte les exigences suivantes :

- Protection contre les programmes malveillants (virus et logiciels espions). La solution doit être capable d'identifier et de supprimer toutes les menaces provenant de messages électroniques, notamment les virus et les logiciels espions.
- Protection contre le courrier indésirable. La solution doit également comporter des fonctionnalités anti-courrier indésirable afin de fournir une console de gestion unique pour la protection contre les programmes malveillants et le courrier indésirable.
- Conçue pour Exchange Server 2013. Une solution antivirus doit être conçue pour prendre en charge la nouvelle architecture Exchange Server 2013. Les solutions antivirus conçues pour les versions Exchange Server précédentes ne peuvent pas être utilisées avec Exchange Server 2013. En outre, nous ne recommandons pas les solutions antivirus de niveau fichier pour protéger Exchange Server 2013. Si vous utilisez une solution antivirus de niveau fichier, suivez la documentation Microsoft sur la façon de configurer ce type de logiciel antivirus.
- Logiciel antivirus d'entreprise. Les organisations peuvent aussi choisir de déployer une solution antivirus d'entreprise dont les agents fournissent une protection pour différentes technologies, y compris la protection de niveau fichier, Exchange Server et Microsoft Lync™ Server. Dans ce scénario, les administrateurs de sécurité disposent d'une seule console pour surveiller plusieurs serveurs et l'état de leur protection.

Options d'implémentation d'une solution antivirus dans Exchange Server 2013

Chaque organisation possède sa propre stratégie en matière de protection contre les virus, en fonction des exigences métier de l'organisation. Certaines organisations choisissent de déployer la protection anti-programmes malveillants intégrée dans Exchange Server 2013, alors que d'autres organisations investissent dans des solutions tierces. Certaines organisations peuvent choisir d'utiliser une solution cloud, telle qu'Exchange Online Protection pour supprimer tout courrier électronique potentiellement infecté avant qu'il n'atteigne le réseau d'entreprise.



Si vous planifiez votre solution antivirus pour Exchange Server 2013, prenez en compte les options suivantes :

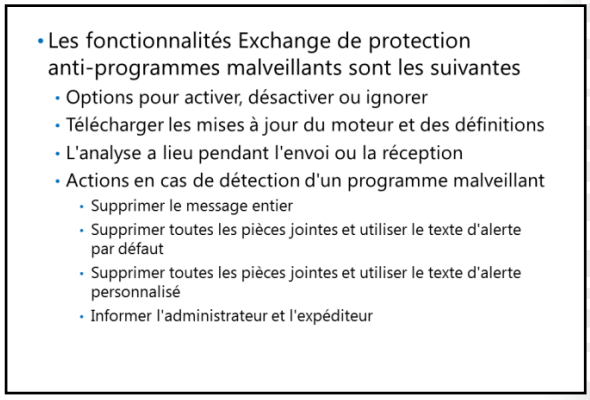
- Utiliser les fonctionnalités anti-programmes malveillants intégrées. Les organisations peuvent utiliser la protection intégrée s'exécutant sur le rôle serveur de boîtes aux lettres d'Exchange Server 2013 et la configurer en fonction de leurs exigences métier. Aucun investissement dans un logiciel antivirus supplémentaire n'est nécessaire.
- Utiliser une solution cloud hébergée ou une solution hybride. Dans ce scénario, les organisations peuvent choisir d'utiliser la protection sur site anti-programmes malveillants d'Exchange Server 2013 et Exchange Online Protection. Les organisations tirent parti de plusieurs filtrages anti-programmes malveillants exécutés à l'aide de différents moteurs dans le cloud et sur site.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Utiliser la solution antivirus d'entreprise existante. Certaines organisations disposent déjà d'une solution antivirus d'entreprise tierce existante. Dans ce scénario, elles désactivent la protection anti-programmes malveillants intégrée pour Exchange Server et installent le logiciel antivirus tiers pour Exchange Server 2013, qui s'intègre à la solution antivirus d'entreprise.
- Déployer une solution antivirus dans le réseau de périmètre. De nombreuses organisations déploient une solution de passerelle SMTP équipée de logiciels antivirus et anti-courrier indésirable. Dans ce scénario, le courrier électronique est analysé afin de détecter les programmes malveillants avant qu'ils ne pénètrent dans le réseau d'entreprise. Il est aussi recommandé que la passerelle SMTP et le rôle de boîte aux lettres Exchange Server aient différents moteurs.

Fonctionnalités d'une solution antivirus dans Exchange Server 2013

Exchange Server 2013 propose la protection anti-programmes malveillants intégrée qui est déployée sur le rôle serveur de boîtes aux lettres. Cette protection n'est pas disponible sur le rôle serveur d'accès au client.



Les fonctionnalités Exchange de protection anti-programmes malveillants sont les suivantes :

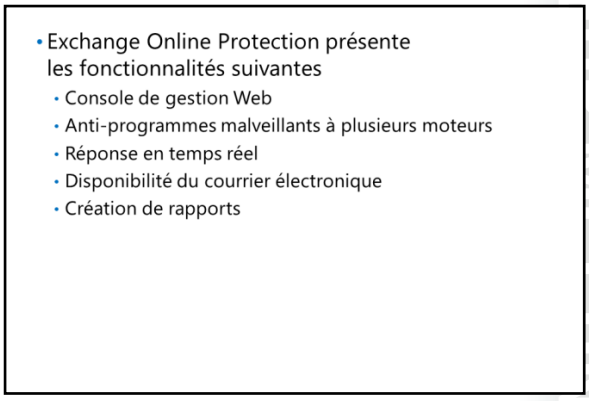
- La protection anti-programmes malveillants peut être activée ou désactivée. Les organisations peuvent choisir entre la protection anti-programmes malveillants Exchange Server 2013 et une solution antivirus tierce. Si une solution antivirus tierce est utilisée, la protection anti-programmes malveillants Exchange doit être désactivée. Vous pouvez activer ou désactiver la protection anti-programmes malveillants uniquement dans l'environnement de ligne de commande Exchange Management Shell. La protection anti-programmes malveillants Exchange peut également être contournée à l'aide de l'environnement de ligne de commande Exchange Management Shell, utilisé dans les scénarios où vous résolvez les problèmes liés à la protection anti-programmes malveillants Exchange.
- Une fois activée, la protection anti-programmes malveillants se connecte à Internet à l'aide du port HTTP 80 afin de télécharger les mises à jour du moteur et des définitions. Par défaut, les mises à jour du moteur et des définitions sont téléchargées toutes les heures. Nous vous recommandons vivement de télécharger les mises à jour du moteur et des définitions avant que le serveur Exchange Server ne soit déployé dans un environnement de production, car un serveur Exchange Server non mis à jour est plus exposé aux menaces de sécurité. Vous pouvez télécharger manuellement les mises à jour du moteur et des définitions à l'aide de l'environnement de ligne de commande Exchange Management Shell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- L'analyse est exécutée sur chaque message envoyé ou reçu par le rôle serveur de boîtes aux lettres. L'analyse ne s'exécute pas sur un message consulté par l'utilisateur, car ce message a déjà été analysé lors de sa réception.
- Vous pouvez configurer la stratégie anti-programmes malveillants par défaut à l'aide du Centre d'administration Exchange et de l'environnement de ligne de commande Exchange Management Shell. La stratégie anti-programmes malveillants par défaut ne peut pas être supprimée. Les paramètres de configuration vous permettent de choisir l'une des actions suivantes si un programme malveillant est détecté dans un message :
    - Supprimer le message entier. Il s'agit du paramètre par défaut, qui supprime le message entier, pièces jointes incluses, et empêche qu'il ne soit remis aux utilisateurs. Ce paramètre s'applique également si un programme malveillant est détecté dans le corps du message, indépendamment de la configuration de la stratégie anti-programmes malveillants.
    - Supprimer toutes les pièces jointes et utiliser le texte d'alerte par défaut. Si un programme malveillant est détecté dans une pièce jointe, cette action supprime toutes les pièces jointes des messages, y compris celles qui ne sont pas infectées. En outre, le texte d'alerte par défaut suivant est inséré dans un fichier texte qui remplace les pièces jointes : « Un programme malveillant a été détecté dans une ou plusieurs pièces jointes incluses dans ce courrier électronique. Toutes les pièces jointes ont été supprimées. »
    - Supprimer toutes les pièces jointes et utiliser le texte d'alerte personnalisé. Si un programme malveillant est détecté dans une pièce jointe, cette action supprime toutes les pièces jointes des messages, y compris celles qui ne sont pas infectées. En outre, vous pouvez configurer un message personnalisé qui sera inséré dans un fichier texte remplaçant les pièces jointes.
    - Informer l'administrateur et l'expéditeur. Un message peut être envoyé à l'expéditeur ou à l'administrateur pour l'avertir qu'un message électronique n'a pas été livré suite à la détection d'un programme malveillant.

Qu'est-ce qu'Exchange Online Protection ?



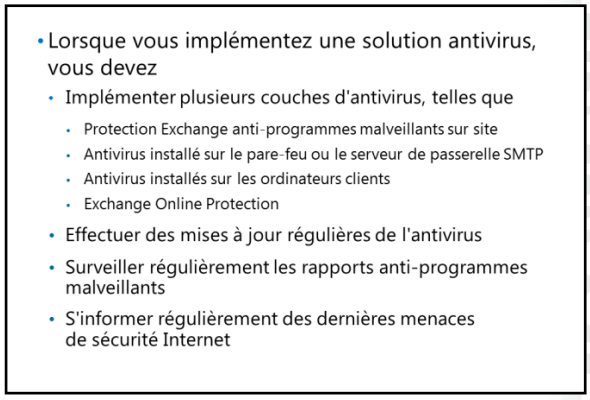
Exchange Online Protection (anciennement Microsoft Forefront Protection pour Exchange) est une solution cloud anti-courrier indésirable et anti-programmes malveillants. Les organisations peuvent choisir de la déployer comme solution unique ou comme solution hybride avec la protection anti-programmes malveillants sur site Exchange Server. Comme il s'agit d'un produit basé sur le cloud, aucun déploiement matériel ou logiciel n'est requis. À la place, les enregistrements de serveur de messagerie (MX) du serveur Exchange Server sur site sont reconfigurés pour pointer vers les serveurs où Exchange Online Protection est hébergé.

Exchange Online Protection présente les fonctionnalités suivantes :

- Console de gestion Web. Les administrateurs peuvent gérer la protection anti-programmes malveillants selon les exigences de leur organisation, même si le serveur n'est pas hébergé sur site.
- Antivirus à plusieurs moteurs. Plusieurs moteurs qui s'exécutent sous Exchange Online Protection aident à supprimer les menaces de programmes malveillants avant qu'elles n'atteignent le réseau d'entreprise.
- Réponse en temps réel. Exchange Online Protection est mis à jour toutes les deux heures avec les mises à jour des définitions et les règles anti-programmes malveillants. Les moteurs anti-programmes malveillants sont mis à jour avant d'être mis publiquement à disposition.
- Disponibilité des messages électroniques. Si une infrastructure Exchange Server sur site n'est pas disponible pour une raison quelconque, Exchange Online Protection met automatiquement les courriers électroniques en file d'attente et délivre les messages une fois que l'infrastructure Exchange Server a été remise en ligne.
- Création de rapports. Inclut les fonctions de création de rapports, d'audit et de suivi des messages.

Meilleures pratiques de déploiement d'une solution antivirus

Le déploiement et la gestion d'une solution antivirus dans Exchange Server sont un processus continu. Les administrateurs Exchange doivent régulièrement surveiller et évaluer leur solution antivirus pour rendre compte de son efficacité ; le rapport peut inclure des statistiques telles que le pourcentage de messages supprimés considérés comme malveillants. En outre, les administrateurs Exchange et les administrateurs de sécurité doivent également se tenir informés des dernières menaces contre la sécurité.



Tenez compte des meilleures pratiques suivantes lorsque vous déployez une solution antivirus :

- Fournir une protection multicouche. Pour fournir une sécurité renforcée contre les virus, implémentez plusieurs couches de protection antivirus. Un virus peut pénétrer dans votre organisation depuis Internet via un message électronique ou à partir d'un client non protégé dans votre société. Par conséquent, nous vous recommandons d'implémenter plusieurs couches de protection antivirus, comme une protection anti-programmes malveillants Exchange sur site, un pare-feu, un serveur de passerelle SMTP au niveau de l'ordinateur client et une protection Exchange Online Protection basée sur le cloud. En outre, il est recommandé que les moteurs anti-programmes malveillants de la solution cloud ou de la passerelle SMTP soient différents de ceux de la solution anti-programmes malveillants sur site.
- Effectuer des mises à jour régulières de l'antivirus. L'installation d'un antivirus ne signifie pas automatiquement que votre organisation est totalement protégée. Les mises à jour régulières du modèle de l'antivirus sont essentielles à une solution antivirus bien implémentée. Vous devez aussi contrôler fréquemment que vos modèles antivirus sont à jour.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Surveiller les rapports antivirus. Les administrateurs Exchange doivent consulter régulièrement les rapports des logiciels antivirus pour analyser les informations statistiques, telles que le nombre total de messages reçus en provenance d'Internet et le nombre de messages bloqués suite à la présence d'un programme malveillant.
- Demeurer informé des dernières menaces de programmes malveillants ou contre la sécurité Internet. Les administrateurs Exchange et les administrateurs de sécurité doivent régulièrement mettre à jour leurs connaissances sur les dernières menaces de sécurité, de courrier indésirable et de programmes malveillants. Vous devez également reconfigurer les paramètres anti-programmes malveillants conformément aux meilleures pratiques et recommandations les plus récentes.

Démonstration : Configuration de la protection anti-programmes malveillants pour Exchange Server

Procédure de démonstration

Activation des fonctionnalités anti-programmes malveillants dans Exchange Server 2013

1. Sur LON-MBX1, dans l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante :

```
CD “C:\Program Files\Microsoft\Exchange Server\V15\Scripts”
```

2. Dans l'environnement de ligne de commande Exchange Management Shell, activez l'analyse anti-programmes malveillants en tapant le script suivant :

```
.\Enable-AntimalwareScanning.ps1
```

3. Vérifiez que le message suivant apparaît : **Les moteurs anti-programmes malveillants sont en cours de mise à jour. Ce processus peut prendre quelques minutes**.
4. Dans l'environnement de ligne de commande Exchange Management Shell, redémarrez le **service de Microsoft Exchange Transport** en exécutant l'applet de commande suivante :

```
Restart-Service MSExchangeTransport
```

5. Attendez la fin du processus de mise à jour.
6. Dans l'environnement de ligne de commande Exchange Management Shell, répertoriez les agents de transport installés en exécutant l'applet de commande suivante :

```
Get-TransportAgent
```

7. Vérifiez que l'agent anti-programmes malveillants suivant est répertorié : **Malware Agent**. Vérifiez que le statut de l'agent anti-programmes malveillants est **Enabled True**.

Configuration de la stratégie anti-programmes malveillants par défaut

1. Basculez vers **LON-CAS1**.
2. Dans le Centre d'administration Exchange, ouvrez l'onglet **Filtre des programmes malveillants**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Modifiez la stratégie anti-programmes malveillants par défaut en sélectionnant :
   - **Réponse à la détection de programmes malveillants** : sélectionnez **Supprimer toutes les pièces jointes et utiliser le texte d'alerte personnalisé**.
   - Dans la zone **Texte d'alerte personnalisé**, tapez :

     La pièce jointe a été supprimée, car elle contenait des programmes malveillants. Contactez votre administrateur.
   - **Notifications** : activez les deux cases à cocher **Informer les expéditeurs internes** et **Informer les expéditeurs externes**.
   - **Notifications de l'administrateur** : activez la case à cocher **Informer l'administrateur des messages d'expéditeurs internes non remis**.
   - Zone **Adresse** de messagerie de l'administrateur : tapez **administrateur@adatum.com**.
4. Ensuite, continuez à modifier les paramètres anti-programmes malveillants par défaut :
   - **Notifications de l'administrateur** : activez la case à cocher **Informer l'administrateur des messages d'expéditeurs externes non remis**.
   - Zone **Adresse** de messagerie de l'administrateur : tapez **administrateur@adatum.com**.
5. Enregistrez les paramètres de configuration.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3

Implémentation d'une solution anti-courrier indésirable pour Exchange Server 2013

Les messages de courrier indésirable peuvent avoir un impact négatif sur l'environnement de messagerie de votre organisation. Par conséquent, l'implémentation d'une solution anti-courrier indésirable est essentielle pour préserver l'hygiène de l'environnement de messagerie de votre organisation. Exchange Server 2013 inclut plusieurs fonctionnalités que vous pouvez utiliser pour implémenter la protection contre le courrier indésirable dans votre organisation.

Cette leçon fournit une vue d'ensemble des options disponibles pour le filtrage anti-courrier indésirable et décrit comment vous pouvez configurer Exchange Server 2013 pour réduire le courrier indésirable dans votre organisation.

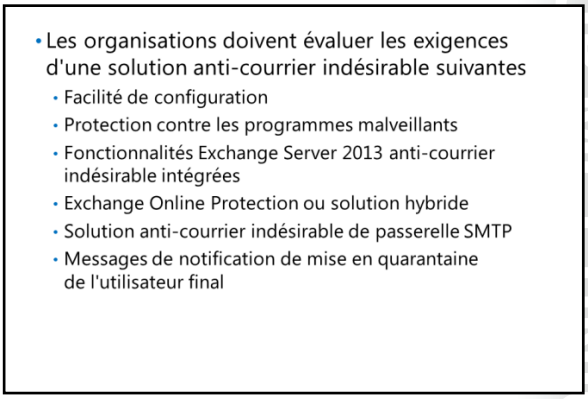
Objectifs de la leçon

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

- définir des solutions anti-courrier indésirable ;
- décrire les fonctionnalités Exchange Server 2013 de filtrage du courrier indésirable ;
- appliquer les filtres de courrier indésirable Exchange Server 2013 ;
- configurer le filtrage par ID de l'expéditeur ;
- configurer le filtrage par réputation de l'expéditeur ;
- configurer le filtrage de contenu ;
- comprendre le seuil de probabilité de courrier indésirable (SCL) dans Exchange Server 2013 ;
- appliquer les meilleures pratiques pour déployer une solution anti-courrier indésirable.

Vue d'ensemble des solutions anti-courrier indésirable

Les organisations doivent évaluer et planifier leur stratégie de solutions anti-courrier indésirable la plus appropriée en fonction de leur infrastructure réseau et de leurs exigences métier. Elles peuvent envisager d'utiliser différentes solutions, y compris des logiciels ou périphériques sur site, ou des services cloud anti-courrier indésirable.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous envisagez de déployer une solution antivirus, prenez en compte les options suivantes :

- Facilité de configuration. La solution doit être simple à configurer et à gérer. Elle doit également se montrer efficace dans la façon dont elle identifie et bloque les courriers indésirables.
- Protection contre les programmes malveillants. Idéalement, la solution doit également comporter des fonctionnalités anti-programmes malveillants afin de fournir une seule console de gestion pour assurer la protection contre le courrier indésirable et contre les programmes malveillants.
- Utiliser les fonctionnalités intégrées anti-courrier indésirable. Les organisations peuvent utiliser la protection intégrée s'exécutant sur le rôle serveur de boîtes aux lettres d'Exchange Server 2013 et la configurer en fonction de leurs exigences métier. Aucun investissement dans un logiciel antivirus supplémentaire n'est nécessaire.
- Solution cloud hébergée ou solution hybride. Dans ce scénario, les organisations peuvent choisir d'utiliser les fonctionnalités anti-courrier indésirable sur site d'Exchange 2013, ainsi qu'Exchange Online Protection. Les organisations tirent parti de l'utilisation de plusieurs solutions de filtrage anti-courrier indésirable, qui aident à maintenir le courrier indésirable en dehors du réseau d'entreprise.
- Déploiement d'une solution anti-courrier indésirable dans le réseau de périmètre. De nombreuses organisations déploient une solution de passerelle SMTP qui possède également des fonctionnalités anti-courrier indésirable. Dans ce scénario, le courrier électronique est analysé afin de détecter le courrier indésirable avant qu'il n'entre dans le réseau d'entreprise.
- Messages de notification de mise en quarantaine de l'utilisateur final. La solution notifie les utilisateurs si un message électronique est bloqué. Si un message électronique est bloqué, il est mis en quarantaine. Les messages mis en quarantaine sont très probablement des faux positifs, ce qui signifie que le message électronique a été bloqué à la suite de l'analyse anti-courrier indésirable ou anti-programmes malveillants. Si le message n'est pas du courrier indésirable et qu'il ne contient aucun programme malveillant, les utilisateurs peuvent demander à l'administrateur de transférer le message mis en quarantaine vers la boîte aux lettres de l'utilisateur. Certaines solutions anti-courrier indésirable peuvent permettre aux utilisateurs de récupérer leurs messages mis en quarantaine sans l'autorité de l'administrateur.

Vue d'ensemble des fonctionnalités de filtrage anti-courrier indésirable

La fonctionnalité de filtrage anti-courrier indésirable disponible sur le rôle serveur de boîtes aux lettres n'est pas activée par défaut. Si vous ne disposez pas d'une solution de passerelle SMTP, de transport Edge d'Exchange Server 2010 ou anti-courrier indésirable en ligne, vous devez activer le filtrage anti-courrier indésirable dans Exchange Server 2010. Pour activer et configurer le filtrage anti-courrier indésirable dans Exchange Server 2013, vous devez utiliser l'environnement de ligne de commande Exchange Management Shell. Vous ne pouvez pas configurer le filtrage anti-courrier indésirable avec le Centre d'administration Exchange.

Fonctionnalité	Filtre des messages d'après
Filtrage du contenu	Le contenu des messages
ID de l'expéditeur	L'adresse IP du serveur d'envoi à partir duquel le message a été reçu
Filtrage des expéditeurs	L'expéditeur au niveau de l'en-tête MAIL FROM:
Filtrage des destinataires	Les destinataires au niveau de l'en-tête RCPT TO:
Réputation de l'expéditeur	Plusieurs caractéristiques de l'expéditeur accumulées pendant un certain temps

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Agents anti-courrier indésirable du serveur de boîtes aux lettres

Le tableau ci-dessous répertorie les agents anti-courrier indésirable implémentés lors de l'installation par défaut du rôle serveur de boîtes aux lettres.

Agent	Description
Filtrage du contenu	Filtre les messages d'après leur contenu. Cet agent utilise la technologie Microsoft SmartScreen pour évaluer le contenu d'un message. Il prend également en charge l'agrégation de listes fiables.
ID de l'expéditeur	Filtre les messages en comparant l'adresse IP du serveur d'envoi SMTP avec le propriétaire supposé du domaine d'émission.
Filtrage des expéditeurs	Filtre les messages d'après l'expéditeur au niveau de l'en-tête SMTP MAIL FROM: du message.
Filtrage des destinataires	Filtre les messages d'après les destinataires au niveau de l'en-tête SMTP RCPT TO: du message.
Filtrage de réputation de l'expéditeur	Filtre les messages en fonction de nombreuses caractéristiques de l'expéditeur recueillies sur une période spécifique.

À la différence des versions précédentes d'Exchange Server, Exchange Server 2013 ne fournit d'option pour le filtrage des connexions en fonction des fournisseurs d'adresses IP ou de la liste rouge en temps réel (RBL) des expéditeurs. Il est primordial que les organisations déploient une passerelle de filtrage des connexions ou une solution cloud anti-courrier indésirable qui inclut le filtrage des connexions en fonction de la liste d'adresses IP ou de la liste rouge en temps réel (RBL) des expéditeurs.

Le filtrage de la configuration anti-courrier indésirable dans Exchange Server 2013 ne s'effectue qu'à l'aide de l'environnement de ligne de commande Exchange Management Shell. Les agents de filtrage ne sont pas installés par défaut. Pour installer tous les agents de filtrage, vous devez exécuter le script **Install-AntiSpamAgents.ps1** dans l'environnement de ligne de commande Exchange Management Shell, situé dans l'emplacement suivant **ExchangeInstallPath\Scripts**, où **ExchangeInstallPath** est une variable qui représente un dossier dans lequel les fichiers Exchange Server ont été installés.

 **Remarque :** Vous pouvez afficher tous les agents installés sur le serveur de boîtes aux lettres en utilisant l'applet de commande **Get-TransportAgent** sur le serveur de boîtes aux lettres.

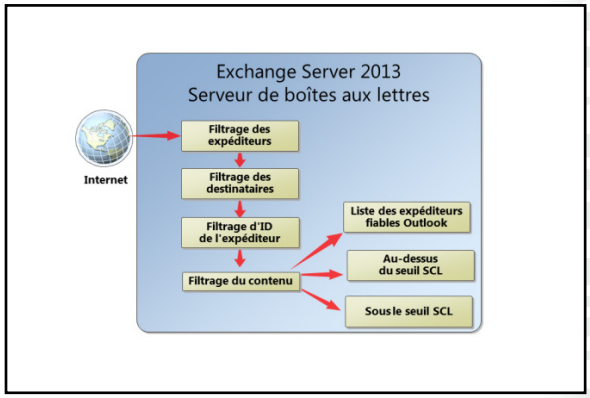
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Agrégation de listes fiables

Dans Exchange Server 2013, l'agent de filtrage du contenu sur le serveur de boîtes aux lettres utilise les listes d'expéditeurs et de destinataires fiables de Microsoft Office Outlook®, ainsi que les contacts fiables pour optimiser le filtrage du courrier indésirable. L'agrégation de listes fiables est un ensemble de fonctions anti-courrier indésirable partagées par Outlook et Exchange Server 2013. Cette fonctionnalité anti-courrier indésirable collecte les données à partir des listes fiables de blocage du courrier indésirable que les utilisateurs de Microsoft Outlook configurent et met ces données à la disposition des agents anti-courrier indésirable sur le serveur de boîtes aux lettres. Vous devez utiliser l'applet de commande **Update-Safelist** pour configurer l'agrégation de listes fiables.

Application des filtres de courrier indésirable Exchange Server 2013

Dans Exchange Server 2013, le rôle serveur de boîtes aux lettres utilise les agents de filtrage du courrier indésirable pour analyser chaque connexion SMTP et les messages qui transitent par ces connexions. Lorsqu'un serveur SMTP sur Internet se connecte au serveur d'accès au client Exchange et lance une session SMTP, le protocole SMTP est transmis par proxy au serveur de boîtes aux lettres, et ce dernier examine chaque message à l'aide de la séquence suivante :



1. Le serveur de boîtes aux lettres compare l'adresse de messagerie de l'expéditeur à la liste d'expéditeurs configurée dans le filtrage des expéditeurs. Si l'adresse SMTP est un destinataire ou un domaine bloqué, le serveur peut rejeter la connexion et aucun autre filtre n'est appliqué. De plus, vous pouvez configurer le serveur pour accepter le message de l'expéditeur bloqué, mais en marquant le message avec les informations de l'expéditeur bloqué, puis poursuivre le traitement. Les informations de l'expéditeur bloqué sont incluses comme l'un des critères lorsque le filtrage du contenu traite le message.
2. Le serveur de boîtes aux lettres compare le destinataire à la liste rouge des destinataires configurée dans le filtrage des destinataires. Si le destinataire concerné correspond à une adresse de messagerie filtrée, le serveur de boîtes aux lettres rejette le message de ce destinataire particulier. Si plusieurs destinataires figurent dans le message et si certains ne sont pas répertoriés dans la liste rouge des destinataires, le traitement du message continue.

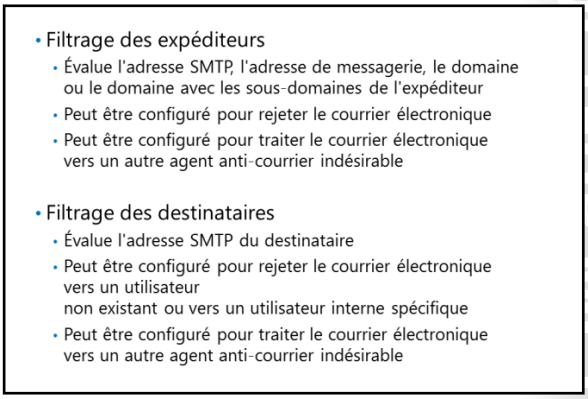
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Exchange Server 2013 applique le filtrage d'ID de l'expéditeur. En fonction de la configuration de l'ID de l'expéditeur, le serveur peut supprimer, rejeter ou accepter le message. Si le message est accepté, le serveur ajoute l'échec de validation de l'ID de l'expéditeur aux propriétés du message. L'état d'échec de l'ID de l'expéditeur figure sous forme de critère lors du traitement du message par le filtrage du contenu.
4. Le serveur de boîtes aux lettres applique le filtrage du contenu, qui compare l'expéditeur aux expéditeurs des données d'agrégation de listes fiables des utilisateurs Office Outlook. Si l'expéditeur figure dans la liste des expéditeurs fiables du destinataire, le message est envoyé à la banque de boîte aux lettres de l'utilisateur. Si l'expéditeur ne figure pas sur la liste des expéditeurs fiables du destinataire, une valeur de seuil de probabilité de courrier indésirable (SCL) est attribuée au message et le filtrage de contenu exécute l'une des actions suivantes :
    - Si la valeur SCL est supérieure à l'un des seuils du serveur de boîtes aux lettres configuré, le filtrage du contenu prend la mesure appropriée et supprime, rejette ou met en quarantaine le message.
    - Si la valeur SCL est inférieure à l'un des seuils du serveur de boîtes aux lettres, le message est passé à un composant transport du serveur de boîtes aux lettres contenant la boîte aux lettres de l'utilisateur.

Remarque : Vous pouvez ignorer le filtrage de courrier indésirable pour un destinataire spécifique en définissant la propriété **AntispamBypassEnabled** avec la valeur **True** dans la boîte aux lettres de l'utilisateur. Le message ainsi ignoré par le filtrage est donc remis directement à la boîte aux lettres du destinataire.

Qu'est-ce que le filtrage des expéditeurs et des destinataires ?

Le filtrage des expéditeurs et le filtrage des destinataires sont des fonctionnalités qui fournissent une protection contre le courrier indésirable dans l'en-tête SMTP MAIL FROM: du message entrant. En fonction de ces informations, le filtrage des expéditeurs peut rejeter le message s'il provient d'un domaine indésirable. Le filtrage des destinataires évalue l'en-tête SMTP RCPT TO provenant d'un message indésirable. En fonction de ces informations, le filtrage des destinataires peut envoyer un message d'erreur SMTP au serveur d'envoi si le message est envoyé à un destinataire non existant.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Filtrage des expéditeurs

Le filtrage des expéditeurs est effectué par l'agent de filtrage des destinataires. Si l'adresse de messagerie des expéditeurs ou un domaine correspond à la configuration du filtre des expéditeurs, l'agent de filtrage effectue l'une des actions suivantes :

- L'agent de filtrage des expéditeurs rejette les demandes SMTP avec une erreur de session **554 5.1.0 Sender Denied SMTP** et ferme la connexion.
- L'agent de filtrage des expéditeurs ne rejette pas le message, mais il marque le message avec les informations envoyées par l'expéditeur bloqué. D'autres agents anti-courrier indésirable qui traitent le même message utilisent les informations de marquage pour augmenter la valeur SCL du message électronique envoyé par l'expéditeur bloqué.

Vous pouvez configurer le filtrage des expéditeurs pour bloquer une adresse de messagerie, un domaine ou un domaine avec ses sous-domaines spécifiques. Par défaut, le filtrage des expéditeurs est effectué sur le courrier électronique envoyé uniquement à partir de serveurs non authentifiés, qui sont des serveurs externes.

Après avoir installé les agents anti-courrier indésirable sur le rôle de boîte aux lettres Exchange Server, vous devez vérifier si l'agent d'ID de l'expéditeur est activé en tapant l'applet de commande suivante dans l'environnement de ligne de commande Exchange Management Shell :

```
Get-SenderFilterConfig | Format-List Enabled
```

Pour configurer le filtrage des expéditeurs afin de bloquer les messages en provenance de **marketing@contoso.com**, vous devez taper l'applet de commande suivante :

```
Set-SenderFilterConfig -BlockedSenders marketing@contoso.com
```

Pour configurer le filtrage des expéditeurs pour bloquer tous les messages en provenance de la société avec le domaine SMTP **contoso.com**, vous devez taper l'applet de commande suivante :

```
Set-SenderFilterConfig -BlockedDomains contoso.com
```

Filtrage des destinataires

Le filtrage des destinataires est effectué par l'agent de filtrage des destinataires. En fonction de l'adresse de messagerie de destination du destinataire, l'agent de filtrage des destinataires effectue l'une des actions suivantes :

- Si l'adresse de messagerie du destinataire n'existe pas ou s'il faut l'empêcher de recevoir du courrier électronique d'expéditeurs externes, une action appropriée est exécutée par l'agent de filtrage, telle que l'envoi d'une erreur de session SMTP **550 5.1.1 User unknown** au serveur Exchange.
- Si un message électronique entrant est envoyé à une adresse de messagerie existante et que le destinataire ne correspond pas aux critères de blocage, l'agent de filtrage des destinataires traite le message et l'agent anti-courrier indésirable suivant évalue le message et l'expéditeur.

Après avoir installé les agents anti-courrier indésirable sur le rôle de boîte aux lettres Exchange Server, vous devez vérifier si l'agent de filtrage des expéditeurs est activé en tapant l'applet de commande suivante dans l'environnement de ligne de commande Exchange Management Shell :

```
Get-RecipientFilterConfig | Format-List Enabled
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

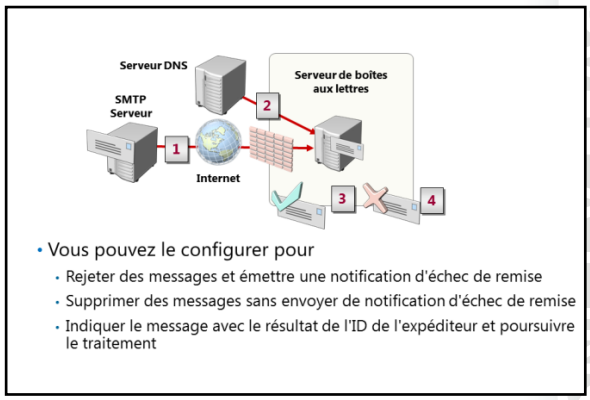
Pour configurer le filtrage des destinataires afin de bloquer les messages externes envoyés à **helpdesk@adatum.com**, vous devez exécuter l'applet de commande suivante :

```
Set-RecipientFilterConfig -BlockListEnabled $true -BlockedRecipients helpdesk@adatum.com
```

Pour configurer le filtrage des destinataires afin de bloquer les messages aux destinataires qui n'existent pas dans votre organisation, exécutez l'applet de commande suivante :

```
Set-RecipientFilterConfig -RecipientValidationEnabled $true
```

Qu'est-ce que le filtrage d'ID de l'expéditeur ?



Le filtrage d'ID de l'expéditeur permet que les messages électroniques reçus soient filtrés en fonction des serveurs dont ils proviennent. Le filtrage d'ID de l'expéditeur requiert l'implémentation du protocole Sender ID Framework, norme d'authentification qui vérifie le domaine Internet dont provient chaque message électronique en fonction de l'adresse IP du serveur de l'expéditeur. Le protocole Sender ID Framework assure une protection contre l'usurpation de domaine de messagerie et les plans d'hameçonnage. En utilisant le protocole Sender ID Framework, les expéditeurs de courrier peuvent inscrire tous les serveurs de messagerie qui envoient des messages à partir de leur domaine SMTP. Puis, les destinataires peuvent filtrer les messages du domaine qui ne provient pas des serveurs spécifiés.

Enregistrements SPF (Sender Policy Framework)

Pour activer le filtrage des ID de l'expéditeur, chaque expéditeur doit créer un enregistrement SPF (Sender Policy Framework) et l'ajouter aux enregistrements DNS de son domaine. L'enregistrement SPF correspond à un seul enregistrement texte (TXT) de la base de données DNS qui identifie les serveurs de messagerie de chaque domaine. Les enregistrements SPF peuvent utiliser plusieurs formats, notamment :

- **Adatum.com. IN TXT "v=spf1 mx -all"**. Cet enregistrement indique que n'importe quel serveur disposant d'un enregistrement MX pour le domaine Adatum.com est autorisé à envoyer des messages électroniques pour ce domaine.
- **Mail IN TXT "v=spf1 a -all"**. Cet enregistrement indique que tout hôte comportant un enregistrement A peut envoyer un courrier électronique.
- **Adatum.com IN TXT "v=spf1 ip4:10.10.0.20 –all"**. Cet enregistrement indique qu'un serveur avec l'adresse IP 10.10.0.20 peut envoyer un courrier pour le domaine Adatum.com.

Remarque : Microsoft fournit l'Assistant Création d'un enregistrement SPF à partir de l'ID de l'expéditeur pour créer les enregistrements SPF de votre organisation. Il est accessible via la page de création d'un enregistrement SPF à partir de l'ID de l'expéditeur sur le site Web de Microsoft.

Fonctionnement des ID de l'expéditeur

Après avoir configuré les enregistrements SPF, tous les serveurs de messagerie de destination qui utilisent les fonctionnalités d'ID de l'expéditeur peuvent identifier votre serveur à l'aide de l'ID de l'expéditeur. Une fois le filtrage d'ID de l'expéditeur activé, le processus suivant montre comment tous les messages électroniques sont filtrés :

1. L'expéditeur transmet un message électronique à l'organisation du destinataire. Le serveur de messagerie de destination reçoit le message électronique.
2. Le serveur de destination contrôle le domaine qui prétend avoir envoyé le message et vérifie le DNS pour l'enregistrement SPF de ce domaine. Le serveur de destination détermine si l'adresse IP du serveur d'envoi de courrier électronique correspond à chacune des adresses IP qui sont dans l'enregistrement SPF. L'adresse IP du serveur autorisée à envoyer du courrier électronique pour ce domaine est appelée « adresse prétendue responsable ».
3. Si les adresses IP correspondent, le serveur de destination authentifie le message et le remet au destinataire. Toutefois, d'autres analyseurs anti-courrier indésirable tels que le filtrage du contenu sont encore appliqués.
4. Si les adresses ne correspondent pas, l'authentification du courrier échoue. Selon la configuration du serveur de messagerie, le serveur de destination peut supprimer le message ou le transférer en insérant des informations supplémentaires dans son en-tête pour indiquer que l'authentification a échoué.

Procédure de configuration de l'ID de l'expéditeur

Après avoir installé les agents anti-courrier indésirable sur le rôle de boîte aux lettres Exchange Server, vous devez vérifier si l'ID de l'expéditeur est activé en tapant l'applet de commande suivante dans l'environnement de ligne de commande Exchange Management Shell :

```
Get-SenderIDConfig | Format-List Enabled
```

Afin de configurer le filtrage des ID de l'expéditeur pour rejeter le courrier électronique en provenance de domaines falsifiés, vous devez taper l'applet de commande suivante dans l'environnement de ligne de commande Exchange Management Shell :

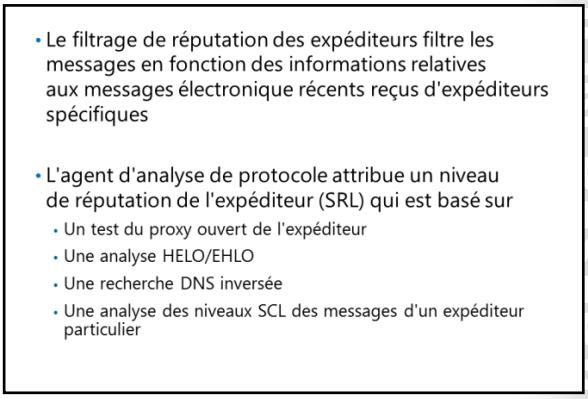
```
Set-SenderIDConfig -SpoofedDomainAction Reject
```

Vous pouvez également configurer le filtrage des ID de l'expéditeur pour ignorer un destinataire interne spécifique, ou pour un domaine d'expéditeur spécifique. Pour configurer une exception du filtrage des ID de l'expéditeur pour un utilisateur interne spécifique, pour le courrier électronique reçu par le domaine contoso.com, vous devez taper l'applet de commande suivante dans l'environnement de ligne de commande Exchange Management Shell :

```
Set-SenderIDConfig -BypassedRecipients adam@adatum.com -BypassedSenderDomains
contoso.com
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que le filtrage de réputation de l'expéditeur ?



La réputation de l'expéditeur fait partie des fonctionnalités anti-courrier indésirable d'Exchange Server 2013 ; les décisions du filtrage des messages s'appuient sur les informations relatives aux derniers messages électroniques reçus d'expéditeurs spécifiques. L'agent de réputation de l'expéditeur analyse différentes statistiques relatives à l'expéditeur et au courrier électronique pour créer un niveau de réputation de l'expéditeur (SRL). Ce SRL est un nombre compris entre 0 et 9, où 0 indique moins d'1 % de probabilité que l'expéditeur soit un créateur de courrier indésirable et 9 indique qu'il y a plus de 99 % de probabilité que l'expéditeur soit un créateur de courrier indésirable. Si un expéditeur semble être la source du courrier indésirable, l'agent de réputation de l'expéditeur ajoute automatiquement l'adresse IP du serveur SMTP qui envoie le message à la liste rouge des adresses IP.

Fonctionnement du filtrage de réputation de l'expéditeur

Lorsque le serveur de boîtes aux lettres reçoit le premier message d'un expéditeur spécifique, un SRL de valeur 0 est assigné à l'expéditeur SMTP. Au fur et à mesure de l'arrivée d'autres messages de la même source, l'agent de réputation de l'expéditeur évalue les messages et commence à ajuster le niveau de l'expéditeur. Pour évaluer chaque expéditeur, l'agent de réputation de l'expéditeur utilise les critères suivants :

- Test du proxy ouvert de l'expéditeur. Le proxy ouvert est un serveur proxy qui accepte les demandes de connexion depuis tout serveur SMTP et transmet les messages comme s'ils provenaient de l'hôte local. Il est également connu sous le nom de serveur de relais ouvert. Lorsque l'agent de réputation de l'expéditeur calcule un SRL, il met en forme une demande SMTP et tente de se reconnecter au serveur de boîtes aux lettres à partir du proxy ouvert. Si une demande SMTP est reçue du proxy, l'agent de réputation de l'expéditeur vérifie que le proxy est ouvert et met à jour les statistiques de test de proxy ouvert pour cet expéditeur.
- Analyse HELO/EHLO. Les commandes SMTP HELO et EHLO sont destinées à fournir un nom de domaine (tel que Contoso.com) ou une adresse IP de serveur d'envoi SMTP au serveur de destination. Les expéditeurs de courrier indésirable modifient fréquemment l'instruction HELO/EHLO afin d'utiliser une adresse IP qui ne correspond pas à l'adresse IP dont provient la connexion ou encore d'utiliser un nom de domaine différent du nom de domaine d'origine réel. Si le même expéditeur utilise plusieurs noms de domaine ou adresses IP dans les commandes HELO ou EHLO, cela augmente la probabilité que l'expéditeur soit un créateur de courrier indésirable.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- Recherche DNS inversée. L'agent de réputation de l'expéditeur vérifie également que l'adresse IP d'origine à partir de laquelle l'expéditeur transmet le message correspond au nom de domaine enregistré soumis par l'expéditeur dans la commande SMTP HELO ou EHLO. Cet agent effectue une recherche DNS inversée en soumettant l'adresse IP d'origine au DNS. Si les noms de domaines ne correspondent pas, il est probable que l'expéditeur soit un expéditeur de courrier indésirable ; le seuil SRL global pour l'expéditeur est alors ajusté à la hausse.
- Analyse des notations SCL des messages d'un expéditeur donné. Lorsque l'agent de filtrage du contenu traite un message, il affecte une notation SCL au message. Cette valeur est jointe au message en tant que SCL, qui est une valeur numérique comprise entre 0 et 9. L'agent de réputation de l'expéditeur analyse les données relatives aux notations SCL de chaque expéditeur et les utilise pour calculer les valeurs SRL.

L'agent de réputation de l'expéditeur calcule la valeur SRL pour chaque expéditeur pendant une période spécifique. Lorsque la valeur SRL dépasse la limite configurée, l'adresse IP du serveur d'envoi SMTP est ajoutée à la liste rouge IP pour une certaine durée.

Configuration de la réputation de l'expéditeur

Vous ne pouvez configurer les paramètres de réputation de l'expéditeur qu'à partir de l'environnement de ligne de commande Exchange Management Shell. Les paramètres incluent le seuil de blocage de réputation de l'expéditeur, et la configuration de la durée de rétention d'un expéditeur dans la liste rouge IP. By default, si le seuil de réputation de l'expéditeur est atteint, les adresses IP des expéditeurs sont bloquées pendant 24 heures.

L'agent qui effectue le filtrage de réputation de l'expéditeur est appelé agent d'analyse de protocole, et n'est pas installé par défaut. Après avoir installé les agents anti-courrier indésirable sur le rôle de boîte aux lettres Exchange Server, vous devez vérifier les paramètres de configuration du filtrage de réputation en tapant l'applet de commande suivante dans l'environnement de ligne de commande Exchange Management Shell :

```
Get-SenderReputationConfig | Format-List Enabled,*MailEnabled
```

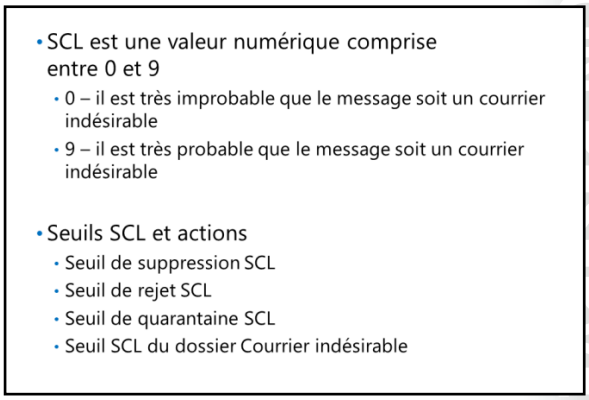
Pour configurer le seuil de blocage SRL de l'expéditeur sur 7 et ajouter des expéditeurs qui ont atteint la valeur de ce seuil à la liste rouge IP pendant 36 heures, vous devez taper l'applet de commande suivante dans l'environnement de ligne de commande Exchange Management Shell :

```
Set-SenderReputationConfig -SrlBlockThreshold 7 -SenderBlockingPeriod 48
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Présentation du seuil de probabilité de courrier indésirable (SCL) dans Exchange Server 2013



L'agent de filtrage du contenu analyse le contenu de chaque message électronique pour déterminer si le message est un courrier indésirable. Lorsque le serveur de boîtes aux lettres reçoit un message, l'agent de filtrage du contenu évalue le contenu du message à la recherche d'éléments reconnaissables, puis attribue une note en fonction de la probabilité que le message soit un courrier indésirable. Cette valeur numérique comprise entre 0 et 9 est jointe au message (0 indique qu'il est hautement improbable que le message soit un courrier indésirable et 9 qu'il est hautement probable qu'il le soit). Cette valeur est conservée avec le message lorsqu'il est envoyé à d'autres serveurs exécutant Exchange Server.

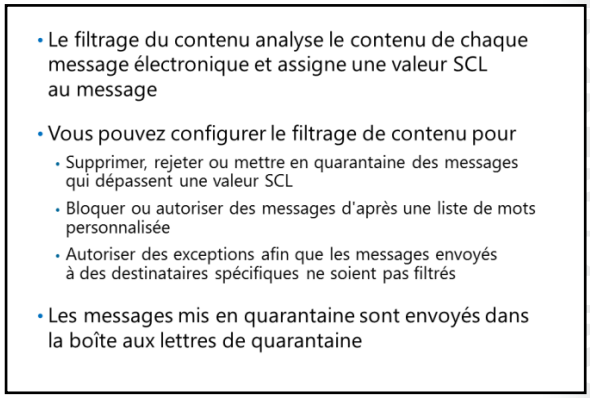
Seuils SCL et actions

Vous pouvez configurer les seuils SCL et les actions uniquement dans l'environnement de ligne de commande Exchange Management Shell. Le serveur Exchange évalue la valeur SCL d'un message spécifique et exécute l'action correspondante définie pour cette valeur dans l'environnement de ligne de commande Exchange Management Shell. Les administrateurs Exchange peuvent configurer le seuil SCL avec une valeur comprise entre 0 et 9 et définir les actions suivantes :

- Seuil de suppression SCL. Si la valeur SCL est égale ou supérieure au seuil de suppression SCL, le message sera supprimé. Si la valeur est inférieure au seuil de suppression SCL, le message sera comparé au seuil de rejet SCL.
- Seuil de rejet SCL. Si la valeur SCL est égale ou supérieure au seuil de rejet SCL, le message sera rejeté et un rapport de non-remise sera adressé à l'expéditeur original du message. Si la valeur est inférieure au seuil de rejet SCL, le message est comparé au seuil de quarantaine SCL.
- Seuil de quarantaine SCL. Si la valeur SCL est égale ou supérieure au seuil de quarantaine SCL, le message est envoyé à la boîte aux lettres de quarantaine. Les utilisateurs qui ont les autorisations administratives d'ouvrir la boîte aux lettres de quarantaine peuvent vérifier les éventuels messages faux positifs et les transférer aux destinataires. Un faux positif est un message électronique bloqué suite à l'analyse anti-courrier indésirable ou anti-programmes malveillants, alors qu'en réalité il ne s'agit pas d'un message électronique et qu'il ne contient pas de programmes malveillants. Si la valeur est inférieure au seuil de quarantaine SCL, le message est comparé au seuil SCL du dossier Courrier indésirable.
- Seuil SCL du dossier Courrier indésirable. Si la valeur SCL est égale ou supérieure au seuil de quarantaine SCL, le message est envoyé dans le dossier Courrier indésirable de l'utilisateur. Si la valeur est inférieure au seuil SCL du dossier Courrier indésirable, le message est remis dans la boîte aux lettres de l'utilisateur.

Qu'est-ce que le filtrage de contenu ?

Le filtrage de contenu est configuré pour rejeter tous les messages dont la valeur SCL est supérieure à 7. Vous pouvez modifier les paramètres par défaut de filtrage de contenu à l'aide de l'environnement de ligne de commande Exchange Management Shell.



Dans l'environnement de ligne de commande Exchange Management Shell, vous pouvez modifier les paramètres suivants :

- Configurer les mots personnalisés. Vous pouvez spécifier une liste de mots clés ou d'expressions pour empêcher le blocage d'un message qui contient ces mots. Cette fonctionnalité est utile si votre organisation doit recevoir un courrier électronique contenant des mots qui seraient normalement bloqués par l'agent de filtrage du contenu. Vous pouvez également spécifier des mots clés ou des expressions qui provoqueront le blocage de tout message qui contient ces mots par l'agent de filtrage du contenu.
- Définir des exceptions. Vous pouvez configurer des exceptions pour exclure du filtrage du contenu les messages envoyés aux destinataires figurant dans la liste des exceptions.
- Définir des actions. Vous pouvez configurer les seuils SCL et les actions de seuil. Vous pouvez configurer l'agent de filtrage du contenu pour supprimer, rejeter ou mettre en quarantaine des messages dont la valeur SCL est supérieure à la valeur spécifiée.

Remarque : Lorsque l'agent de filtrage du contenu rejette un message, il utilise la réponse par défaut **550 5.7.1 Message rejeté en raison des restrictions de contenu**. Vous pouvez personnaliser ce message à l'aide de l'applet de commande **set-ContentFilterConfig** de l'environnement de ligne de commande Exchange Management Shell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration de la boîte aux lettres de quarantaine

Lorsque la valeur SCL d'un message spécifique dépasse le seuil de mise en quarantaine SCL, l'agent de filtrage du contenu envoie le message à une boîte aux lettres de quarantaine. Avant de pouvoir configurer cette option sur le serveur de boîtes aux lettres, vous devez configurer une boîte aux lettres en tant que boîte aux lettres de quarantaine en définissant le paramètre **–quarantinemailbox** de l'applet de commande **set- contentfilterconfig**. En tant qu'administrateur de messagerie, vous devez vérifier régulièrement la boîte aux lettres de quarantaine afin de vous assurer que le filtre de contenu ne filtre pas de messages légitimes.

Remarque : Les messages sont envoyés à la boîte aux lettres de quarantaine uniquement lorsque le seuil SCL dépasse la valeur que vous avez configurée dans le filtre de contenu. Pour afficher les détails de toutes les actions que les agents de transport exécutent sur un serveur de boîtes aux lettres, utilisez les scripts situés dans le dossier suivant : **%programfiles%\Microsoft\Exchange Server\Scripts**. Le script Get-AgentLog.ps1 produit une liste brute de toutes les actions exécutées par les agents de transport. Le dossier contient plusieurs autres scripts qui génèrent des rapports sous forme de listes ; par exemple, les principaux domaines d'expéditeur bloqués, les principaux expéditeurs bloqués et les principaux destinataires bloqués. Par défaut, les journaux des agents de transport sont situés dans le dossier suivant : **%programfiles%\Microsoft\ExchangeServer\TransportRoles\Logs\AgentLog**.

Seuil SCL du dossier Courrier indésirable

Si la valeur SCL d'un message spécifique est supérieure au seuil SCL du dossier Courrier indésirable, le serveur de boîtes aux lettres place le message dans le dossier Courrier indésirable de l'utilisateur Outlook. Si la valeur SCL d'un message est inférieure à celles des seuils de suppression, de rejet, de mise en quarantaine et de dossier Courrier indésirable SCL, le serveur de boîtes aux lettres place le message dans la boîte de réception de l'utilisateur.

Meilleures pratiques de déploiement d'une solution anti-courrier indésirable

La protection anti-courrier indésirable requiert une surveillance permanente des rapports de solution anti-courrier indésirable. Les administrateurs doivent évaluer les paramètres anti-courrier indésirable et ajuster la configuration en fonction des menaces Internet actives de courrier indésirable et des commentaires des utilisateurs. Par exemple, les utilisateurs d'une organisation peuvent se plaindre qu'ils reçoivent plus de cinq courriers indésirables par jour, ce qui signifie que la configuration anti-courrier indésirable doit être améliorée à l'aide de paramètres supplémentaires.

- Considérez les meilleures pratiques suivantes
  - Mettre à jour régulièrement les définitions anti-courrier indésirable
  - Surveiller les rapports anti-courrier indésirable
  - S'informer régulièrement des dernières menaces de courrier indésirable et contre la sécurité Internet
  - Évaluer régulièrement les commentaires des utilisateurs finaux
  - Mettre à jour régulièrement la configuration anti-courrier indésirable
  - Utiliser une protection anti-courrier indésirable multicouche

Lors de la configuration des paramètres anti-courrier indésirable, considérez les meilleures pratiques suivantes :

- Mettre à jour les définitions anti-courrier indésirable. Les logiciels anti-courrier indésirable utilisent des définitions pour analyser les courriers électroniques et détecter ceux qui constituent probablement un courrier indésirable. Cependant, les expéditeurs de courrier indésirable tentent en permanence d'utiliser de nouvelles techniques pour masquer le contenu des courriers indésirables et échapper ainsi aux filtres anti-courrier indésirable les moins rigoureux. Par conséquent, les fournisseurs de logiciels anti-courrier indésirable doivent s'appliquer à mettre régulièrement à jour leurs définitions anti-courrier indésirable. De même, les organisations doivent régulièrement mettre à jour leurs définitions anti-courrier indésirable pour rester à hauteur des dernières modifications de leurs fournisseurs anti-courrier indésirable.
- Surveiller les rapports anti-courrier indésirable. Les administrateurs Exchange doivent surveiller régulièrement les rapports des logiciels anti-courrier indésirable pour évaluer le nombre total de messages reçus depuis Internet, le nombre de messages bloqués comme courriers indésirables, et le nombre de messages mis en quarantaine.
- S'informer régulièrement des dernières menaces de courrier indésirable et contre la sécurité Internet. Les administrateurs Exchange et les administrateurs de sécurité doivent régulièrement mettre à jour leurs connaissances sur les dernières menaces de sécurité, de courrier indésirable et de programmes malveillants. Les paramètres anti-courrier indésirable doivent être reconfigurés conformément aux meilleures pratiques et recommandations les plus récentes.
- Évaluer régulièrement les commentaires des utilisateurs finaux. Les commentaires des utilisateurs sur le nombre de courriers indésirables reçus par jour ou par semaine et le nombre de courriers indésirables mis en quarantaine par jour ou par semaine sont essentiels lorsque vous évaluez l'efficacité de votre solution anti-courrier indésirable. Les administrateurs Exchange et les administrateurs de sécurité doivent régulièrement analyser les commentaires des utilisateurs finaux sur leur expérience quotidienne, et reconfigurer leur solution, si nécessaire, pour assurer une meilleure protection. Par exemple, les utilisateurs peuvent se plaindre du nombre excessif de courriers indésirables reçus chaque jour. Inversement, les utilisateurs peuvent indiquer qu'ils ne reçoivent pas de courriers électroniques des partenaires commerciaux ; cela pourrait signifier que le logiciel anti-courrier indésirable doit être reconfiguré avec des paramètres de protection moins agressifs.
- Utiliser une protection anti-courrier indésirable multicouche. Les agents anti-courrier indésirable Exchange Server 2013 sont situés sur le rôle serveur de boîtes aux lettres du réseau interne ; par conséquent, il est recommandé que les courriers indésirables soient arrêtés avant qu'ils n'accèdent au réseau interne. L'un des moyens à la disposition d'une organisation consiste à déployer la protection anti-courrier indésirable hybride ; en d'autres termes, à utiliser la solution Exchange Protection Online basée sur le Cloud et les fonctionnalités Exchange anti-courrier indésirable sur site. Une autre option consiste à déployer une passerelle SMTP avec la fonctionnalité anti-courrier indésirable dans le réseau de périmètre, en plus des fonctionnalités anti-courrier indésirable du déploiement Exchange sur site.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Configuration des fonctionnalités anti-courrier indésirable sur Exchange Server 2013

Procédure de démonstration

Activation des fonctionnalités anti-courrier indésirable sur LON-MBX1

1. Basculez vers **LON-MBX1**.
2. Basculez vers l'**environnement de ligne de commande Exchange Management Shell**.
3. Dans l'environnement de ligne de commande Exchange Management Shell, installez les agents anti-courrier indésirable en exécutant le script Windows PowerShell suivant :

```
.\Install-AntiSpamAgents.ps1
```

4. Dans l'environnement de ligne de commande Exchange Management Shell, redémarrez le **service de Microsoft Exchange Transport** en exécutant l'applet de commande suivante :

```
Restart-Service MSExchangeTransport
```

5. Dans l'environnement de ligne de commande Exchange Management Shell, spécifiez les adresses IP des serveurs SMTP internes, **LON-MBX1 et LON-MBX2**, qui doivent être ignorées par l'agent d'ID de l'expéditeur, en exécutant l'applet de commande suivante :

```
Set-TransportConfig -InternalSMTPServers @{Add="172.16.0.22","172.16.0.223"}
```

6. Dans l'environnement de ligne de commande Exchange Management Shell, répertoriez les agents de transport installés en exécutant l'applet de commande suivante :

```
Get-TransportAgent
```

7. Vérifiez que les agents anti-courrier indésirable suivants sont présents : **agent de filtrage du contenu, agent d'ID de l'expéditeur, agent de filtrage des expéditeurs, agent de filtrage des destinataires, agent d'analyse de protocole**.

Configuration du filtrage du contenu sur LON-MBX1

1. Dans l'environnement de ligne de commande Exchange Management Shell, vérifiez que le filtrage du contenu est activé en exécutant l'applet de commande suivante :

```
Get-ContentFilterConfig | Format-List Enabled
```

   Vérifiez que **Enabled:True** s'affiche.

2. Dans l'environnement de ligne de commande Exchange Management Shell, configurez l'expression bloquée **Poker results** en exécutant l'applet de commande suivante :

```
Add-ContentFilterPhrase -Influence BadWord -Phrase Poker results
```

3. Dans l'environnement de ligne de commande Exchange Management Shell, configurez l'expression autorisée **Report document** en exécutant l'applet de commande suivante :

```
Add-ContentFilterPhrase -Influence GoodWord -Phrase Report document
```

Atelier pratique : Planification et configuration de la sécurité des messages

Scénario

Vous êtes l'administrateur de la messagerie chez A. Datum Corporation, qui est une grande entreprise multinationale. Votre organisation a déployé Exchange Server 2013 en interne, et maintenant vous devez configurer les options relatives à la sécurité des messages.

Objectifs

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

- configurer les logiciels anti-programmes malveillants dans Exchange Server 2013.
- configurer les logiciels anti-courrier indésirable dans Exchange Server 2013 ;

Configuration de l'atelier pratique

Durée approximative : **45 minutes**

Ordinateurs virtuels	22341B-LON-DC1 22341B-LON-CAS1 22341B-LON-MBX1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V® Windows, cliquez sur **22341B-LON-DC1**, puis, dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
   a. Nom d'utilisateur : **ADATUM\Administrateur**
   b. Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22341B-LON-MBX1** et **22341B-LON-CAS1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Configurer les options anti-programmes malveillants dans Exchange Server 2013

Scénario

L'organisation A. Datum a décidé d'utiliser les fonctionnalités anti-programmes malveillants d'Exchange Server 2013. Vous devez configurer les fonctionnalités anti-programmes malveillants pour empêcher que les programmes malveillants n'accèdent à votre réseau.

Les tâches principales de cet exercice sont les suivantes :

1. Activer les fonctionnalités anti-programmes malveillants dans Exchange Server 2013.
2. Configurer la stratégie anti-programmes malveillants par défaut dans Exchange Server 2013.

▶ Tâche 1 : Activer les fonctionnalités anti-programmes malveillants dans Exchange Server 2013

1. Sur LON-MBX1, sur l'écran Accueil, cliquez sur l'environnement de ligne de commande **Exchange Management Shell**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, passez du dossier actif au dossier **\Program Files\Microsoft\Exchange Server\V15\Scripts** en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
cd "\Program Files\Microsoft\Exchange Server\V15\Scripts"
```

3. Dans l'environnement de ligne de commande Exchange Management Shell, activez l'analyse anti-programmes malveillants en tapant le script suivant :

```
.\Enable-AntimalwareScanning.ps1
```

4. Vérifiez que le message suivant apparaît : **Les moteurs anti-programmes malveillants sont en cours de mise à jour. Cette opération peut prendre quelques minutes**. Attendez la fin du processus de mise à jour..
5. Dans l'environnement de ligne de commande Exchange Management Shell, redémarrez le **service de Microsoft Exchange Transport** en exécutant l'applet de commande suivante :

```
Restart-Service MSExchangeTransport
```

6. Dans l'environnement de ligne de commande Exchange Management Shell, répertoriez les agents de transport installés en exécutant l'applet de commande suivante :

```
Get-TransportAgent
```

7. Vérifiez que l'agent anti-programmes malveillants suivant est répertorié : **Malware Agent**. Notez que l'état de l'agent anti-programmes malveillants est **Enabled True** si le script a été autorisé à s'exécuter.

▶ Tâche 2 : Configurer la stratégie anti-programmes malveillants par défaut dans Exchange Server 2013

1. Basculez vers **LON-CAS1**.
2. Démarrez **Internet Explorer**.

3. Dans Internet Explorer, ouvrez le Centre d'administration Exchange situé à l'adresse suivante : **https://lon-cas1.adatum.com/ecp**.
4. Connectez-vous au CAE en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
5. Dans le Centre d'administration Exchange, à partir de la fonctionnalité de protection, ouvrez l'onglet **filtre anti-programme malveillant**.

   Modifiez la stratégie anti-programmes malveillants par défaut avec les paramètres suivants :

   - **Réponse à la détection de programmes malveillants** : sélectionnez **Supprimer toutes les pièces jointes et utiliser le texte d'avertissement personnalisé**.
   - Dans la zone **Texte d'avertissement personnalisé**, tapez le texte suivant : **La pièce jointe a été supprimée, car elle contenait des programmes malveillants. Contactez votre administrateur**.
   - **Notifications** : activez les deux cases à cocher **Informer les expéditeurs internes et Informer les expéditeurs externes**.
   - **Notifications de l'administrateur** : activez la case à cocher **Informer l'administrateur des messages d'expéditeurs internes non remis**.
   - Zone Adresse de messagerie de l'administrateur : tapez **administrateur@adatum.com.**
6. Ensuite, continuez à modifier les paramètres de la stratégie anti-programmes malveillants par défaut :
   - **Notifications de l'administrateur** : activez la case à cocher **Informer l'administrateur des messages d'expéditeurs externes non remis**.
   - Zone Adresse de messagerie de l'administrateur : tapez **administrateur@adatum.com**.
7. Enregistrez les paramètres de configuration.

Exercice 2 : Configuration des options anti-courrier indésirable sur Exchange Server

Scénario

L'organisation A. Datum a décidé d'utiliser les fonctionnalités anti-courrier indésirable d'Exchange Server 2013. Vous devez configurer les fonctionnalités anti-courrier indésirable pour empêcher que le courrier indésirable n'accède à votre réseau.

Les tâches principales de cet exercice sont les suivantes :

1. Activer les fonctionnalités anti-courrier indésirable sur LON-MBX1.
2. Configurer le filtrage de contenu sur LON-MBX1.
3. Configurer le filtrage des expéditeurs et des destinataires sur LON-MBX1.

▶ Tâche 1 : Activer les fonctionnalités anti-courrier indésirable sur LON-MBX1

1. Basculez vers **LON-MBX1**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, installez les agents anti-courrier indésirable en exécutant le script PowerShell suivant :

```
.\Install-AntiSpamAgents.ps1
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans l'environnement de ligne de commande Exchange Management Shell, redémarrez le **service de Microsoft Exchange Transport** en exécutant l'applet de commande suivante :

```
Restart-Service MSExchangeTransport
```

4. Dans l'environnement de ligne de commande Exchange Management Shell, spécifiez les adresses IP des serveurs SMTP internes, **LON-MBX1 et LON-MBX2**, qui doivent être ignorées par l'agent d'ID de l'expéditeur, en exécutant l'applet de commande suivante :

```
Set-TransportConfig -InternalSMTPServers @{Add="172.16.0.22","172.16.0.223"}
```

5. Dans l'environnement de ligne de commande Exchange Management Shell, répertoriez les agents de transport installés en exécutant l'applet de commande suivante :

```
Get-TransportAgent
```

6. Vérifiez que les agents anti-courrier indésirable suivants sont présents : **Content Filter Agent, Sender ID Agent, Sender Filter Agent, Recipient Filter Agent, Protocol Analysis Agent**.

▶ Tâche 2 : Configurer le filtrage de contenu sur LON-MBX1

1. Dans l'environnement de ligne de commande Exchange Management Shell, vérifiez que le filtrage du contenu est activé en exécutant l'applet de commande suivante :

```
Get-ContentFilterConfig | Format-List Enabled
```

2. Vérifiez que **Enabled:True** s'affiche.

3. Dans l'environnement de ligne de commande Exchange Management Shell, configurez l'expression bloquée **Poker results** en exécutant l'applet de commande suivante :

```
Add-ContentFilterPhrase -Influence BadWord -Phrase "Poker results"
```

4. Dans l'environnement de ligne de commande Exchange Management Shell, configurez l'expression autorisée **Report document** en exécutant l'applet de commande suivante :

```
Add-ContentFilterPhrase -Influence GoodWord -Phrase "Report document"
```

5. Dans l'environnement de ligne de commande Exchange Management Shell, configurez la boîte aux lettres de quarantaine **quarantaine@adatum.com** en exécutant l'applet de commande suivante, puis appuyez sur Entrée :

```
Set-ContentFilterConfig
-QuarantineMailbox quarantaine@adatum.com
```

Remarque : dans un environnement de production, vous devez également créer une boîte aux lettres utilisateur et la configurer comme une boîte aux lettres de quarantaine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans l'environnement de ligne de commande Exchange Management Shell, configurez les seuils SCL avec les valeurs suivantes **SCLRejectThreshold 8**, **SCLQuarantineThreshold 7**, et activez la quarantaine en exécutant l'applet de commande suivante :

```
Set-ContentFilterConfig -SCLRejectEnabled $true -SCLRejectThreshold 8 -
SCLQuarantineEnabled $true -SCLQuarantineThreshold 7
```

7. Dans l'environnement de ligne de commande Exchange Management Shell, configurez la réponse de rejet personnalisée **Your message was rejected by our spam filter. Contact your administrator.** en exécutant l'applet de commande suivante :

```
Set-ContentFilterConfig -RejectionResponse "Your message was rejected by our spam
filter. Contact your administrator."
```

8. Dans l'environnement de ligne de commande Exchange Management Shell, configurez le **seuil SCL de courrier indésirable** avec la valeur **6** pour toutes les boîtes aux lettres de votre organisation en exécutant l'applet de commande suivante :

```
Set-OrganizationConfig -SCLJunkThreshold 6
```

▶ Tâche 3 : Configurer le filtrage des expéditeurs et des destinataires sur LON-MBX1

1. Sur LON-MBX1, dans l'environnement de ligne de commande Exchange Management Shell, configurez le filtrage des expéditeurs pour bloquer les messages en provenance de **marketing@contoso.com** en exécutant l'applet de commande suivante :

```
Set-SenderFilterConfig -BlockedSenders marketing@contoso.com
```

2. Dans l'environnement de ligne de commande Exchange Management Shell, configurez le filtrage des destinataires pour bloquer les messages envoyés à **helpdesk@adatum.com** en exécutant l'applet de commande suivante **:**

```
Set-RecipientFilterConfig -BlockListEnabled $true -BlockedRecipients
helpdesk@adatum.com
```

Remarque : dans ce scénario nous supposons que l'adresse de messagerie helpdesk@adatum.com est à utilisation interne uniquement et qu'elle ne doit recevoir aucun message électronique d'expéditeurs externes.

Exercice 3 : Validation de la configuration des logiciels anti-courrier indésirable et anti-programmes malveillants

Scénario

Dans cet exercice, vous devrez valider la configuration des logiciels anti-courrier indésirable et anti-programmes malveillants en envoyant un message électronique de test qui contient des programmes malveillants de test simulés. Vous vous connecterez ensuite à LON-MBX1 à l'aide de la commande **telnet**, puis vous enverrez des messages électroniques qui devront être bloqués par les agents anti-courrier indésirable.

Les tâches principales de cet exercice sont les suivantes :

1. Valider la configuration anti-programmes malveillants.
2. Valider la configuration anti-courrier indésirable.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 1 : Valider la configuration anti-programmes malveillants

1. Basculez vers **LON-CAS1**.
2. Modifiez le fichier **E:\Labfiles\Mod09\Eicar.txt** et supprimez les sauts de ligne entre la première ligne et la ligne de texte suivante. La totalité du texte doit se trouver sur une ligne. Enregistrez le fichier.
3. Fermez toutes les instances d'Internet Explorer.
4. Ouvrez **Internet Explorer** et tapez **https://lon-cas1.adatum.com/owa**.
5. Connectez-vous en tant qu'**ADATUM\Michael** avec le mot de passe **Pa$$w0rd**, puis enregistrez les paramètres par défaut dans la page **Langue et Fuseau horaire**.
6. Dans la fenêtre Outlook Web App, créez un message électronique pour **mark@adatum.com** dont l'objet est **Message de test**, le corps du message **Rapport quotidien**, puis joignez le fichier nommé **Eicar.txt** situé dans **E:\Labfiles\Mod09**.
7. Dans la fenêtre **Outlook Web App**, cliquez sur **Michael Allen**, puis sur **Se déconnecter**.
8. Dans Internet Explorer, dans la page de connexion **Outlook Web App**, connectez-vous en tant qu'**ADATUM\Mark** avec le mot de passe **Pa$$w0rd**. Cliquez sur **enregistrer**.
9. Dans la fenêtre **Outlook Web App**, double-cliquez sur le nouveau message en provenance de **Michael Allen**. Ouvrez la pièce jointe et vérifiez que le code présent dans le fichier a été supprimé et remplacé par le texte personnalisé que vous avez configuré.
10. Dans la fenêtre **Outlook Web App**, cliquez sur **Mark Bebbington**, puis sur **Se déconnecter**.

▶ Tâche 2 : Valider la configuration anti-courrier indésirable

1. Basculez vers **LON-DC1.**
2. Sur **LON-DC1**, ouvrez Windows PowerShell dans la barre des tâches.
3. À l'invite de commandes, tapez **telnet LON-CAS1 smtp** et appuyez sur Entrée.
4. Tapez **helo** et appuyez sur Entrée.
5. Tapez **mail from: info@internet.com** et appuyez sur Entrée.

   Vous devriez recevoir la réponse : **250 2.1.0 Sender OK**
6. Tapez **rcpt to: michael@adatum.com** et appuyez sur Entrée.

   Réponse : **250 2.1.5 Recipient OK**
7. Tapez **data** et appuyez sur Entrée.

   Réponse : **354 Start mail input; end with <CRLF>.<CRLF>**
8. Tapez **Subject: Information for you**, puis appuyez deux fois sur Entrée. Tapez **Please find below poker results**, puis appuyez sur Entrée.
9. Appuyez sur la touche point (**.**), puis sur **Entrée**.
10. Vérifiez que le message suivant s'affiche : **Your message was rejected by our spam filter. Contact your administrator**.
11. Tapez **Quit** et appuyez sur **Entrée**.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels en procédant comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V®**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-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 **22341B-LON-CAS1** et **22341B-LON-MBX1**.

Résultats : À la fin de cet exercice, vous aurez validé l'analyse anti-programmes malveillants lors de l'envoi d'un message de test avec une pièce jointe de simulation de programmes malveillants, dans laquelle la pièce jointe sera supprimée par la fonctionnalité anti-programmes malveillants d'Exchange Server 2013. Vous aurez également validé le filtrage de contenu anti-courrier indésirable lors de l'envoi d'une simulation de message indésirable dans laquelle le message sera stocké dans le dossier Courrier indésirable du destinataire par la fonctionnalité de filtrage de contenu d'Exchange Server 2013.

Question : Quels sont les agents anti-courrier indésirable disponibles dans Exchange Server 2013 ?

Question : Quelle est la fonction du seuil SCL ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quelle stratégie de protection anti-courrier indésirable et anti-programmes malveillants allez-vous proposer pour votre organisation ?

Problèmes réels et scénarios

Vos employés se plaignent souvent que leurs messages électroniques sont bloqués à tort comme courrier indésirable ou programme malveillant. Ce courrier électronique faussement positif est l'un des problèmes les plus importants de la protection anti-courrier indésirable et anti-programmes malveillants. Un faux positif est un message électronique bloqué suite à l'analyse anti-courrier indésirable ou anti-programmes malveillants, alors qu'en réalité il ne s'agit pas d'un message électronique indésirable et qu'il ne contient aucun programme malveillant.

Pour résoudre le problème, contactez les administrateurs de sécurité pour qu'ils enquêtent sur les raisons pour lesquelles ces messages ont été identifiés comme du courrier indésirable ou des programmes malveillants. Réévaluez vos paramètres de protection anti-courrier indésirable et anti-programmes malveillants, et modifiez les paramètres si nécessaire.

Méthode conseillée

Lors de la configuration d'une solution anti-courrier indésirable et antivirus, suivez toujours la documentation technique du fournisseur sur la façon de déployer, de gérer et de maintenir ces solutions. Comme les menaces Internet changent tous les jours, les administrateurs Exchange et les administrateurs de sécurité doivent se tenir régulièrement informés des dernières menaces contre la sécurité. Comme les menaces de sécurité évoluent, les solutions et les meilleures pratiques de gestion anti-courrier indésirable et antivirus peuvent également changer.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Vous avez configuré le filtrage de contenu anti-courrier indésirable, mais les employés se plaignent qu'ils continuent à recevoir des courriers indésirables.	
Vous avez configuré le filtrage de contenu anti-courrier indésirable, mais les employés se plaignent de ne pas recevoir de courrier électronique des partenaires commerciaux.	
Un employé s'est plaint que, lorsqu'il a reçu un courrier électronique, la pièce jointe était manquante et qu'elle a été remplacée par une autre pièce jointe contenant un avertissement au sujet de programmes malveillants.	

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Outils

- Centre d'administration Exchange (CAE) : utilisé pour configurer la stratégie anti-programmes malveillants
- Environnement de ligne de commande Exchange Management Shell : utilisé pour configurer la stratégie anti-programmes malveillants, les paramètres anti-programmes malveillants et les paramètres anti-courrier indésirable

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 10

Planification et configuration de la sécurité et de l'audit administratifs

Table des matières :

Vue d'ensemble du module **10-1**

Leçon 1 : Configuration du contrôle d'accès basé sur les rôles **10-2**

Leçon 2 : Configuration de la journalisation d'audit **10-16**

Atelier pratique : Configuration de la sécurité et de l'audit administratifs **10-21**

Contrôle des acquis et éléments à retenir **10-28**

Vue d'ensemble du module

Dans de nombreuses organisations, Microsoft® Exchange Server fournit une fonction métier essentielle aux utilisateurs internes et externes. En outre, bon nombre d'organisations exposent au moins quelques-uns de leurs serveurs Exchange à Internet. Pour ces raisons, il est important de prendre les mesures appropriées pour sécuriser le déploiement d'Exchange Server. La sécurisation de votre déploiement d'Exchange Server implique plusieurs composants : la configuration correcte des autorisations d'administration et la sécurisation de la configuration d'Exchange Server. Ce module décrit comment configurer les autorisations et sécuriser Microsoft® Exchange Server 2013.

Objectifs

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

- configurer des autorisations à l'aide du contrôle d'accès basé sur les rôles (RBAC, Role-Based Access Control) ;
- configurer la journalisation d'audit.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Configuration du contrôle d'accès basé sur les rôles

Exchange Server 2013 utilise le modèle d'autorisations à l'aide du contrôle d'accès basé sur les rôles (RBAC, Role-Based Access Control) pour restreindre les tâches d'administration que les utilisateurs peuvent effectuer sur les rôles serveur de boîtes aux lettres, de transport Edge et d'accès au client. Avec le contrôle d'accès basé sur les rôles, vous pouvez contrôler les ressources que les administrateurs peuvent configurer et les fonctionnalités auxquelles les utilisateurs peuvent accéder. Cette leçon décrit comment implémenter des autorisations RBAC dans Exchange Server 2013 et comment configurer des autorisations sur les serveurs de transport Edge.

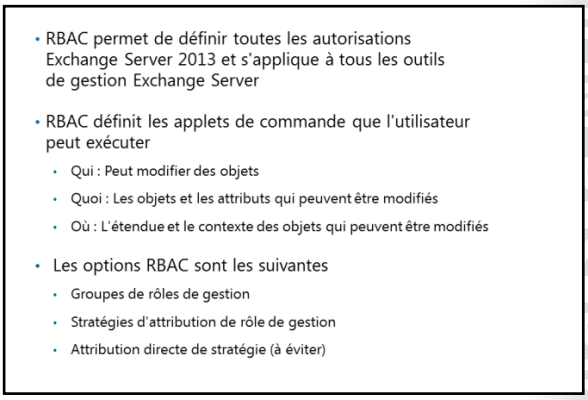
Objectifs de la leçon

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

- décrire le contrôle d'accès basé sur les rôles (RBAC) ;
- décrire les groupes de rôles de gestion ;
- identifier les groupes de rôles de gestion prédéfinis d'Exchange Server 2013 ;
- gérer les autorisations RBAC ;
- configurer des groupes de rôles de gestion personnalisés ;
- décrire les stratégies d'attribution de rôle de gestion ;
- décrire les autorisations fractionnées d'Exchange Server ;
- configurer des autorisations fractionnées RBAC ;
- configurer les autorisations fractionnées des services de domaine Active Directory® (AD DS).

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Qu'est-ce que le contrôle d'accès basé sur les rôles ?



RBAC est le modèle d'autorisations disponible depuis la version finale de Microsoft® Exchange Server 2010. Avec RBAC, vous ne devez pas modifier et gérer des listes de contrôle d'accès (ACL) sur des objets Exchange Server ou services de domaine Active Directory (AD DS). Dans Exchange Server 2013, RBAC contrôle les tâches d'administration que les utilisateurs peuvent effectuer et jusqu'à quel point ils peuvent administrer leurs propres boîtes aux lettres et groupes de distribution. Lorsque vous configurez des autorisations RBAC, vous pouvez définir très exactement les applets de commande de l'environnement de ligne de commande Exchange Management Shell qu'un utilisateur peut exécuter et les objets et attributs qu'il peut modifier.

Tous les outils d'administration Exchange Server, y compris l'environnement de ligne de commande Exchange Management Shell et le Centre d'administration Exchange (CAE), utilise RBAC pour déterminer les autorisations des utilisateurs. Par conséquent, les autorisations sont cohérentes quel que soit l'outil que vous utilisez.

Remarque : Si RBAC autorise un utilisateur à exécuter une applet de commande spécifique, celle-ci s'exécute en fait dans le contexte de sécurité du sous-système approuvé Exchange et non dans le contexte de l'utilisateur. Le sous-système approuvé Exchange est un groupe universel de sécurité doté de privilèges élevés disposant de l'accès en lecture et écriture à tous les objets associés à Exchange Server dans l'organisation Exchange. C'est aussi un membre des groupes de sécurité locaux des administrateurs et le groupe universel de sécurité des autorisations Windows Exchange qui permettent à Exchange Server 2013 de créer et de gérer des objets AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

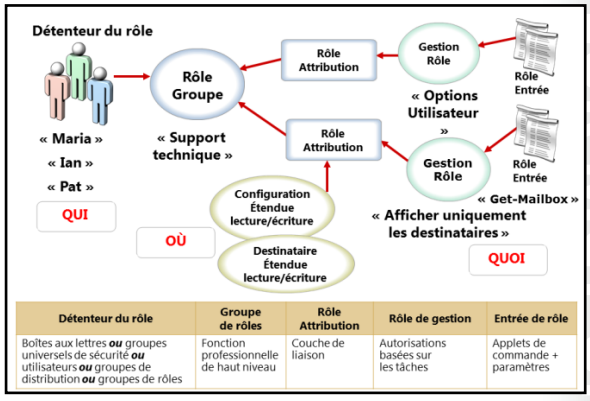
Options RBAC

RBAC attribue des autorisations aux utilisateurs de deux manières principales, selon que l'utilisateur est un administrateur ou un utilisateur final :

- *Groupes de rôles de gestion*. RBAC utilise des groupes de rôles de gestion pour attribuer des autorisations aux administrateurs. Ces administrateurs peuvent avoir besoin d'autorisations pour gérer l'organisation Exchange ou une partie de celle-ci. Certains administrateurs peuvent avoir besoin d'autorisations limitées pour gérer certaines fonctionnalités d'Exchange Server, telles que la conformité ou des destinataires spécifiques. Pour utiliser des groupes de rôles de gestion, ajoutez des utilisateurs au groupe de rôles de gestion prédéfini approprié ou à un groupe de rôles de gestion personnalisé. RBAC attribue à chaque groupe de rôles un ou plusieurs rôles de gestion qui définissent les autorisations précises qu'il accorde à ce groupe.
- *Stratégies d'attribution de rôle de gestion*. Les stratégies d'attribution de rôle de gestion sont utilisées pour attribuer des rôles de gestion aux utilisateurs finaux. Les stratégies d'attribution de rôle se composent des rôles qui contrôlent ce que les utilisateurs peuvent faire avec leurs boîtes aux lettres ou groupes de distribution. Ces rôles n'autorisent pas la gestion des fonctionnalités auxquelles les utilisateurs ne sont pas directement associés.

Remarque : Vous pouvez également utiliser l'attribution de rôle directe pour attribuer des autorisations. L'attribution de rôle directe est une méthode avancée permettant d'attribuer directement des rôles de gestion à un utilisateur ou à un groupe universel de sécurité sans avoir besoin d'utiliser un groupe de rôles ou une stratégie d'attribution de rôle. Les attributions de rôle directes sont utiles lorsque vous devez fournir un jeu granulaire d'autorisations à un utilisateur spécifique uniquement. Toutefois, nous vous recommandons d'éviter d'utiliser l'attribution de rôle directe, car elle est plus compliquée à configurer et à gérer que d'utiliser les groupes de rôles de gestion.

Que sont les groupes de rôles de gestion ?



Un groupe de rôles de gestion est un groupe universel de sécurité qui simplifie le processus d'attribution des rôles de gestion à un groupe d'utilisateurs. Tous les membres d'un groupe de rôles sont attribués au même ensemble de rôles. Dans Exchange Server 2013, des groupes tels que Gestion de l'organisation et Gestion des destinataires sont attribués aux rôles d'administrateurs et de spécialistes qui définissent les tâches d'administration principales. Les groupes de rôles vous permettent d'attribuer plus facilement un éventail plus large d'autorisations à un groupe d'administrateurs ou d'utilisateurs spécialistes.

Les groupes de rôles de gestion sont utilisés pour attribuer des autorisations d'administrateur à des groupes d'utilisateurs. Pour comprendre le fonctionnement des groupes de rôles de gestion, vous devez comprendre leurs composants.

Composants des groupes de rôles de gestion

Les groupes de rôles de gestion utilisent plusieurs composants sous-jacents pour définir comment RBAC attribue les autorisations. En voici quelques-uns :

- *Détenteur du rôle*. Un détenteur de rôle est un utilisateur ou groupe de sécurité qui peut être ajouté à un groupe de rôles de gestion. Lorsqu'un utilisateur devient membre d'un groupe de rôles de gestion, RBAC lui accorde toutes les autorisations fournies par les rôles de gestion. Vous pouvez soit ajouter des comptes d'utilisateurs au groupe dans AD DS, soit utiliser l'applet de commande **Add-RoleGroupMember**.
- *Groupe de rôles de gestion*. Le groupe de rôles de gestion est un groupe universel de sécurité qui contient les utilisateurs ou les groupes qui sont membres du groupe de rôles. Les groupes de rôles de gestion sont attribués à des rôles de gestion. La combinaison de tous les rôles attribués à un groupe de rôles définit tout ce que les utilisateurs ajoutés à ce groupe de rôles peuvent gérer dans l'organisation Exchange.
- *Rôle de gestion*. Un rôle de gestion est un conteneur pour un groupe d'entrées de rôle de gestion. Ces entrées définissent les tâches que les utilisateurs peuvent effectuer si RBAC leur attribue le rôle à l'aide d'attributions de rôle de gestion.
- *Entrées de rôle de gestion*. Une entrée de rôle de gestion est une applet de commande, y compris ses paramètres, que vous ajoutez à un rôle de gestion. En ajoutant des applets de commande à un rôle en tant qu'entrées de rôle de gestion, vous accordez des droits de gestion ou d'affichage des objets associés à cette applet de commande.
- *Attribution de rôle de gestion*. Une attribution de rôle de gestion attribue un rôle de gestion à un groupe de rôles. Une fois que vous avez créé un rôle de gestion, vous devez l'attribuer à un groupe de rôles afin que les détenteurs du rôle puissent l'utiliser. L'attribution d'un rôle de gestion à un groupe de rôles accorde aux détenteurs du rôle la capacité d'utiliser les applets de commande que ce rôle de gestion définit.
- *Étendue de rôle de gestion*. Une étendue de rôle de gestion est le champ d'influence ou l'impact qu'a le détenteur du rôle une fois que le contrôle d'accès basé sur les rôles lui attribue un rôle de gestion. Lorsque vous attribuez un rôle de gestion, vous pouvez utiliser des étendues de gestion pour cibler les objets contrôlés par ce rôle. Les étendues peuvent inclure des serveurs, des unités d'organisation, et des objets destinataires, entre autres.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exemples de groupes de rôles de gestion

Les groupes de rôles de gestion définissent qui peut exécuter des tâches spécifiques et l'étendue dans laquelle les administrateurs peuvent exécuter ces tâches. Par exemple, vous pouvez utiliser le contrôle d'accès basé sur les rôles pour attribuer des autorisations comme indiqué dans le tableau suivant :

Détenteur du rôle	Groupe de rôles de gestion	Rôle de gestion	Entrées de rôle de gestion	Étendue de rôle de gestion
Stan	Gestion de l'organisation	Gestion de l'organisation	Toutes les applets de commande Exchange	Organisation
Joel	Support technique	HelpDesk	Applets de commande relatives à la gestion des boîtes aux lettres et des comptes d'utilisateurs	Organisation
Andy	Administrateurs des ventes	SalesAdminRole	Applets de commande relatives à la gestion des destinataires uniquement	Unité d'organisation (OU) du service des ventes dans AD DS ou Active Directory

Groupes de rôles de gestion prédéfinis

Exchange Server 2013 inclut plusieurs groupes de rôles prédéfinis que vous pouvez utiliser pour fournir divers niveaux d'autorisations d'administration aux groupes d'utilisateurs. Vous pouvez ajouter des utilisateurs à tout groupe de rôles prédéfini ou en supprimer. Vous pouvez également ajouter des attributions de rôle à la plupart des groupes de rôles ou en supprimer.

Les groupes de rôles de gestion sont notamment les suivants

- Gestion de l'organisation
- Gestion de l'organisation en affichage seul
- Gestion des destinataires
- Gestion de la messagerie unifiée
- Gestion de la détection
- Gestion des enregistrements
- Gestion du serveur
- Support technique
- Gestion des dossiers publics
- Installation déléguée
- Gestion de la conformité (nouveauté dans Exchange Server 2013)
- Gestion de l'hygiène (nouveauté dans Exchange Server 2013)

Groupe de rôles	Description
Gestion de l'organisation	Les détenteurs du rôle ont accès à l'organisation Exchange Server 2013 entière et peuvent exécuter quasiment n'importe quelle tâche sur n'importe quel objet Exchange Server.
Gestion de l'organisation en affichage seul	Les détenteurs du rôle peuvent afficher les propriétés de tout objet de l'organisation.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(*suite*)

Groupe de rôles	Description
Gestion des destinataires	Les détenteurs du rôle peuvent créer ou modifier des destinataires Exchange Server 2013 dans l'organisation Exchange Server.
Gestion de la messagerie unifiée	Les détenteurs du rôle peuvent gérer les fonctionnalités de messagerie unifiée dans l'organisation, telles que la configuration du serveur de messagerie unifiée, les propriétés des boîtes aux lettres, les invites et la configuration du standard automatique.
Gestion de la détection	Les détenteurs du rôle peuvent exécuter des recherches dans les boîtes aux lettres de l'organisation Exchange pour trouver les données conformes à des critères spécifiques.
Gestion des enregistrements	Les détenteurs du rôle peuvent configurer les fonctionnalités de conformité, telles que les balises de stratégie de rétention, la classification des messages et les règles de transport. Les détenteurs du rôle peuvent également exporter des journaux d'audit.
Gestion du serveur	Les détenteurs du rôle ont accès à la configuration Exchange Server. Ils n'ont pas accès aux fonctions d'administration de la configuration des destinataires.
Support technique	Les détenteurs du rôle peuvent exécuter une gestion limitée des destinataires.
Gestion des dossiers publics	Les détenteurs du rôle peuvent gérer les dossiers publics et les bases de données sur les serveurs Exchange.
Installation déléguée	Les détenteurs du rôle peuvent déployer les serveurs Exchange précédemment configurés.
Gestion de la conformité	Les détenteurs du rôle peuvent configurer et gérer les paramètres de conformité. Ce groupe de rôles est une nouveauté d'Exchange Server 2013.
Gestion de l'hygiène	Les détenteurs du rôle peuvent gérer les fonctionnalités anti-courrier indésirable d'Exchange Server et accorder des autorisations pour que les produits antivirus soient intégrés à Exchange Server. Ce groupe de rôles est une nouveauté d'Exchange Server 2013.

 **Remarque :** Tous ces groupes de rôles se trouvent dans l'unité d'organisation (OU) Groupes de sécurité Microsoft Exchange Server dans AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Démonstration : Gestion des autorisations à l'aide des groupes de rôles prédéfinis

Dans cette démonstration, vous allez étudier comment gérer les autorisations RBAC dans Exchange Server 2013 à l'aide des groupes de rôles prédéfinis. Vous allez voir comment ajouter des utilisateurs aux groupes de rôles prédéfinis et comment le contrôle d'accès basé sur les rôles attribue les autorisations obtenues aux comptes d'utilisateurs.

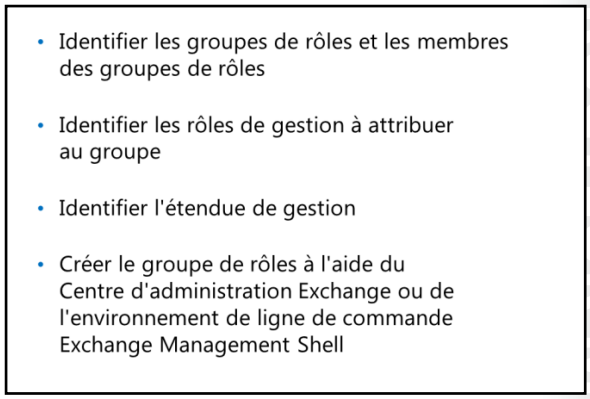
Procédure de démonstration

1. Sur LON-DC1, ouvrez **Utilisateurs et ordinateurs Active Directory** et ajoutez **Tony** au groupe **Recipient Management** situé dans l'unité d'organisation Adatum.com\Microsoft Exchange Security Groups.
2. Sur LON-CAS1, ouvrez le CAE, connectez-vous en tant qu'**Adatum\Tony** et vérifiez que vous voyez les serveurs Exchange mais que vous ne pouvez pas les modifier. Vérifiez également que vous pouvez modifier les propriétés de l'utilisateur Adam Barr.
3. Ouvrez l'**environnement de ligne de commande Exchange Management Shell** et exécutez les applets de commande suivantes :

```
Get-ExchangeServer | FL
Set-User Adam -Title Manager
```

Processus de configuration des groupes de rôles personnalisés

Outre les groupes de rôles prédéfinis, vous pouvez également créer des groupes de rôles personnalisés pour déléguer des autorisations spécifiques dans l'organisation Exchange. Utilisez cette option lorsque votre capacité à limiter les autorisations est au-delà de l'étendue des groupes de rôles prédéfinis.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Configuration d'un groupe de rôles de gestion personnalisé

Le contrôle d'accès basé sur les rôles offre plusieurs manières possibles d'attribuer des autorisations dans un environnement Exchange Server 2013. Par exemple, il vous permet d'attribuer des autorisations à un groupe d'administrateurs d'une filiale qui doivent uniquement gérer des tâches de destinataire pour les utilisateurs et les boîtes aux lettres de la filiale sur les serveurs de boîtes aux lettres de celle-ci. Pour implémenter ce scénario, vous devez procéder comme suit :

1. Créez un groupe de rôles et ajoutez-y les administrateurs de la filiale. Vous pouvez utiliser l'applet de commande **New-RoleGroup** pour créer le groupe ou créer le groupe à l'aide du Centre d'administration Exchange. Lorsque vous créez ce groupe, vous devez spécifier les rôles de gestion. En outre, vous pouvez également spécifier l'étendue de gestion du rôle.
2. Attribuez des rôles de gestion aux administrateurs de la filiale. Pour déléguer des autorisations à un groupe de rôles personnalisé, vous pouvez utiliser un ou plusieurs des rôles de gestion prédéfinis par défaut, ou vous pouvez créer un rôle de gestion personnalisé basé sur l'un des rôles de gestion prédéfinis. Exchange Server 2013 inclut environ 70 rôles de gestion prédéfinis qui fournissent des niveaux granulaires d'autorisations. Pour afficher la liste complète de tous les rôles de gestion, utilisez l'applet de commande **get-managementrole**. Pour afficher des informations détaillées sur un rôle de gestion, tapez **get-managementrole nom_rôle | FL**, puis appuyez sur Entrée. Vous pouvez également afficher ces informations détaillées dans le Centre d'administration Exchange.

 **Remarque :** Vous pouvez également configurer un nouveau rôle de gestion au lieu d'utiliser l'un des rôles de gestion existants. Pour ce faire, utilisez l'applet de commande **New-ManagementRole** pour créer un rôle de gestion personnalisé basé sur l'un des rôles de gestion existants. Vous pouvez ensuite ajouter ou supprimer des entrées de rôle de gestion en fonction des besoins. Par défaut, le nouveau rôle de gestion hérite de toutes les autorisations attribuées au rôle parent. Si nécessaire, vous pouvez supprimer des autorisations du rôle à l'aide de l'applet de commande **Remove-managementroleentry**. Cependant, il peut s'avérer compliqué de créer un rôle de gestion et de supprimer les entrées de rôle de gestion inutiles, par conséquent, nous vous recommandons d'utiliser autant que possible l'un des rôles existants.

3. Identifiez l'étendue de gestion du rôle de gestion. Par exemple, dans le scénario de la filiale, vous pouvez créer une attribution de rôle ayant une étendue OU spécifique à l'unité d'organisation de la filiale.
4. Créez le groupe de rôles de gestion à l'aide des informations que vous collectez. Vous pouvez utiliser le CAE ou l'applet de commande **New-RoleGroup** pour créer le lien entre le groupe de rôles, les rôles de gestion et l'étendue de gestion. Par exemple, envisagez la commande suivante : **New-RoleGroup – Name BranchOfficeAdmins –roles "Mail Recipients", "Distribution Groups", "Move Mailboxes", "Mail Recipient Creation"– RecipientOrganizationalUnitScope Adatum.com/BranchOffice**

   L'applet de commande effectue les opérations suivantes :

   - Elle crée un groupe de rôles nommé BranchOfficeAdmins.
   - Elle attribue les rôles de gestion Destinataires du courrier, Groupes de distribution, Déplacer des boîtes aux lettres et Création de destinataire du courrier au groupe de rôles BranchOfficeAdmins.
   - Elle configure une étendue de rôle de gestion limitée à l'unité d'organisation BranchOffice dans le domaine Adatum.com.

Démonstration : Configuration des groupes de rôles personnalisés

Dans cette démonstration, vous allez apprendre à créer un rôle personnalisé de groupe, ajouter des rôles et des membres au rôle de groupe, et vérifier que les autorisations que vous avez accordées fonctionnent comme prévu.

Procédure de démonstration

1. Sur LON-CAS1, dans le CAE, créez un groupe de rôles nommé **MarketingAdmins**. Ce groupe doit se trouver dans l'unité d'organisation Marketing et les rôles Destinataires du courrier et Création de destinataire du courrier devront lui être attribués. Brad Sutton doit au départ être membre.
2. Basculez vers **LON-MBX1**, vérifiez dans Utilisateurs et ordinateurs Active Directory que le nouveau groupe a été créé.
3. Vérifiez dans le CAE que les autorisations fonctionnent correctement.

Que sont les stratégies d'attribution de rôle de gestion ?

Les stratégies d'attribution de rôle de gestion associent des rôles de gestion d'utilisateur final à des utilisateurs. Vous ne configurez pas d'autorisations d'administration avec les stratégies d'attribution de rôle de gestion. Vous utilisez plutôt celles-ci pour configurer les modifications que les utilisateurs peuvent apporter aux paramètres de leur propre boîte aux lettres et aux groupes de distribution qu'ils possèdent. Chaque utilisateur disposant d'une boîte aux lettres Exchange Server 2013 reçoit une stratégie d'attribution de rôle par défaut. Vous pouvez :

Les stratégies d'attribution de rôle de gestion attribuent aux utilisateurs des autorisations leur permettant de gérer leurs boîtes aux lettres ou groupes de distribution

Composant	Explication
Boîte aux lettres	Une stratégie d'attribution de rôle est attribuée à chaque boîte aux lettres
Stratégie d'attribution de rôle de gestion	Objet permettant d'associer des rôles de gestion aux boîtes aux lettres
Rôle de gestion	Conteneur permettant de regrouper les autres composants RBAC
Attribution de rôle de gestion	Associe des rôles de gestion à des stratégies d'attribution de rôle de gestion
Entrée de rôle de gestion	Définit les applets de commande Exchange que les utilisateurs peuvent exécuter sur leurs boîtes aux lettres ou groupes

- décider quelle stratégie d'attribution de rôle attribuer par défaut ;
- choisir les éléments à inclure dans la stratégie d'attribution de rôle par défaut ;
- remplacer la stratégie par défaut pour des boîtes aux lettres spécifiques.

Dans Exchange Server 2013, vous pouvez utiliser le CAE pour afficher et modifier la stratégie par défaut d'attribution de rôle de gestion et configurer des stratégies supplémentaires d'attribution de rôle de gestion avec différentes autorisations. Par exemple, vous pouvez modifier la stratégie par défaut d'attribution de rôle de gestion pour permettre aux utilisateurs de modifier leurs propres propriétés, telles que leurs adresses ou numéros de téléphone. Si vous créez une stratégie d'attribution des rôles de gestion personnalisée, vous devez l'attribuer aux boîtes aux lettres applicables.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Composants d'attribution de rôle

Les stratégies d'attribution de rôle sont constituées des composants suivants qui définissent ce que les utilisateurs peuvent faire avec leurs boîtes aux lettres :

- *Boîte aux lettres*. Une stratégie d'attribution de rôle unique est attribuée aux boîtes aux lettres. Lorsqu'une stratégie d'attribution de rôle est attribuée à une boîte aux lettres, cette stratégie est appliquée à la boîte aux lettres. Cela accorde à celle-ci toutes les autorisations fournies par les rôles de gestion.
- *Stratégie d'attribution de rôle de gestion*. La stratégie d'attribution de rôle de gestion est un objet d'Exchange Server 2013. Les utilisateurs sont associés à une stratégie d'attribution de rôle lorsque vous créez leurs boîtes aux lettres ou modifiez la stratégie d'attribution de rôle appliquée à leurs boîtes aux lettres. La combinaison de tous les rôles inclus dans une stratégie d'attribution de rôle définit tout ce que les utilisateurs associés peuvent gérer sur leurs boîtes aux lettres ou groupes de distribution.
- *Attribution de rôle de gestion*. Les attributions de rôle de gestion lient des rôles de gestion et des stratégies d'attribution de rôle. L'attribution d'un rôle de gestion à une stratégie d'attribution de rôle accorde aux utilisateurs la possibilité d'utiliser les applets de commande de ce rôle de gestion. Lorsque vous créez une attribution de rôle, vous ne pouvez pas spécifier d'étendue. L'étendue appliquée par l'attribution dépend du rôle de gestion. Sa valeur peut être Self ou MyGAL.
- *Rôle de gestion*. Un rôle de gestion est un conteneur pour un groupe d'entrées de rôle de gestion. Les rôles définissent les tâches spécifiques que les utilisateurs peuvent effectuer avec leurs boîtes aux lettres ou groupes de distribution.
- *Entrée de rôle de gestion*. Une entrée de rôle de gestion est une applet de commande, un script ou une autorisation spéciale qui permet aux utilisateurs d'exécuter une tâche spécifique. Chaque entrée de rôle est constituée d'une applet de commande unique et des paramètres auxquels le rôle de gestion peut accéder.

Que sont les autorisations fractionnées Exchange Server ?

AD DS et Exchange Server 2013 disposent d'un degré d'intégration très élevé, et il n'existe aucune option pour modifier cela. Dans de nombreuses petites et moyennes entreprises, les mêmes administrateurs sont chargés de gérer à la fois l'environnement Exchange Server et l'environnement AD DS. Cela s'appelle un modèle d'autorisations partagées.

- Les autorisations fractionnées séparent la création des entités de sécurité dans AD DS, telles que les utilisateurs et les groupes de sécurité, de la configuration suivante de ces objets via les outils Exchange Server 2013
- Avec les autorisations fractionnées d'Exchange Server, vous pouvez
  - Séparez la capacité de créer ou de supprimer les entités de sécurité de l'administration Exchange
  - Choisissez entre deux modèles
    - Autorisations fractionnées RBAC
    - Autorisations fractionnées Active Directory
- Disponibles depuis Exchange Server 2010 SP1

Cependant, dans bon nombre de grandes organisations, les différentes équipes d'administrateurs sont chargés de gérer les infrastructures AD DS et Exchange Server. Ces organisations disposent souvent de deux groupes informatiques distincts qui gèrent l'infrastructure Exchange Server de l'organisation (y compris les serveurs et les destinataires) et son infrastructure AD DS. Normalement, cela signifie que les administrateurs Exchange Server ne peuvent pas gérer les objets AD DS, et inversement. Ce modèle d'administration est souvent appelé modèle d'autorisations fractionnées. Les autorisations fractionnées permettent aux organisations d'attribuer des autorisations spécifiques et des tâches associées à des groupes spécifiques au sein de l'organisation.

Lorsque vous implémentez des autorisations fractionnées, vous supprimez la capacité des administrateurs Exchange Server à créer des entités de sécurité, telles que des objets d'utilisateur ou de groupe de sécurité, dans AD DS à l'aide des outils de gestion Exchange Server. Ceci s'applique à la fois au compte d'utilisateur et aux groupes de sécurité. Le résultat final de l'implémentation des autorisations fractionnées est que les entités de sécurité doivent être créées à l'aide des outils de gestion AD DS. Une fois l'objet créé, vous pouvez utiliser les outils de gestion Exchange pour configurer les attributs spécifiques à Exchange sur les entités de sécurité.

Dans Exchange Server 2013, le modèle par défaut est le modèle d'autorisations partagées. Vous n'avez rien à faire, s'il s'agit du modèle d'autorisations que vous souhaitez utiliser. Ce modèle ne sépare pas la gestion des objets Exchange Server et Active Directory des outils de gestion Exchange Server. Il permet aux administrateurs d'utiliser les outils de gestion Exchange Server pour créer des entités de sécurité dans AD DS.

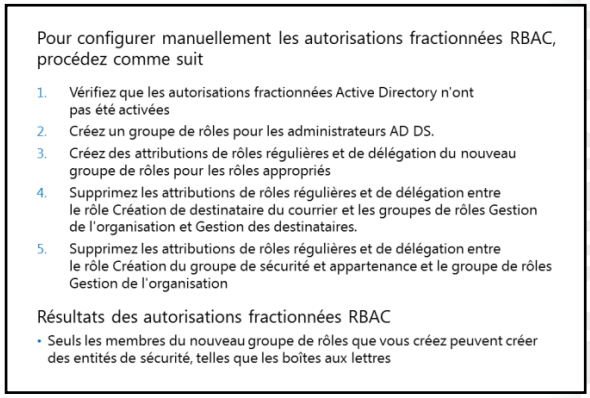
Options des autorisations fractionnées dans Exchange Server 2013

Voici les options d'Exchange Server 2013 pour l'implémentation des autorisations fractionnées :

- *Autorisations fractionnées RBAC.* Lorsque vous implémentez des autorisations fractionnées RBAC, vous supprimez la capacité des administrateurs Exchange à exécuter les applets de commande qui créent des entités de sécurité dans AD DS.
- *Autorisations fractionnées Active Directory.* Lorsque vous implémentez des autorisations fractionnées Active Directory, vous supprimez les autorisations des serveurs Exchange relatives à la création d'entités de sécurité dans AD DS. Puisque les applets de commande de l'environnement de ligne de commande Exchange Management Shell s'exécutent dans le contexte de sécurité des serveurs Exchange, cela empêche toute personne d'utiliser les outils de gestion Exchange Server pour créer des entités de sécurité AD DS.

Configuration des autorisations fractionnées RBAC

Par défaut, les administrateurs qui sont attribués au rôle Création de destinataire du courrier ou au rôle Création du groupe de sécurité et appartenance peuvent créer des entités de sécurité dans AD DS. Dans Exchange Server 2013, le groupe de rôles Gestion de l'organisation est attribué à ces deux attributions de rôle, alors que le groupe de rôles Gestion des destinataires est attribué à l'attribution de rôle Création de destinataire du courrier.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lorsque vous configurez des autorisations fractionnées RBAC, vous supprimez ces attributions de rôle aux groupes de rôles de gestion par défaut. Cela signifie que les membres des groupes de rôles de gestion n'ont plus l'autorisation d'exécuter les applets de commande utilisées pour créer des entités de sécurité, les empêchant ainsi de créer ces objets à l'aide d'un des outils de gestion Exchange Server 2013. Lorsque vous activez les autorisations fractionnées RBAC, les administrateurs Exchange Server ne pourront pas utiliser les applets de commande suivantes :

- **New-Mailbox**
- **New-MailContact**
- **New-MailUser**
- **New-RemoteMailbox**
- **Remove-Mailbox**
- **Remove-MailContact**
- **Remove-MailUser**
- **Remove-RemoteMailbox**

En outre, les fonctionnalités associées à la console de gestion Exchange Server et au Centre d'administration Exchange (telles que l'**Assistant Nouvelle boîte aux lettres**) génèrent une erreur si vous essayez de les utiliser.

La configuration des autorisations fractionnées RBAC n'empêchent pas les administrateurs d'utiliser les outils de gestion AD DS pour créer des entités de sécurité. Si des administrateurs Exchange Server disposent des autorisations AD DS pour créer des entités de sécurité, ils peuvent le faire à l'aide des outils AD DS. Ils peuvent alors configurer les attributs Exchange Server en utilisant les outils de gestion Exchange Server.

En outre, la configuration des autorisations fractionnées RBAC ne modifie pas le principe RBAC sous-jacent que les serveurs Exchange via le groupe du sous-système approuvé Exchange disposent des autorisations pour créer des entités de sécurité dans Active Directory. Les autorisations fractionnées RBAC ne suppriment pas d'autorisations du compte du sous-système approuvé Exchange, il supprime uniquement l'autorisation d'exécuter des applets de commande des administrateurs Exchange Server.

Pour configurer les autorisations fractionnées RBAC, procédez comme suit :

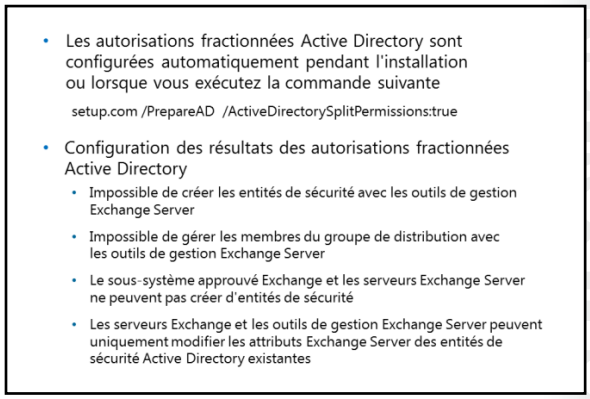
1. Désactivez les autorisations fractionnées Active Directory si elles sont activées. Vous pouvez le faire en exécutant l'installation d'Exchange Server avec setup.com avec les paramètres **/PrepareAD** et **/ActiveDirectorySplitPermissions** définis sur **false**. Si les autorisations fractionnées AD DS ne sont pas activées, et que votre organisation utilise le modèle d'autorisations partagées, vous pouvez ignorer cette étape.
2. Créez un groupe de rôles qui contiendra les administrateurs qui pourront créer des entités de sécurité dans AD DS. C'est une étape facultative, mais elle vous permet de configurer un groupe spécial d'administrateurs Exchange Server qui pourront toujours utiliser les outils de gestion Exchange Server pour créer des entités de sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Créez des attributions de rôles régulières et de délégation entre le rôle Création de destinataire du courrier et le nouveau groupe de rôles. Cette étape est facultative, et elle s'applique uniquement si vous avez créé le groupe spécial de rôles mentionné dans l'étape précédente.
4. Créez des attributions de rôles régulières et de délégation entre le rôle Création du groupe de sécurité et appartenance, et le nouveau groupe de rôles. Cette étape est facultative.
5. Supprimez les attributions de rôles régulières et de délégation entre le rôle Création de destinataire du courrier et les groupes de rôles Gestion de l'organisation et Gestion des destinataires.
6. Supprimez les attributions de rôles régulières et de délégation entre le rôle Création du groupe de sécurité et appartenance, et le groupe de rôles Gestion de l'organisation.

Après avoir configuré les autorisations fractionnées RBAC, seuls les membres du nouveau groupe de rôles que vous créez peuvent créer des entités de sécurité, telles que les boîtes aux lettres. Le nouveau groupe de rôles pourra seulement créer les objets. Il ne pourra pas configurer les attributs Exchange Server sur le nouvel objet. Un administrateur Active Directory qui est membre du nouveau groupe devra créer l'objet, et un administrateur Exchange Server devra ensuite configurer les attributs Exchange Server sur l'objet. Si vous souhaitez que le nouveau groupe de rôles puisse également gérer les attributs Exchange Server sur le nouvel objet, vous devez attribuer le rôle Destinataires du courrier au nouveau groupe de rôles.

Configuration des autorisations fractionnées Active Directory



Les autorisations fractionnées Active Directory diffèrent des autorisations fractionnées RBAC. Lorsque vous implémentez des autorisations fractionnées Active Directory, les serveurs Exchange n'ont plus l'autorisation de créer des entités de sécurité AD DS, car les autorisations qui sont normalement accordées au groupe Autorisations Windows Exchange sont supprimées. Puisque le groupe Sous-système approuvé Exchange qui contient tous les serveurs Exchange Server 2010 et Exchange Server 2013 est le seul membre du groupe Autorisations Windows Exchange, celles-ci sont supprimées des serveurs Exchange.

L'activation des autorisations fractionnées Active Directory signifie ce qui suit :

- Vous ne pouvez plus créer de boîtes aux lettres, d'utilisateurs à extension messagerie, de groupes de distribution, et d'autres entités de sécurité à partir des outils de gestion Exchange Server.
- Vous ne pouvez pas ajouter et supprimer des membres du groupe de distribution à partir des outils de gestion Exchange Server.
- Le sous-système approuvé Exchange et les serveurs Exchange Server n'ont plus l'autorisation de créer des entités de sécurité.
- Les serveurs Exchange et les outils de gestion Exchange Server peuvent uniquement modifier les attributs Exchange Server des entités de sécurité existantes dans AD DS.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Vous pouvez activer des autorisations fractionnées Active Directory lorsque vous exécutez le programme d'installation d'Exchange Server 2013 pendant le déploiement initial d'Exchange Server 2013. Vous pouvez également utiliser le programme d'installation de ligne de commande avec l'option **/PrepareAD** et l'option **/ActiveDirectorySplitPermissions** définies sur **true** lorsque vous installez Exchange Server 2013 en premier, ou vous pouvez exécuter cette commande après l'installation d'Exchange Server pour modifier un déploiement existant afin d'utiliser des autorisations fractionnées Active Directory.

Vous activez ou désactivez les autorisations fractionnées Active Directory à l'aide du programme d'installation d'Exchange Server 2013. Si vous activez les autorisations fractionnées Active Directory, l'installation d'Exchange Server 2013 effectue les modifications suivantes aux déploiements AD DS et Exchange Server :

- Il crée une unité d'organisation appelée groupes protégés par Microsoft Exchange.
- Il crée le groupe de sécurité Autorisations Windows Exchange sur l'unité d'organisation Groupes protégés par Microsoft Exchange.
- Il n'ajoute pas le groupe de sécurité Sous-système approuvé Exchange au groupe de sécurité Autorisations Windows Exchange.
- Il ne crée pas d'attributions de rôle de gestion de non délégation aux rôles de gestion avec le type de rôle de gestion suivant :
    - **MailRecipientCreation**
    - **SecurityGroupCreationandMembership**
- Il n'ajoute pas d'entrées de contrôle d'accès qui auraient été attribuées au groupe de sécurité Autorisations Windows Exchange sur l'objet de domaine Active Directory.

Pour désactiver les autorisations fractionnées Active Directory, vous pouvez exécuter une nouvelle fois l'installation d'Exchange avec **/PrepareAD** et les paramètres **/ActiveDirectorySplitPermissions**, en définissant le paramètre **ActiveDirectorySplitPermissions** sur false.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Configuration de la journalisation d'audit

Dans les organisations dans lesquelles plusieurs administrateurs Exchange Server existent, il peut parfois s'avérer difficile de suivre les modifications qui ont été apportées aux objets de configuration Exchange Server. En outre, il peut être difficile de fournir des informations sur les utilisateurs qui accèdent aux autres boîtes aux lettres ou d'exécuter d'autres types d'accès aux données. Exchange Server 2013 contient les fonctionnalités de journalisation qui peuvent vous fournir des informations sur les tâches d'administration effectuées sur vos serveurs Exchange.

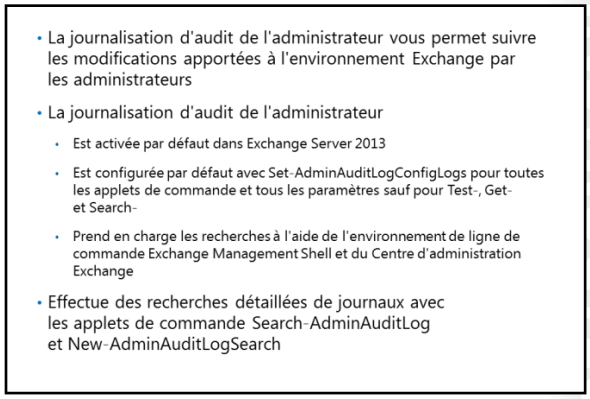
Objectifs de la leçon

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

- décrire la journalisation d'audit de l'administrateur ;
- décrire la journalisation d'audit de boîte aux lettres ;
- configurer la journalisation d'audit.

Qu'est-ce que la journalisation d'audit de l'administrateur ?

Dans Exchange Server 2013, la journalisation d'audit de l'administrateur capture des données relatives aux modifications apportées à votre organisation par les utilisateurs et les administrateurs. Par défaut, la journalisation d'audit de l'administrateur capture les informations sur toutes les modifications apportées au déploiement Exchange Server.



Les journaux d'audit d'administrateur Exchange Server 2013 suivent toutes les applets de commande de l'environnement de ligne de commande Exchange Management Shell qui modifient l'environnement Exchange Server. Puisque toutes les tâches effectuées dans le CAE sont traduites dans les applets de commande de l'environnement de ligne de commande Exchange Management Shell, toutes les modifications sont consignées, indépendamment de l'outil que vous utilisez pour effectuer la tâche.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

La journalisation d'audit est destinée à montrer les mesures qui ont été prises pour modifier des objets dans une organisation Exchange, plutôt que des objets qui ont été affichés. Les applets de commande sont auditées si l'applet de commande est sur la liste d'audit d'applets de commande, et un ou plusieurs paramètres sur cette applet de commande sont sur la liste d'audit de paramètres. Par défaut, les applets de commande Test, Get et Search ne sont pas consignées, car ces applets de commande ne sont pas généralement critiques en matière de sécurité, et ne peuvent rien modifier directement sur des objets Exchange Server. Toutes autres applets de commande sont consignées.

Vous pouvez configurer la journalisation d'audit de l'administrateur dans l'environnement de ligne de commande Exchange Management Shell à l'aide de l'applet de commande **Set-AdminAuditLogConfig**. Cette applet de commande utilise plusieurs paramètres qui vous permettent de configurer la journalisation d'audit. Les paramètres les plus importants de cette applet de commande sont les suivants :

- *AdminAuditLogEnabled***.** Lorsqu'il est défini sur False, la journalisation n'est pas activée. Par défaut, la journalisation est activée dans Exchange Server 2013.
- *TestCmdletLoggingEnabled***.** Ce paramètre permet la journalisation de l'applet de commande Test.
- *AdminAuditLogCmdlets***.** Ce paramètre spécifie les applets de commande qui sont consignées lorsque la journalisation d'audit de l'administrateur est activée. Par défaut, toutes les applets de commande sont consignées, comme indiqué par le caractère générique *.
- *AdminAuditLogParameters***.** Ce paramètre spécifie si les paramètres des applets de commande sont consignés. Par défaut, ce paramètre est défini pour consigner tous les paramètres des applets de commande, comme indiqué par le caractère générique *.
- *AdminAuditLogAgeLimit***.** Ce paramètre spécifie la durée de consignation de chaque entrée de journal avant que celle-ci soit supprimée. La durée par défaut est de 90 jours.

Si vous souhaitez voir comment la journalisation d'audit de l'administrateur est configurée actuellement, exécutez l'applet de commande **Get-AdminAuditLogConfig**.

Chaque fois qu'une applet de commande est consignée, Exchange Server crée une entrée de journal d'audit. Exchange Server 2013 stocke les journaux d'audit dans une boîte aux lettres d'arbitrage masquée et dédiée à laquelle vous pouvez uniquement accéder à l'aide de la page d'affichage des rapports d'audit du CAE ou des applets de commande **Search-AdminAuditLog** ou **New-AdminAuditLogSearch**. Les journaux ne sont pas accessibles à partir de Microsoft Outlook® Web App ou Microsoft Office® Outlook. En outre, personne ne peut supprimer d'entrées de journal d'audit, et vous ne pouvez pas modifier cette boîte aux lettres dédiée.

Dans le CAE, vous pouvez afficher ou exporter des rapports de journalisation d'audit d'administrateur. Si vous souhaitez rechercher les journaux en spécifiant vos propres paramètres de recherche, vous devez utiliser l'environnement de ligne de commande Exchange Management Shell.

Par exemple, supposez que vous souhaitez rechercher l'utilisation de Set-Mailbox entre 16/2/2013 et 16/3/2013, puis envoyez les résultats de recherche à Andreas@adatum.com. Pour cela, vous pouvez exécuter l'applet de commande suivante :

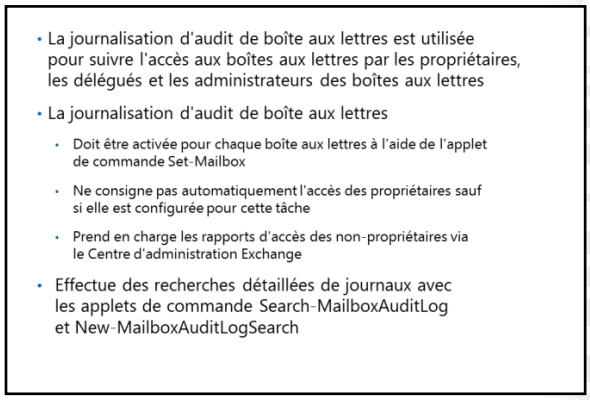
```
New-AdminAuditLogSearch -Cmdlets Set-Mailbox -StartDate 16/02/2013 -EndDate 16/03/2013
-StatusMailRecipients Andreas@adatum.com -Name "Rapport des modifications de la boîte
aux lettres"
```

Exécutez ensuite l'applet de commande **New-AdminAuditLogSearch**, Exchange Server peut prendre jusqu'à 15 minutes pour fournir le rapport au destinataire spécifié.

Vous pouvez également utiliser les mêmes paramètres avec l'applet de commande **Search-AdminAuditLog**, excepté pour le paramètre StatusMailRecipients qui spécifie l'envoi d'un rapport par courrier électronique. L'applet de commande **Search-AdminAuditLog** fournit le rapport dans la fenêtre de l'environnement de ligne de commande Exchange Management Shell.

Qu'est-ce que la journalisation d'audit de boîte aux lettres ?

La journalisation d'audit de boîte aux lettres vous permet de consigner l'accès aux boîtes aux lettres par les propriétaires, les délégués (y compris les administrateurs avec un accès total aux boîtes aux lettres) et les administrateurs des boîtes aux lettres. Un administrateur peut accéder aux boîtes aux lettres uniquement dans les scénarios suivants :



- Pour les recherches de découverte.
- Lorsque des exportations de boîtes aux lettres sont spécifiées via l'applet de commande **New-MailboxExportRequest**.
- Pour l'accès aux boîtes aux lettres de l'éditeur d'interface de programmation d'applications de messagerie (MAPI) de Microsoft Exchange Server.

Lorsque vous activez la journalisation d'audit pour une boîte aux lettres, vous pouvez spécifier les actions des utilisateurs qui doivent être consignées. Vous pouvez également spécifier s'il faut consigner les actions du propriétaire, du délégué ou de l'administrateur des boîtes aux lettres. Les entrées du journal d'audit comprennent également les informations importantes telles que l'adresse IP du client, le nom d'hôte et le processus ou le client utilisé pour accéder à la boîte aux lettres. Pour les éléments qui sont déplacés, l'entrée comprend le nom du dossier de destination.

Les journaux d'audit de boîte aux lettres sont générés pour chaque boîte aux lettres dont la journalisation d'audit de boîte aux lettres est activée. Les entrées du journal sont stockées dans le sous-dossier Audits du dossier Éléments récupérables de la boîte aux lettres auditée. Si vous déplacez une boîte aux lettres vers un autre serveur de boîtes aux lettres, les journaux d'audit de boîte aux lettres pour cette boîte aux lettres se déplacent également, car ils sont localisés dans la boîte aux lettres.

Par défaut, les entrées du journal d'audit de boîte aux lettres sont conservées dans la boîte aux lettres pendant 90 jours.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification de la journalisation d'audit de boîte aux lettres

À la différence de la journalisation d'audit de l'administrateur, la journalisation d'audit de boîte aux lettres n'est pas activée par défaut, vous devez donc l'activer manuellement. En outre, la journalisation d'audit de boîte aux lettres est activée pour chaque boîte aux lettres, et non comme une option générale. Lorsque vous activez la journalisation d'audit de boîte aux lettres pour une boîte aux lettres, l'accès à la boîte aux lettres et à certaines actions des administrateurs et des délégués sont consignés par défaut.

Pour consigner des actions effectuées par le propriétaire de la boîte aux lettres, vous devez spécifier les actions du propriétaire à auditer. Cependant, pour les boîtes aux lettres telles que la boîte aux lettres de détection, qui peut contenir plus d'informations confidentielles, envisagez d'activer la journalisation d'audit de boîte aux lettres pour les actions du propriétaire telles que la suppression d'un message. Nous vous recommandons d'activer uniquement l'audit des actions spécifiques du propriétaire nécessaires pour répondre aux exigences métier et de sécurité.

Pour activer l'audit de boîte aux lettres sur une boîte aux lettres spécifique, utilisez l'environnement de ligne de commande Exchange Management Shell. L'exemple suivant active l'audit de boîte aux lettres sur la boîte aux lettres d'Anil Elson :

Set-Mailbox -Identity "Anil Elson" -AuditEnabled $true

Pour désactiver l'audit de boîte aux lettres, donnez au paramètre **$true** la valeur **$false**.

Pour effectuer des recherches dans le journal d'audit de boîte aux lettres, vous pouvez utiliser le CAE et l'environnement de ligne de commande Exchange Management Shell. Le CAE vous permet de générer des rapports de l'accès aux boîtes aux lettres des non-propriétaires. Il s'agit du rapport le plus courant pour ce type d'audit. Cependant, dans ce rapport, vous pouvez uniquement définir une plage de dates comme filtre. Si vous souhaitez spécifier toutes les options disponibles, utilisez l'environnement de ligne de commande Exchange Management Shell pour effectuer votre recherche.

L'exemple suivant recherche les utilisateurs qui ont accédé à la boîte aux lettres de Terri au cours de l'année 2013, en limitant les résultats à 2,000 :

```
Search-MailboxAuditLog -Identity Anil -LogonTypes Admin,Delegate -StartDate 1/1/2013 -
EndDate 31/12/2013 -ResultSize 2000
```

Les résultats retournent à la fenêtre de l'environnement de ligne de commande Exchange Management Shell.

L'exemple suivant recherche les boîtes aux lettres de Terri et de Jan, puis envoie les résultats à une boîte aux lettres spécifique :

```
New-MailboxAuditLogSearch –Name "Acces Admin et Delegue" -Mailboxes "Terri Chudzik","Jan
Dryml" -LogonTypes Admin,Delegate -StartDate 1/1/2013 -EndDate 31/12/2013 -
StatusMailRecipients "auditors@adatum.com"
```

Cette applet de commande localise les tentatives d'accès par les administrateurs et les délégués au cours de l'année 2013. Les résultats sont envoyés à alias de courrier électronique auditors@adatum.com.

Démonstration : Configuration de la journalisation d'audit

Dans cette démonstration, vous allez découvrir comment configurer la journalisation d'audit de l'administrateur et la journalisation d'audit de boîte aux lettres, et comment rechercher des journaux d'audit dans le CAE dans l'environnement de ligne de commande Exchange Management Shell.

Procédure de démonstration

1. Sur LON-CAS1, dans l'environnement de ligne de commande Exchange Management Shell, examinez comment le journal d'audit est actuellement configuré.
2. Dans le CAE, ajoutez les autorisations **Envoyer** en tant que sur la boîte aux lettres d'**Anil Elson** pour Allie Bellew.
3. Dans l'environnement de ligne de commande Exchange Management Shell, vérifiez que vous voyez la modification des autorisations dans le journal de l'administrateur.
4. Activez la journalisation d'audit sur la boîte aux lettres d'Anil.
5. Envoyez un message de la boîte aux lettres d'Allie en tant qu'Anil.
6. Dans le CAE, exécutez un rapport d'accès aux boîtes aux lettres par des non-propriétaires pour vérifier que le message a été consigné correctement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Configuration de la sécurité et de l'audit administratifs

Scénario

L'entreprise A. Datum Corporation a déployé Exchange Server 2013. Le responsable de la sécurité de l'entreprise vous a fourni une série d'exigences visant à garantir que le déploiement d'Exchange Server 2013 est aussi sécurisé que possible. Les points spécifiques de la configuration requise sont les suivants :

- Les administrateurs Exchange Server doivent avoir des autorisations minimales. Ceci signifie que vous devez déléguer autant que possible les autorisations de gestion Exchange Server.
- Toutes les modifications de configuration apportées à l'environnement Exchange Server doivent être auditées. Les journaux d'audit doivent être disponibles pour l'inspection par les auditeurs de la société.
- L'organisation doit avoir l'option d'auditer tout accès par les non-propriétaires aux boîtes aux lettres utilisateur. Les journaux d'audit doivent être disponibles pour l'inspection par les auditeurs de la société.
- La création d'objets AD DS doit être effectuée uniquement par le groupe HRAdmins. Personne d'autre ne doit créer d'objets AD DS tels que les comptes d'utilisateurs dans Exchange.

Objectifs

Les stagiaires pourront configurer des autorisations RBAC et la journalisation d'audit d'Exchange Server 2013 pour les administrateurs et les utilisateurs.

Configuration de l'atelier pratique

Durée approximative : **60 minutes**

Ordinateurs virtuels	22341B-LON-DC1 22341B-LON-CAS1 22341B-LON-MBX1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22341B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous avec les informations d'identification suivantes :
   - Nom d'utilisateur : **ADATUM\Administrateur**
   - Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22341B-LON-MBX1** et **22341B-LON-CAS1**.

Exercice 1 : Configuration des autorisations Exchange Server

Scénario

L'entreprise A. Datum Corporation a terminé le déploiement d'Exchange Server 2013 et s'efforce maintenant d'intégrer la gestion d'Exchange Server et des destinataires à ses pratiques actuelles en matière de gestion. Pour répondre aux exigences en matière de gestion, vous devez vérifier les points suivants :

- Les membres du groupe Administrateurs informatiques peuvent administrer des serveurs Exchange Server 2013 individuels, mais ils ne peuvent modifier aucun paramètre de l'organisation Exchange Server. Tony Smith est membre du groupe informatique.
- Les membres du groupe HelpDeskAdmins doivent pouvoir gérer les destinataires du courrier dans toute l'organisation. Ils ne doivent pas pouvoir gérer les groupes de distribution, ni créer de boîtes aux lettres.
- Les membres du groupe SupportDesk doivent pouvoir gérer les boîtes aux lettres et les groupes de distribution des utilisateurs de l'organisation. Ils doivent également pouvoir créer des boîtes aux lettres.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer des autorisations Exchange Server pour le groupe Administrateurs informatiques.
2. Configurer les autorisations pour les groupes SupportDesk et HelpDeskAdmins.
3. Vérifier les autorisations pour les trois groupes de rôles créés.

▶ Tâche 1 : Configurer des autorisations Exchange Server pour le groupe Administrateurs informatiques

1. Sur LON-MBX1, ouvrez le **Gestionnaire de serveur**, puis **Utilisateurs et ordinateurs Active Directory**.
2. Ajoutez le groupe **informatique** comme membre du groupe **Server Management** localisé dans l'unité d'organisation Adatum.com\Microsoft Exchange Security Groups.

▶ Tâche 2 : Configurer les autorisations pour les groupes SupportDesk et HelpDeskAdmins

1. Sur LON-MBX1, sur l'écran Accueil, ouvrez **Exchange Management Shell**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, exécutez les applets de commande suivantes :

```
New-RoleGroup -Name HelpDeskAdmins -roles "Mail Recipients"
New-RoleGroup -Name SupportDesk -roles "Mail Recipients", "Mail Recipient Creation",
"Distribution Groups"
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Ouvrez **Internet Explorer**, connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Dans le CAE, dans **Autorisations**, ajoutez **Ryan Spanton** au groupe de rôles **SupportDesk** et **Carol Troup** au groupe de rôles **HelpDeskAdmins**.
5. Fermez Internet Explorer.

▶ Tâche 3 : Vérifier les autorisations pour les trois groupes de rôles créés

1. Sur LON-MBX1, ouvrez **Internet Explorer**, puis connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Tony** avec le mot de passe **Pa$$w0rd**.
2. Modifiez la base de données Research :
   - Émettre un avertissement à (Go) : **unlimited**
3. Vérifiez que vous pouvez voir les paramètres de domaines acceptés, mais que vous ne pouvez pas les ajouter ni les modifier. Rappelez-vous que Tony fait partie du groupe informatique, et peut donc modifier les propriétés de serveur mais pas les paramètres du flux de messages organisationnels.
4. Fermez Internet Explorer, ouvrez **Internet Explorer**, puis connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Ryan** avec le mot de passe **Pa$$w0rd**. Constatez que, dans le volet de fonctionnalités, il n'y a aucun serveur. Cela est dû au fait que Ryan n'est pas autorisé à gérer les serveurs.
5. Dans la fonction des destinataires, dans les boîtes aux lettres, modifiez **Alan Steiner** :
   - Service : **Informatique**
6. Dans la fonction du destinataire, dans les groupes, essayez de modifier la **Research** :
   - Description du groupe : test
7. Dans la fonction des destinataires, dans les boîtes aux lettres, créez une boîte aux lettres :
   - Alias : **Test**
   - Prénom : **Test**
   - Nom : **Test**
   - Nom d'overture de session de l'utilisateur : **Test**
   - Nouveau mot de passe : **Pa$$word**
   - Confirmer le mot de passe : **Pa$$word**
8. Fermez Internet Explorer, ouvrez **Internet Explorer**, puis connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Carol** avec le mot de passe **Pa$$w0rd**.
9. Dans le volet de fonctionnalités, accédez aux **Destinataires**. Notez qu'il n'y a aucun bouton Nouvel utilisateur dans la barre d'outils.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Dans la fonction des destinataires, dans les boîtes aux lettres, modifiez **Alan Steiner** :
    - Service : **Service client**
11. Vérifiez que les groupes ne sont pas disponibles dans les onglets, car Carol n'a pas l'autorisation de gérer les groupes.
12. Fermez Internet Explorer.

Résultats : À la fin de cet exercice, les stagiaires auront configuré des rôles RBAC et vérifié que les autorisations sont accordées en conséquence.

Exercice 2 : Configuration de la journalisation d'audit

Scénario

Vous devez maintenant configurer la journalisation d'audit sur la boîte aux lettres partagée Info@Adatum.com. Cette boîte aux lettres est utilisée par le groupe informatique pour envoyer des informations à tout le monde dans l'organisation.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer la journalisation d'audit sur la boîte aux lettres Info@Adatum.com.
2. Exercez l'activité SendAs sur la boîte aux lettres Info@Adatum.com.
3. Vérifier que l'activité est consignée.

▶ Tâche 1 : Configurer la journalisation d'audit sur la boîte aux lettres Info@Adatum.com

1. Sur LON-MBX1, ouvrez **Exchange Management Shell**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, exécutez l'applet de commande suivante :

   Set-Mailbox -Identity "Info" -AuditDelegate SendAs,SendOnBehalf -AuditEnabled $true

▶ Tâche 2 : Exercez l'activité SendAs sur la boîte aux lettres Info@Adatum.com

1. Sur LON-CAS1, ouvrez **Internet Explorer**, puis connectez-vous à **https://LON-CAS1.adatum.com/owa**. Connectez-vous en tant qu'**ADATUM\Tony** avec le mot de passe **Pa$$w0rd**.
2. Créez et envoyez un message électronique :
   - De : **Info@adatum.com**
   - À : **Tony Smith**
   - Objet : **Test de la journalisation Envoyer en tant que**
3. Vérifiez que le message est envoyé.
4. Fermez Internet Explorer

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Vérifier que l'activité est consignée

1. Sur LON-MBX1, ouvrez **Internet Explorer**, puis connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans **Gestion de la conformité**, dans **Audit**, **Exécuter un rapport d'accès aux boîtes aux lettres par des non-propriétaires** :
   - **Rechercher les accès par**: **Tous les non-propriétaires**
3. Dans les résultats de recherche, affichez le rapport qui montre que Tony Smith a accédé à la boîte aux lettres Info.

Résultats : À la fin de cet exercice, les stagiaires auront configuré la journalisation d'audit de boîte aux lettres et vérifié que la journalisation d'audit fonctionne correctement.

Exercice 3 : Configuration des autorisations fractionnées RBAC sur Exchange Server 2013

Scénario

Vous souhaitez séparer ceux qui peuvent créer des entités de sécurité dans la partition de domaine AD DS de ceux qui administrent les données d'organisation Exchange dans la partition de configuration d'AD DS. Seul le groupe HRAdmins doit pouvoir créer des objets dans la partition de domaine AD DS. Vous décidez d'implémenter le modèle d'autorisations fractionnées RBAC dans votre organisation.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un groupe de rôles appelé HRAdmins et attribuer des autorisations.
2. Supprimer l'autorisation de création d'objets AD DS à partir d'autres groupes d'administrateurs Exchange Server.
3. Valider la fonctionnalité d'autorisations fractionnées RBAC.

▶ Tâche 1 : Créer un groupe de rôles appelé HRAdmins et attribuer des autorisations

1. Sur LON-MBX1 (si le Exchange Management Shell n'est pas encore ouvert), ouvrez **Exchange Management Shell**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, exécutez les applets de commande suivantes :

```
New-RoleGroup "HRAdmins" -Roles "Mail Recipient Creation", "Security Group Creation
and Membership"
New-ManagementRoleAssignment -Role "Mail Recipient Creation" -SecurityGroup
"HRAdmins" -Delegating
New-ManagementRoleAssignment -Role "Security Group Creation and Membership" -
SecurityGroup "HRAdmins" –Delegating
Add-RoleGroupMember "HRAdmins" -Member Tony
```

3. Dans le Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory** et modifiez le groupe HRAdmins situé dans **Microsoft Exchange Security Groups** :
   - Géré par : **HRAdmins**
   - Le gestionnaire peut mettre à jour la liste des membres : **activé**
4. Ajoutez **HRAdmins** au groupe **Recipient Management**. Ceci est requis pour attribuer au groupe HRAdmins les autorisations nécessaires permettant de créer une boîte aux lettres.

▶ Tâche 2 : Supprimer l'autorisation de création d'objets AD DS à partir d'autres groupes d'administrateurs Exchange Server

1. Sur LON-MBX1, ouvrez **Exchange Management Shell**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, exécutez les applets de commande suivantes :

```
Get-ManagementRoleAssignment -Role "Mail Recipient Creation" | Format-Table Name,
Role, RoleAssigneeName –Auto
Get-ManagementRoleAssignment -Role "Mail Recipient Creation" | Where {
$_.RoleAssigneeName -NE "HRAdmins" } | Remove-ManagementRoleAssignment
Get-ManagementRoleAssignment -Role "Security Group Creation and Membership" | Where {
$_.RoleAssigneeName -NE "HRAdmins" } | Remove-ManagementRoleAssignment
```

3. Fermez l'environnement de ligne de commande Exchange Management Shell.

▶ Tâche 3 : Valider la fonctionnalité d'autorisations fractionnées RBAC

1. Sur LON-MBX1, ouvrez **Internet Explorer**, puis connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la fonction des **Destinataires**, dans les boîtes aux lettres, créez une boîte aux lettres. Lorsque vous cliquez sur **Nouvel utilisateur**, tous les champs requis pour créer un utilisateur sont grisés. Cela est dû au fait que vous n'avez pas l'autorisation de créer un compte d'utilisateur dans AD DS.
3. Fermez Internet Explorer, ouvrez **Internet Explorer**, puis connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**Adatum\Tony** avec le mot de passe **Pa$$w0rd**.
4. Dans la fonction des destinataires, dans les boîtes aux lettres, créez une boîte aux lettres avec un nouvel utilisateur :
   - Alias : **Test2**
   - Prénom : **Test2**
   - Nom : **Test2**
   - Nom d'overture de session de l'utilisateur : **Test2**
   - Nouveau mot de passe : **Pa$$word**
   - Confirmer le mot de passe : **Pa$$word**

   Ceci confirme que Tony peut créer des comptes d'utilisateurs pour les nouvelles boîtes aux lettres.
5. Fermez Internet Explorer.

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 il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1** et **22341B-LON-MBX1**.

Résultats : À la fin de cet exercice, les stagiaires auront créé un groupe de rôles, configuré des autorisations fractionnées RBAC et validé que les autorisations fractionnées RBAC fonctionnent comme prévu.

Question : Vous avez une boîte aux lettres partagée qui requiert la journalisation de toute activité dans laquelle d'autres utilisateurs effectuent des envois au nom de cette boîte aux lettres. Que devez-vous faire ?

Question : Votre bureau de conformité requiert l'autorisation de configurer et de gérer des paramètres de conformité dans votre organisation Exchange. Vous souhaitez vous assurer que le responsable de la mise en conformité dispose des autorisations minimales nécessaires pour effectuer son travail. Quel groupe de rôles de gestion prédéfini devez-vous utiliser ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

Complétez ou adaptez les meilleures pratiques suivantes à vos propres conditions de travail :

- Lorsque vous configurez des autorisations dans l'organisation Exchange Server, vérifiez que les utilisateurs disposent des autorisations minimales requises pour exécuter leurs tâches. Ajoutez uniquement des utilisateurs approuvés au groupe de rôles Gestion de l'organisation, car ce groupe a le contrôle total de toute l'organisation. N'activez pas les autorisations fractionnées RBAC ou Active Directory si vous n'avez pas de scénario d'utilisation pour prendre en charge ces modèles d'autorisations. Activez la journalisation d'audit administrative sur les boîtes aux lettres partagées.
- Utilisez autant que possible les groupes de rôles prédéfinis pour attribuer des autorisations dans l'organisation Exchange. La création de groupes de rôles personnalisés avec des autorisations personnalisées est plus compliquée et risque d'attribuer trop ou trop peu d'autorisations aux utilisateurs.
- Activez la journalisation d'audit administrative sur les boîtes aux lettres partagées.
- N'activez pas les autorisations fractionnées RBAC ou Active Directory si vous n'avez pas de scénario d'utilisation pour prendre en charge ces modèles d'autorisations.

Veillez à documenter toutes les autorisations que vous attribuez dans l'organisation Exchange. Si les utilisateurs ne peuvent pas exécuter les tâches requises ou s'ils exécutent des tâches auxquelles ils ne devraient pas avoir accès, vous devez être capable d'en identifier la cause en vous reportant à votre documentation.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Les administrateurs de boîtes aux lettres Exchange ne peuvent pas créer de comptes d'utilisateurs lorsqu'ils créent une boîte aux lettres.	
Un administrateur peut se connecter au serveur Exchange et démarrer l'environnement de ligne de commande Exchange Management Shell, mais ne peut pas exécuter les applets de commande pour gérer les objets destinataires.	

Questions de contrôle des acquis

Question : Dans quel scénario devez-vous implémenter les autorisations fractionnées AD dans votre organisation Exchange Server 2013 ?

Question : Vous devez permettre aux membres du service des ressources humaines de configurer des boîtes aux lettres utilisateur pour toute l'organisation. Que devez-vous faire ?

Question : Comment pouvez-vous identifier si quelqu'un a accédé à la boîte aux lettres d'un autre utilisateur ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 11

Analyse et résolution des problèmes de Microsoft® Exchange Server 2013

Table des matières :

Vue d'ensemble du module **11-1**

Leçon 1 : Analyse d'Exchange Server 2013 **11-2**

Leçon 2 : Maintenance d'Exchange Server 2013 **11-17**

Leçon 3 : Résolution des problèmes liés à Exchange Server 2013 **11-25**

Atelier pratique : Analyse et résolution des problèmes d'Exchange Server 2013 **11-35**

Contrôle des acquis et éléments à retenir **11-41**

Évaluation du cours **11-44**

Vue d'ensemble du module

Les processus d'analyse et de résolution des problèmes pour Microsoft® Exchange Server 2013 sont très importants car ils permettent aux administrateurs de mettre à disposition des infrastructures de messagerie aux performances optimisées. Les processus d'analyse peuvent améliorer votre capacité à identifier, résoudre et réparer les problèmes avant que les utilisateurs finaux ne les rencontrent.

Grâce à la conception d'une solution complète d'analyse pour Exchange Server 2013 dans votre organisation, vous pouvez réduire les problèmes rencontrés par les utilisateurs finaux et empêcher la survenue de problèmes potentiellement graves.

Une fois Exchange Server 2013 déployé, vous devez vérifier qu'il continue à s'exécuter efficacement en préservant un environnement stable. Ce module décrit comment analyser, assurer la maintenance de votre environnement Exchange Server 2013 et y résoudre les problèmes.

Objectifs

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

- analyser Exchange Server 2013 ;
- assurer la maintenance d'Exchange Server 2013 ;
- résoudre les problèmes liés à Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 1
Analyse d'Exchange Server 2013

Les administrateurs d'Exchange doivent en comprendre le fonctionnement afin de pouvoir implémenter les outils d'analyse au moyen des mesures appropriées, de sorte de constituer un environnement Exchange sain. Vous devez développer une solution d'analyse susceptible d'améliorer la capacité d'identification, de résolution et de réparation des problèmes avant qu'ils n'affectent les utilisateurs.

Pour réduire et éviter les problèmes éventuels rencontrés par les utilisateurs finaux, vous devez entreprendre l'étude d'éléments et d'une planification supplémentaires afin de développer une solution d'analyse pour votre organisation Exchange Server 2013. Dans cette leçon, vous examinerez les outils d'analyse élémentaires et les mesures à utiliser pour analyser Exchange Server 2013.

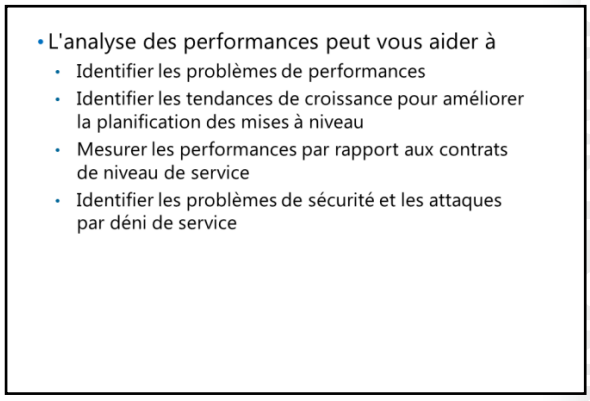
Objectifs de la leçon

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

- expliquer pourquoi l'Analyseur de performances est important ;
- décrire une base de référence de la performance ;
- établir une base de référence des performances ;
- décrire les outils d'analyse Exchange Server 2013 ;
- collecter les données de performance principales pour Exchange Server 2013 ;
- relever les compteurs de performance à analyser sur le rôle serveur de boîtes aux lettres ;
- relever les compteurs de performance à analyser sur les composants de transport ;
- relever les compteurs de performance à analyser sur le rôle serveur d'accès au client ;
- utiliser les données de performance collectées.

Pourquoi l'analyse des performances est-elle importante ?

Chaque organisation doit disposer de procédures d'analyse bien définies pour son environnement Exchange Server. L'analyse fournit des informations à jour relatives à l'intégrité d'Exchange Sevrer et aux paramètres d'optimisation du traitement. En outre, les procédures d'analyse doivent être réévaluées régulièrement pour s'adapter aux changements de l'infrastructure informatique de l'organisation.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

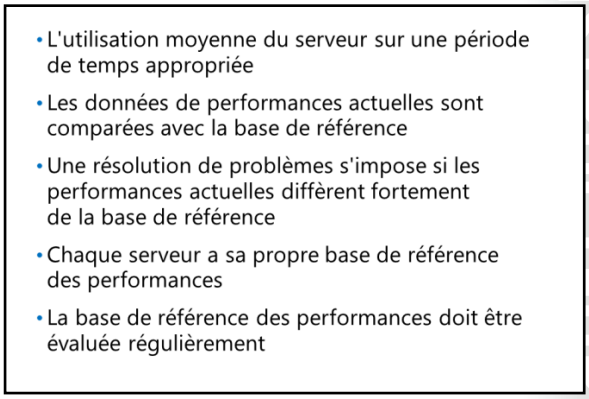
Pour analyser efficacement les performances d'Exchange Server, vous devez :

- identifier les problèmes de performances. Lorsque les problèmes surviennent, vous pouvez les identifier et les résoudre sans que les utilisateurs aient besoin de les signaler ;
- identifier les tendances de croissance pour améliorer la planification des mises à niveau. Au fur et à mesure que le système grandit et que les modèles d'utilisation évoluent, le matériel peut nécessiter des modifications pour prendre en compte ces changements. Vous devez identifier ces tendances pour pouvoir prévoir les modifications qui pourront s'avérer nécessaires dans le futur ;
- mesurer les performances par rapport aux contrats de niveau de service. Vous devez démontrer que le serveur Exchange répond aux impératifs des contrats de niveau de service basés sur les performances, et la mesure de l'expérience de l'utilisateur indique la valeur apportée par les administrateurs d'Exchange Server ;
- identifier les problèmes de sécurité et les attaques par déni de service. Lorsque les performances ou d'autres mesures ne correspondent par à la base de référence établie, vous pouvez mettre en relation ces incidents pour identifier et atténuer leur source.

Pour surveiller efficacement les performances, vous devez collecter et analyser des mesures issues du processeur, de la mémoire, du disque et des services Exchange. Vous pouvez analyser des informations supplémentaires, en fonction des rôles Exchange Server que vous installez.

Qu'est-ce qu'une base de référence des performances ?

Les administrateurs d'Exchange ont tout intérêt à examiner les résultats produits par l'analyse des performances d'Exchange Server. Ils doivent étudier ces données pour déterminer si le comportement et les performances du système répondent aux exigences métier. L'analyse des données aide les administrateurs Exchange à identifier des modèles de croissance, des problèmes de performances, l'impact des applications ou des services et l'impact des modifications apportées par l'organisation ou l'utilisateur. L'analyse des données aide également les administrateurs à décider s'il est nécessaire de procéder à une mise à niveau d'Exchange Server ou à un remplacement du serveur.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Lors du processus d'analyse, les administrateurs doivent comparer les données de performances actuelles avec l'utilisation moyenne de leurs serveurs. Vous pouvez souhaiter surveiller l'utilisation du serveur de manière journalière, ou sur une période d'un mois pour en déterminer l'utilisation moyenne. Cette utilisation moyenne est appelée base de référence des performances. En fonction de la comparaison entre les données de performances actuelles et la base de référence des performances, vous pouvez opter pour l'une ou l'autre des actions suivantes :

- si les performances du serveur sont similaires à la base de référence, les administrateurs peuvent conclure qu'il s'agit des performances prévues. Les administrateurs n'ont besoin de procéder à aucune résolution de problème si la base de référence est prédictible ; ils peuvent en revanche poursuivre la surveillance des serveurs ;
- si les performances du serveur s'écartent notablement de la base de référence des performances, les administrateurs doivent prendre des mesures immédiates pour rechercher les raisons de cet écart et entamer une procédure de résolution des problèmes.

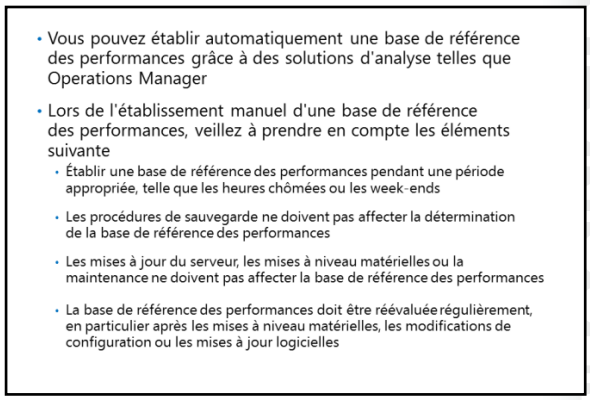
Sans base de référence des performances, les administrateurs ne peuvent pas procéder à une analyse correcte des données de performance, et ne peuvent par conséquent pas décider de l'action à entreprendre. Les administrateurs doivent créer une base de référence pour chaque serveur. Cela est important, car les serveurs peuvent être configurés différemment. Les serveurs peuvent différer selon plusieurs facteurs, notamment s'il s'agit d'un ordinateur physique ou virtuel, des quantités de mémoire disponible et des types de processeur.

Même des serveurs identiques peuvent avoir des bases de référence différentes ; par exemple, ils peuvent héberger différents rôles serveur, tels que l'accès au client ou les boîtes aux lettres. En fait, même lorsque deux serveurs identiques ont les mêmes rôles, comme la boîte aux lettres, leur base de référence des performances peut être différente. Cela peut se produire lorsque le nombre des boîtes aux lettres d'utilisateurs situé sur chacun des serveurs n'est pas le même.

Vous devez évaluer les bases de référence des performances régulièrement. L'infrastructure informatique dans les organisations est dynamique, et les serveurs sont mis à niveau ou remplacés régulièrement ; par conséquent, les bases de référence des performances évoluent également. La base de référence des performances d'Exchange dépend aussi du nombre de boîtes aux lettres utilisateur ainsi que des mises à jour des logiciels et des Service Packs. De plus, les nouvelles installations et mises à jour de logiciels, telles que les logiciels antivirus ou de sauvegarde, peuvent également altérer la base de référence des performances.

Mise en place d'une base de référence des performances

L'établissement d'une base de référence des performances est une étape essentielle pour l'analyse d'Exchange Server. Les organisations qui utilisent un logiciel de gestion et d'analyse tel que Microsoft® System Center Operations Manager 2012 (Operations Manager) peuvent l'utiliser pour créer automatiquement une base de référence des performances. Operations Manager alerte des administrateurs de n'importe quel écart substantiel par rapport à la base de référence. En outre, Operations Manager actualise dynamiquement la base de référence des performances au fil du temps, en respect des modifications apportées à l'infrastructure Exchange Server.



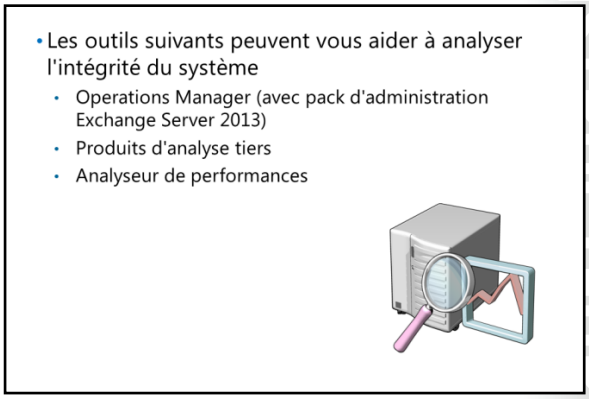
Si votre organisation n'utilise pas Operations Manager ou un autre logiciel qui crée automatiquement une base de référence des performances, vous devez en créer une manuellement en respectant les recommandations suivantes :

- la base de référence des performances est établie pendant une période de temps appropriée, comme un mois ;
- si l'utilisation d'Exchange Server pendant les week-ends ou après les heures de bureau n'est pas identique à celle des heures ouvrées, vous ne devez pas tenir compte des données de performance acquises pendant ces heures ;
- si les procédures de sauvegarde affectent les performances du serveur, ces procédures doivent être planifiées après les heures de bureau, et cette tranche horaire ne doit pas être intégrée dans le calcul de la base de référence des performances ;
- la base de référence des performances ne doit pas être mesurée pendant les mises à jour, les mises à niveau matérielles ou la maintenance du serveur ;
- la base de référence des performances doit être réévaluée régulièrement, en particulier après les mises à jour matérielles, les modifications de la répartition des boîtes aux lettres sur les serveurs, les mises à jour logicielles ou les nouvelles installations de logiciel, telles qu'un antivirus ou un logiciel de sauvegarde.

Outils d'analyse d'Exchange Server

Les organisations utilisent différents types de logiciels ou d'outils pour surveiller leurs environnements Exchange Server. En fonction de la taille des organisations et de la complexité de leur infrastructure informatique, les logiciels d'analyse peuvent être classés en deux catégories :

- les solutions d'analyse pour les entreprises, telles qu'Operations Manager ;
- les solutions d'analyse pour les organisations petites et moyennes, telles que l'Analyseur de performances.



Solutions d'analyse pour les entreprises

La plupart des environnements d'entreprise utilise déjà des solutions d'analyse et de gestion des services dans leur infrastructure informatique. Par exemple, Operations Manager avec le pack d'administration Exchange Server 2013 offre une solution de surveillance pour les infrastructures informatiques, y compris l'analyse pour Exchange Server 2013.

Operations Manager réalise plusieurs tâches de surveillance, telles que :

- la surveillance des événements d'Exchange Server 2013 ;
- le rassemblement des compteurs de performance spécifiques aux composants d'Exchange en un emplacement centralisé ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- l'alerte des opérateurs si une intervention est nécessaire ;
- la mise en corrélation automatique d'événements critiques ;
- la gestion des serveurs Exchange et l'identification des problèmes avant qu'ils ne deviennent critiques.

Operations Manager vous permet également de personnaliser les données dont vous avez besoin. Vous pouvez par conséquent faire des réglages pour répondre à vos scénarios d'utilisation et de matériel particuliers.

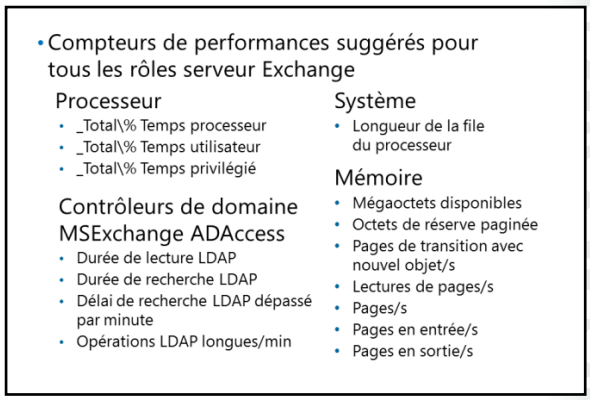
Analyse des solutions à l'aide de l'Analyseur de performances

Dans les situations où il n'existe aucune solution d'analyse pour les entreprises, vous pouvez utiliser l'Analyseur de performances du système d'exploitation Windows Server® 2012 pour collecter les données de performances et analyser l'intégrité d'Exchange Server. L'Analyseur de performances analyse comment Exchange Server 2013 affecte les performances de votre ordinateur, en temps réel et en recueillant les données du journal en vue d'une analyse ultérieure.

L'Analyseur de performances utilise des compteurs de performances, des données de suivi d'événements et des données de configuration ; ces données peuvent être combinées en ensembles de collecteurs de données. Il fournit également une vue d'ensemble de la stabilité du système et des détails sur les événements susceptibles d'affecter la fiabilité.

Collecte des données de performance pour le serveur Exchange

Lorsque vous analysez les serveurs Exchange Server 2013, vous devez connaître les aspects de la performance qui sont les plus importants pour votre organisation. Vous pouvez utiliser les compteurs couramment utilisés et les valeurs de seuil détaillées dans cette leçon pour identifier des problèmes potentiels de manière proactive et identifier la cause principale des problèmes lors de leur résolution.



Ces valeurs sont des recommandations générales. Elles constituent un repère important et peuvent être ajustées pour répondre aux besoins de chaque environnement. Vous pouvez déterminer les valeurs qui fonctionnent dans un environnement spécifique en documentant les valeurs de fonctionnement normales pour créer une base de référence. Une fois la base de référence créée, définissez les seuils qui vous permettent d'être averti lorsque les mesures de performance ne sont pas respectées. Vous saurez alors que le serveur ne fonctionne pas de façon optimale.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

En outre, lorsque vous exécutez Exchange Server 2013 dans un environnement virtuel, vous devez envisager d'ajouter des compteurs de virtualisation dans votre stratégie de surveillance. Ces compteurs de virtualisation sont notamment :

- les compteurs du résumé d'intégrité de l'ordinateur virtuel Hyper-V ;
- les compteurs liés à l'utilisation du processeur Hyper-V, tels que le processeur logique de l'hyperviseur Hyper-V et le processeur virtuel de l'hyperviseur Hyper-V ;
- les compteurs liés à l'utilisation de la mémoire sur les ordinateurs physiques et virtuels ;
- les compteurs liés à l'utilisation de la mise en réseau Hyper-V, tels que la carte réseau Hyper-V héritée, la carte réseau virtuel Hyper-V et le commutateur réseau virtuel Hyper-V ;
- les compteurs liés à l'utilisation du stockage Hyper-V, tels que le périphérique de stockage virtuel Hyper-V.

Processeur

Le processeur est un composant fondamental qu'il est indispensable de surveiller pour garantir l'intégrité du serveur pour les rôles Exchange Server 2013. Le tableau suivant comporte la description et la valeur prévue des compteurs utilisables pour analyser le serveur.

Compteur	Description
_Total\% Temps processeur	Affiche le pourcentage de temps pendant lequel le processeur exécute des processus d'application ou du système d'exploitation.
_Total\% Temps utilisateur	Affiche le pourcentage de temps processeur en mode utilisateur. Cette valeur représente le temps consacré au traitement des applications, des sous-systèmes de l'environnement et des sous-systèmes intégraux.
_Total\% temps privilégié	Affiche le pourcentage de temps processeur en mode privilège. Cette valeur représente le temps consacré au traitement des composants du système d'exploitation et des pilotes matériels.

Le compteur de longueur de la file du processeur est un compteur supplémentaire lié à la performance du processeur. Si la longueur de la file d'attente du processeur est supérieure à la valeur seuil spécifiée, cela peut signifier que la quantité de travail à exécuter est supérieure à celle que le processeur peut gérer. Si cette valeur est supérieure à 10 par cœur de processeur, le processeur a atteint sa capacité, en particulier lorsqu'il est associé à une utilisation élevée du processeur. Bien qu'il ne soit pas courant d'utiliser le compteur de longueur de la file du processeur dans la cadre de la planification de la capacité, il est tout de même possible de l'utiliser pour déterminer s'il sera nécessaire d'acheter des unités de traitement plus rapides pour les futurs serveurs.

Le tableau suivant présente la description et la valeur prévue du compteur de la longueur de la file du processeur dans le groupe System.

Groupe	Compteur	Description
System	Processeur Longueur de queue	Affiche le nombre de threads géré par chaque processeur. Vous pouvez utiliser ce compteur pour savoir si la contention du processeur ou l'utilisation élevée du processeur est causée par une insuffisance de capacité du processeur.

Mémoire

Le compteur de mémoire est un autre indicateur de performance clé. En suivant la quantité de mémoire disponible et la quantité de mémoire qui doit être écrite dans le fichier d'échange, vous pouvez déterminer à quel moment il est nécessaire d'augmenter la mémoire du serveur ou de réduire sa charge.

Le tableau suivant présente la description et les valeurs prévues pour les compteurs de mémoire.

Compteur	Description
Mégaoctets disponibles	Affiche la quantité de mémoire physique, en mégaoctets (Mo), immédiatement disponible pour être allouée à un processus ou pour être utilisée par le système. Cette valeur est égale à la quantité de mémoire affectée à l'attente (mise en cache), libre et sans listes de pages.
Octets de réserve paginée	Affiche la partie de mémoire système partagée que vous pouvez paginer au fichier d'échange du disque. La réserve paginé est créée pendant l'initialisation du système et est utilisée par les composants en mode noyau pour allouer la mémoire système.
Pages de transition avec nouvel objet/s	Indique la pression sur le cache du système.
Lectures de pages/s	Affiche que les données doivent être lues à partir du disque plutôt qu'à partir de la mémoire. Indique que la mémoire n'est pas suffisante et que la pagination commence. Une valeur supérieure à 30 par seconde signifie que le serveur ne peut plus faire face à la charge.
Pages/s	Affiche la cadence à laquelle les pages sont lues ou écrites sur le disque pour résoudre les défauts de page. Ce compteur est un indicateur essentiel des types d'erreurs qui entraînent des délais à l'échelle du système. Pages/s est la somme de Mémoire\Pages en entrée/s et de Mémoire\pages en sorties/s. Elle est chiffrée en nombres de pages ; elle peut ainsi être comparée à d'autres comptages de pages, tels que Mémoire\Défauts de page/s, sans nécessiter de conversion. Pages/s inclut les pages extraites pour répondre aux erreurs du cache du système de fichiers, généralement demandées par les applications, et aux fichiers mappés en mémoire non mis en cache.
Pages en entrée/s	Affiche la cadence à laquelle les pages sont lues à partir du disque pour résoudre les défauts de page. Les défauts de page se produisent lorsqu'un processus fait référence à une page dans la mémoire virtuelle qui n'est pas dans sa plage de travail ou qui est ailleurs dans la mémoire physique, et qui doit être récupérée à partir du disque. Quand une page est en erreur, le système tente de lire plusieurs pages contiguës dans la mémoire pour tirer le meilleur parti de l'opération de lecture. Pour déterminer le nombre moyen de pages lues dans la mémoire pendant chaque opération de lecture, comparez la valeur de Mémoire\Pages en entrée/s avec la valeur Mémoire\Lecture de pages/s.
Pages en sortie/s	Affiche la cadence à laquelle les pages sont écrites sur le disque pour libérer de l'espace dans la mémoire physique. Les pages sont écrites sur le disque uniquement si elles sont modifiées dans la mémoire physique. Elles contiennent en général des données et non du code. Un grand nombre de pages produit peut indiquer une insuffisance de mémoire. Le système d'exploitation Windows® Server réécrit des pages supplémentaires sur le disque pour libérer de l'espace lorsque la mémoire physique devient insuffisante. Ce compteur affiche le nombre de pages, et vous pouvez le comparer à d'autres nombres de pages sans conversion.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôleurs de domaine MSExchange ADAccess

Exchange Server 2013 repose fortement sur les services de domaine Active Directory® (AD DS) pour le stockage et la lecture de ses données de configuration. Il est donc essentiel de mesurer le temps de réponse et l'intégrité de la connexion à AD DS.

Le tableau suivant présente les descriptions et les valeurs prévues pour les compteurs liés au protocole LDAP (Lightweight Directory Access Protocol).

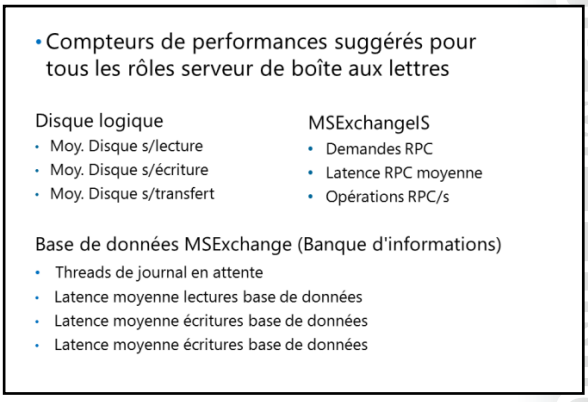
Compteur	Description
Durée de lecture LDAP privilégié	Affiche le temps (en millisecondes, ms) qu'il faut pour envoyer une requête de lecture LDAP au contrôleur de domaine indiqué et pour recevoir une réponse.
Durée de recherche LDAP privilégié	Affiche la durée (en ms) nécessaire pour envoyer une demande de recherche LDAP et recevoir une réponse.
Opérations LDAP longues/min	Affiche le nombre d'opérations LDAP sur ce contrôleur de domaine qui ont duré plus longtemps que le seuil par minute spécifié. (le seuil par défaut est de 15 secondes).
Délai de recherche LDAP dépassé par minute	Affiche le nombre de recherches LDAP renvoyées dont le délai de recherche LDAP est dépassé au cours de la dernière minute.

Analyse des services et des journaux

Il est également important de vérifier que chacun des services Exchange Server 2013 s'exécute et traite les demandes. Vous pouvez analyser les services en interrogeant leur état à l'aide de l'outil Gestion des services, de l'applet de commande **Get-Services** ou d'un outil d'analyse tiers. Les éléments enregistrés dans les journaux des événements peuvent également indiquer des problèmes avec Exchange Server 2013. Ces événements sont en général classés comme des erreurs ou des avertissements.

Collecte des données de performance pour le serveur de boîtes aux lettres

Lorsque vous collectez les données de performance associées aux serveurs de boîtes aux lettres, vous pouvez vous concentrer sur le temps de réponse du disque et sur la vitesse à laquelle le serveur répond aux demandes. Si la longueur de file d'attente du disque commence à augmenter, cela indique que le système de disque ne répond pas à la demande. Tous ces indicateurs peuvent signifier que vous devez peut-être acheter des disques supplémentaires ou plus rapides, ou modifier leur configuration.



Il existe de nombreux compteurs de performances pour les boîtes aux lettres que vous pouvez surveiller, en fonction de votre environnement de messagerie. Les compteurs suivants sont très importants et constituent un bon point de départ pour collecter les données de performances du serveur de boîtes aux lettres.

Disque logique

Les compteurs de disque logique déterminent si les performances du disque satisfont les demandes. Au fur et à mesure que la latence du disque augmente, la lecture et l'écriture de la base de données prennent plus de temps.

Le tableau suivant présente les descriptions et les valeurs prévues des compteurs de disques logiques.

Compteur	Description
Moyenne Disque s/lecture	Affiche la durée moyenne de lecture des données à partir du disque.
Moyenne Disque s/écriture	Affiche la durée moyenne pour l'écriture des données sur le disque.
Moyenne Disque s/transfert	Affiche le nombre moyen d'octets transférés depuis ou vers le disque pendant les opérations de lecture ou d'écriture.

Banque d'informations MSExchangeIS

Les services d'accès client et de transport utilisent l'appel de procédure distante (RPC) de Microsoft pour communiquer avec les serveurs de boîtes aux lettres. Par conséquent, il est important de surveiller le temps de réponse des demandes RPC pour garantir que le serveur de boîtes aux lettres est assez rapide pour supporter la charge.

Le tableau suivant répertorie les descriptions et les valeurs prévues des compteurs liés au RPC.

Compteur	Description
% demandes RPC	Affiche les requêtes RPC en cours d'exécution dans le processus de banque d'informations.
Latence RPC moyenne	Affiche la latence RPC (en ms) moyenne pour toutes les opérations dans les 1 024 derniers paquets.
Opérations RPC/s	Affiche le nombre actuel d'opérations RPC qui se produisent par seconde.

MSExchangeDatabase ==> Instances

Dans Exchange Server, les performances des bases de données font partie des paramètres les plus importants. Le tableau suivant répertorie les compteurs que vous pouvez utiliser pour analyser les performances des bases de données.

Compteur	Description
Threads de journal en attente	Affiche le nombre de threads en attente que leurs données soient écrites dans le journal pour effectuer une mise à jour de la base de données. Si ce pourcentage est élevé pendant une durée prolongée, il peut y avoir un goulot d'étranglement au niveau du journal.
Latence moyenne lectures base de données E/S	Affiche la durée moyenne (en ms) des opérations de lecture par base de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

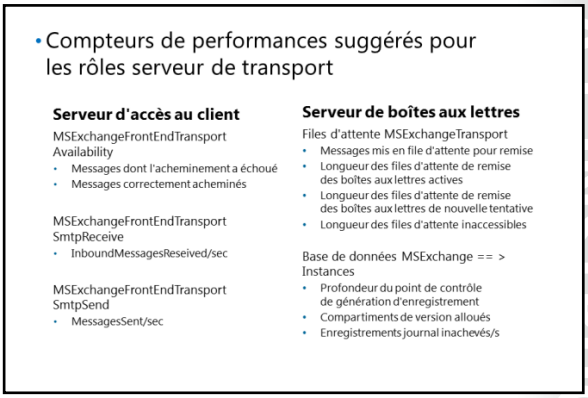
(*suite*)

Compteur	Description
Latence moyenne d'écritures base de données E/S	Affiche la durée moyenne (en ms) des opérations d'écriture par base de données.
% de cache base de données atteint	Affiche le pourcentage des demandes de page de base de données satisfait par le cache de la base de données sans causer une opération de fichier. Si ce pourcentage est trop bas, la taille du cache de la base de données est peut-être trop faible.

Question : si la mesure de l'un de ces compteurs de performances se trouve en dehors de sa plage normale, qu'affectera-t-il le plus probablement dans l'environnement de production ?

Collecte des données de performances pour les composants de transport

Les composants de transport sont installés sur les rôles serveur d'accès au client et de boîtes aux lettres. Par conséquent, il existe différents compteurs pour chaque rôle qui doivent être surveillés.



Composants de transport sur le rôle serveur de boîtes aux lettres

Le composant de transport sur le rôle serveur de boîtes aux lettres utilise une base de données de file d'attente, qui est un emplacement temporaire d'attente pour les messages traités dans un ordre spécifique. Par conséquent, un système de disque doit répondre aux exigences de performances pour le traitement du courrier électronique d'une organisation. Si le système de disque ne répond pas à ces exigences de performances, vous devrez le remplacer par des disques plus rapides, ou modifier leur configuration. Pour plus d'informations sur l'analyse du disque logique sur le serveur de boîtes aux lettres, lisez la rubrique précédente « Collecte des données de performance pour le serveur de boîtes aux lettres ».

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Base de données MSExchange ==> Instances

L'analyse des performances de la base de données vous aide à identifier les problèmes liés à la lecture ou au stockage des informations de la file d'attente dans les bases de données. Le tableau suivant présente les descriptions des compteurs de base de données de transport.

Compteur	Description
Profondeur du point de contrôle de génération d'enregistrement	Affiche le volume de travail (en nombre de fichiers journaux) qui doit être refait ou annulé dans les fichiers de base de données en cas d'arrêt du processus.
Compartiments de version alloués	Affiche le nombre total de compartiments de version alloués. Indique les valeurs de régulation du flux par défaut, telles qu'elles sont répertoriées dans le fichier EdgeTransport.exe.config. **Remarque :** Les compartiments de version sont des transactions de base de données de file d'attente de messages en attente, qui sont conservées dans la mémoire mais ne sont pas validées ni écrites dans la base de données de file d'attente de messages.
Enregistrements journal inachevés/s	Affiche le nombre d'enregistrements de journal qui n'ont pas pu être ajoutés aux tampons du journal par seconde parce qu'ils sont saturés. Si ce compteur est différent de zéro la plupart du temps, la taille du tampon du journal peut être un goulot d'étranglement.

Files d'attente MSExchangeTransport

Les messages qui sont mis en file d'attente avant envoi peuvent indiquer un problème de connectivité au composant de transport du serveur d'accès au client. Le tableau suivant présente la description et les valeurs prévues pour les compteurs relatifs à la longueur de la file d'attente de transport.

Compteur	Description
Messages placés en file d'attente pour remise	Affiche le nombre actuel de messages déposés qui ne sont pas encore traités par le transport.
Longueur des files d'attente de remise des boîtes aux lettres du disque	Affiche le nombre de messages dans les files d'attente des boîtes aux lettres actives.
Longueur des files d'attente de remise des boîtes aux lettres du disque	Affiche le nombre de messages en attente de nouvelle tentative de remise d'un message à une boîte aux lettres distante.
Longueur des files d'attente inaccessibles du disque	Affiche le nombre de messages des files d'attente inaccessibles.
Longueur de la file d'attente du disque	Affiche le nombre de messages dans la file d'attente de messages incohérents. La file d'attente des messages incohérents contient les messages identifiés comme dangereux pour le système Exchange 2013 après une défaillance du serveur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Composants de transport sur le rôle serveur d'accès au client

Le composant de transport sur le rôle serveur d'accès au client joue le rôle de proxy entre le protocole SMTP et le rôle serveur de boîtes aux lettres où se situe la base de données de boîtes aux lettres de l'utilisateur. Par conséquent, il est important que vous mesuriez le taux de réussite du routage des messages. En outre, il est aussi important de mesurer les compteurs de performance tels que le nombre de messages envoyés et reçus et la disponibilité du service smtp.

Le tableau suivant comporte la description des compteurs des composants de transport sur le serveur d'accès au client.

Groupe	Compteur	Description
MSExchangeFrontEndTransportSmtpAvailability	MessagesFailedToRoute	Affiche le nombre de messages dont le routage a échoué.
	MessagesSuccesfullyRouted	Affiche le nombre de messages qui ont été correctement acheminés.
MSExchangeFrontEndTransportSmtpReceive	InboundMessagesReseived/sec	Affiche le nombre de messages reçus par seconde.
MSExchangeFrontEndTransportSmtpSend	MessagesSent/sec	Affiche le nombre de messages envoyés par seconde.

Question : Si la mesure de l'un de ces compteurs de performances se trouve en dehors de sa plage normale, qu'affectera-t-il le plus probablement dans l'environnement de production ?

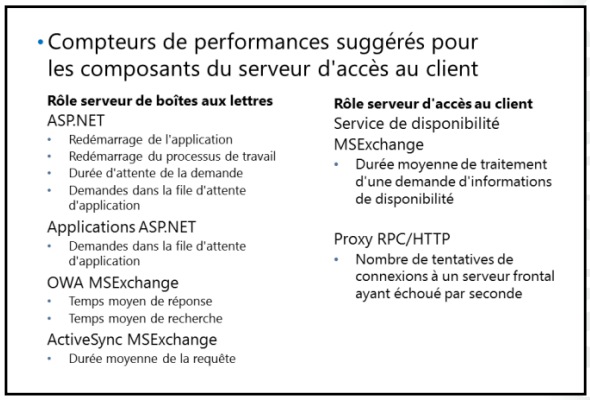
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Collecte des données de performance pour les composants d'accès au client

L'évaluation des composants d'accès au client implique la surveillance d'un grand nombre d'objets et de compteurs. L'expérience de vos utilisateurs est affectée par le temps de réponse des services utilisés par les composants d'accès au client.

Tout comme les composants de transport, les composants d'accès au client sont installés sur le rôle serveur de boîtes aux lettres et sur le rôle serveur d'accès au client. Vous devez par conséquent analyser différents compteurs pour chaque rôle serveur.



Compteurs de performance pour les composants d'accès au client sur le rôle serveur de boîtes aux lettres

ASP.NET et applications

Microsoft Outlook® Web App et les services Web Exchange dépendent largement des fichiers Microsoft .NET Framework et ASP.NET qui sont lus, traités et restitués pour les utilisateurs finaux. L'analyse du temps de réponse et du nombre de fois où l'application a dû redémarrer peut vous aider à vérifier l'intégrité de l'ensemble des services.

Groupe	Compteur	Description
ASP.NET	Redémarrage de l'application	Indique le nombre de fois où l'application a été redémarrée pendant la durée de vie du serveur Web.
	Redémarrage du processus de travail	Indique le nombre de fois où un processus de travail a redémarré sur l'ordinateur.
	Demandes en cours	Indique le nombre de demandes (y compris les demandes en file d'attente) en cours d'exécution ou en attente d'écriture dans le client. Dans le modèle de processus ASP.NET, lorsque ce compteur dépasse la valeur de requestQueueLimit définie dans la section de configuration du modèle de processus, ASP.NET commence à rejeter les demandes. La valeur maximale est de 5 000. Le serveur retourne une erreur 503 si le compteur dépasse cette valeur.
	Durée d'attente de la demande	Indique la durée d'attente dans la file (en ms) de la demande la plus récente.
Applications ASP.NET	Demandes dans la file d'attente d'application	Indique le nombre de demandes dans la file d'attente des demandes d'application. La valeur maximale est de 5 000. Le serveur retourne une erreur 503 si le compteur dépasse cette valeur.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Services Web MSExchange

Les temps de réponse des services Web, tels que Outlook Web App, le proxy Outlook Anywhere (RPC/HTTP), Microsoft® Exchange ActiveSync®, les téléchargements de carnet d'adresses en mode hors connexion et le service de disponibilité sont également des valeurs importantes à analyser. Si un administrateur d'Exchange remarque que la valeur de ces compteurs de performances diffèrent de la valeur de la base de référence des performances, un client peut avoir une réponse lente du serveur.

Groupe	Compteur	Description
OWA MSExchange	Temps moyen de réponse	Indique le temps moyen (en ms) qui s'est écoulé pour la demande. Utilisé pour déterminer la latence rencontrée par un client.
	Temps moyen de recherche	Indique le temps moyen (en ms) écoulé jusqu'à l'achèvement d'une recherche.
Proxy RPC/HTTP	Nombre de tentatives de connexions à un serveur frontal ayant échoué par seconde	Indique la cadence à laquelle les tentatives du proxy RPC ne parviennent pas à établir une connexion à un serveur principal.
ActiveSync MSExchange	Durée moyenne de la requête	Indique la durée moyenne d'attente jusqu'à ce qu'une demande soit achevée. Détermine la cadence à laquelle les demandes de disponibilité du service se produisent.
Service de disponibilité MSExchange	Durée moyenne de traitement d'une demande d'informations de disponibilité	Indique le nombre de requêtes traitées par seconde.

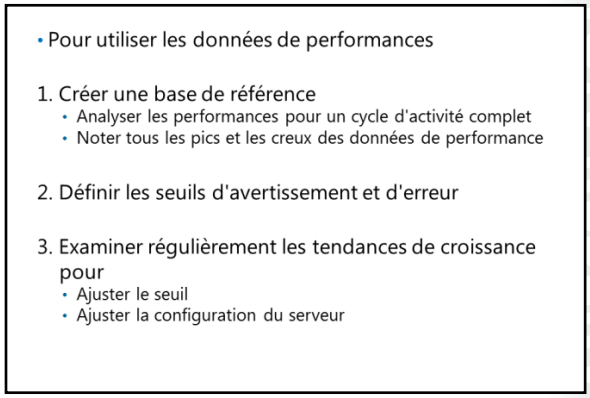
Compteurs de performance pour les composants d'accès au client du rôle serveur d'accès au client

Dans Exchange Server 2013, les composants d'accès au client sur le serveur d'accès au client assurent l'authentification et le rôle de proxy pour le trafic HTTP vers les composants d'accès au client du rôle serveur de boîtes aux lettres. Le tableau suivant décrit quelques-uns des compteurs de performance recommandés concernant les composants du rôle serveur d'accès au client :

Groupe	Compteur	Description
Proxy HTTP MSExchange	Requêtes proxy/s	Indique le nombre de requêtes de proxy traitées par seconde.
Proxy RPC/HTTP	Nombre de tentatives de connexions à un serveur frontal ayant échoué par seconde	Indique la cadence à laquelle les tentatives du proxy RPC ne parviennent pas à établir une connexion à un serveur principal.
Authentification MSExchange	Total des requêtes d'authentification	Indique le nombre de requêtes d'authentifications traitées par seconde.

Question : Si la mesure de l'un de ces compteurs de performances du serveur d'accès au client se trouve en dehors de sa plage normale, qu'affectera-t-il le plus probablement dans l'environnement de production ?

Utilisation des données de performance collectées



Pour déterminer les seuils qui indiquent un problème existant, définissez base de référence d'analyse en examinant les données de performances sur un cycle d'activité complet. Les cycles d'activité varient d'une entreprise à une autre, mais ils doivent comprendre des périodes chargées et des périodes calmes. Pour certaines entreprises, les périodes les plus chargées peuvent être liées au processus de clôture de comptabilité en fin de mois, ou être des périodes pendant lesquelles le chiffre d'affaires est plus élevé. Rassembler un large éventail de données fournit les données nécessaires pour déterminer les seuils de fonctionnement appropriés.

Pour utiliser les données de performance collectées :

1. Créer une base de référence d'analyse en faisant la moyenne de mesures de la performance d'un système fonctionnant correctement :
   - analyser les performances pour un cycle d'activité complet ;
   - noter tous les pics et les creux des données de performance.
2. Définir les seuils d'avertissement et d'erreur.
3. Examiner régulièrement les tendances de croissance pour :
   - ajuster les seuils ;
   - ajuster les configurations du serveur.

Il est important d'examiner régulièrement les seuils afin de procéder à des réglages sur les serveurs (ou sur les seuils) et veiller au bon fonctionnement du système.

Remarque : Operations Manager utilise une technologie de réglage automatique des seuils. Cette fonctionnalité règle automatiquement les seuils des compteurs d'un objet, en fonction des valeurs acquises antérieurement. Ces seuils sont réglés automatiquement en fonction de l'utilisation actuelle du système et de la comparaison avec la base de référence qui a été apprise au cours de la période de surveillance précédente.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 2
Maintenance d'Exchange Server 2013

La maintenance de la solution de messagerie Exchange Server est un processus continu qui requiert des procédures établies qui n'affecteront pas la disponibilité et l'expérience utilisateur du serveur. Les administrateurs doivent également suivre les meilleures pratiques et les recommandations Microsoft relatives aux procédures de maintenance. L'utilisation de techniques de gestion des changements pour contrôler les modifications présente de nombreux avantages, qui sont décrits dans cette leçon. La gestion des changements comprend souvent le contrôle des mises à jour logicielles qui sont appliquées, et comment et quand ces mises à jour sont appliquées. Elle inclut également la gestion des mises à jour matérielles.

Dans cette leçon, vous allez étudier l'importance de la gestion des changements et les techniques que vous pouvez utiliser pour réaliser des mises à niveau de vos ordinateurs Exchange Server.

Exchange Server 2013 introduit deux nouveaux concepts pour la gestion de l'intégrité et des performances : la gestion de la charge de travail et la disponibilité gérée.

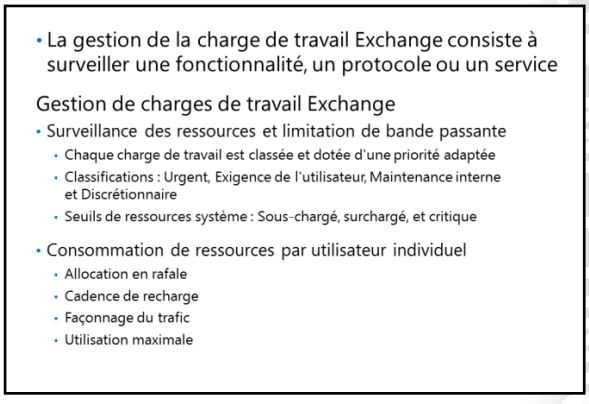
Objectifs de la leçon

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

- décrire la gestion de la charge de travail Exchange ;
- configurer la gestion de la charge de travail Exchange ;
- décrire la disponibilité gérée ;
- décrire la gestion des modifications ;
- planifier le déploiement des mises à jour logicielles d'Exchange ;
- planifier les mises à niveau matérielles d'Exchange.

Qu'est-ce que la gestion de la charge de travail Exchange ?

Exchange Server 2013 introduit un nouveau concept d'analyse et de gestion nommé Gestion de la charge de travail. La charge de travail est définie comme une fonctionnalité un protocole ou un service, tel que Outlook Web App, Exchange ActiveSync, ou la migration des boîtes aux lettres. Les charges de travail telles que Outlook Web App sont surveillées et gérées au lieu des services dont dépend Outlook Web App ou qu'elle utilise, comme les services Internet (IIS) et Active Directory.

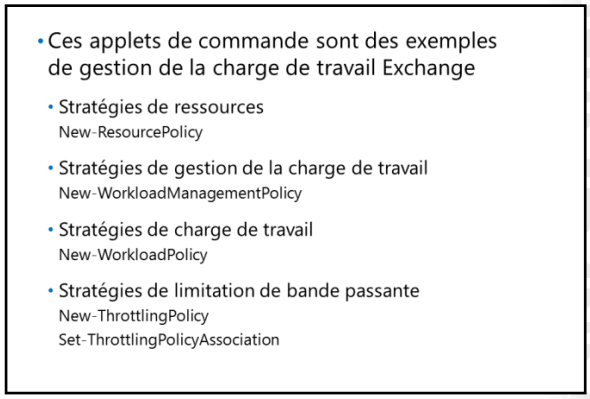


Vous pouvez gérer les charges de travail dans Exchange Server 2013 comme suit :

- Analyse des ressources système. Ce type de surveillance a été introduit dans Microsoft® Exchange Server 2010, et était appelée limitation de bande passante. Pour surveiller la charge de travail d'Exchange, les ressources utilisées par cette application sont surveillées :par exemple l'utilisation du processeur, la consommation de mémoire et l'utilisation du réseau, entre autres. Si les ressources du serveur sont fortement sollicitées, Exchange Server ralentit progressivement les charges de travail ayant la priorité la plus basse. Les priorités sont définies par la classification attribuée à la charge de travail : Urgent, Exigence de l'utilisateur, Maintenance interne et Discrétionnaire ; la classe Urgent a la priorité la plus élevée et Discrétionnaire, la moins élevée. Les seuils de ressources système, appliqués sur les mesures de l'utilisation, comportent trois niveaux : Sous-chargé, surchargé, et critique.
- Contrôle de la consommation des ressources par les utilisateurs individuels. Cette méthode de gestion des charges de travail comporte différents types d'utilisation de la charge de travail par les utilisateurs, notamment :
    - Allocation en rafale. Exchange Server autorise les utilisateurs à consommer davantage de ressources pendant un bref laps de temps sans limitation de bande passante ;
    - Cadence de recharge. Exchange Server utilise un système de budget des ressources, où les administrateurs définissent une cadence à laquelle les budgets des utilisateurs sont rechargés en des laps de temps définis. Par exemple, une valeur de 300 000 millisecondes signifie que les budgets des utilisateurs sont rechargés de 5 minutes d'utilisation par heure ;
    - Façonnage du trafic. Exchange Server reporte à plus tard les requêtes d'un utilisateur si celui-ci a atteint la limite configurée pour l'intervalle de temps défini. Ce type d'utilisation de la charge de travail empêche les utilisateurs de surcharger le serveur. En général, les tâches des utilisateurs ne sont pas affectées car ces retards sont courts et presque indétectables ;
    - Utilisation maximale. Exchange Server empêche temporairement les utilisateurs de réaliser leurs tâches, car ils ont atteint leur seuil d'utilisation des ressources. Les utilisateurs sont débloqués une fois que leur budget est rechargé.

Configuration de la gestion de la charge de travail Exchange

La gestion de la charge de travail d'Exchange est configurée dans l'environnement de ligne de commande Exchange Management Shell par la création ou la modification des paramètres de stratégie de gestion de la charge de travail. Ces paramètres peuvent être configurés au niveau de l'organisation et être appliqués à tous les serveurs Exchange de l'organisation, ou être configurés au niveau du serveur et n'être appliqués qu'à ce serveur spécifique.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Les applets de commande utilisés pour gérer la stratégie de ressources sont :

- **New-ResourcePolicy**
- **Remove-ResourcePolicy**
- **Get-ResourcePolicy**
- **Set-ResourcePolicy**

Les applets de commande utilisés pour gérer la stratégie de gestion de la charge de travail sont :

- **New-WorkloadManagementPolicy**
- **Remove-WorkloadManagementPolicy**
- **Get-WorkloadManagementPolicy**

Les applets de commande utilisés pour gérer les stratégies de charge de travail sont :

- **New-WorkloadPolicy**
- **Remove-WorkloadPolicy**
- **Get-WorkloadPolicy**
- **Set-ResourcePolicy**

Les stratégies de limitation de bande passante sont gérées et attribuées à l'aide des applets de commande suivantes :

- **New-ThrottlingPolicy**
- **Get-ThrottlingPolicy**
- **Set-ThrottlingPolicy**
- **Remove-ThrottlingPolicy**
- **Get-ThrottlingPolicyAssociation**
- **Set-ThrottlingPolicyAssociation**

Pour afficher les stratégies de gestion de la charge de travail actuelles, utilisez l'applet de commande suivante :

- **Get-WorkloadManagementPolicy**

Pour modifier la stratégie de gestion par défaut de la charge de travail pour l'application Outlook Web App de votre organisation, utilisez l'applet de commande suivante :

```
New-WorkloadPolicy OrgOWAWorkloadPolicy -WorkloadType OWA -WorkloadClassification
Discretionary -WorkloadManagementPolicy GlobalOverrideWorkloadManagementPolicy.
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Pour créer une stratégie de gestion de la charge de travail pour Outlook Web App pour un serveur spécifique, effectuez les étapes suivantes :

1. Créez une stratégie de gestion personnalisée de la charge de travail qui sera appliquée ultérieurement à un serveur spécifique à l'aide de l'applet de commande suivante :

```
New-WorkloadManagementPolicy LondonWorkloadManagementPolicy
```

2. Créez ensuite une stratégie de charge de travail pour Outlook Web App en utilisant l'applet de commande suivante :

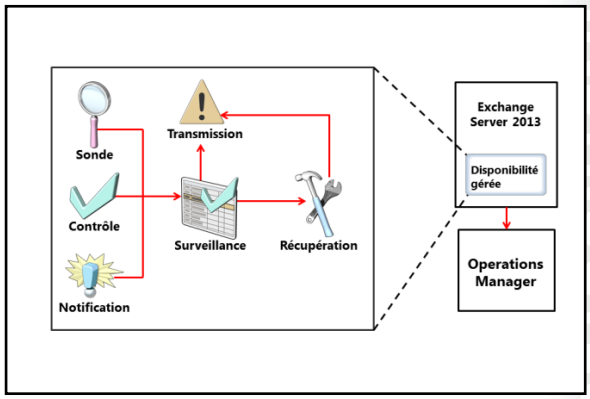
```
New-WorkloadPolicy LondonOWAWorkloadPolicy -WorkloadType OWA -WorkloadClassification
Discretionary -WorkloadManagementPolicy LondonWorkloadManagementPolicy
```

3. Pour finir, appliquez la stratégie de gestion personnalisée de la charge de travail que vous venez de créée à un serveur spécifique à l'aide de l'applet de commande suivante :

```
Set-ExchangeServer -WorkloadManagementPolicy LondonWorkloadManagementPolicy -Identity
LON-MBX01
```

Qu'est-ce que la disponibilité gérée ?

La disponibilité gérée est une nouvelle infrastructure de surveillance et de gestion des charges de travail Exchange. La disponibilité gérée surveille l'état d'intégrité des charges de travail Exchange. Si l'intégrité des charges de travail Exchange présente des problèmes, la disponibilité gérée tentera de réaliser la récupération de la charge de travail Exchange. Cette fonctionnalité permet aux utilisateurs d'accéder sans interruption à leurs boîtes aux lettres sans rencontrer aucune défaillance ou déconnexion.



Dans les versions précédentes d'Exchange Server, quand des problèmes de serveur ou de performances apparaissaient, les administrateurs effectuaient généralement effectué l'une des procédures suivantes pour diagnostiquer et résoudre le problème :

- vérifier si le service fonctionne dans la console Services ;
- exécuter différentes applets de commande de test ;
- examiner les données dans la console Analyseur de performances.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Dans Exchange Server 2013, la disponibilité gérée analyse des charges de travail au lieu des services ou des performances. Si une charge de travail Exchange présente une réponse lente ou ne répond pas, la disponibilité gérée essaie de détecter et récupérer la charge de travail. La disponibilité gérée est intégrée à la haute disponibilité Exchange Server. Par exemple, il est possible que le basculement de base de données se déclenche même lorsque la base de données active est intègre, mais que le protocole qui connecte les clients vers leurs boîtes aux lettres situées dans cette base de données ne répond pas.

La disponibilité gérée est constituée de trois composants :

- *les sondes*. Elles contrôlent les connexions utilisateur actuelles et créent des notifications basées sur les informations de l'état actuel et de la disponibilité ;
- *le moteur d'analyse*. Il analyse les données issues des sondes et réagit par deux décisions possibles : intègre ou non-intègre ;
- *le moteur de répondeur*. Il tente de récupérer la charge de travail Exchange si l'état est d'intégrité non conforme. Selon le type du problème, l'action de récupération peut prendre différentes formes : redémarrage du service, réinitialisation du pool d'applications et basculement de la base de données de boîtes aux lettres, entre autres. Si aucune de ces actions ne résout le problème, le répondeur transmettra celui-ci en informant les administrateurs ou en créant une alerte dans Operations Manager.

Éléments à prendre en compte pour la gestion des changements

Le processus de gestion des changements varie considérablement d'une organisation à une autre. Les fondamentaux de la gestion des changements sont :

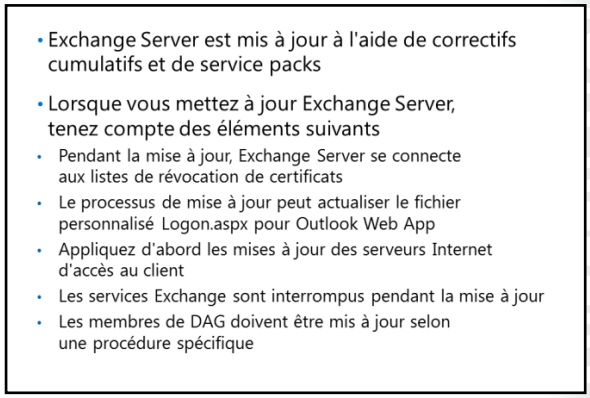
- Les fondamentaux de la gestion des changements sont
  - Définir un processus et l'utiliser de façon cohérente
  - Prendre en charge le processus de gestion des changements
  - Utiliser un modèle de processus tel que Microsoft Operations Framework pour décrire le cycle de vie d'un système

- adopter un modèle de processus. Un certain nombre d'infrastructures bien définies sont disponibles, comme Microsoft Operations Framework. Adopter une infrastructure établie peut permettre de former plus facilement les employés, car ils la connaissent peut-être déjà.
- définir un processus et l'utiliser de façon cohérente. Une fois que vous avez implémenté un processus, assurez-vous que toutes les personnes impliquées comprennent pourquoi il a été adopté et comment le suivre ;
- prendre en charge le processus de gestion des changements. Si vous ne prenez pas correctement en charge le processus, vous ne pourrez pas optimiser son efficacité. Il est essentiel que toutes les personnes impliquées travaillent à la mise en œuvre du processus.

Le succès de la gestion des changements dépend de tous : des ingénieurs qui implémentent les modifications aux cadres de l'organisation qui doivent comprendre le processus et le suivre. Bien que la gestion des changements requière un travail supplémentaire préalable, le processus garantit des changements bénéfiques et effectifs. Une implémentation bien menée des changements fait gagner du temps, épargne des efforts et améliore la satisfaction des utilisateurs.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Planification du déploiement des mises à jour logicielles d'Exchange



Vous pouvez mettre Microsoft Exchange Server 2013 à jour en installant les correctifs cumulatifs et les service packs. À la différence d'autres produits tels que Windows Server, vous ne pouvez pas mettre Exchange Server à jour au moyen de fichiers de mise à jour isolés ; au lieu de cela, vous devez utiliser les packages qui contiennent plusieurs mises à jour et correctifs.

Les service packs et les correctifs cumulatifs font partie du programme de service pour Exchange Server 2013. Ces ressources offrent une méthode efficace et facile pour distribuer les correctifs et les modifications d'Exchange Server 2013. Il est recommandé d'installer les derniers service packs et correctifs cumulatifs pour maintenir le produit à jour.

Le dernier correctif cumulatif de la série comprend les correctifs qui ont été publiés dans les correctifs cumulatifs précédents de la même série. Par exemple, si vous installez le correctif cumulatif 3 pour Exchange Server 2013 RTM, il comprend les correctifs qui ont été publiés dans le correctif cumulatif 1 et le correctif cumulatif 2. Par conséquent, vous n'avez besoin que du plus récent correctif cumulatif pour être à jour.

L'application des correctifs cumulatifs et des service packs est généralement une procédure simple. Cependant, dans certains cas, vous devez tenir compte des éléments suivants :

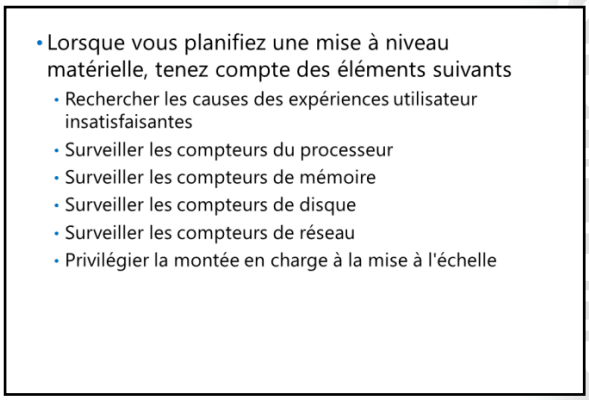
- quand vous installez un package de correctif cumulatif, Exchange tente de se connecter au site Web contenant la liste de révocation des certificats. Exchange l'examine pour vérifier le code de signature du certificat. Si Exchange Server ne peut pas se connecter à ce site Web, l'installation du correctif cumulatif peut prendre beaucoup de temps, ou alors vous pouvez recevoir un message d'erreur pendant l'installation. Pour contourner ce problème et réduire le temps d'installation, désactivez l'option **Vérifier la révocation des certificats de l'éditeur** sur le serveur que vous mettez à niveau ;
- lorsque vous appliquez un package de correctif cumulatif, le processus de mise à jour peut mettre à jour le fichier Logon.aspx. Si vous avez modifié le fichier Logon.aspx, vous ne pourrez pas le mettre à jour avec succès. Par exemple, si vous avez modifié le fichier Logon.aspx pour personnaliser Outlook Web App, il peut ne pas être mis correctement à jour ; alors une fois le processus de mise à jour terminé, Outlook Web App peut afficher une page vierge. Pour contourner ce problème, renommez le fichier Logon.aspx avant d'appliquer le correctif cumulatif, puis, une fois la mise à jour terminée, restaurez vos personnalisations de Outlook Web App dans le fichier Logon.aspx ;
- si vous avez déployé la transmission par proxy entre serveurs d'accès au client, vous devez appliquer le correctif cumulatif aux serveurs d'accès au client Internet avant de l'appliquer aux serveurs d'accès au client non-Internet ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

- lorsque vous installez un correctif cumulatif, le programme d'installation arrête automatiquement les services Exchange et les services IIS appropriés. Par conséquent, pendant le processus d'installation, le serveur peut ne pas être capable de répondre aux demandes de services des utilisateurs. Il est recommandé d'installer un correctif cumulatif au cours d'une période de maintenance planifiée ou au cours d'une période d'impact modéré sur l'activité ;
- lorsque vous installez un correctif cumulatif sur un serveur qui est membre d'un groupe de disponibilité de bases de données (DAG), plusieurs services seront arrêtés pendant l'installation, y compris tous les services Exchange et le service de cluster Windows. Le processus général pour installer des correctifs cumulatifs sur un membre d'un groupe DAG est le suivant :
    a. Exécuter le script StartDagServerMaintenance.ps1 pour mettre le membre du groupe DAG en mode de maintenance et le préparer pour l'installation du correctif cumulatif.
    b. Installer le correctif cumulatif.
    c. Exécuter le script StopDagServerMaintenance.ps1 pour mettre le membre du groupe DAG hors du mode de maintenance et le remettre en production.
    d. Éventuellement, rééquilibrer le DAG à l'aide du script RedistributeActiveDatabases.ps1.
    e. Appliquer cette procédure pour installer les mises à jour du système d'exploitation à partir de Microsoft Update.

Planification des mises à niveau matérielles Exchange

L'utilisation matérielle d'Exchange Server 2013 est plus efficace par rapport aux versions précédentes d'Exchange Server. Le besoin de mises à niveau matérielles est donc moindre. Exchange Server 2013 réduit en particulier l'activité du disque. La capacité du disque est l'une des mises à niveau matérielles nécessaires les plus courantes.



L'analyse proactive des performances matérielles (processeur, mémoire, disque ou réseau) constitue le meilleur moyen d'identifier s'il existe d'éventuels goulots d'étranglement dans l'environnement. Une autre manière de rechercher des problèmes liés au matériel consiste à collecter et examiner le retour des utilisateurs. Vous ne devez pas compter uniquement sur les commentaires des utilisateurs pour identifier les problèmes, mais ces commentaires peuvent vous aider à identifier des problèmes particuliers avec le matériel.

Cependant, puisque Exchange Server 2013 prend entièrement en charge les environnements virtuels, vous pouvez envisager de déployer de nouveaux serveurs Exchange virtuels au lieu de mettre à niveau le matériel sur les serveurs physiques existants. Cette approche fournit un meilleur équilibrage de charge et une meilleure distribution des ressources, ainsi qu'un niveau de redondance plus élevé.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Par exemple, si vous souhaitez héberger plus de boîtes aux lettres, vous n'avez pas besoin de mettre à niveau les ressources matérielles sur le serveur de boîtes aux lettres actuel. Au lieu de cela, vous pouvez déployer un nouveau serveur de boîtes aux lettres, y déplacer quelques boîtes aux lettres puis constituer un DAG. De cette façon, vous montez en charge votre environnement Exchange au lieu de le mettre à l'échelle.

Si vous projetez la virtualisation, envisagez de déployer un matériel qui vous permettra d'augmenter les ressources physiques allouées à l'environnement virtuel quand cela sera nécessaire. Lorsque vous planifiez le déploiement d'un serveur Exchange physique, pensez à utiliser des serveurs lames pour la montée en charge, car ils ont la même architecture et offrent une surveillance et une gestion uniformisées.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Leçon 3
Résolution des problèmes liés à Exchange Server 2013

Même dans une organisation dans laquelle Exchange Server 2013 est correctement géré, des problèmes peuvent survenir. Vous devez alors les identifier et les corriger. Il existe des instructions de résolution des problèmes générales. Cependant, votre expérience et l'analyse fournissent souvent les meilleurs outils pour détecter la source du problème et résoudre le problème.

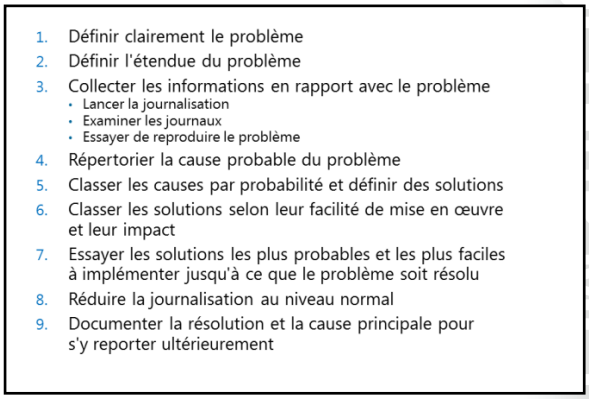
Objectifs de la leçon

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

- développer une méthodologie de résolution des problèmes ;
- résoudre les défaillances de bases de données ;
- résoudre les problèmes de réplication de base de données ;
- résoudre les problèmes de performances ;
- résoudre les problèmes de connectivité ;
- décrire les outils de résolution des problèmes ;
- décrire comment résoudre les problèmes des serveurs de boîtes aux lettres ;
- décrire comment résoudre les problèmes des serveurs d'accès au client ;
- décrire comment résoudre les problèmes des composants de transport.

Développement d'une méthodologie de résolution des problèmes

Pour résoudre efficacement les problèmes, vous devez les identifier et les diagnostiquer, puis choisir et réaliser la réparation nécessaire. Il existe de nombreuses méthodes de résolution des problèmes, qui varient en fonction du type de problème rencontré. L'essentiel est d'implémenter un processus de résolution des problèmes reproductible afin de pouvoir les résoudre rapidement. Une méthode de résolution des problèmes courante est la suivante :



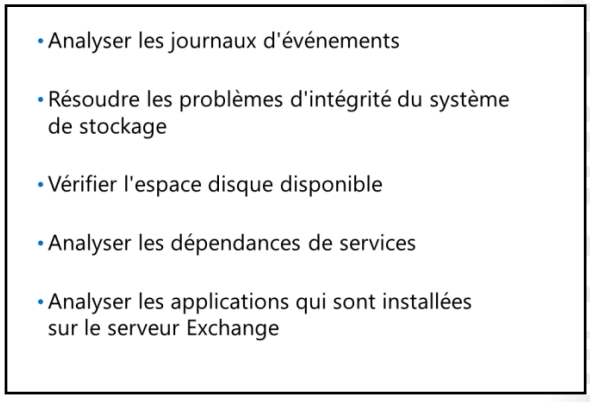
1. Définir clairement le problème. Obtenez une description précise du problème en vérifiant le problème signalé, notamment le moment où vous l'avez remarqué et comment vous pouvez le reproduire. Plus la définition du problème est claire, plus les étapes restantes seront faciles à mettre en œuvre.
2. Définir l'étendue du problème. En définissant l'étendue du problème, vous déterminez en réalité la zone affectée par le problème. Par exemple, l'étendue peut être définie par le nombre d'utilisateurs affectés par un problème spécifique. L'étendue peut concerner un certain nombre de services qui rencontrent des difficultés.

3. Collecter les informations en rapport avec le problème. Lancez la journalisation, examinez les journaux des événements et essayez de reproduire le problème. La plupart du temps, vous aurez une idée plus précise du problème après en avoir terminé la déclaration. Veillez cependant à rassembler le maximum d'informations précises, sans tirer de conclusions et sans prendre de décisions hâtives concernant la nature du problème.
4. Répertorier la cause probable du problème. La déclaration du problème et les données collectées vous permettent d'énumérer toutes les causes potentielles du problème. Cette étape nécessite une réflexion approfondie afin de penser à tous les composants liés au problème. Il est important d'être exhaustif et d'explorer toutes les options possibles. Effectuez des recherches dans la base de connaissances de votre entreprise, dans la documentation du produit et sur Internet pour trouver des informations sur les causes possibles.
5. Classer les causes possibles par probabilité et définir les solutions. Créez une liste de solutions ou de résolutions des problèmes supplémentaires nécessaires pour répondre à chaque cause potentielle. Effectuez des recherches dans votre base de connaissances, documentation du produit et sur Internet pour trouver des informations sur les résolutions possibles.
6. Classez les solutions selon leur facilité de mise en œuvre et leur impact. Vous devez essayer en premier les solutions les plus probables, l'une après l'autre, jusqu'à ce que vous trouviez la solution. Toutefois, dans certains cas, les solutions sont lourdes et nécessitent de longues interruptions ou une grande quantité de ressources. Dans ce cas, vous pouvez commencer par essayer des solutions moins probables mais moins lourdes à mettre en œuvre.
7. Essayer en premier les solutions les plus probables et les plus faciles à implémenter. Étudiez la liste des solutions, l'une après l'autre, jusqu'à ce que le problème soit résolu ou rassemblez des informations supplémentaires qui modifient la définition du problème.
8. Réduire la journalisation au niveau normal. Pour réduire les charges du serveur, réinitialisez tous les paramètres au niveau normal.
9. Documenter la résolution et la cause principale pour s'y reporter ultérieurement. Même si vous êtes susceptible de vous souvenir ultérieurement des détails de la solution, documenter la cause principale et la résolution permet de réduire le temps de résolution si le problème se présente à nouveau.

   Question : pourquoi est-il est important d'appliquer une méthodologie de résolution des problèmes ?

Résolution des problèmes liés aux défaillances de bases de données

La disponibilité et l'intégrité des bases de données sont capitales pour le bon fonctionnement d'Exchange Server, parce que toutes les boîtes aux lettres et les données sont stockées dans les bases de données de boîtes aux lettres. Les administrateurs doivent respecter les instructions et les meilleures pratiques pour la création, la configuration, la gestion et la maintenance des bases de données de boîtes aux lettres.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

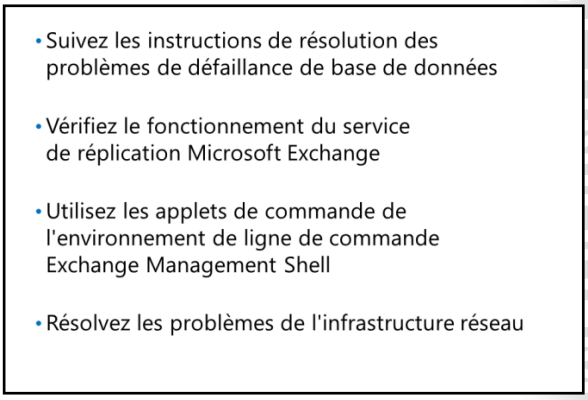
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Si une défaillance de base de données de boîtes aux lettres se produit, appliquez la méthodologie de résolution des problèmes précédemment décrite et incorporez-y les indications suivantes :

- analyser les journaux d'événements. Si votre organisation n'utilise pas de solution de surveillance telle que System Center 2012, vous devez analyser les journaux d'événements pour trouver tous les messages d'erreur qui vous guideront dans les étapes suivantes du processus de résolution des problèmes ;
- résoudre les problèmes d'intégrité du système de stockage. Les bases de données peuvent être corrompues dans un scénario dans lequel le système de stockage présente des problèmes ou des erreurs internes. En général, les systèmes de stockage ont leurs propres logiciel de diagnostic capables de détecter tous les problèmes. Si vous localisez un problème dans le système de stockage, remplacez-le, récupérez les bases de données à partir d'une sauvegarde, ou réamorcez la base de données si elle est configurée dans un DAG. Dans une configuration DAG, n'activez pas la base de données tant que vous n'avez pas testé le système de stockage pendant une durée suffisante, comme une semaine ;
- vérifier l'espace disque disponible. Si le disque logique où se trouvent vos bases de données est saturé, la base de données sera démontée automatiquement et les utilisateurs ne pourront pas se connecter à leurs boîtes aux lettres. S'il n'y a plus d'espace libre sur le disque, étendez le disque logique ou déplacez la base de données sur un autre disque logique comportant davantage d'espace libre ;
- analyser les dépendances de services. Les bases de données de boîtes aux lettres sont gérées par le service Banque d'informations de Microsoft Exchange, qui dépend également d'autres services tels que la topologie Active Directory de Microsoft Exchange. Si les services dont dépend la base de données de boîtes aux lettres sont défaillants, vous devez étudier ces défaillances et tenter de rétablir leur fonctionnement ;
- analyser les applications qui sont installées sur le serveur Exchange. Certaines organisations déploient des applications métier tierces qui communiquent avec leurs serveurs Exchange. Si ces applications ne sont pas installées conformément aux indications du fournisseur, les logiciels peuvent provoquer la défaillance de la base de données. De plus, les antivirus qui ne sont pas conçus pour Exchange Server sont susceptibles d'endommager la base de données, ce qui aura également comme conséquence la défaillance de cette dernière. Assurez-vous qu'aucune application non recommandée par Microsoft ou qui n'est pas installée conformément aux indications du fournisseur ne peut accéder à Exchange Server.

Résolution des problèmes de réplication de base de données

Les organisations qui ont déployé des DAG doivent surveiller et gérer avec soin leurs composants et services. La surveillance de la réplication vous permet de conserver des bases de données intègres et redondantes sur plusieurs membres d'un groupe DAG.



Si une réplication de base de données échoue, appliquez la méthodologie de résolution des problèmes précédemment décrite et incorporez-y les indications suivantes :

- suivez les instructions de résolution des problèmes de défaillance de base de données. Consultez les instructions relatives à l'intégrité des bases de données individuelles susceptibles d'influer sur l'intégrité de la réplication. Par exemple, si l'espace libre sur le disque est essentiel pour les membres d'un groupe DAG, la réplication ne pourra pas se poursuivre ;
- vérifiez le fonctionnement du service de réplication Microsoft Exchange. La réplication de la base de données pour les membres d'un groupe DAG dépend de l'intégrité du service de réplication Microsoft Exchange. Vérifiez si le service est sain sur tous les membres DAG. Vérifiez également toutes les dépendances de ce service, telles que le service de topologie Active Directory de Microsoft Exchange ;
- utilisez les applets de commande de l'environnement de ligne de commande Exchange Management Shell. Vous pouvez utiliser différentes applets de commande de test pour résoudre les problèmes de réplication ;
- vous pouvez utiliser l'applet de commande **Test-ReplicationHealth** pour dépanner la réplication de la base de données et pour examiner l'état d'un membre de groupe DAG. Par exemple, prenez l'applet de commande suivante pour dépanner la réplication de la base de données sur LON-MBX1 :

```
Test-ReplicationHealth -Identity LON-MBX1
```

- vous pouvez utiliser les applets de commande **Get-MailboxDatabaseCopyStatus** pour analyser l'intégrité et les informations d'état concernant les copies de base de données de boîtes aux lettres dans un DAG. Par exemple, prenez l'applet de commande suivante pour dépanner la réplication de la base de données sur la base de données ExecutivesDB :

```
Get-MailboxDatabaseCopyStatus -Identity ExecutivesDB | Format-List
```

- vous pouvez utiliser le script **CollectOverMetrics.ps1** qui rassemble des mesures en temps réel pendant son exécution. Le script **CollectReplicationMetrics.ps1** rassemble les données des compteurs de performance et génère un rapport sur différentes données statistiques. Par exemple, utilisez le script suivant pour dépanner la réplication de la base de données sur la base de données « ExecutivesDB » :

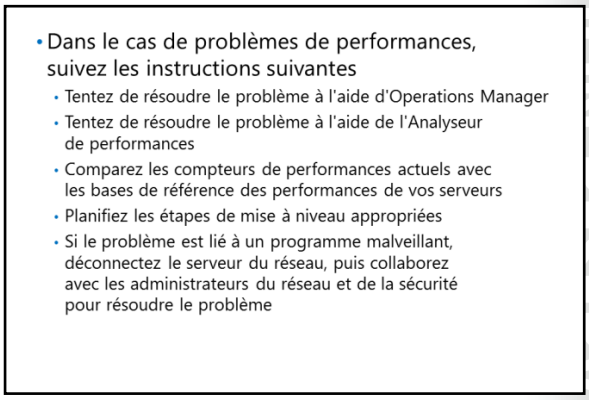
```
CollectOverMetrics.ps1 -DatabaseAvailabilityGroup DAG1 -Database:"ExecutivesDB" -
GenerateHTMLReport –ShowHTMLReport
```

- résolvez les problèmes de l'infrastructure réseau. Si l'infrastructure réseau que les membres DAG utilisent pour la réplication est déconnectée ou présente des problèmes de connectivité ou de latence, ces difficultés affecteront la réplication de la base de données. Vous devez vérifier que l'infrastructure réseau fonctionne correctement, ou dans le cadre de certains scénarios, fournit les chemins d'accès réseau redondants pour la réplication de la base de données ;

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Résolution des problèmes de performances

Les problèmes de performances peuvent affecter les utilisateurs et les organisations dans un environnement de production Exchange Server. Par conséquent, vous devez effectuer une analyse détaillée et diagnostiquer les raisons de ces problèmes de performances. Les problèmes de performances peuvent découler de circonstances diverses, notamment :



- l'augmentation du nombre de boîtes aux lettres en raison de l'embauche de nouveaux employés ;
- l'installation d'un nouveau logiciel, tel qu'un logiciel de sauvegarde, d'un logiciel connecté à Exchange Server qui n'est pas configuré conformément aux recommandations de sa documentation ;
- l'installation d'une nouvelle mise à jour qui n'est pas configurée conformément aux recommandations de sa documentation, ou un processus de mise à jour qui n'a pas été exécuté selon la méthode conseillée ;
- un problème de sécurité, un programme malveillant, ou une attaque de réseau.

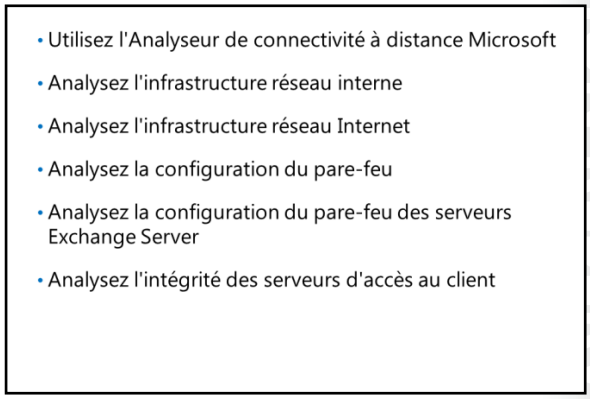
Si des problèmes de performances apparaissent, appliquez la méthodologie de résolution des problèmes discutée précédemment, et incorporez-y les indications suivantes :

- Operations Manager. Si vous utilisez Operations Manager, examinez les événements signalés et utilisez ses fonctions de diagnostic et de résolution.
- Analyseur de performances. Si vous utilisez l'Analyseur de performances dans Windows Server 2012, examinez les compteurs de performance appropriés, puis ajoutez des compteurs supplémentaires si nécessaire afin d'obtenir autant d'informations que possible relativement aux performances du serveur.
- Compteurs de performance. Comparez les compteurs de performances actuels avec les bases de référence des performances de vos serveurs. Suivez ensuite les instructions d'utilisation des bases de référence des performances qui ont été présentées précédemment dans ce module.
- Problèmes de mise à jour de logiciel. Si le problème de performance est lié à une mise à niveau d'un logiciel, planifiez les étapes de mise à niveau appropriées. Déterminez dans quelle mesure votre matériel prend en charge des composants supplémentaires. Vous aurez peut-être besoin d'un nouveau serveur et vous devrez peut-être faire migrer Exchange Server sur celui-ci.
- Problèmes causés par des programmes malveillants. Si le problème de performance est lié à un programme malveillant, déconnectez le serveur du réseau, puis collaborez avec les administrateurs du réseau et de la sécurité pour résoudre le problème. Réalisez une analyse détaillée des paramètres de sécurité et de la protection contre les programmes malveillants sur toute votre infrastructure informatique, et pas simplement sur vos serveurs Exchange.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Résolution des problèmes de connectivité

Exchange Server 2013 repose sur des connexions réseau rapides et fiables avec les contrôleurs de domaine, parce que la majeure partie des données de configuration d'Exchange Server est stockée sur ceux-ci. Les connexions clientes dépendent également d'une connectivité réseau stable avec les serveurs d'accès au client pour fournir aux utilisateurs un environnement de messagerie productif qui leur permette d'accomplir leurs tâches.

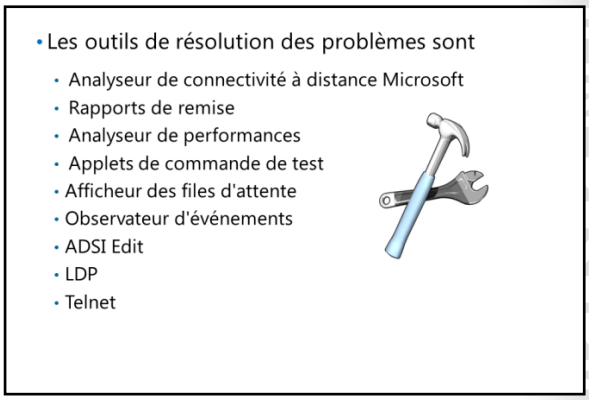


Si des problèmes de connectivité apparaissent, suivez la méthodologie de résolution des problèmes discutée précédemment en y incorporant les indications suivantes :

- Utilisez l'Analyseur de connectivité à distance Microsoft. L'Analyseur de connectivité à distance Microsoft est un outil Web qui simule des connexions clientes externes à votre infrastructure Exchange Server. L'outil Analyseur de connectivité à distance se trouve sur le site http://go.microsoft.com/fwlink/?LinkId=290683.
- Utilisez l'outil Analyseur de connectivité Microsoft. L'Analyseur de connectivité Microsoft est un programme client qui simule des connexions clientes internes à votre infrastructure Exchange Server. Vous pouvez télécharger l'Analyseur de connectivité à partir du site http://go.microsoft.com/fwlink/?LinkId=290683.
- Analysez l'infrastructure réseau interne. Collaborez avec vos administrateurs réseau pour identifier les problèmes susceptibles d'être causés par :
    - des défaillances d'équipement réseau internes ;
    - les équipements de communication réseau Internet ;
    - les dispositifs de pare-feu.
- Analysez la configuration du pare-feu des serveurs Exchange Server. Chaque serveur Exchange dispose de ses propres réglages du Pare-feu Windows avec fonctions avancées de sécurité du système d'exploitation Windows Server 2012. Vérifiez que les ports utilisés par Exchange Server 2013 sont ouverts dans le Pare-feu Windows avec fonctions avancées de sécurité.
- Analysez l'intégrité des serveurs d'accès au client. Chaque fois que des utilisateurs signalent des problèmes de connectivité, vérifiez l'intégrité et la connectivité du serveur d'accès au client. Lorsque vous utilisez la technologie d'équilibrage de la charge réseau, s'il existe un problème avec un serveur d'accès au client particulier, ses communications basculeront vers un autre membre du tableau d'accès au client.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Outils de résolution des problèmes



Au fil du temps, de nombreux outils de résolution de problèmes d'Exchange Server ont été introduits. Chaque outil doit être utilisé de façon spécifique, mais ils nécessitent tous une connaissance détaillée du produit et des informations relatives à votre environnement pour déterminer des solutions possibles. Deux de ces principaux outils sont :

- *L'Analyseur de connectivité à distance Microsoft*. L'Analyseur de connectivité à distance Microsoft est un outil Web qui simule des connexions clientes externes à votre infrastructure Exchange Server. Cet outil réalise plusieurs tests et résout les problèmes potentiels de connectivité. L'outil Analyseur de connectivité à distance Microsoft se trouve sur le site http://go.microsoft.com/fwlink/?LinkId=290683.
- *L'Analyseur de connectivité Microsoft*. L'Analyseur de connectivité Microsoft est un programme client qui simule des connexions clientes internes à votre infrastructure Exchange Server. Vous pouvez télécharger l'Analyseur de connectivité à partir du site http://go.microsoft.com/fwlink/?LinkId=290683.
- *Les rapports de remise*. Les rapports de remise sont un outil de suivi de message dans le Centre d'administration Exchange (CAE), utiles pour résoudre les problèmes de remise de messages électroniques jusqu'à 14 jours après qu'ils ont été envoyés ou reçus.

D'autres outils, comme l'Analyseur de fiabilité et de performances, vérifient l'intégrité des processus du serveur Exchange. Vous pouvez utiliser l'Afficheur des files d'attente pour afficher l'état du message dans les files d'attente du transport. Les outils comme le moniteur réseau et Telnet peuvent vous aider à résoudre des problèmes de réseau et de suivi des messages, et la visionneuse du journal de routage peut vous aider à résoudre des problèmes de remise de messages.

En complément à la Console de gestion Exchange, l'environnement de ligne de commande Exchange Management Shell et Utilisateurs et ordinateurs Active Directory, il existe de nombreux autres outils pour gérer et résoudre les problèmes d'une organisation Exchange Server 2013. Un certain nombre de ces outils sont décrits dans le tableau suivant.

Nom de l'outil	Description
ADSI Edit (adsiedit.msc)	Utilisez cet outil pour effectuer des modifications de bas niveau des objets et des attributs Active Directory. Sous Windows Server 2012, il est installé avec les outils d'administration de serveur distant.
Observateur d'événements (eventvwr.msc)	Ce composant logiciel enfichable MMC est utilisé pour afficher les événements enregistrés tels que les erreurs et les avertissements.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

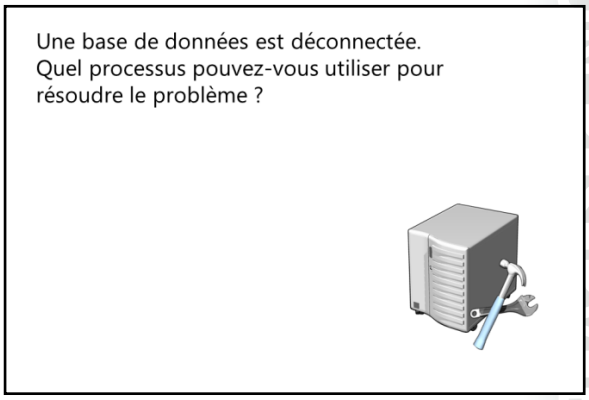
Nom de l'outil	Description
Analyseur de performances	Utilisez cet outil pour surveiller les performances des composants matériels, du système d'exploitation et des applications.
Gestionnaire des tâches	Utilisez cet outil pour examiner les services en cours d'exécution et la quantité de ressources qu'ils utilisent.
Utilitaires de base de données de serveur Exchange (Eseutil.exe)	Utilisez cet outil pour effectuer des procédures de base de données hors connexion, comme la défragmentation et la récupération.
New-MailboxRepairRequest	Utilisez cet outil pour rechercher et éliminer les erreurs dans les bases de données de boîte aux lettres et les bases de données de dossiers publics. Vous pouvez également exécuter les applets de commande **New-MailboxRepairRequest** sur les boîtes aux lettres.
LDP (ldp.exe)	Utilisez cet outil pour exécuter des opérations telles que : connexion, liaison, recherche, modification, ajout et suppression sur les services de domaine Active Directory (AD DS).
Interface graphique utilisateur Microsoft Baseline Security Analyzer (MBSA) : MBSA.exe Ligne de commande : mbsacli.exe	Utilisez cet outil pour déterminer l'état de sécurité des serveurs de l'organisation selon les recommandations de sécurité Microsoft. Il offre également une aide à la mise à jour spécifique.
Service de rapports d'erreurs Microsoft	Exchange Server 2013 utilise cet outil pour collecter des informations sur les vidages sur incident et des informations de débogage. Il permet aux administrateurs de suivre et de résoudre des erreurs associées au système d'exploitation Windows, aux composants Windows et aux applications, comme Exchange Server 2013. Ce service permet aux administrateurs et aux utilisateurs d'envoyer à Microsoft des données relatives aux erreurs et de recevoir des informations sur celles-ci. Les administrateurs peuvent utiliser le service de rapports d'erreurs Microsoft pour traiter les problèmes des clients en temps voulu et pour contribuer à l'amélioration de la qualité des produits Microsoft.
Process Monitor (procmon.exe)	Utilisez cet outil pour analyser un système de fichiers, un registre et une activité de processus/thread en temps réel.
Test-Outlook Connectivity	Utilisez cette applet de commande outil pour confirmer la connectivité Outlook Anywhere entre l'ordinateur qui exécute le serveur Exchange et les stations de travail clientes Outlook du réseau.
Telnet (telnet.exe)	Utilisez cet outil pour résoudre les problèmes de flux de messagerie Exchange Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Discussion : Résolution des problèmes liés aux serveurs de boîtes aux lettres

Lorsque vous résolvez des problèmes de serveurs de boîtes aux lettres, vous devez en premier lieu vérifier l'intégrité et la disponibilité des bases de données. Utilisez des outils tels que la Résolution des problèmes de bases de données et l'Observateur d'événements pour identifier le problème et tenter de le résoudre.

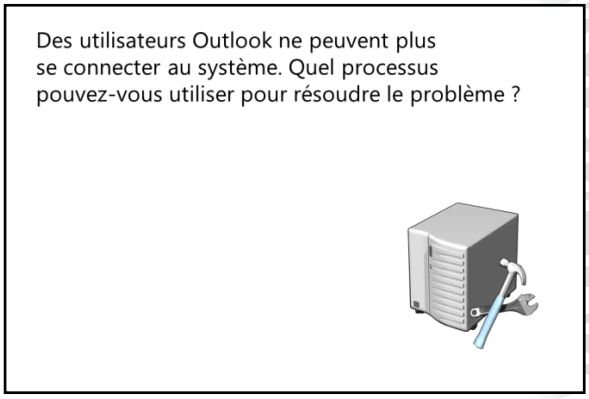
Question : une base de données est déconnectée. Quel processus pouvez-vous utiliser pour résoudre le problème ?



Discussion : Résolution des problèmes liés aux serveurs d'accès au client

Vous pouvez appliquer des techniques de résolution des problèmes standards aux problèmes spécifiques qui peuvent survenir avec les serveurs d'accès au client. Utilisez les outils tels que l'Analyseur de connectivité à distance et l'Observateur d'événements pour identifier le problème et élaborer une solution.

Question : des utilisateurs Outlook ne peuvent plus se connecter au système. Quel processus pouvez-vous utiliser pour résoudre le problème ?



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Discussion : Résolution des problèmes des composants de transport

Les problèmes liés au serveur de transport sont généralement causés par l'altération de la base de données de file d'attente du courrier ou à des problèmes de connectivité réseau. Utilisez les outils tels que l'Analyseur de connectivité à distance Microsoft, les rapports de remise et l'afficheur de files d'attente, puis élaborez une solution.

Question : des utilisateurs signalent des messages électroniques sortants non remis et des remises de messages lentes. Quel processus pouvez-vous utiliser pour résoudre le problème ?



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Atelier pratique : Analyse et résolution des problèmes d'Exchange Server 2013

Scénario

Vous êtes l'administrateur de messagerie de A. Datum Corporation. Vous devez configurer l'analyse de base en utilisant l'Analyseur de performances. Vous devez également résoudre les problèmes de la base de données de boîtes aux lettres et les problèmes liés au serveur d'accès au client.

Objectifs

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

1. analyser Exchange Server ;
2. résoudre les problèmes liés à la disponibilité des bases de données ;
3. résoudre les problèmes liés aux serveurs d'accès au client.

Configuration de l'atelier pratique

Durée approximative : **60 minutes**

Ordinateurs virtuels	22341B-LON-DC1 22341B-LON-CAS1 22341B-LON-MBX1
Nom d'utilisateur	ADATUM\Administrateur
Mot de passe	Pa$$w0rd

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de débuter cet atelier pratique, vous devez effectuer les opérations suivantes :

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22341B-LON-DC1**, puis dans le volet Actions, cliquez sur **Démarrer**.
3. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous avec les informations d'identification suivantes :
   a. Nom d'utilisateur : **ADATUM\Administrateur**
   b. Mot de passe : **Pa$$w0rd**
5. Répétez les étapes 2 à 4 pour **22341B-LON-MBX1** et **22341B-LON-CAS1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 1 : Analyse d'Exchange Server

Scénario

Vous êtes l'administrateur de messagerie de A. Datum Corporation. Vous devez configurer l'analyse de base en utilisant l'Analyseur de performances Windows. Avant d'implémenter Microsoft System Center Operations Manager pour analyser vos ordinateurs Exchange Server 2013, vous devez créer un ensemble de collecteurs de données pour analyser les composants de performance clés qui s'exécutent sur votre serveur de boîtes aux lettres.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un ensemble de collecteurs de données nommé Analyse Exchange.
2. Créer un ensemble de collecteurs de données de compteur de performances pour analyser les performances de base du serveur Exchange.
3. Créer un ensemble de collecteurs de données de compteur de performances pour analyser les performances du rôle serveur de boîtes aux lettres.
4. Vérifier que l'ensemble de collecteurs de données fonctionne correctement.

▶ Tâche 1 : Créer un ensemble de collecteurs de données nommé Analyse Exchange

- Sur LON-MBX1, dans le Gestionnaire de serveur, ouvrez l'Analyseur de performances, puis créez un ensemble de collecteurs de données nommé **Analyse Exchange**. Configurez l'ensemble de collecteurs de données de manière à y inclure les journaux de données du compteur de performances.

▶ Tâche 2 : Créer un ensemble de collecteurs de données de compteur de performances pour analyser les performances de base du serveur Exchange

1. Ajoutez un nouveau collecteur de données à l'ensemble de collecteurs de données Analyse Exchange nommé **Analyse Exchange de base**.
2. Ajoutez les compteurs de performances du tableau suivant pour analyser la performance de base du serveur Exchange sur LON-MBX1. Configurez l'intervalle d'échantillonnage sur 1 minute.

Objet	Compteur
Processeur	% temps processeur % temps utilisateur % temps privilégié
Contrôleurs de domaine MSExchange ADAccess	Durée de lecture LDAP Durée de recherche LDAP Délai de recherche LDAP dépassé par minute Opérations LDAP longues/min

(suite)

Objet	Compteur
Mémoire	Mégaoctets disponibles Lectures de pages/s Pages en entrée/s Pages/s Pages en sortie/s Octets de réserve paginée Pages de transition avec nouvel objet/s
System	Longueur de la file du processeur

▶ Tâche 3 : Créer un ensemble de collecteurs de données de compteur de performances pour analyser les performances du rôle serveur de boîtes aux lettres

1. Ajoutez un nouveau collecteur de données à l'ensemble de collecteurs de données Analyse Exchange nommé **Analyse de rôle serveur de boîte aux lettres**.
2. Ajoutez les compteurs de performances suivants pour analyser la performance de base du serveur Exchange 2013 sur LON-MBX1. Configurez l'intervalle d'échantillonnage sur 1 minute.

Objet	Compteur
Disque logique	Moyenne disque s/lecture Moyenne disque s/transfert Moyenne disque s/écriture
Banque d'informations MSExchangeIS	RPC Average Latency RPC Operations/sec Demandes RPC Messages remis/s

▶ Tâche 4 : Vérifier que l'ensemble de collecteurs de données fonctionne correctement

1. Lancez l'ensemble de collecteurs de données **Analyse Exchange** et exécutez-le pendant cinq minutes.
2. Arrêtez l'ensemble de collecteurs de données **Analyse Exchange**, puis examinez le rapport le plus récent.
3. Fermez l'Analyseur de performances.

Résultats : À la fin de cet exercice, vous aurez créé un ensemble de collecteurs de données pour l'analyse de LON-MBX1 en utilisant les compteurs de performances recommandés.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Résolution des problèmes liés à la disponibilité des bases de données

Scénario

Vous êtes l'administrateur de messagerie de la société A. Datum Corporation. Après avoir récupéré d'une défaillance matérielle, votre logiciel d'analyse indique que l'une des bases de données de boîtes aux lettres n'est pas montée. Vous devez résoudre et réparer le problème de la base de données.

Les tâches principales de cet exercice sont les suivantes :

1. Identifier l'étendue du problème.
2. Examiner les journaux des événements.
3. Répertorier les causes probables du problème et classer les solutions possibles, si plusieurs options existent.
4. Vérifier la configuration de la base de données.
5. Reconfigurer et monter la base de données.

▶ Tâche 1 : Identifier l'étendue du problème

Avant de commencer cet exercice, procédez comme suit :

1. Sur LON-MBX1, ouvrez Exchange Management Shell. À l'invite, tapez **c:\scripts\Lab11Prep1.ps1**, puis appuyez sur Entrée. Ce script simulera une défaillance de base de données.
2. Sur LON-MBX1, ouvrez le Centre d'administration Exchange à l'aide du lien **https://lon-cas1.adatum.com/ecp**, et dans la zone **Nom d'utilisateur**, tapez **ADATUM\Administrateur**, et dans la zone **Mot de passe**, tapez **Pa$$w0rd**.
3. Identifiez les bases de données de boîtes aux lettres qui ne sont pas montées sur LON-MBX1, le cas échéant. Vérifiez que la base de données **MailboxDB100** est démontée.
4. Essayez de monter la base de données et vérifiez que deux fenêtres **avertissement** apparaissent ; la deuxième affiche un message indiquant qu'au moins une base de données est manquante. Dans cette fenêtre **avertissement**, cliquez sur le bouton **annuler** pour annuler le montage.

▶ Tâche 2 : Examiner les journaux des événements

- Ouvrez **l'Observateur d'événements**. Dans le journal des applications et le journal système, examinez les événements générés et prenez note de toutes les erreurs.

▶ Tâche 3 : Répertorier les causes probables du problème et classer les solutions possibles, si plusieurs options existent

- Répertoriez les problèmes et les solutions possibles :

Problème	Solution suggérée

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Vérifier la configuration de la base de données

1. Sur LON-MBX1, ouvrez le **Centre d'administration Exchange**, puis examinez la configuration de base de données.
2. Ouvrez une fenêtre **Explorateur de fichiers**, puis localisez les fichiers de bases de données.

▶ Tâche 5 : Reconfigurer et monter la base de données

1. Sur LON-MBX1, dans Exchange Management Shell, reconfigurez la base de données MailboxDB100 en exécutant l'applet de commande suivante :

```
Move-DatabasePath MailboxDB100 –LogFolderPath "C:\Program Files\Microsoft\Exchange
Server\V15\Mailbox\MailboxDB100" –EdbFilePath "C:\Program Files\Microsoft\Exchange
Server\V15\Mailbox\MailboxDB100\MailboxDB100.edb" –ConfigurationOnly –force
```

2. Montez la base de données en exécutant l'applet de commande suivante :

```
Mount-Database MailboxDB100
```

3. Dans le CAE, vérifiez que l'état de la base de données **MailboxDB100** est **Monté**.

Résultats : À la fin de cet exercice, vous aurez utilisé une technique de résolution des problèmes pour identifier et résoudre un problème de serveur de boîtes aux lettres.

Exercice 3 : Résolution des problèmes liés aux serveurs d'accès au client

Scénario

Vous êtes l'administrateur de messagerie de la société A. Datum Corporation. Des utilisateurs signalent qu'ils ne peuvent pas se connecter à Outlook Web App. Vous devez déterminer puis réparer le problème.

Les tâches principales de cet exercice sont les suivantes :

1. Utiliser les applets de commande Test pour vérifier l'intégrité du serveur.
2. Répertorier les causes probables du problème et classer les solutions possibles si plusieurs options existent.
3. Vérifier la configuration d'Outlook Web App.
4. Vérifier que vous avez résolu le problème.

▶ Tâche 1 : Utiliser les applets de commande Test pour vérifier l'intégrité du serveur

Avant de commencer cet exercice, procédez comme suit :

1. Sur LON-MBX1, dans Exchange Management Shell, tapez **c:\scripts\Lab11Prep2.ps1** et appuyez sur Entrée.
2. Fermez l'environnement de ligne de commande Exchange Management Shell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Sur LON-MBX1, ouvrez l'environnement de ligne de commande **Exchange Management Shell** et exécutez l'applet de commande **Test-ServiceHealth**.
4. Vérifiez que le résultat ne renvoie aucune erreur.
5. Exécutez l'applet de commande **Test-OwaConnectivity –URL https://LON-MBX1.Adatum.com/OWA -TrustAnySSLCertificate** pour tester la connectivité d'Outlook Web App.
6. Notez les erreurs d'authentification.

▶ Tâche 2 : Répertorier les causes probables du problème et classer les solutions possibles si plusieurs options existent

- Répertoriez les problèmes et les solutions possibles :

Problème	Solution suggérée

▶ Tâche 3 : Vérifier la configuration d'Outlook Web App

1. Sur LON-MBX1, vérifiez que vous ne pouvez pas vous connecter au CAE.
2. À partir de Exchange Management Shell, affichez les méthodes de vérification pour le répertoire virtuel **owa**, et vérifiez que toutes les méthodes sont définies sur **False**.
3. À partir de l'environnement de ligne de commande Exchange Management Shell, configurez la méthode de vérification pour le répertoire virtuel **owa**, de sorte qu'elle soit définie sur **FormsAuthentication**.
4. À partir de l'environnement de ligne de commande Exchange Management Shell, exécutez la commande **IISReset**.
5. Vérifiez que vous pouvez lancer le **Centre d'administration Exchange**.

▶ Tâche 4 : Vérifier que vous avez résolu le problème

1. Essayez de vous connecter à **https://LON-CAS1.adatum.com/owa** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Confirmez qu'Administrateur peut maintenant accéder à l'application Outlook Web App, puis fermez Internet Explorer.

Résultats : À la fin de cet exercice, vous aurez utilisé une technique de résolution des problèmes pour identifier et résoudre un problème de serveur d'accès au client.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Contrôle des acquis et éléments à retenir

Méthode conseillée

Complétez ou adaptez les meilleures pratiques suivantes à vos propres conditions de travail :

- Suivez les mêmes étapes chaque fois que vous résolvez un problème. Vous prendrez ensuite l'habitude de prendre des décisions informées et vous trouverez les réponses rapidement.
- Ayez soin de distinguer les faits relatifs au problème de toute autre information de nature subjective. L'opinion subjective d'une seule personne pourrait vous amener à vous concentrer sur un problème secondaire et retarder la résolution du problème réel.
- Posez-vous beaucoup de questions sur le problème avant de commencer à tenter de le résoudre. Si vous n'avez pas correctement défini le problème, vous ne pouvez pas cibler correctement les étapes de la résolution.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Une entreprise connait une croissance récente, depuis le lancement d'un nouveau produit. Le serveur de messagerie de l'entreprise rencontre de nombreuses interruptions et des arrêts fréquents en raison de modifications non documentées. Dans quel domaine l'entreprise doit-elle investir pour préserver une croissance continue ?	
Une base de données est déconnectée et l'organisation doit résoudre le problème. Les boîtes aux lettres de plusieurs utilisateurs impatients sont stockées dans la base de données déconnectée. Quel est le meilleur moyen de répondre à cette situation ?	
Un service pack Exchange Server a été récemment publié et l'entreprise a décidé de le déployer. Que devez-vous faire avant de planifier le déploiement ?	

Questions de contrôle des acquis

Question : Après avoir examiné les informations relatives à la tendance que vous avez récupérées grâce au système d'analyse, vous remarquez que l'utilisation du processeur de l'un des quatre serveurs de boîtes aux lettres est plus élevée que la moyenne. Que devez-vous faire ?

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Problèmes réels et scénarios

Votre organisation a déployé Exchange Server 2013, avec deux serveurs d'accès au client et deux serveurs de boîtes aux lettres. La haute disponibilité n'est pas configurée. Après plusieurs mois, de nombreux utilisateurs se plaignent de la lenteur de réponse. Votre tâche consiste à résoudre ce problème. Comment procéderez-vous ?

Tout d'abord, vous devez déterminer si ce problème concerne tous les utilisateurs ou seulement quelques-uns. Commencez par utiliser l'Analyseur de connectivité à distance pour résoudre les problèmes de connectivité des utilisateurs. Vous pouvez également analyser les informations de l'Analyseur de performances pour vérifier si ce comportement est lié à un problème de performances. Si vous utilisez System Center Operations Manager, vous pourrez corriger l'expérience utilisateur avec les fonctions d'analyse de bout en bout du produit.

En complément, vous pouvez déployer la haute disponibilité pour les rôles serveur d'accès au client et de boîtes aux lettres. Dans ce scénario, la nouvelle fonction de disponibilité gérée de Exchange Server 2013 entamera une démarche en plusieurs étapes pour améliorer l'expérience de l'utilisateur. Par exemple, si la réponse lente est causée par des problèmes du protocole HTTPS entre le serveur d'accès au client et le serveur de boîtes aux lettres, la fonction de disponibilité gérée d'Exchange exécutera un basculement de base de données vers un autre membre DAG. Une fois le processus de basculement terminé, le serveur d'accès au client sera connecté à un autre serveur de boîtes aux lettres qui ne rencontre pas de problèmes de protocole HTTPS.

Outils

Nom de l'outil	Description
Analyseur de connectivité à distance Microsoft	Utilisez cet outil Web pour simuler des connexions clientes externes vers l'infrastructure Exchange Server. Se trouve à l'adresse http://go.microsoft.com/fwlink/?LinkId=290683.
Outil Analyseur de connectivité à distance Microsoft	Utilisez ce programme client pour simuler des connexions clientes internes vers l'infrastructure d'Exchange Server. Se trouve à l'adresse http://go.microsoft.com/fwlink/?LinkId=290683.
ADSI Edit (adsiedit.msc)	Utilisez cet outil pour effectuer des modifications de bas niveau des objets et des attributs Active Directory. Sous Windows Server 2012, il est installé avec les outils d'administration de serveur distant.
Observateur d'événements (eventvwr.msc)	Ce composant logiciel enfichable MMC est utilisé pour afficher les événements enregistrés tels que les erreurs et les avertissements.
Analyseur de performances	Utilisez cet outil pour surveiller les performances des composants matériels, du système d'exploitation et des applications.
Gestionnaire des tâches	Utilisez cet outil pour examiner les services en cours d'exécution et la quantité de ressources qu'ils utilisent.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

(suite)

Nom de l'outil	Description
Utilitaires de base de données de serveur Exchange (Eseutil.exe)	Utilisez cet outil pour effectuer des procédures de base de données hors connexion, comme la défragmentation et la récupération.
New-MailboxRepairRequest	Utilisez cet outil pour rechercher et éliminer les erreurs dans les bases de données de boîte aux lettres et les bases de données de dossiers publics. Vous pouvez également exécuter la commande **New-MailboxRepairRequest** sur les boîtes aux lettres.
LDP (ldp.exe)	Utilisez cet outil pour exécuter des opérations telles que : connexion, liaison, recherche, modification, ajout et suppression sur AD DS.
Interface graphique utilisateur Microsoft Baseline Security Analyzer (MBSA) : MBSA.exe Ligne de commande : mbsacli.exe	Utilisez cet outil pour déterminer l'état de sécurité des serveurs de l'organisation selon les recommandations de sécurité Microsoft. Utilisez-le également pour obtenir une aide à la mise à jour spécifique.
Service de rapports d'erreurs Microsoft	Utilisez cet outil dans Exchange Server 2013 pour collecter des informations sur les vidages sur incident et des informations de débogage. Cet outil permet aux administrateurs de suivre et de résoudre des erreurs associées au système d'exploitation Windows, aux composants Windows et aux applications, comme Exchange Server 2013. Ce service permet aux administrateurs et aux utilisateurs d'envoyer à Microsoft des données relatives aux erreurs et de recevoir des informations sur celles-ci. Les administrateurs peuvent utiliser le service de rapports d'erreurs Microsoft pour traiter les problèmes des clients en temps voulu et pour contribuer à l'amélioration de la qualité des produits Microsoft.
Process Monitor (procmon.exe)	Utilisez cet outil pour analyser un système de fichiers, un registre et une activité de processus/thread en temps réel.
Test-OutlookConnectivity	Utilisez cette applet de commande outil pour confirmer la connectivité Outlook Anywhere entre l'ordinateur qui exécute le serveur Exchange et les stations de travail clientes Outlook du réseau.
Telnet (telnet.exe)	Utilisez cet outil pour résoudre les problèmes de flux de messagerie Exchange Server.

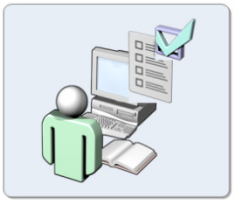
UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Évaluation du cours

Votre évaluation de ce cours aidera Microsoft à comprendre la qualité de votre expérience de formation.

Consultez votre formateur pour accéder au formulaire d'évaluation du cours.

Votre évaluation est strictement confidentielle et vos réponses à cette enquête seront utilisées dans le seul but d'améliorer la qualité des prochains cours Microsoft. Vos commentaires ouverts et honnêtes sont très précieux.



UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 1 : Déploiement et gestion de Microsoft® Exchange Server 2013

Atelier pratique : Déploiement et gestion d'Exchange Server 2013

Exercice 1 : Évaluation de la configuration requise et des conditions préalables pour une installation d'Exchange Server 2013

▶ Tâche 1 : Évaluer la configuration requise pour Active Directory

1. Sur LON-DC1-B, si nécessaire, dans la barre des tâches, cliquez sur **Gestionnaire de serveur**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
3. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de : Adatum.com**, vérifiez que les niveaux fonctionnels du domaine et de la forêt sont compatibles avec la configuration requise pour Exchange Server 2013. (**Remarque :** il doit s'agir au moins de Windows Server 2003.)
5. Cliquez sur **OK**, puis fermez la fenêtre **Utilisateurs et ordinateurs Active Directory**.
6. Cliquez sur l'écran **Accueil**, tapez **modification adsi**, puis appuyez sur Entrée.
7. Cliquez avec le bouton droit sur **Modification ADSI** et cliquez sur **Connexion**.
8. Dans la boîte de dialogue **Paramètres de connexion**, dans la section **Point de connexion**, dans la liste **Sélectionnez un contexte d'attribution de noms connu**, cliquez sur **Configuration**, puis sur **OK**.
9. Dans le volet gauche, développez **Configuration [LON-DC1.adatum.com]**, puis cliquez sur **CN=Configuration,DC=adatum,DC=com**.
10. Développez **CN=Services** et vérifiez que **CN=Microsoft Exchange** n'a pas été créé.
11. Fermez l'**Modification ADSI**.

▶ Tâche 2 : Évaluer la configuration requise pour DNS

1. Sur LON-EX1-B, dans la barre des tâches, cliquez sur **Windows PowerShell**.
2. Dans la fenêtre Windows PowerShell, tapez **IPConfig /all**, puis appuyez sur Entrée. Vérifiez que l'adresse IP du serveur DNS (Domain Name System) pour la connexion au réseau local est **172.16.0.10**.
3. À l'invite de commandes, tapez **Ping LON-DC1.adatum.com**, puis appuyez sur Entrée. Vérifiez que la connectivité réseau avec le contrôleur de domaine est établie.
4. À l'invite de commandes, tapez **Nslookup** et appuyez sur Entrée.
5. À l'invite de commandes, tapez **set type=all** et appuyez sur Entrée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. À l'invite de commandes, tapez **_ldap._tcp.dc._msdcs.adatum.com** et appuyez sur **Entrée**. Vérifiez qu'un enregistrement SRV pour lon-dc1.adatum.com est renvoyé.
7. Fermez Windows PowerShell.

Résultats : Après avoir terminé cet exercice, les stagiaires auront évalué la configuration requise pour les services AD DS.

Exercice 2 : Déploiement d'Exchange Server 2013

▶ Tâche 1 : Préparation d'AD DS pour le déploiement d'Exchange Server 2013

1. Sur LON-DC1-B, dans la fenêtre **Connexion à un ordinateur virtuel**, cliquez sur le menu **Support**, sélectionnez **Lecteur de DVD**, puis cliquez sur **Insérer un disque**.
2. Accédez à **C:\Programmes\Microsoft Learning\22341\Drives\ExchangeServer2013CU1.iso**, puis cliquez sur **Ouvrir**.
3. Dans la barre des tâches, cliquez sur **Windows PowerShell**.
4. Tapez **D:** et appuyez sur **Entrée**.
5. Tapez la commande suivante, puis appuyez sur Entrée :

```
.\Setup.exe /PrepareAD /IAcceptExchangeServerLicenseTerms /OrganizationName:Adatum
```

6. Patientez jusqu'à la fin du processus.
7. Fermez Windows PowerShell.

▶ Tâche 2 : Exécuter l'installation d'Exchange Server 2013 sur un serveur unique

1. Sur LON-EX1-B, dans la fenêtre **Connexion à un ordinateur virtuel**, cliquez sur le menu **Support**, sélectionnez **Lecteur de DVD**, puis cliquez sur **Insérer un disque**.
2. Accédez à **C:\Programmes\Microsoft Learning\22341\Drives\ExchangeServer2013CU1.iso**, puis cliquez sur **Ouvrir**.
3. Sur LON-EX1-B, ouvert la fenêtre **Windows PowerShell** à partir de la barre des tâches.
4. Tapez la commande suivante pour installer les composants Windows d'Exchange Server 2013 :

   Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, puis appuyez sur Entrée. (Si vous ne voulez pas taper cette commande, copiez le contenu du fichier **cmdlet.txt** à partir du lecteur C:\.)
5. Attendez que l'installation des composants Windows se termine.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Fermez la fenêtre **PowerShell**, puis redémarrez le serveur.
7. Ouvrez une session sur LON-EX1-B en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
8. À partir du Bureau, ouvrez l'**Explorateur de fichiers** et accédez au lecteur **D:**.
9. Double-cliquez sur **setup.exe**.
10. Dans la page **Check for Updates?**, cliquez sur **Don't check for updates right now**, puis sur **next**. Attendez que le programme d'installation copie les fichiers, puis initialise le processus.
11. Dans la page **Introduction**, cliquez sur **next**.
12. Dans la page **License Agreement**, cliquez sur **I accept the terms in the license agreement**, puis sur **next**.
13. Dans la page **Recommended Settings**, cliquez sur **next**.
14. Dans la page **Server Role Selection**, sélectionnez le **Mailbox role** et le **Client Access role**, puis cliquez sur **next**.
15. Dans la page **Installation Space and Location**, acceptez les valeurs par défaut, puis cliquez sur **next**.
16. Dans la page **Malware Protection Settings**, assurez-vous que **Non** est sélectionné, puis cliquez sur **next**.
17. Dans la page **Readiness Checks**, assurez-vous que toutes les conditions préalables sont remplies, puis cliquez sur **install**.
18. Attendez que l'installation se termine. Cela peut prendre entre 30 et 40 minutes. Dans la page Installation terminée, cliquez sur **finish**.
19. Redémarrez LON-EX1-B et ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

▶ Tâche 3 : Vérifier l'installation d'Exchange Server

1. Sur LON-EX1-B, ouvrez la console du **Gestionnaire de serveur**, puis cliquez sur **Outils**.
2. Sélectionnez **Services**.
3. Faites défiler la liste des services et cliquez sur le service **Microsoft Exchange Active Directory Topology**. Examinez la description du service.
4. Examinez l'état des autres services Exchange Server. Vérifiez que tous les services qui sont configurés pour démarrer automatiquement sont exécutés.
5. Fermez la fenêtre **Services**.
6. Dans la barre des tâches, ouvrez l'**Explorateur de fichiers**.
7. Accédez à **C:\Programmes\Microsoft\Exchange Server\V15**. Cette liste de dossiers inclut ClientAccess, Mailbox et TransportRoles. Ces rôles ont été installés dans le cadre de l'installation par défaut.
8. Fermez l'**Explorateur de fichiers**.
9. Sur l'écran d'accueil, cliquez sur **Internet Explorer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Dans la barre d'adresses, tapez **https://lon-ex1.adatum.com/owa**, puis appuyez sur Entrée.
11. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
12. Dans la page Langue et fuseau horaire, cliquez sur **enregistrer**.
13. Cliquez sur **nouveau message**.
14. Envoyez un message électronique à l'Administrateur.
15. Vérifiez que le message électronique est bien reçu dans la boîte de réception.
16. Fermez Outlook Web App.

Résultats : À la fin de cet exercice, les stagiaires auront déployé Exchange Server 2013.

Exercice 3 : Gestion d'Exchange Server 2013

▶ Tâche 1 : Explorer le Centre d'administration Exchange Server 2013

1. Sur LON-EX1-B, sur l'écran Accueil, ouvrez **Internet Explorer**, tapez **https://lon-ex1.adatum.com/ecp**, puis appuyez sur Entrée.
2. Dans la zone de texte Domaine\Nom d'utilisateur, tapez **ADATUM\Administrateur**, dans le champ Mot de passe, tapez **Pa$$w0rd**, puis cliquez sur **se connecter**.
3. Dans la console du Centre d'administration Exchange, cliquez dans le volet gauche sur **Destinataires**, puis cliquez sur **Boîtes aux lettres** dans le volet central.
4. Cliquez sur le signe **+**, puis sur **Boîte aux lettres utilisateur**.
5. Dans la fenêtre **nouvelle boîte aux lettres utilisateur**, sélectionnez **Utilisateur existant**, puis cliquez sur **parcourir...**.
6. Dans la fenêtre **Sélectionner un utilisateur - Forêt entière**, sélectionnez **Aidan Delaney**, puis cliquez sur **ok**.
7. Dans la zone de texte **Alias**, tapez **AidanD**, puis cliquez sur **enregistrer**.
8. Assurez-vous qu'**Aidan Delaney** apparaît dans la liste des boîtes aux lettres.
9. Sous le nœud **Destinataires** du Centre d'administration Exchange, cliquez sur **Groupes**.
10. Cliquez sur la flèche à côté du signe **+**.
11. Sélectionnez **Groupe de distribution**.
12. Dans la fenêtre **nouveau groupe de distribution**, tapez **Adatum News** dans la zone de texte **Nom d'affichage**.
13. Dans la zone de texte **Alias**, tapez **AdatumNews**.
14. Faites défiler l'affichage et assurez-vous que l'option **ouvert : tout utilisateur peut faire partie de ce groupe sans l'approbation des propriétaires du groupe** est sélectionnée dans les deux dernières sections. Cliquez sur **enregistrer**.
15. Dans le coin supérieur droit, cliquez sur la flèche située à côté d'**Administrateur**, puis sélectionnez **Se déconnecter**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Gérer Exchange Server à l'aide de l'environnement de ligne de commande Exchange Management Shell

1. Sur LON-EX1-B, basculez vers l'écran d'accueil, puis cliquez sur **Exchange Management Shell**.
2. Dans Exchange Management Shell, tapez **get-user** et appuyez sur Entrée.

   Tous les utilisateurs du domaine Adatum.com sont listés.
3. Tapez **enable-mailbox -identity Robert**, puis appuyez sur Entrée.
4. Tapez **Get-Mailbox**, puis appuyez sur Entrée. Vous recevez toutes les boîtes aux lettres du serveur dans la liste.
5. Tapez **get-mailbox | set-mailbox -issuewarningquota 209715200 -prohibitsendquota 262144000**, puis appuyez sur Entrée.
6. Tapez **get-mailbox**, puis appuyez sur Entrée. Assurez-vous que **ProhibitSendQuota** est fixé à **250 MB** pour tous les utilisateurs.
7. Tapez **Get-User | Where-Object {$_.distinguishedname –ilike "*ou=IT,dc=adatum,dc=com"} | Enable-Mailbox**, puis appuyez sur Entrée.
8. Assurez-vous que les boîtes aux lettres de l'unité d'organisation IT ont été créées.
9. Fermez la fenêtre de Exchange Management Shell.

▶ Tâche 3 : Explorer Outlook Web App

1. Sur LON-EX1-B, sur l'écran d'accueil, ouvrez **Internet Explorer** et tapez **https://lon-ex1.adatum.com/owa**.
2. Dans la fenêtre **Outlook Web App**, connectez-vous à **Adatum\Aidan** avec le mot de passe **Pa$$w0rd**.
3. Cliquez sur **enregistrer** dans la page suivante.
4. Dans la fenêtre **Outlook Web App**, cliquez sur **nouveau message**.
5. Dans la fenêtre de droite, envoyez un nouveau message électronique à l'Administrateur.
6. Cliquez sur l'icône de roulette dans le coin supérieur droit. Sélectionnez **Options**.
7. Dans la fenêtre Options, cliquez dans le volet gauche sur **groupes**.
8. Dans le volet central, cliquez sur le bouton **Rejoindre**.
9. Dans la fenêtre **Tous les groupes**, double-cliquez sur **Adatum News**.
10. Dans la fenêtre **Adatum News**, cliquez sur **Rejoindre**.
11. Fermez la fenêtre **Tous les groupes**.
12. Dans le volet gauche, cliquez sur **paramètres**.
13. Dans la zone Signature électronique, tapez **Aidan Delaney**, **Adatum Corp.**, puis sélectionnez **Ajouter automatiquement ma signature aux messages envoyés**.
14. Cliquez sur **enregistrer**.
15. Cliquez sur la flèche dans le coin supérieur gauche (retour).

16. Cliquez sur l'icône de roulette dans le coin supérieur droit.
17. Sélectionnez **Modifier le thème**.
18. Cliquez sur le thème de votre choix, puis sur **OK**.
19. Fermez la fenêtre Internet Explorer.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1-B**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-EX1-B**.

Résultats : À la fin de cet exercice, les stagiaires auront exploré les outils de gestion Exchange.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 2 : Planification et configuration de serveurs de boîtes aux lettres

Atelier pratique : Configuration de serveurs de boîtes aux lettres

Exercice 1 : Planifier la configuration des serveurs de boîtes aux lettres

▶ Tâche 1 : Analyser les conditions requises pour le déploiement Exchange Server d'A. Datum

- Lisez le scénario de l'exercice et de l'atelier pratique. Résumez les conditions requises à partir du scénario de l'exercice.

▶ Tâche 2 : Utiliser Exchange Mailbox Server Role Requirements Calculator

1. Sur LON-CL1, cliquez sur la vignette du **Bureau**.
2. Dans la barre des tâches, cliquez sur l'**Explorateur de fichiers**, accédez à **C:\Files**, puis double-cliquez sur **E2013Calc.xlsm**. Dans l'avertissement de sécurité, cliquez sur **Activer le contenu**. Si la page Bienvenue dans votre nouvelle installation d'Office s'affiche, cliquez sur **Suivant** trois fois de suite, puis cliquez sur **Terminé**.
3. Dans le fichier **E2013Calc**, dans la feuille **Input**, entrez les valeurs suivantes pour chaque section :
    - Exchange Environment Configuration (Configuration de l'environnement Exchange)
        - Server Multi-Role Configuration (MBX+CAS) (Configuration de plusieurs rôles serveur (MBX+CAS)) : **No** (Non)
        - Server Role Virtualization (Virtualisation du rôle serveur) : **Yes** (Oui)
        - High Availability Deployment (Déploiement de la haute disponibilité) : **Yes** (Oui)
        - Number of Mailbox Servers Hosting Active Mailboxes / DAG (Nombre de serveurs de boîtes aux lettres hébergeant des boîtes aux lettres actives/DAG) : **4**
        - Number of Database Availability Groups (Nombre de groupes de disponibilité de la base de données) : **2**
    - Mailbox Database Copy Configuration (Configuration d'une copie de base de données de boîtes aux lettres)
        - Total Number of HA Database Copy Instances (Includes Active Copy) within DAG (Nombre total d'instances de copie de base de données HA [y compris la copie active] dans le DAG) : **3**
        - Total number of Lagged Database Copy Instances within DAG (Nombre total d'instances de copie de base de données décalée dans le DAG) : **1**
    - Exchange Data Configuration (Configuration des données Exchange)
        - Mailbox Moves/Week Percentage (Pourcentage de déplacement de boîtes aux lettres par semaine) : **2%**
        - LUN Free Space Percentage (Pourcentage d'espace libre par LUN) : **25%**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MGT UNIQUEMENT

- Tier-1 User Mailbox Configuration (Configuration de boîtes aux lettres d'utilisateur de niveau 1)
  - Total Number of Tier-1 User Mailboxes/Environment (Nombre total de boîtes aux lettres d'utilisateur de niveau 1/environnement) : **5000**
  - Projected Mailbox Number Growth Percentage (Pourcentage d'augmentation prévu du nombre de boîtes aux lettres) : **5%**
  - Total Send/Receive Capability/ Mailbox/Day (Capacité totale d'envoi/de réception par boîte aux lettres et par jour) : **150 messages**
  - Average Message Size (KB) (Taille moyenne des messages [Ko]) : **75**
  - Mailbox Size Limit (MB) (Taille maximale des boîtes aux lettres [Mo]) : **1024**
  - Personal Archive Mailbox Size Limit (MB) (Taille maximale des boîtes aux lettres d'archivage personnel [Mo]) : **2048**
  - Deleted Item Recovery Window (Days) (Fenêtre de rétention des éléments supprimés [jours]) : **30**
  - Single Item Recovery (Récupération d'élément unique) : **Enabled** (Activé)
  - Calendar Version Storage (Stockage des versions de calendrier) : **Enabled** (Activé)
- Backup Configuration (Configuration de la sauvegarde)
  - Backup Methodology (Méthodologie de sauvegarde) : **Software VSS Backup/Restore** (Sauvegarde/restauration VSS logicielle)
  - Backup Frequency (Fréquence des sauvegardes) : **Weekly Full / Daily incremental** (Complète hebdomadaire/incrémentielle quotidienne)
  - Database and Log Isolation Configured (Isolation de base de données et de journal configurée) : **Yes** (Oui)
  - Backup/Truncation Failure Tolerance (Tolérance d'échec des sauvegardes/troncations) : **3**
  - Network Failure Tolerance (Days) (Tolérance de défaillance réseau [jours]) : **0**
- Primary Datacenter Server Disk Configuration (Configuration des disques de serveur du centre de données principal)
  - Database (Base de données) : **1000 GB, 7.2K RPM SAS 3.5"** (Lecteur SAS 3,5 pouces, 7 200 tours/minute, 1 000 Go)
  - Log (Journal) : **500 GB, 7.2K RPM SAS 3.5"** (Lecteur SAS 3,5 pouces, 7 200 tours/minute, 500 Go)
  - Restore LUN (LUN de restauration) : **1500 GB, 7.2K RPM SAS 3.5"** (Lecteur SAS 3,5 pouces, 7 200 tours/minute, 1 500 Go)

▶ Tâche 3 : Analyser les résultats de l'outil Exchange Mailbox Server Role Requirements Calculator

1. Dans le fichier **E2013Calc**, cliquez sur l'onglet **Role Requirements** (Configuration requise pour le rôle).
2. Vérifiez les conditions requises indiquées sur cette feuille.
3. Cliquez sur la feuille **Distribution**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Cliquez sur **Fail Server** (Serveur en échec) pour chaque serveur. Observez où les bases de données seront distribuées.
5. Cliquez sur **Export DAG Scripts** (Exporter les scripts DAG).
6. Dans la fenêtre **Storage Calculator – Export Scripts** (Outil de calcul de stockage – Exporter les scripts), cliquez sur **OK** deux fois.
7. Cliquez sur la feuille **LUN Requirements** (Conditions requises pour LUN). Vérifiez les conditions requises indiquées sur cette feuille.
8. Cliquez sur la feuille **Backup Requirements** (Conditions requises pour les sauvegardes). Vérifiez les conditions requises indiquées sur cette feuille.
9. Cliquez sur la feuille **Replication Requirements** (Conditions requises pour les réplications). Vérifiez les conditions requises indiquées sur cette feuille.
10. Cliquez sur la feuille **Storage Design** (Conception du stockage). Vérifiez les conditions requises indiquées sur cette feuille.
11. Ouvrez l'**Explorateur de fichiers**, et accédez à **C:\Files**.
12. Cliquez avec le bouton droit sur le fichier **CreateMBDatabases.ps1**, puis sélectionnez **Modifier**. Examinez le contenu du script généré.
13. Cliquez avec le bouton droit sur le fichier **CreateMBDatabaseCopies.ps1**, puis sélectionnez **Modifier**. Examinez le contenu du script généré.
14. Cliquez avec le bouton droit sur le fichier **Diskpart.ps1**, puis sélectionnez **Modifier**. Examinez le contenu du script généré.
15. Fermez la fenêtre **Windows PowerShell ISE**.

▶ Tâche 4 : Comparer votre solution avec celle de l'instructeur et des autres stagiaires

1. Discutez de la solution fournie par l'outil de calcul de configuration requise pour le rôle serveur de boîtes aux lettres d'Exchange avec les autres stagiaires et avec l'instructeur.
2. Modifiez les valeurs figurant dans l'onglet **Input** (Entrée) d'Exchange Mailbox Server Role Requirements Calculator et observez la façon dont cela se reflète dans les résultats obtenus par l'outil.

Résultats : À la fin de cet exercice, les stagiaires auront créé un plan pour la configuration de leurs serveurs de boîtes aux lettres.

Exercice 2 : Configurer le stockage sur les serveurs de boîtes aux lettres

▶ Tâche 1 : Créer et configurer une cible et des lecteurs iSCSI

1. Sur LON-DC1, ouvrez le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
2. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, dans la page **Avant de commencer**, cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR ICT UNIQUEMENT

3. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionner des rôles de serveurs**, développez **Service de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, activez la case à cocher **Serveur cible iSCSI**, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
8. Une fois l'installation terminée, cliquez sur **Fermer**.
9. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez dans le volet de navigation sur **Services de fichiers et de stockage**.
10. Dans le volet Services de fichiers et de stockage, cliquez sur **iSCSI**.
11. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES**, puis dans la liste déroulante **TÂCHES**, sélectionnez **Nouveau disque virtuel iSCSI**.
12. Dans l'Assistant Nouveau disque virtuel iSCSI, dans la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur **C:**, puis sur **Suivant**.
13. Dans la page **Indiquer le nom du disque dur virtuel iSCSI**, dans la zone **Nom**, tapez **iSCSIDisk1**, puis cliquez sur **Suivant**.
14. Dans la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone **Taille**, tapez **2**, assurez-vous que **Go** est sélectionné dans la liste déroulante, puis cliquez sur **Suivant**.
15. Dans la page **Affecter la cible iSCSI**, cliquez sur **Nouvelle cible iSCSI**, puis sur **Suivant**.
16. Dans la page **Indiquer le nom de la cible**, dans la zone **Nom**, tapez **LON-MBX1**, puis cliquez sur **Suivant**.
17. Dans la page **Indiquer les serveurs d'accès**, cliquez sur **Ajouter**.
18. Dans la boîte de dialogue **Sélectionnez une méthode pour identifier l'initiateur**, cliquez sur **Parcourir**. Dans la fenêtre **Sélectionnez un ordinateur**, tapez **LON-MBX1**, cliquez sur **Vérifier les noms**, sur **OK**, puis à nouveau sur **OK**.
19. Dans la page **Indiquer les serveurs d'accès**, cliquez sur **Suivant**.
20. Dans la page **Activer l'authentification**, cliquez sur **Suivant**.
21. Dans la page **Confirmer les sélections**, cliquez sur **Créer**.
22. Dans la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.
23. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES**, puis dans la liste déroulante **TÂCHES**, sélectionnez **Nouveau disque virtuel iSCSI**.
24. Dans l'Assistant Nouveau disque virtuel iSCSI, dans la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur **C:**, puis sur **Suivant**.
25. Dans la page **Indiquer le nom du disque dur virtuel iSCSI**, dans la zone **Nom**, tapez **iSCSIDisk2**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

26. Dans la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone **Taille**, tapez **2**, assurez-vous que **Go** est sélectionné dans la liste déroulante, puis cliquez sur **Suivant**.
27. Dans la page **Affecter la cible iSCSI**, cliquez sur **lon-mbx1**, puis sur **Suivant**.
28. Dans la page **Confirmer les sélections**, cliquez sur **Créer**.
29. Dans la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.
30. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES**, puis dans la liste déroulante **TÂCHES**, sélectionnez **Nouveau disque virtuel iSCSI**.
31. Dans l'Assistant Nouveau disque virtuel iSCSI, dans la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur **C:**, puis sur **Suivant**.
32. Dans la page **Indiquer le nom du disque dur virtuel iSCSI**, dans la zone **Nom**, tapez **iSCSIDisk3**, puis cliquez sur **Suivant**.
33. Dans la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone **Taille**, tapez **500**, assurez-vous que **Mo** est sélectionné dans la liste déroulante, puis cliquez sur **Suivant**.
34. Dans la page **Affecter la cible iSCSI**, cliquez sur **lon-mbx1**, puis sur **Suivant**.
35. Dans la page **Confirmer les sélections**, cliquez sur **Créer**.
36. Dans la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.

▶ Tâche 2 : Connecter Exchange Server au stockage

1. Sur **LON-MBX1**, cliquez sur la vignette du Bureau
2. Dans la barre des tâches, cliquez sur **Gestionnaire de serveur**.
3. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Initiateur iSCSI**.
4. Dans la boîte de dialogue **Microsoft iSCSI**, cliquez sur **Oui**.
5. Cliquez sur l'onglet **Découverte**.
6. Cliquez sur **Découvrir un portail**.
7. Dans la zone **Adresse IP ou nom DNS**, tapez **172.16.0.10**, puis cliquez sur **OK**.
8. Cliquez sur l'onglet **Cibles**.
9. Cliquez sur **Actualiser**.
10. Dans la liste **Cibles découvertes**, sélectionnez **iqn.1991-05.com.microsoft:lon-dc1-lon-mbx1-target**, puis cliquez sur **Connexion**.
11. Sélectionnez **Ajoutez cette connexion à la liste des cibles favorites**, puis cliquez deux fois sur **OK**.

▶ Tâche 3 : Configurer le stockage

1. Sur LON-MBX1, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion de l'ordinateur**.
2. Développez **Stockage**, puis cliquez sur **Gestion des disques**.
3. Cliquez avec le bouton droit sur **Disque 1**, puis cliquez sur **En ligne**.

4. Cliquez avec le bouton droit sur **Disque 1**, puis cliquez sur **Initialiser le disque**. Dans la boîte de dialogue **Initialiser le disque**, cliquez sur **OK**.
5. Cliquez avec le bouton droit sur l'espace non alloué en regard de **Disque 1**, puis cliquez sur **Nouveau volume simple**.
6. Dans la page **Assistant Création d'un volume simple**, cliquez sur **Suivant**.
7. Dans la page **Spécifier la taille du volume**, cliquez sur **Suivant**.
8. Dans la page **Attribuer une lettre de lecteur ou de chemin d'accès**, cliquez sur **Suivant**.
9. Dans la page **Formater une partition**, dans la zone **Nom de volume**, tapez **DB1**. Activez la case à cocher **Effectuer un formatage rapide**, puis cliquez sur **Suivant**.
10. Cliquez sur **Terminer**. (Remarque : si la fenêtre Microsoft Windows s'affiche avec une invite de formatage du disque, cliquez sur **Annuler**.)
11. Répétez les étapes 3 à 10 pour les **Disque 2** et **Disque 3**. (Remarque : utilisez **DB2** et **Logs** pour les noms de volume respectivement.)
12. Fermez la fenêtre **Gestion de l'ordinateur**.

Résultats : À la fin de cet exercice, les stagiaires disposeront d'un stockage iSCSI configuré pour leurs bases de données de boîtes aux lettres et leurs journaux.

Exercice 3 : Créer et configurer des bases de données de boîtes aux lettres

▶ Tâche 1 : Configurer les paramètres de boîte aux lettres pour la base de données de boîtes aux lettres existante

1. Sur LON-MBX1, cliquez sur l'écran Accueil, puis cliquez sur **Internet Explorer**.
2. Dans **Internet Explorer**, tapez **https://lon-cas1.adatum.com/ecp**, puis appuyez sur Entrée.

Remarque : Vérifiez que tous les services de votre environnement Exchange et type de démarrage automatique sont en cours d'exécution sur LON-CAS1.

3. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Dans le Centre d'administration Exchange, dans le volet Fonctionnalités, cliquez sur **Serveurs**.
5. Cliquez sur l'onglet **Bases de données**.
6. Double-cliquez sur **Mailbox Database 1**.
7. Dans la fenêtre **Base de données de boîtes aux lettres**, cliquez sur **Limites**.
8. Dans la zone de texte **Émettre un avertissement à (Go)**, tapez **0,9**.
9. Dans la zone de texte **Interdire l'envoi à (Go)**, tapez **1**.
10. Dans la zone de texte **Interdire l'envoi et la réception à (Go)**, tapez **1,3**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Dans la zone de texte **Conserver les éléments supprimés pendant (jours)**, tapez **30**.
12. Cliquez sur **enregistrer**. Réduisez la fenêtre du Centre d'administration Exchange.
13. Sur LON-MBX1, cliquez sur l'écran Accueil, puis sur l'environnement de ligne de commande **Exchange Management Shell**.
14. Dans la fenêtre Exchange Management Shell, tapez **Get-MailboxDatabase** et appuyez sur Entrée.
15. Consultez la liste des bases de données de boîtes aux lettres créées.
16. Dans la fenêtre de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante, puis appuyez sur Entrée :

    Move-DatabasePath –Identity "Mailbox Database 1" –EdbFilePath E:\DB1\DB1.edb – LogFolderPath G:\Logs\DB1
17. Tapez **O**, puis appuyez sur Entrée.
18. Tapez **O**, puis appuyez sur Entrée.
19. Réduisez la fenêtre **Exchange Management Shell**.
20. Ouvrez l'**Explorateur de fichiers**, accédez à **E:** et ouvrez le dossier **DB1**. Vérifiez que le fichier de base de données **DB1.edb** y figure.
21. Accédez à **G:** et ouvrez le dossier **Logs\DB1**. Assurez -vous que les fichiers journaux sont présents.
22. Fermez l'**Explorateur de fichiers**.

► Tâche 2 : Créer et configurer des bases de données de boîtes aux lettres supplémentaires

1. Restaurez la fenêtre du Centre d'administration Exchange.
2. Cliquez sur **Serveurs** dans le volet Fonctionnalités, puis sur l'onglet **Bases de données**.
3. Cliquez sur **Nouveau**.
4. Dans la fenêtre **Base de données**, dans la zone de texte **Base de données de boîtes aux lettres**, tapez **DB2**.
5. Cliquez sur **parcourir...**.
6. Dans la fenêtre **Sélectionner un serveur**, sélectionnez **LON-MBX1**, puis cliquez sur **OK**.
7. Dans la zone de texte **Chemin d'accès au fichier de base de données**, tapez : **F:\DB2\DB2.edb**.
8. Dans la zone de texte **Chemin d'accès au dossier Journal**, tapez **G:\Logs\DB2**.
9. Vérifiez que **Monter cette base de données** est sélectionné, puis cliquez sur **enregistrer**. Cliquez sur **ok**.
10. Restaurez la fenêtre de l'environnement de ligne de commande **Exchange Management Shell**.
11. Dans la fenêtre de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante :

    Set-MailboxDatabase –identity DB2 –DeletedItemRetention 20.00:00:00 – CircularLoggingEnabled $true –ProhibitSendQuota "2.2GB", puis appuyez sur Entrée.

12. Tapez **Dismount-Database –identity DB2**, puis appuyez sur Entrée.
13. Tapez **O**, puis appuyez sur Entrée.
14. Tapez **Mount-Database –identity DB2**, puis appuyez sur Entrée.
15. Laissez la fenêtre de l'environnement de ligne de commande **Exchange Management Shell** ouverte.

▶ Tâche 3 : Exportez les données de boîtes aux lettres dans le fichier .pst

1. Sur l'ordinateur virtuel **LON-MBX1**, restaurez la fenêtre de l'environnement de ligne de commande **Exchange Management Shell**.
2. Tapez **New-ManagementRoleAssignment –Role "Mailbox Import Export" –User Administrateur**, puis appuyez sur Entrée.
3. Fermez l'environnement de ligne de commande **Exchange Management Shell**.
4. Sur l'écran Accueil, cliquez sur **Exchange Management Shell**.
5. Tapez la commande suivante et appuyez sur Entrée : **New-MailboxExportRequest -Mailbox aidan -FilePath \\lon-dc1\MailboxExport\aidan.pst**.
6. Tapez **Get-MailboxExportrequest**, puis appuyez sur Entrée.
7. Assurez -vous que l'état de la demande indique Terminé. (Si elle n'est pas terminée, patientez quelques minutes, puis répétez l'étape 6.)
8. Basculez vers LON-DC1. Ouvrez l'**Explorateur de fichiers**, puis accédez au dossier **C:\MailboxExport** et vérifiez que le fichier **aidan.pst** est présent.
9. Fermez **l'Explorateur de fichiers**.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1**, **22341B-LON-MBX1** et **22341B-LON-CL1**.

Résultats : À la fin de cet exercice, les stagiaires auront créé et configuré leurs bases de données de boîtes aux lettres.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 3 : Gestion d'objets destinataires

Atelier pratique : Gestion d'objets destinataires

Exercice 1 : Configurer les destinataires Trey Research

▶ Tâche 1 : Créer des objets Active Directory Trey Research

1. Sur LON-CAS1, sur la mosaïque Bureau, cliquez sur **Gestionnaire de serveur** dans la barre des tâches.
2. Cliquez sur **Outils**, puis sur **Module Active Directory pour Windows PowerShell**.
3. Tapez **e:** et appuyez sur Entrée.
4. Tapez **cd Labfiles\Mod03**, puis appuyez sur Entrée.
5. Tapez **.\TreyResearchSetup.ps1**, puis appuyez sur Entrée.
6. À l'invite **Tapez le mot de passe**, tapez **Pa$$w0rd** et appuyez sur Entrée.
7. Fermez la fenêtre du Module Active Directory pour Windows PowerShell.
8. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
9. Développez **Adatum.com**, développez **TreyResearch**, et vérifiez que l'unité d'organisation TreyResearch contient des unités d'organisation enfants avec des groupes et des comptes d'utilisateur.
10. Fermez Utilisateurs et ordinateurs Active Directory.

▶ Tâche 2 : Créer les boîtes aux lettres Trey Research

1. Sur LON-CAS1, cliquez sur l'écran d'accueil, puis sur l'environnement de ligne de commande **Exchange Management Shell**.
2. À l'invite de commandes, tapez **New-MailboxDatabase –Name TreyResearchDB –Server LON-MBX1**, puis appuyez sur Entrée.
3. À l'invite de commandes, tapez **Invoke-Command –ComputerName LON-MBX1 –ScriptBlock {Restart-Service msexchangeis}**, puis appuyez sur Entrée.
4. À l'invite de commandes, tapez **Mount-Database –id TreyResearchDB**, puis appuyez sur Entrée.
5. À l'invite de commandes, tapez **Get-User –OrganizationalUnit TreyResearch | Enable-Mailbox -Database TreyResearchDB**.
6. À l'invite de commandes, tapez **Get-Group -OrganizationalUnit TreyResearch | Enable-DistributionGroup**, puis appuyez sur Entrée.
7. Sur LON-CAS1, ouvrez Internet Explorer et connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Cliquez sur **OK** dans la fenêtre d'avertissement.
8. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

9. Cliquez sur l'onglet **Ressources**.
10. Cliquez sur **Nouveau**, puis sur **Boîte aux lettres de salle**.
11. Renseignez les champs suivants :
    - Nom de la salle : **TR_Room1**
    - Adresse de messagerie : **TR_Room1**
    - Unité d'organisation : Cliquez sur **parcourir...**, sur **TreyResearch**, puis sur **ok**.
    - Emplacement : **Harrow**
    - Capacité : **20**
12. Cliquez sur **Sélectionner des délégués capables d'accepter ou de refuser des demandes de réservation**.
13. Cliquez sur **Ajouter**, cliquez sur **Charlotte Weiss**, sur **ajouter**, puis sur **ok**.
14. Cliquez sur **Options supplémentaires**, sous **Base de données de boîtes aux lettres** cliquez sur **parcourir...**, puis sur **TreyResearchDB**, et enfin sur **ok**.
15. Cliquez sur **enregistrer**.
16. Dans l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante et appuyez sur Entrée.

    Set-CalendarProcessing –id TR_Room1
    –BookinPolicy AllTreyResearch
17. Sur LON-CAS1, dans le CAE, dans le volet de fonctionnalités, cliquez sur **Destinataires**.
18. Cliquez sur l'onglet **Partagé**.
19. Cliquez sur **Nouveau**.
20. Renseignez les champs suivants :
    - Nom d'affichage : **TreyResearch Sales**
    - Unité d'organisation : **TreyResearch/Sales**
    - Adresse de messagerie : **TreyResearchSales**
21. Sous **Accès total**, cliquez sur **Ajouter**, cliquez sur **TR_Sales**, sur **ajouter**, puis sur **ok**.
22. Cliquez sur **Options supplémentaires**.
23. Sous **Base de données de boîtes aux lettres**, cliquez sur **parcourir...**, sur **TreyResearchDB**, puis sur **ok**.
24. Cliquez sur **enregistrer**.

▶ Tâche 3 : Créer des groupes de distribution Trey Research

1. Sur LON-CAS1, dans le CAE, cliquez sur l'onglet **Groupes**.
2. Cliquez sur **Nouveau**, et cliquez sur **Groupe de distribution**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Renseignez les champs suivants :
   - Nom d'affichage : **Trey_SalesMgrs**
   - Alias : **TreySalesMgrs**
   - Unité d'organisation : **TreyResearch/Sales**
   - Membres : **Florence Flipo**, **Sidney Higa**
   - Choisir si l'approbation du propriétaire du groupe est requise pour rejoindre ce dernier : **Fermé**
   - Choissisez s'il est possible de quitter le groupe : **Fermé**
4. Cliquez sur **enregistrer**.
5. Dans l'onglet **Groupes**, cliquez sur **Nouveau**, puis sur **Groupe de distribution**.
6. Renseignez les champs suivants :
   - Nom d'affichage : **TreyResearchNews**
   - Alias : **TreyResearchNews**
   - Unité d'organisation : **TreyResearch**
   - Membres : Aucun
   - Choisir si l'approbation du propriétaire du groupe est requise pour rejoindre ce dernier : **Ouvert**
   - Choisissez s'il est possible de quitter le groupe : **Ouvert**
7. Cliquez sur **enregistrer**.
8. Sur LON-CAS1, dans l'environnement de ligne de commande Exchange Management Shell, tapez **cd E:\Labfiles\Mod03**, puis appuyez sur Entrée.
9. Tapez **$users=import-csv .\TreyResearchIntegrationTeam.csv** et appuyez sur Entrée.
10. Tapez **foreach ($i in $users) {set-mailbox –Identity $i.alias –CustomAttribute1 "TreyResearch Integration Project Team"}**, et appuyez sur Entrée.
11. Sur LON-CAS1, dans le CAE, dans l'onglet **Groupes**, cliquez sur **Nouveau**, puis sur **Groupe de distribution dynamique**.
12. Renseignez les champs suivants :
    - Nom d'affichage : **TreyIntegration**
    - Alias : **TreyIntegration**
    - Unité d'organisation : **TreyResearch**
    - Propriétaire : **Administrateur**
13. Sous **Membres**, cliquez sur **Uniquement les types de destinataires suivants**, et sélectionnez la case à cocher **Utilisateurs avec boîtes aux lettres Exchange**.
14. Cliquez sur **ajouter une règle**.
15. À partir de la liste déroulante, cliquez sur **Conteneur de destinataires**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Cliquez sur **Adatum.com**, puis sur **ok**.
17. Cliquez sur **ajouter une règle**.
18. À partir de la liste déroulante, cliquez sur **Attribut personnalisé 1**.
19. Dans la page **spécifier des mots ou des expressions**, tapez **TreyResearch Integration Project Team**, cliquez sur **Ajouter**, puis sur **ok**.
20. Cliquez sur **enregistrer**.

Résultats : Dans cet exercice, vous avez créé des comptes de groupes et d'utilisateurs Active Directory pour Trey Research, vous avez également créé une boîte aux lettres de salles avec des autorisations personnalisées et vous avez configuré une boîte aux lettres partagée. Vous avez en outre configuré des groupes de distribution pour les utilisateurs Trey Research.

Exercice 2 : Configurez les stratégies et listes d'adresses pour Trey Research

▶ Tâche 1 : Configurer TreyResearch.net en tant que domaine accepté

1. Sur LON-CAS1, dans le CAE, cliquez sur **Flux de messagerie** dans le volet de fonctionnalités, puis sur l'onglet **Domaines acceptés**, cliquez sur **Nouveau**.
2. Dans la fenêtre **nouveau domaine accepté**, tapez **TreyResearch** comme **Nom**, et **TreyResearch.net** comme **Domaine accepté**.
3. Cliquez sur **enregistrer**.

▶ Tâche 2 : Configurer une stratégie d'adresse de messagerie pour les utilisateurs Trey Research

1. Dans l'onglet **Stratégies d'adresse de messagerie**, cliquez sur **Nouveau**.
2. Dans la fenêtre **nouvelle stratégie d'adresse de messagerie**, tapez **Adresse de messagerie TreyResearch** comme **Nom de la stratégie**.
3. Sous **Format de l'adresse de messagerie**, cliquez sur **Ajouter**.
4. À partir de la liste déroulante **Sélectionner un domaine accepté**, sélectionnez **TreyResearch.net**.
5. Cliquez sur **John.Smith@contoso.com**, puis sur **enregistrer**.
6. Dans la fenêtre **nouvelle stratégie d'adresse de messagerie**, cliquez sur **ajouter une règle**.
7. Cliquez sur **Sélectionner un**, puis sur **Conteneur de destinataires**.
8. Cliquez sur **TreyResearch**, puis sur **ok**.
9. Cliquez sur **enregistrer**, puis sur **ok**.
10. Cliquez sur **Adresse de messagerie TreyResearch**. Dans le volet d'informations, cliquez sur **Actualiser**, sur **Appliquer**, puis sur **oui**.
11. Cliquez sur **fermer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 3 : Configurer une liste d'adresses pour les utilisateurs Trey Research

1. Dans le CAE, cliquez sur **Organisation** dans le volet des fonctionnalités, puis sur **Listes d'adresses**.
2. Dans l'onglet **Listes d'adresses**, cliquez sur **Nouveau**.
3. Dans la fenêtre **nouvelle liste d'adresses**, tapez **TreyResearch** comme **Nom**.
4. Cliquez sur **ajouter une règle**.
5. Dans la liste **Choisir dans la liste**, cliquez sur **Conteneur de destinataires**.
6. Dans la boîte de dialogue Sélectionner une unité d'organisation, cliquez sur **TreyResearch**, et cliquez sur **ok**.
7. Cliquez sur **enregistrer**, sur **ok**, puis sur **Mettre à jour**.
8. Cliquez sur **oui**, puis sur **fermer**.

▶ Tâche 4 : Configurer une stratégie de carnet d'adresses pour les utilisateurs Trey Research

1. Sur LON-CAS1, si nécessaire, ouvrez l'environnement de ligne de commande Exchange Management Shell.
2. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
New-GlobalAddressList -Name TreyResearchGAL -RecipientContainer TreyResearch
```

3. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
Update-GlobalAddressList -id TreyResearchGAL
```

4. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
New-OfflineAddressBook -Name TreyResearchOAB -AddressLists TreyResearch
```

5. À l'invite de commandes, tapez la commande suivante, puis Entrée.

```
New-AddressList -Name TreyResearchRooms –RecipientContainer TreyResearch –
IncludedRecipients Resources
```

6. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
Update-AddressList TreyResearchRooms
```

7. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
Set-OfflineAddressBook -id "TreyResearchOAB" –VirtualDirectories “LON-CAS1\oab
(Default Web Site)”,”LON-MBX1\oab (Exchange Back End)”
```

8. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
Update-OfflineAddressBook -id "TreyResearchOAB"
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT PENDANT

9. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
New-AddressBookPolicy -Name TreyResearchABP -AddressLists \TreyResearch -
OfflineAddressBook TreyResearchOAB -GlobalAddressList TreyResearchGAL -RoomList
\TreyResearchRooms
```

10. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
Get-Mailbox -OrganizationalUnit TreyResearch | Set-Mailbox -AddressBookPolicy
TreyResearchABP
```

▶ Tâche 5 : Valider le déploiement

1. Dans le CAE, cliquez sur **Destinataires** dans le volet des fonctionnalités.
2. Cliquez sur **Boîtes aux lettres**, puis double-cliquez sur **Aaron Nicholls** et cliquez sur l'onglet **Fonctionnalités de boîte aux lettres**.
3. Vérifiez que la stratégie de carnet d'adresses TreyResearchABP a été attribuée à la boîte aux lettres d'Aaron. Cliquez sur **annuler**.
4. Sur LON-CL1, connectez-vous en tant qu'**ADATUM\Aaron** avec le mot de passe **Pa$$w0rd**.
5. Cliquez avec le bouton droit sur l'écran d'accueil, puis cliquez sur **Toutes les applications**.
6. Ouvrez Outlook 2013.
7. Dans la page Bienvenue dans Outlook 2013, cliquez sur **Suivant**.
8. Dans la page Ajouter un compte de messagerie, cliquez sur **Suivant**.
9. Dans la page Configuration de compte automatique, vérifiez que les informations d'Aaron ont été ajoutées automatiquement, puis cliquez sur **Suivant**.
10. Cliquez sur **Terminer** et attendez l'ouverture d'Outlook.
11. Dans la fenêtre Commençons par le début, cliquez sur **Me demander plus tard**, et cliquez sur **Accepter**.
12. Une fois qu'Outlook est ouvert, cliquez sur **Nouveau message électronique**. Dans la fenêtre Sans titre - Message (HTML), cliquez sur **À**.
13. Vérifiez que l'utilisateur peut voir uniquement les utilisateurs et les groupes de l'unité d'organisation TreyResearch.
14. Cliquez sur **Trey_SalesMgrs**, sur **À** et sur **OK**.
15. Tapez un objet de **test** et un bref message électronique, puis cliquez sur **Envoyer**.
16. Cliquez sur l'icône Calendrier.
17. Cliquez sur **Nouvelle réunion**.
18. Dans la fenêtre Sans titre - Réunion (HTML), cliquez sur **À**.
19. Cliquez sur **Cindy White**, puis sur **Obligatoire**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

20. Sous Carnet d'adresses, cliquez sur **TreyResearchRooms**. Cliquez sur **TR_Room1**, puis sur **Resources**. Cliquez sur **OK**.
21. Dans la fenêtre Sans titre - Réunion, choisissez une heure demain dans la zone **Heure de début**.
22. Tapez un objet de **réunion test** et un bref message électronique, puis cliquez sur **Envoyer**.
23. Examinez le message de réponse de réunion et fermez le message.
24. Ouvrez Internet Explorer, et connectez-vous à **https://lon-cas1.adatum.com/owa**.
25. Connectez-vous en tant qu'**ADATUM\Aaron** avec le mot de passe **Pa$$w0rd**.
26. Dans la fenêtre Outlook Web App, cliquez sur **enregistrer**.
27. Dans la fenêtre Outlook Web App, cliquez sur l'icône **Paramètres** dans l'angle supérieur droit, puis cliquez sur **Options**.
28. Sous **Options**, cliquez sur **groupes**.
29. Sous **groupes de distribution auxquels j'appartiens**, cliquez sur **Rejoindre**.
30. Dans la boîte de dialogue Tous les groupes, double-cliquez sur **Trey_SalesMgrs**.
31. Dans la boîte de dialogue Trey_SalesMgrs, cliquez sur **Rejoindre**.
32. Examinez le message d'erreur stipulant que le groupe est fermé et cliquez sur **OK**. Cliquez sur **fermer**.
33. Dans la boîte de dialogue Tous les groupes, double-cliquez sur **TreyResearchNews**.
34. Dans la boîte de dialogue TreyResearchNews, cliquez sur **Rejoindre**.
35. Fermez la boîte de dialogue Tous les groupes, puis vérifiez qu'Aaron est maintenant membre du groupe de distribution TreyResearchNews. Fermez Internet Explorer.
36. Dans Outlook 2013, cliquez sur l'icône **Courrier**, puis sur **Nouveau message électronique**.
37. Dans la zone **À**, tapez **treyintegration@treyresearch.net**. Tapez un objet et un bref message, puis cliquez sur **Envoyer**.
38. Ouvrez Internet Explorer, et connectez-vous à **https://lon-cas1.adatum.com/owa**.
39. Connectez-vous en tant qu'**ADATUM\Aidan** avec le mot de passe **Pa$$w0rd**. Cliquez sur **enregistrer**.
40. Dans la fenêtre Outlook Web App, vérifiez qu'Aidan a reçu le message envoyé au groupe de distribution dynamique treyintegration.

Résultats : Dans cet exercice, vous avez créé une stratégie d'adresse de messagerie et une liste d'adresses pour Trey Research. Vous avez créé une stratégie de carnet d'adresses pour Trey Research et validé le déploiement.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 3 : Configurer les dossiers publics pour Trey Research

▶ Tâche 1 : Créer la boîte aux lettres de dossiers publics

1. Sur LON-CAS1, basculez vers le Centre d'administration Exchange.
2. Dans le volet des fonctionnalités, cliquez sur **dossiers publics**.
3. Cliquez sur l'onglet **Boîtes aux lettres de dossier public**, puis sur **nouvelle boîte aux lettres de dossier public**.
4. Dans la page **nouvelle boîte aux lettres de dossier public**, tapez **PFMBX1** dans le champ **Nom**.
5. **Sous Unité d'organisation**, cliquez sur **parcourir...**, cliquez sur **TreyResearch**, puis sur **ok**.
6. Sous **Base de données de boîtes aux lettres**, cliquez sur **parcourir...**, sur **TreyResearchDB**, puis sur **ok**.
7. Cliquez sur **enregistrer**.

▶ Tâche 2 : Créer les dossiers publics

1. Cliquez sur **Dossiers publics**, puis sur **Nouveau dossier public**.
2. Dans la page **Nouveau dossier public**, dans le champ **Nom**, tapez **TreyResearch**, puis cliquez sur **enregistrer**.
3. Cliquez sur **TreyResearch**, puis sur **Nouveau dossier public**.
4. Dans la fenêtre **Nouveau dossier public**, dans le champ **Nom**, tapez **Research**, puis cliquez sur **enregistrer**.

▶ Tâche 3 : Configurer les autorisations de dossiers publics

1. Cliquez sur **Atteindre le dossier parent**.
2. Vérifiez que **TreyResearch** est répertorié dans la liste des dossiers, sélectionnez le dossier, puis sous **Autorisations du dossier**, cliquez sur **Gérer**.
3. Dans la fenêtre **TreyResearch**, cliquez sur **Ajouter**.
4. Dans la fenêtre Autorisations de dossiers publics, en regard d'**Utilisateur**, cliquez sur **parcourir...**.
5. Dans la fenêtre **Sélectionner un destinataire**, cliquez sur **TR_IT**, puis sur **ok**.
6. Sous **Niveau d'autorisation**, cliquez sur **Propriétaire**, puis sur **enregistrer**.
7. Sélectionnez la case à cocher **Appliquer les changements à ce dossier public et à tous ses sous-dossiers**.
8. Dans la fenêtre **TreyResearch**, cliquez sur **Ajouter**.
9. Dans la fenêtre Autorisations des dossiers publics, en regard d'**Utilisateur**, cliquez sur **parcourir...**.
10. Dans la fenêtre **Sélectionner un destinataire**, cliquez sur **AllTreyResearch**, puis sur **ok**.
11. Sous **Niveau d'autorisation**, cliquez sur **Auteur**, puis sur **enregistrer**.
12. Cliquez sur **enregistrer**, puis sur **fermer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Valider le déploiement des dossiers publics

1. Sur LON-CL1, dans Outlook 2013, ouvrez l'affichage des dossiers.
2. Vérifiez que les dossiers publics sont répertoriés dans le volet de gauche.
3. Développez les dossiers publics et vérifiez que les dossiers publics TreyResearch et Research sont visibles.

Remarque : L'affichage des dossiers publics peut prendre plusieurs minutes. Si les dossiers publics ne s'affichent pas, patientez quelques minutes, fermez Outlook 2013 et ouvrez-le à nouveau. Si les dossiers publics n'apparaissent toujours pas, déconnectez-vous de LON-CL1, connectez-vous en tant que **Cindy** avec le mot de passe **Pa$$w0rd**, et ouvrez Outlook 2013. Configurez le profil d'Outlook, et vérifiez que les dossiers publics sont visibles.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1**, **22341B-LON-MBX1** et **22341B-LON-CL1**.

Résultats : Dans cet exercice, vous avez créé des boîtes aux lettres de dossiers publics pour Trey Research et avez vérifié que les utilisateurs peuvent y accéder.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 4 : Planification et déploiement des serveurs d'accès au client

Atelier pratique : Déploiement et configuration d'un rôle serveur d'accès au client

Exercice 1 : Configuration de certificats pour le serveur d'accès au client

▶ Tâche 1 : Effectuer une demande de certificat sur Exchange Server

1. Sur LON-CAS1, ouvrez **Internet Explorer**, tapez **https://lon-cas1.adatum.com/ecp** et appuyez sur Entrée.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans le CAE, dans le volet de navigation gauche, cliquez sur **Serveurs**.
4. Cliquez sur **Certificats** dans le volet droit.
5. Cliquez sur le signe **+**.
6. Dans la fenêtre **Certificat Exchange – Windows Internet Explorer**, dans **nouveau certificat Exchange**, sélectionnez **Créez une demande de certificat d'une autorité de certification**, puis cliquez sur **suivant**.
7. Dans le champ **Nom convivial** de ce certificat, tapez **mail.adatum.com**, puis cliquez sur **suivant**.
8. Dans la page avec l'option pour l'utilisation des certificats génériques, n'apportez aucune modification, puis cliquez sur **suivant**.
9. Cliquez sur **parcourir...**.
10. Dans la fenêtre **Sélectionner un serveur**, cliquez sur **LON-CAS1**, puis cliquez sur **ok**.
11. Cliquez sur **suivant**.
12. Dans la page suivante, cliquez sur **Outlook Web App (si accessible à partir d'Internet)**, puis cliquez sur l'icône **Modifier**.
13. Dans le champ **Spécifiez les domaines pour le type d'accès ci-dessus**, entrez **mail.adatum.com** et cliquez sur **ok**.
14. Répétez les étapes 12 et 13 pour les éléments où **<non spécifié>** apparaît dans la colonne **DOMAINE**.
15. Cliquez sur **suivant**.
16. Dans la page suivante, assurez-vous que les noms suivants sont présents dans la liste : **mail.adatum.com**, **lon-cas1.adatum.com**, **AutoDiscover.Adatum.com, LON-CAS1** et **Adatum.com**, puis cliquez sur **suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

17. Dans la page suivante, complétez les champs suivants comme suit :
    a. Nom d'organisation : **A.Datum**
    b. Nom du service : **Informatique**
    c. Ville/Localité : **Seattle**
    d. Département/région : **WA**
    e. Nom de pays/région : **États-Unis**
18. Cliquez sur **suivant**.
19. Dans la page suivante, tapez **\\lon-cas1\C$\windows\temp\certreq.req** et cliquez sur **terminer**.

▶ Tâche 2 : Délivrer un certificat d'une autorité de certification interne

1. Sur LON-DC1, dans le menu Accueil, cliquez sur Autorité de certification.
2. 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**.
3. Cliquez avec le bouton droit sur **Adatum-LON-DC1-CA**, pointez le curseur sur **Toutes les tâches**, puis cliquez sur **Démarrer le service**.
4. Sur LON-CAS1, ouvrez l'Explorateur de fichiers et accédez à **C:\Windows\Temp**.
5. Cliquez avec le bouton droit sur **certreq.req**, puis cliquez sur **Ouvrir avec**.
6. Dans la boîte de dialogue Windows, cliquez sur **Plus d'options** si nécessaire, puis sur **Bloc-notes**.
7. Dans la fenêtre certreq.req – Bloc-notes, cliquez sur **Ctrl+A** pour sélectionner tout le texte, puis cliquez sur **Ctrl+C** pour le copier et enregistrez-le dans le Presse-papiers. Fermez le Bloc-notes.
8. Cliquez sur l'écran **Accueil**, puis ouvrez une nouvelle fenêtre Internet Explorer.
9. Connectez-vous à **http://lon-dc1.adatum.com/certsrv**.
10. Connectez-vous en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
11. Dans la **Bienvenue**, cliquez sur **Demander un certificat**.
12. Dans la page **Demander un certificat**, cliquez sur **Demande de certificat avancée**.
13. Dans la page **demande de certificat avancée**, cliquez sur **Soumettez une demande de certificat en utilisant un fichier CMC ou PKCS #10 codé en base 64, ou soumettez une demande en utilisant un fichier PKCS #7 codé en base 64**.
14. Dans la page **Soumettre une demande de certificat ou de renouvellement**, cliquez dans le champ **Demande enregistrée** et appuyez sur **Ctrl+V** pour copier les informations de la demande de certificat dans le champ.
15. Dans la zone de liste déroulante **Modèle de certificat**, cliquez sur **Serveur Web**, puis sur **Envoyer**.
16. Dans la page **Certificat émis**, cliquez sur **Télécharger le certificat**.
17. Dans la boîte de dialogue **Téléchargement de fichiers**, cliquez sur la flèche en regard de **Enregistrer**. Sélectionnez **Enregistrer sous**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Dans la boîte de dialogue **Enregistrer sous**, cliquez sur **Enregistrer**.
19. Dans la boîte de dialogue **Téléchargement terminé**, cliquez sur **Ouvrir**.
20. Dans la boîte de dialogue **Certificat**, sous l'onglet **Détails**, cliquez sur **Autre nom de l'objet**. Vérifiez que le certificat inclut plusieurs autres noms de l'objet, puis cliquez sur **OK**.
21. Sur LON-CAS1, ouvrez l'**Explorateur de fichiers** et créez un nouveau dossier nommé **cert** sur le lecteur de C:\. Partagez le dossier et accordez l'autorisation Lecture à **Tout le monde**.
22. Copiez le fichier **certnew.cer** de C:\Utilisateurs\administrateur.ADATUM\Téléchargements vers C:\cert.
23. Fermez **l'Explorateur de fichiers**.

▶ Tâche 3 : Attribuer un certificat aux services Exchange

1. Sur LON-CAS1, basculez vers le CAE.
2. Cliquez sur **Serveurs**, puis sur **Certificats**.
3. À côté de **Sélectionner le serveur**, cliquez sur **LON-CAS1.Adatum.com**.
4. Cliquez sur **mail.adatum.com**, puis cliquez sur **...** dans la barre d'outils et sélectionnez **Importer un certificat Exchange**.
5. Tapez **\\lon-cas1\cert\certnew.cer** et cliquez sur **suivant**.
6. Dans la page **importer le certificate Exchange**, cliquez sur le signe **+**.
7. Sélectionnez LON-CAS1 et cliquez sur **ajouter**, puis sur **ok**.
8. Cliquez sur **terminer**.
9. Vérifiez que mail.adatum.com apparaît dans la liste.
10. Cliquez sur **mail.adatum.com**, puis cliquez sur l'icône en forme de crayon dans la barre d'outils.
11. Cliquez sur **Services**.
12. Sélectionnez **IIS** et cliquez sur **enregistrer**.

Résultats : À la fin de cet exercice, les stagiaires auront installé un certificat sur le serveur d'accès au client Exchange Server.

Exercice 2 : Configuration des options des services d'accès au client

▶ Tâche 1 : Configurer les options du serveur d'accès au client

1. Dans le CAE, sur LON-CAS1, cliquez sur **Serveurs** dans le volet gauche.
2. Dans le volet central, cliquez sur **Répertoires virtuels** dans la barre d'outils.
3. Dans la liste Sélectionner le serveur, cliquez sur **LON-CAS1.Adatum.com**.
4. Cliquez sur l'icône représentant une clé mécanique dans la barre d'outils.
5. Dans la fenêtre configurer le domaine d'accès externe, cliquez sur le signe **+**.
6. Cliquez sur **LON-CAS1**, puis sur le bouton **ajouter**, puis sur **ok**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Dans la zone de texte située sous la mention Entrer le nom de domaine, tapez **mail.adatum.com**, puis cliquez sur **enregistrer**.
8. Une fois l'opération terminée, cliquez sur **fermer**.
9. Dans le volet central, cliquez sur Serveurs.
10. Cliquez sur **LON-CAS1**, puis sur l'icône représentant un crayon dans la barre d'outils.
11. Dans le volet de navigation gauche, cliquez sur **POP3**.
12. Définissez la **Méthode de connexion** sur **Sécuriser la connexion TLS**.
13. Faites défiler l'écran et sélectionnez **Options supplémentaires**.
    - Définissez Nombre maximal de connexions sur **100**.
    - Définissez Nombre maximal de connexions à partir d'une seule adresse IP sur **20**.
    - Définissez Nombre maximal de connexions pour un seul utilisateur sur **2**.
14. Cliquez sur **enregistrer**.
15. Cliquez sur **ok** dans la fenêtre d'avertissement.

▶ Tâche 2 : Vérifier les options d'authentification sur le serveur d'accès au client

1. Sur LON-CAS1, dans le Centre d'administration Exchange, dans le nœud des serveurs, cliquez sur **Répertoires virtuels**.
2. Passez en revue la liste des répertoires virtuels pour LON-CAS1.
3. Cliquez sur le répertoire virtuel **Autodiscover**, puis sur l'icône représentant un crayon dans la barre d'outils.
4. Dans la fenêtre Répertoire virtuel – Windows Internet Explorer, cliquez sur **Authentification**.
5. Examinez les options prises en charge et sélectionnées pour l'authentification.
6. N'effectuez aucune modification, puis cliquez sur **annuler**.
7. Cliquez sur Répertoire virtuel ecp, puis cliquez sur l'icône représentant un crayon dans la barre d'outils.
8. Examinez les options prises en charge et sélectionnées pour l'authentification.
9. N'effectuez aucune modification, puis cliquez sur **annuler**.
10. Cliquez sur le répertoire virtuel **PowerShell**, puis sur l'icône représentant un crayon dans la barre d'outils.
11. Dans la fenêtre Répertoire virtuel – Windows Internet Explorer, cliquez sur **Authentification**.
12. Examinez les options prises en charge et sélectionnées pour l'authentification.
13. N'effectuez aucune modification, puis cliquez sur **annuler**.
14. Cliquez sur Répertoire virtuel **Microsoft-Server-ActiveSync**, puis sur l'icône représentant un crayon dans la barre d'outils.
15. Dans la fenêtre **Répertoire virtuel – Windows Internet Explorer**, cliquez sur **Authentification**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Examinez les options prises en charge et sélectionnées pour l'authentification. Notez que les options d'authentification des certificats sont présentes dans ce répertoire virtuel.
17. N'effectuez aucune modification, puis cliquez sur **annuler**.
18. Cliquez sur le répertoire virtuel **OAB**, puis cliquez sur l'icône représentant un crayon dans la barre d'outils.
19. Dans la fenêtre **Répertoire virtuel – Windows Internet Explorer**, notez qu'il n'y a aucune option d'authentification pour ce répertoire virtuel.
20. N'effectuez aucune modification, puis cliquez sur **annuler**.

Résultats : À la fin de cet exercice, les stagiaires auront configuré le serveur d'accès au client.

Exercice 3 : Configuration des infos-courrier personnalisées

▶ Tâche 1 : Configurer des infos-courrier

1. Sur LON-CAS1, dans le CAE, cliquez sur **Destinataires**, puis sur **Boîtes aux lettres**.
2. Dans la liste des boîtes aux lettres, cliquez sur **April Reagan**, puis sur l'icône **Modifier** dans la barre d'outils.
3. Dans la fenêtre April Reagan, cliquez sur **Info courrier**.
4. Dans la zone de texte, tapez **Info-courrier de test pour April**, puis cliquez sur **enregistrer**.
5. Sur l'écran Accueil, cliquez sur l'environnement de ligne de commande **Exchange Management Shell**.
6. Tapez la commande suivante et appuyez sur Entrée :

```
Set-Mailbox –Identity Aidan –Mailtip “c'est info-courrier en français” –
MailtipTranslation (“DE: Dies ist die deutsche Sprache”)
```

7. Fermez la fenêtre Windows PowerShell.

▶ Tâche 2 : Tester les infos-courrier

1. Ouvrez Internet Explorer et tapez **https://lon-cas1.adatum.com/owa**.
2. Déconnectez-vous si nécessaire, et connectez-vous en tant qu'**ADATUM\Don** avec le mot de passe **Pa$$w0rd**.
3. Dans la page **Langue et fuseau horaire**, sélectionnez **français (France)**, ne modifiez pas le fuseau horaire, puis cliquez sur **enregistrer**.
4. Dans la fenêtre Outlook Web App, cliquez sur **nouveau message**.
5. Dans le champ **À**, tapez **April** et appuyez sur **Tab**. Vérifiez que la valeur du champ est **April Reagan**.
6. Cliquez dans le champ **Objet**. Vérifiez que l'info-courrier apparaît.
7. Cliquez sur **IGNORER**, puis sur **ignorer Ce message sera supprimé** à nouveau.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

8. Dans la fenêtre **Outlook Web App**, cliquez sur **nouveau message**.
9. Dans le champ **À**, tapez **Aidan** et appuyez sur **Tab**. Vérifiez que le champ prend la valeur **Aidan Delaney**.
10. Cliquez dans le champ **Objet**. Vérifiez que l'**info-courrier** s'affiche et qu'elle est en **Français**.
11. Déconnectez-vous d'OWA.
12. Connectez-vous en tant qu'**ADATUM\Amr** avec le mot de passe Pa$$w0rd.
13. Dans la page **Langue et fuseau horaire**, sélectionnez **Deutsch (Deutschland)**, ne modifiez pas le fuseau horaire, puis cliquez sur **enregistrer**.
14. Dans la fenêtre Outlook Web App, cliquez sur **Neue E-Mail**.
15. Dans le champ **An**, tapez **Aidan** et appuyez sur **Tab**. Vérifiez que le champ prend la valeur **Aidan Delaney**.
16. Cliquez dans le champ **Betreff**. Vérifiez que l'**info-courrier** s'affiche et qu'elle est en **allemand**.
17. Cliquez sur **VERWERFEN**, puis sur **Verwerfen Diese Nachricht wird gelöscht à nouveau**.
18. Déconnectez-vous.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1** et **22341B-LON-MBX1**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 5: Planification et configuration de la connectivité pour les clients de messagerie

Atelier pratique : Planification et configuration de la connectivité pour les clients de messagerie

Exercice 1 : Planification de la connectivité des clients

▶ Tâche 1 : Lisez et analysez les exigences du scénario

- Lisez le scénario de l'exercice, et analysez les exigences du point de vue de la sécurité et d'une fonctionnalité. Identifiez les technologies qui devraient être utilisées.

▶ Tâche 2 : Proposer une solution pour la connectivité client

1. Quelles plateformes clientes doivent être prises en charge pour les clients internes ?

   Pour les clients internes, vous devez prendre en charge le système d'exploitation Windows 8, Outlook 2003 et Outlook 2010. Cependant, puisqu'Outlook 2003 n'est pas pris en charge par Exchange Server 2013, il ne peut pas être inclus dans votre plan client de connectivité.

2. Quelles plateformes clientes doivent être prises en charge pour les clients externes ?

   Pour les clients externes, vous devez prendre en charge Windows 8 et Outlook 2010 pour les ordinateurs portables, avec les plateformes mobiles Windows Phone 7.5, Windows Phone 8, iOS5 et Android 4.0.

3. Quels problèmes avez-vous avec les clients internes ?

   Le plus grand souci pour les clients internes est le fait qu'il n'y a aucun logiciel client du courrier électronique unique sur les ordinateurs clients.

4. Quels problèmes avez-vous avec les clients externes ?

   Le plus grand souci pour les clients externes est la sécurité. Vous devez prendre en charge des plateformes multiples se connectant de différents emplacements tout en respectant les exigences de sécurité.

5. Comment allez-vous répondre aux exigences en matière de chiffrement de connexion cliente ?

   Les connexions clientes sur le serveur d'accès au client seront chiffrées à l'aide de SSL.

6. Quelle solution allez-vous proposer pour les clients internes ?

   Les clients Outlook 2010 sont pris en charge par défaut. Toutefois, les clients qui exécutent Outlook 2003 ne peuvent pas se connecter à Exchange Server 2013. Pour ces clients, et pour les clients sans logiciel Outlook, vous pouvez proposer deux solutions :

   a. Utiliser l'interface Outlook Web App pour accéder à leur boîte aux lettres.

   b. Utilisez le client de courrier électronique intégré dans Windows 8 pour accéder à leur boîte aux lettres à l'aide du protocole ActiveSync.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Quelle solution allez-vous proposer pour les clients externes ?

   Les clients externes disposant d'ordinateurs portables utiliseront Outlook Anywhere, tandis que les clients sans ordinateur portable peuvent utiliser l'interface Outlook Web App. Les clients équipés de smartphones peuvent se connecter à l'aide du protocole ActiveSync si le système d'exploitation de l'appareil le prend en charge.

8. Comment allez-vous répondre aux exigences en matière de téléchargement de pièces jointes sur les ordinateurs publics ?

   Les clients qui se connectent à partir d'ordinateurs publics utiliseront Outlook Web App. Pour les empêcher de télécharger et d'enregistrer des pièces jointes, vous pouvez implémenter la stratégie Outlook Web App.

9. Comment allez-vous appliquer les exigences en matière de sécurité pour les appareils mobiles ?

   Les exigences de sécurité pour les appareils mobiles peuvent être appliquées en implémentant des stratégies ActiveSync. Windows Phone, iOS 5 et Android 4.0 prennent en charge les stratégies ActiveSync. Cependant, vous devez vérifier si les appareils Symbian peuvent prendre en charge les stratégies ActiveSync. Si ce n'est pas le cas, ils ne pourront pas se connecter.

10. Comment allez-vous déployer le certificat CA racine d'A. Datum sur les périphériques clients (les ordinateurs et les smartphones) ?

    Le certificat de l'autorité de certification racine est déployé sur les ordinateurs clients à l'aide de la stratégie de groupe. Si A. Datum a une autorité de certification d'entreprise implémentée, cette opération s'effectue par défaut. S'il s'agit d'une autorité de certification autonome, vous pouvez la déployer manuellement dans l'objet de stratégie de groupe. Pour les appareils mobiles, vous pouvez utiliser des utilitaires de configuration pour distribuer les certificats ou vous pouvez envoyer un fichier de certificat de l'autorité de certification racine dans un message électronique à tous les utilisateurs ayant un smartphone, avec des instructions sur la façon de l'importer.

11. Existe-t-il une manière de contrôler les fonctionnalités matérielles des appareils mobiles ?

    Exchange Server 2013 ne prend pas en charge de stratégies pour le contrôle de matériel sur les appareils mobiles.

12. Pouvez-vous implémenter une authentification basée sur des certificats pour les appareils mobiles ?

    Actuellement, l'authentification basée sur les certificats est prise en charge de manière sélective. Vous devez vérifier auprès des fournisseurs de plateformes mobiles pour voir si cette fonctionnalité est prise en charge.

13. Comment comptez-vous implémenter les exigences pour supprimer le contenu d'un appareil mobile perdu ?

    Pour supprimer le contenu d'un appareil mobile perdu, vous devez apprendre aux utilisateurs à utiliser la fonctionnalité d'effacement à distance disponible dans l'interface Exchange Outlook Web App.

▶ Tâche 3 : Présenter la solution à la classe

- Présentez la solution que vous proposez. Discutez des solutions alternatives avec les autres stagiaires et l'instructeur.

Résultats : À la fin de cet exercice, les stagiaires auront créé un plan pour la connectivité client.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Exercice 2 : Configuration d'Outlook Web App et d'Outlook Anywhere

▶ Tâche 1 : Configuration des stratégies Outlook Web App

1. Sur LON-CAS1, sur l'écran d'accueil, cliquez sur **Internet Explorer**.
2. Accédez à **https://lon-cas1.adatum.com/ecp**.
3. Connectez-vous au **CAE** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Dans la fenêtre **CAE**, cliquez sur **Autorisations** dans le volet de navigation gauche.
5. Dans le volet central, cliquez sur **Stratégies Outlook Web App**.
6. Cliquez sur l'icône **Nouveau**.
7. Dans la section **nouvelle stratégie de boîte aux lettres Outlook Web App**, tapez **Stratégie des utilisateurs externes** dans la zone de texte **Nom de la stratégie**.
8. Dans la section **Gestion de la communication**, désactivez les cases à cocher **Message instantané** et **Messagerie texte**.
9. Faites défiler l'écran et cliquez sur **Options supplémentaires**.
10. Dans la section **Gestion des informations**, désactivez la case à cocher **Récupérer les éléments supprimés**.
11. Dans la section **Ordinateur public ou partagé**, désactivez la case à cocher **Accès direct au fichier**.
12. Cliquez sur **enregistrer**.
13. Dans la console CAE, cliquez sur **Destinataires**.
14. Double-cliquez sur **Adam Barr**.
15. Dans la fenêtre **Adam Barr**, cliquez sur **Fonctionnalités de boîte aux lettres** dans le volet de navigation gauche. Dans la boîte de dialogue avertissement, cliquez sur **ok**.
16. Dans le volet droit, faites défiler l'écran jusqu'à la section **Connectivité de messagerie** et cliquez sur **Afficher les détails**.
17. Dans la fenêtre **Stratégie de boîte aux lettres Outlook Web App**, cliquez sur **parcourir...**.
18. Sélectionnez **Stratégie des utilisateurs externes**, cliquez sur **ok**, puis sur **enregistrer** à deux reprises.
19. Cliquez sur le menu Démarrer, puis sur l'**Exchange Management Shell**.
20. Tapez la commande suivante : **Set-CASMailbox –identity Aidan@adatum.com –OwaMailboxPolicy:"Stratégie des utilisateurs externes"**, puis appuyez sur Entrée.
21. Dans Internet Explorer, dans le **Centre d'administration Exchange**, cliquez sur **Destinataires** puis, dans le volet central, double-cliquez sur l'utilisateur **Brad Sutton**.
22. Dans la fenêtre **Brad Sutton**, dans l'onglet **Général**, cliquez sur **Options supplémentaires**.
23. Dans la section **Attributs personnalisés**, cliquez sur **Modifier**.
24. Dans la zone de texte **1 :** tapez **externe** et cliquez sur **ok**, puis sur **enregistrer**.
25. Répétez les étapes 21 à 24 pour les utilisateurs nommés **Chad Niswonger** et **Daniel Durrer**.

26. Basculez vers l'environnement de ligne de commande **Exchange Management Shell** et tapez : **get-mailbox –filter {CustomAttribute1 –eq "externe"} | Set-CASMailbox -OwaMailboxPolicy: "Stratégie des utilisateurs externes"**, puis appuyez sur Entrée.
27. Rebasculez vers le **CAE**.
28. Double-cliquez sur **Brad Sutton**.
29. Dans la fenêtre **Brad Sutton**, cliquez sur **Fonctionnalités de boîte aux lettres**. Si un message d'avertissement s'affiche, cliquez sur **OK**.
30. Dans le volet droit, faites défiler l'écran jusqu'à la section **Connectivité de messagerie** et cliquez sur **Afficher les détails**.
31. Vérifiez que la **Stratégie des utilisateurs externes** est appliquée.
32. Cliquez deux fois sur **annuler**.
33. Répétez les étapes 28 à 32 pour les utilisateurs **Chad Niswonger** et **Daniel Durrer**.

▶ Tâche 2 : Configuration d'Outlook Anywhere

1. Sur LON-CAS1, dans le **Centre d'administration Exchange**, cliquez sur **Serveurs** dans le volet de navigation gauche.
2. Dans le volet central, double-cliquez sur **LON-CAS1**.
3. Dans la fenêtre **LON-CAS1**, cliquez sur **Outlook Anywhere**.
4. Dans la première zone de texte, tapez **mail.adatum.com**.
5. Assurez-vous que la deuxième zone de texte contient la valeur **lon-cas1.adatum.com** et que la troisième contient la valeur **Négocier**.
6. Sélectionnez **NTLM** dans la troisième option.
7. Cliquez sur **enregistrer**.

▶ Tâche 3 : Activation et utilisation d'Outlook Web App hors connexion

1. Sur LON-CL1, cliquez sur le Bureau, ouvrez Internet Explorer et tapez **https://lon-cas1.adatum.com/owa**.
2. Connectez-vous en tant qu'**ADATUM\Aidan** avec le mot de passe **Pa$$w0rd**. Cliquez sur **enregistrer**.
3. Dans la fenêtre **Outlook Web App**, ouvrez le menu **Paramètres** en regard du nom d'utilisateur dans l'angle droit du navigateur, cliquez sur **Paramètres hors connexion**, sur **Activer l'accès hors connexion**, puis sur **OK**.
4. Cliquez sur **Suivant** à deux reprises et appuyez sur **Ctrl + D**.
5. Dans la boîte de dialogue **Ajouter un favori**, cliquez sur **Ajouter**.
6. Déconnectez-vous d'Outlook Web App et fermez Internet Explorer.
7. Sur votre ordinateur hôte, ouvrez le **Gestionnaire Hyper-V**.
8. Cliquez avec le bouton droit sur l'ordinateur **22341B-LON-CL1** et sélectionnez **Paramètres**.
9. Cliquez sur **Carte réseau** puis, dans la zone déroulante Réseau, sélectionnez **Non connecté**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Cliquez sur **OK**. Vous déconnectez ainsi temporairement votre client du réseau.
11. Basculez vers l'ordinateur virtuel **22341B-LON-CL1**.
12. Ouvrez Internet Explorer et sélectionnez **Aidan Delaney - Outlook Web App** dans le menu Favoris.
13. Quand la fenêtre Outlook Web App s'ouvre, vérifiez que vous pouvez accéder au contenu de la boîte aux lettres.
14. Envoyez un message électronique de test à administrateur@adatum.com.
15. Sur votre ordinateur hôte, basculez vers le **Gestionnaire Hyper-V**.
16. Cliquez avec le bouton droit sur l'ordinateur **22341B-LON-CL1** et sélectionnez **Paramètres**.
17. Cliquez sur **Carte réseau** puis, dans la zone déroulante Réseau, sélectionnez **Réseau privé**. Cliquez sur **OK**.
18. Patientez 20 à 30 secondes, puis actualisez la fenêtre Outlook Web App. Si la fenêtre Alerte de sécurité s'affiche, cliquez sur **Oui**, puis actualisez la fenêtre Outlook Web App.
19. Sur LON-CAS1, ouvrez **https://lon-cas1.adatum.com/owa** et connectez-vous en tant qu'**Administrateur**.
20. Vérifiez que vous avez reçu le courrier électronique d'Aidan envoyé depuis Outlook Web App hors connexion.

Résultats : À la fin de cet exercice, les stagiaires auront configuré Outlook Web App et Outlook Anywhere.

Exercice 3 : Configuration d'Exchange ActiveSync

▶ Tâche 1 : Planifier le déploiement d'appareil mobile

- Sachant que de nombreuses plateformes de périphérique accéderont au serveur Exchange Server, quels sont les problèmes majeurs ?

  Le principal problème concernant les différentes plateformes d'appareil est leur capacité à prendre en charge des stratégies Exchange. Du point de vue de la sécurité, vous devez pouvoir forcer les exigences en matière de mot de passe pour les appareils mobiles.

- Comment allez-vous faire pour que les paramètres soient cohérents sur chaque appareil mobile ?

  Vous pouvez implémenter une stratégie de boîte aux lettres d'appareil mobile pour obtenir des paramètres cohérents.

- Comment allez-vous implémenter les exigences en matière de mot de passe sur votre appareil mobile ?

  Vous devez appliquer des exigences en matière de mot de passe sur tous les appareils qui se connectent à Exchange en implémentant la stratégie appropriée.

- Comment allez-vous implémenter les exigences en matière de mise en quarantaine ?

  Les configurations requises pour la mise en quarantaine peuvent être implémentées en configurant les options d'accès d'appareil mobile dans le Centre d'administration Exchange.

▶ Tâche 2 : Configurer les stratégies de boîte aux lettres pour les appareils mobiles

1. Sur **LON-CAS1**, basculez vers Internet Explorer et, dans le Centre d'administration Exchange, cliquez sur **Mobile**, puis sur **Stratégies de boîte aux lettres de périphérique mobile**.
2. Cliquez sur l'icône **Nouveau**.
3. Dans la fenêtre de stratégie de boîte aux lettres de périphérique mobile, tapez **Adatum Mobiles** comme nom de stratégie.
4. Activez la case à cocher **Il s'agit de la stratégie par défaut**.
5. N'activez pas la case à cocher **Autoriser la synchronisation des périphériques mobiles qui ne prennent pas entièrement en charge ces stratégies**.
6. Activez la case à cocher **Exiger un mot de passe**.
7. Activez la case à cocher **Mot de passe alphanumérique requis**.
8. Sélectionnez **2** dans la zone déroulante appelée **Le mot de passe doit comporter les jeux de caractères suivants**.
9. Activez la case à cocher **Longueur minimale du mot de passe** et tapez **5** dans la zone de texte.
10. Activez la case à cocher **Nombre d'échecs de connexion avant réinitialisation du périphérique** et tapez **4** dans la zone de texte.
11. Activez la case à cocher **Exiger une connexion lorsque le périphérique est resté inactif pendant** et tapez **5** dans la zone de texte.
12. Cliquez sur **enregistrer**.

▶ Tâche 3 : Configurer les règles d'accès des appareils

1. Sur **LON-CAS1**, dans le Centre d'administration Exchange, cliquez sur **Mobile**, puis sur **Accès au périphérique mobile**.
2. Cliquez sur le bouton **modifier**.
3. Dans la fenêtre **Paramètres d'accès Exchange ActiveSync**, cliquez sur **Mise en quarantaine – Me laisser choisir de bloquer ou d'autoriser plus tard**.
4. Dans la section **Mettre en quarantaine les messages électroniques de notification**, cliquez sur l'icône **Ajouter**.
5. Dans la fenêtre **Sélectionner des administrateurs**, sélectionnez **Administrateur**, cliquez sur **ajouter**, puis sur **ok**.
6. Dans la zone de texte ci-dessous, tapez le texte suivant : **Votre appareil est temporairement en quarantaine**. **L'administrateur examinera votre demande et autorisera ou bloquera votre connexion selon la stratégie**.
7. Cliquez sur **enregistrer**.
8. Dans le volet Règles d'accès aux périphériques, cliquez sur l'icône **Nouveau**.
9. Dans **nouvelle règle d'accès au périphérique**, dans la section **Famille d'appareils** cliquez sur **parcourir...**.
10. Dans la fenêtre **Famille d'appareils**, cliquez sur **Toutes les familles**, puis sur **ok**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION PRIVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

11. Sous la section **Uniquement ce modèle**, cliquez sur **parcourir...**. Vérifiez qu'aucun appareil n'est répertorié, puis cliquez sur **annuler**. Dans un environnement de production, vous pouvez vous attendre à voir plusieurs modèles répertoriés.
12. Dans la fenêtre **Nouvelle règle d'accès aux appareils**, cliquez sur **Mise en quarantaine – Me laisser choisir de bloquer ou d'autoriser plus tard**.
13. Cliquez sur **annuler**.

Résultats : À la fin de cet exercice, les stagiaires auront configuré les options et les stratégies d'appareil mobile.

Exercice 4 : Publication d'Exchange Server 2013 via TMG 2010

▶ Tâche 1 : Publier des services Web Exchange via TMG 2010

1. Sur **LON-CAS1**, ouvrez **Windows PowerShell** à partir de la barre des tâches, tapez **mmc.exe** et appuyez sur Entrée.
2. Dans la fenêtre **Console1**, ouvrez le menu **Fichier** et cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
3. Cliquez sur **Certificats**, puis sur **Ajouter**. Sélectionnez **Un compte d'ordinateur**, puis cliquez sur **Suivant**.
4. Sélectionnez **L'ordinateur local**, puis cliquez sur **Terminer**. Cliquez sur **OK**.
5. Développez **Certificats**, **Personnel**, puis cliquez sur **Certificats**.
6. Cliquez avec le bouton droit sur le certificat **Webmail.adatum.com**, allez dans **Toutes les tâches**, puis sélectionnez **Exporter**.
7. Dans la **Bienvenue**, cliquez sur **Suivant**.
8. Dans la page **Exporter la clé privée**, sélectionnez **Oui, exporter la clé privée** et cliquez sur **Suivant**.
9. Dans la page **Format du fichier d'exportation**, cliquez sur **Suivant**.
10. Dans la page **Sécurité**, sélectionnez **Mot de passe** et tapez **Pa$$w0rd** dans les deux champs. Cliquez sur **Suivant**.
11. Dans la page **Fichier à exporter**, tapez **C:\CAS1.pfx** comme nom de fichier et cliquez sur **Suivant**.
12. Cliquez sur **Terminer**. Dans la fenêtre contextuelle, cliquez sur **OK**. Fermez **Console1** et cliquez sur **Non** à l'invite **Enregistrer les paramètres de la console dans Console1 ?**.
13. Basculez vers l'ordinateur LON-TMG.
14. Sur **LON-TMG**, cliquez sur **Démarrer**. Dans la zone **Rechercher**, tapez **MMC** et appuyez sur Entrée.
15. Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
16. Dans la page **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **Certificats**, puis sur **Ajouter**.
17. Cliquez sur **Un compte d'ordinateur**, puis sur **Suivant**, sur **Terminer**, et enfin sur **OK**.
18. Développez **Certificats**, cliquez avec le bouton droit sur **Personnel**, pointez sur **Toutes les tâches,** puis cliquez sur **Importer**.

19. Dans la page **Assistant Importation de certificat**, cliquez sur **Suivant**.
20. Dans la page **Fichier à importer**, tapez **\\LON-CAS1\C$\CAS1.pfx**, puis cliquez sur **Suivant**.
21. Dans la page **Mot de passe**, tapez **Pa$$w0rd** dans le champ **Mot de passe**, puis cliquez sur **Suivant**.
22. Dans la page **Magasin de certificats**, cliquez sur **Suivant**, puis sur **Terminer**.
23. Cliquez sur **OK**, puis fermez la **Console1** sans enregistrer les modifications.
24. Sur **LON-TMG**, cliquez sur **Démarrer**, pointez sur **Tous les programmes**, cliquez sur **Microsoft Forefront TMG**, puis sur **Gestion Forefront TMG**.
25. Développez **Forefront TMG (LON-TMG)**, puis cliquez sur **Stratégie de pare-feu**.
26. Dans le volet Tâches de stratégie de pare-feu, sous l'onglet **Tâches**, cliquez sur **Publier l'accès de client Web Exchange**.
27. Dans la page **Assistant Nouvelle règle de publication Exchange**, tapez **Règle OWA**, puis cliquez sur **Suivant**.
28. Dans la page **Sélectionnez les services**, dans la liste Version d'Exchange, cliquez sur **Exchange Server 2010**, activez la case à cocher **Outlook Web Access**, puis cliquez sur **Suivant**.
29. Dans la page **Type de publication**, cliquez sur **Suivant**.
30. Dans la page **Sécurité de connexion des serveurs**, vérifiez que l'option **Utiliser le protocole SSL pour se connecter au serveur Web publié ou à la batterie de serveurs** est configurée, puis cliquez sur **Suivant**.
31. Dans la page **Détails de publication internes**, dans la zone de texte **Nom de site local**, tapez **LON-CAS1.Adatum.com**, puis cliquez sur **Suivant**.
32. Dans la page **Informations sur les noms publics**, vérifiez que l'option **Ce nom de domaine (saisissez ci-dessous)** est configurée dans la liste déroulante Accepter les demandes pour. Dans la zone **Nom public**, tapez **webmail.Adatum.com**, puis cliquez sur **Suivant**.
33. Dans la page **Sélectionnez le port d'écoute**, cliquez sur **Nouveau**.
34. Dans la page **Assistant Nouveau port d'écoute Web**, tapez **Port d'écoute HTTPS**, puis cliquez sur **Suivant**.
35. Dans la page **Sécurité de la connexion client**, vérifiez que l'option **Requiert des connexions sécurisées SSL avec des clients** est sélectionnée, puis cliquez sur **Suivant**.
36. Dans la page **Adresses IP des ports d'écoute Web**, activez la case à cocher **Externe**, puis cliquez sur **Suivant**.
37. Dans la page **Certificats de port d'écoute SSL**, cliquez sur **Sélectionner un certificat**.
38. Dans la boîte de dialogue **Sélectionner un certificat**, cliquez sur **Webmail.adatum.com**, sur **Sélectionner**, puis sur **Suivant**.
39. Dans la page **Paramètres d'authentification**, acceptez la valeur par défaut **Authentification des formulaires HTML**, puis cliquez sur **Suivant**.
40. Dans la page **Paramètres d'authentification unique (SSO)**, tapez **Adatum.com** comme nom de domaine SSO, cliquez sur **Suivant**, puis cliquez sur **Terminer**.
41. Dans la page **Sélectionnez le port d'écoute**, cliquez sur **Suivant**.
42. Dans la page **Délégation de l'authentification**, acceptez la valeur par défaut **Authentification de base**, puis cliquez sur **Suivant**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

43. Dans la page **Ensembles d'utilisateurs**, acceptez la valeur par défaut, puis cliquez sur **Suivant**.
44. Dans la page **Fin de l'Assistant Nouveau Règle de publication Exchange**, cliquez sur **Terminer**.
45. Cliquez deux fois sur **Appliquer** pour appliquer les modifications, puis cliquez sur **OK** une fois les modifications appliquées.
46. Basculez vers l'ordinateur LON-CAS1.
47. Basculez vers Internet Explorer puis, dans le CAE, cliquez sur **Serveurs** dans le volet des fonctionnalités.
48. Cliquez sur l'onglet **Répertoires virtuels**.
49. Sur l'onglet des **Répertoires virtuels**, double-cliquez sur **owa (Default Web Site) – LON-CAS1**.
50. Dans la zone **URL externe**, tapez **https://webmail.adatum.com/owa**.
51. Cliquez sur **Authentification**, puis sur **Utiliser une ou plusieurs méthodes d'authentification standard**, puis cochez la case à cocher **Authentification de base**, et cliquez sur **enregistrer**. Lisez les informations dans la fenêtre qui s'affiche, et cliquez sur **ok**.
52. Sur l'onglet des **Répertoires virtuels**, double-cliquez sur **ecp (Default Web Site) – LON-CAS1**.
53. Dans la zone **URL externe**, tapez **https://webmail.Adatum.com/ecp**.
54. Cliquez sur **Authentification**, puis sur **Utiliser une ou plusieurs méthodes d'authentification standard**, puis cochez la case à cocher **Authentification de base**, et cliquez sur **enregistrer**.
55. Cliquez sur **oui** dans la fenêtre d'avertissement. Cliquez sur **ok**.
56. Ouvrez **Windows PowerShell**. À l'invite **PS**, tapez **IISReset /noforce**, puis appuyez sur Entrée.
57. Patientez jusqu'à ce que le service IIS redémarre.
58. Rebasculez vers l'ordinateur LON-TMG.
59. Dans la console **Forefront TMG**, double-cliquez sur **Règle OWA**.
60. Dans la fenêtre **Propriétés de Régle OWA**, cliquez sur l'onglet **Paramètres de l'application**.
61. Dans le champ **URL de fermeture de session du serveur publié**, tapez **/owa/logoff.owa**. (**Remarque :** En effet TMG 2010 n'a pas de règle de publication pour Exchange 2013, et la page de fermeture de session dirige encore les utilisateurs vers l'ancien emplacement utilisé par Exchange Server 2010).
62. Cliquez sur **OK**, puis sur **Appliquer** deux fois.
63. Cliquez sur **OK**.
64. Double cliquez sur **Règle OWA**.
65. Sur l'onglet **Général**, cliquez sur **Tester la règle**.
66. Dans la fenêtre **Résultats des tests des règles de publication Web**, recherchez les résultats pour **https://webmail.Adatum.com:443/ecp/** et **https://webmail.Adatum.com:443/OWA/**. Vous devez avoir des coches vertes pour ces URL. Cliquez sur **Fermer**, puis sur **OK**.

▶ Tâche 2 : Tests de règle de publication

1. Sur l'ordinateur hôte, dans le **Gestionnaire Hyper-V**, cliquez avec le bouton droit sur **22341B-LON-CL1**, puis cliquez sur **Paramètres**.
2. Cliquez sur **Carte réseau**, dans la liste déroulante **Réseau**, cliquez sur **Réseau privé 2**, puis cliquez sur **OK**.
3. Connectez-vous à LON-CL1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Sur LON-CL1, dans l'écran **Accueil**, tapez **Panneau de configuration**. Cliquez sur l'icône **Panneau de configuration**.
5. Ouvrez le **Panneau de configuration** et cliquez sur **Afficher l'état et la gestion du réseau**.
6. Cliquez sur **Modifier les paramètres de la carte**.
7. Cliquez avec le bouton droit sur **Ethernet**, puis cliquez sur **Propriétés**.
8. Cliquez sur **Protocole Internet version 4 (TCP/IP v4)**, puis sur **Propriétés**.
9. Remplacez l'adresse IP par **131.107.0.2**, remplacez la passerelle par défaut par **131.107.0.1.**
10. Supprimez la valeur du serveur DNS.
11. Cliquez sur **OK**, puis sur **Fermer**. Fermez le **Panneau de configuration**.
12. Dans l'écran **Accueil**, tapez **cmd** et appuyez sur Entrée.
13. Dans la fenêtre d'invite de commandes, tapez **notepad c:\windows\system32\drivers\etc\hosts**, puis appuyez sur **Entrée**.
14. En bas du fichier d'hôtes, tapez **131.107.0.1 webmail.adatum.com**, puis enregistrez et fermez le fichier.
15. Ouvrez **Internet Explorer** et connectez-vous à **https://webmail.adatum.com/owa**.
16. Ouvrez une session en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**, cliquez sur OK, puis vérifiez que vous accédez bien à la boîte aux lettres utilisateur.
17. Dans la fenêtre **Outlook Web App**, cliquez sur **Paramètres**, puis sur **Options**. Vérifiez que vous pouvez vous connecter aux options de votre boîte aux lettres.
18. Fermez Internet Explorer.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1, 22341B-LON-MBX1, 22341B-LON-TMG** et **22341B-LON-CL1**.

Résultats : À la fin de cet exercice, les stagiaires auront publié Exchange Server 2013 via TMG 2010.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 6 : Planification et implémentation de la haute disponibilité

Atelier pratique : Implémentation de la haute disponibilité

Exercice 1 : Création et configuration d'un groupe de disponibilité de base de données

▶ Tâche 1 : Préconfigurer l'objet de réseau de cluster pour un DAG

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans **Utilisateurs et ordinateurs Active Directory**, dans la barre de menus, cliquez sur **Affichage**, puis sur **Fonctionnalités avancées**.
3. Dans le volet gauche, développez **Adatum.com**, cliquez sur **Computers**, cliquez avec le bouton droit sur **Computers**, pointez sur **Nouveau**, puis cliquez sur **Ordinateur**.
4. Dans la boîte de dialogue **Nouvel objet – Ordinateur**, dans le champ **Nom de l'ordinateur**, tapez **DAG1**, puis cliquez sur **OK**.
5. Dans le volet droit, cliquez avec le bouton droit sur **DAG1**, puis cliquez sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés de : DAG1**, cliquez sur l'onglet **Sécurité**.
7. Dans l'onglet **Sécurité**, cliquez sur **Ajouter**, et dans le champ **Entrez les noms des objets à sélectionner**, tapez **Exchange Trusted Subsystem**. Cliquez sur **Vérifier les noms,** puis sur **OK**.
8. Dans l'onglet **Sécurité**, cliquez sur **Ajouter**, puis sur **Types d'objets**.
9. Dans la boîte de dialogue **Types d'objets**, activez la case à cocher **Ordinateur**, puis sur **OK**.
10. Dans la fenêtre **Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, dans le champ **Entrez les noms des objets à sélectionner**, tapez **LON-MBX1$**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
11. Dans l'onglet **Sécurité**, sélectionnez **LON-MBX1 (ADATUM\LON-MBX1$)**, puis dans la colonne **Autoriser** de la liste **Autorisations pour LON-MBX1**, cliquez sur **Contrôle total**.
12. Dans l'onglet **Sécurité**, sélectionnez **Exchange Trusted Subsystem (ADATUM\Exchange Trusted Subsystem)**, puis dans la colonne **Autoriser** de la liste **Autorisations pour Exchange Trusted Subsystem**, cliquez sur **Contrôle total**, puis sur **OK**.
13. Dans la fenêtre **Utilisateurs et ordinateurs Active Directory**, dans le volet droit, cliquez avec le bouton droit sur **DAG1**, puis cliquez sur **Désactiver le compte**.
14. Dans la fenêtre d'avertissement, cliquez sur **Oui**, puis cliquez sur **OK** dans la fenêtre d'informations suivante.

▶ Tâche 2 : Créer un DAG et y ajouter les serveurs de boîtes aux lettres

1. Basculez vers LON-CAS1. Ouvrez Internet Explorer, tapez **https://lon-cas1.adatum.com/ecp**, et appuyez sur Entrée.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans le Centre d'administration Exchange, dans le volet **Fonctionnalités**, cliquez sur **Serveurs**.
4. Sur les onglets, cliquez sur **Groupes de disponibilité de la base de données**, puis sur **Nouveau** dans la barre d'outils.
5. Dans la fenêtre **nouveau groupe de disponibilité de base de données**, dans le champ **Nom du groupe de disponibilité de la base de données**, tapez **DAG1**, puis cliquez sur **Serveur témoin** et tapez **LON-CAS1** dans le champ Serveur témoin. Cliquez sur **Répertoire témoin**, dans le champ **Répertoire témoin**, tapez **C:\FSWDAG1**, cliquez sur **Entrer une adresse IP** dans le champ **Adresse IP du groupe de disponibilité de base de données** et tapez **172.16.0.33**. Cliquez ensuite sur **Ajouter**, puis sur **enregistrer**.
6. Dans l'affichage de liste, cliquez sur **DAG1**, puis cliquez sur **gérer l'appartenance au groupe de disponibilité de base de données** dans la barre d'outils.
7. Dans la fenêtre **gérer l'appartenance au groupe de disponibilité de base de données**, cliquez sur **ajouter**.
8. Dans la fenêtre **Sélectionner un serveur**, cliquez sur **LON-MBX1**, cliquez sur **ajouter**, puis sur **LON-MBX2**. Cliquez sur **ajouter**, puis sur **ok**.
9. Dans la fenêtre **gérer l'appartenance au groupe de disponibilité de base de données**, cliquez sur **enregistrer**.
10. Dans la fenêtre **Enregistrement réussi**, cliquez sur **fermer**.

▶ Tâche 3 : Créer une copie de base de données de boîtes aux lettres

1. Dans le Centre d'administration Exchange, dans les onglets, cliquez sur **Bases de données**, sur **Mailbox Database 1** dans la barre d'outils, sur **Plus**, puis sur **Ajouter une copie de base de données**.
2. Dans la fenêtre **ajouter une copie de base de données de boîtes aux lettres**, cliquez sur **parcourir...**.
3. Dans la fenêtre **Sélectionner un serveur**, cliquez sur **LON-MBX2**, puis sur **ok**.
4. Dans la fenêtre **ajouter une copie de base de données de boîtes aux lettres**, cliquez sur **enregistrer**.
5. Attendez que l'enregistrement soit terminé, puis cliquez sur **fermer**.

▶ Tâche 4 : Vérifier la réussite de la copie d'une base de données

1. Dans les onglets, cliquez sur **Actualiser**, puis patientez jusqu'à ce que le volet d'informations marque la **Mailbox Database 1\LON-MBX2 comme Passif Sain**. Cela peut prendre plusieurs minutes et jusqu'à plusieurs heures selon la taille de la base de données.
2. Dans le volet d'informations, sous **Mailbox Database 1\LON-MBX2**, cliquez sur **Afficher les détails**.
3. Vérifiez que **État** affiche **Sain** et **État de l'index de contenu** affiche également **Sain**. Cliquez ensuite sur **annuler**. Notez que cette opération peut prendre un certain temps ; vous devez patienter.

▶ Tâche 5 : Interrompre et reprendre une copie de base de données

1. Dans le Centre d'administration Exchange, dans le volet d'informations, cliquez sur **Mailbox Database 1**, puis sous **Mailbox Database 1\LON-MBX2**, cliquez sur **Interrompre**.
2. Dans la fenêtre **Interrompre la copie de la base de données**, dans le champ **Commentaires**, tapez **Interruption test**, puis cliquez sur **enregistrer**. La copie de la base de données est maintenant interrompue et ne recevra aucune mise à jour.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans le volet d'informations, sous **Mailbox Database 1\LON-MBX2**, cliquez sur **Reprendre**. Si le bouton Reprendre n'est pas disponible, attendez, puis cliquez sur **Actualiser** plusieurs fois.
4. Dans la fenêtre d'avertissement, cliquez sur **oui**.
5. Dans les onglets, cliquez sur **Actualiser**, puis patientez jusqu'à ce que le volet d'informations marque **Mailbox Database 1\LON-MBX2** comme **Longueur de la file d'attente de copie : 0**.

Résultats : À la fin de cet exercice, les stagiaires auront préconfiguré un objet de réseau de cluster dans Active Directory, créé un DAG, ajouté deux serveurs de boîtes aux lettres au DAG et rendu une base de données hautement disponible. Les stagiaires auront aussi interrompu une copie de base de données et l'auront reprise.

Exercice 2 : Déploiement des serveurs d'accès au client hautement disponibles

▶ Tâche 1 : Installer la fonctionnalité d'équilibrage de la charge réseau sur des serveurs d'accès au client

1. Basculez vers **LON-CAS1**.
2. Dans la barre des tâches, cliquez sur l'icône Gestionnaire de serveur pour ouvrir le Gestionnaire de serveur.
3. Cliquez sur **Ajouter des rôles et des fonctionnalités**.
4. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, dans la page **Avant de commencer**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
7. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
8. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Équilibrage de la charge réseau**, et dans la fenêtre **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
9. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Dans **Assistant Ajout de rôles et de fonctionnalités**, attendez que l'installation des fonctionnalités se termine, puis cliquez sur **Fermer**.
11. Basculez vers l'ordinateur virtuel **LON-CAS2**.
12. Cliquez sur la vignette **Gestionnaire de serveur**.
13. Cliquez sur **Ajouter des rôles et des fonctionnalités**.
14. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, dans la page **Avant de commencer**, cliquez sur **Suivant**.
15. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.

UTILISATION PRIVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Dans la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
17. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
18. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Équilibrage de la charge réseau**. Dans la fenêtre **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
19. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
20. Dans **Assistant Ajout de rôles et de fonctionnalités**, attendez que l'installation des fonctionnalités se termine, puis cliquez sur **Fermer**.

▶ Tâche 2 : Créer un cluster de serveurs d'accès au client à charge équilibrée

1. Basculez vers **LON-CAS1**, et dans Gestionnaire de serveur, dans la barre de menus, cliquez sur **Outils**, puis dans la liste déroulante **Outils**, sélectionnez **Gestionnaire d'équilibrage de la charge réseau**.
2. Dans le Gestionnaire d'équilibrage de la charge réseau, dans la barre de menus, cliquez sur **Cluster**, puis sur **Nouveau**.
3. Dans la boîte de dialogue **Nouveau cluster : Connexion**, tapez **LON-CAS1** dans le champ **Hôte**, cliquez sur **Connexion**, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue **Nouveau cluster : Paramètres de l'hôte**, cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Nouveau cluster : Adresses IP de cluster**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Adresse IP**, tapez **172.16.0.6** comme Adresse IPv4, tapez **255.255.0.0** comme Masque de sous-réseau, et cliquez sur **OK**.
7. Dans la boîte de dialogue **Nouveau cluster : Adresses IP de cluster**, cliquez sur **Suivant**.
8. Dans la boîte de dialogue **Nouveau cluster : Paramètres de cluster**, dans la zone **Nom Internet complet**, tapez **webmail.adatum.com**, puis cliquez sur **Suivant**.
9. Dans la boîte de dialogue **Nouveau cluster : Règles de port**, cliquez sur **Terminer**.
10. Dans le Gestionnaire d'équilibrage de la charge réseau, patientez jusqu'à ce que l'icône **LON-CAS1** devienne verte.
11. Dans le volet gauche, cliquez avec le bouton droit sur **webmail.adatum.com (172.16.0.6)**, puis sur **Ajouter l'hôte au cluster**.
12. Dans la boîte de dialogue **Ajouter l'hôte au cluster : Connexion**, tapez **LON-CAS2** dans le champ **Hôte**, cliquez sur **Connexion**, puis sur **Suivant**.
13. Dans la boîte de dialogue **Ajouter l'hôte au cluster : Paramètres de l'hôte**, cliquez sur **Suivant**.
14. Dans la boîte de dialogue **Ajouter l'hôte au cluster : Règles de port**, cliquez sur **Terminer**.
15. Dans **Gestionnaire** d'équilibrage de la charge réseau, patientez jusqu'à ce que l'icône **LON-CAS2** devienne verte et que État indique **Convergé**.

▶ Tâche 3 : Créer un enregistrement DNS pour l'adresse IP virtuelle

1. Basculez vers **LON-DC1**, et dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Dans le Gestionnaire DNS, dans le volet gauche, développez **LON-DC1** si nécessaire, développez **Zones de recherche directes**, sélectionnez et cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la boîte de dialogue **Nouvel hôte**, dans le champ **Nom**, tapez **Webmail**, dans le champ **Adresse IP**, tapez **172.16.0.6**, puis cliquez sur **Ajouter un hôte**.
4. Cliquez sur **OK**, puis sur **Terminé**.

Résultats : À la fin de cet exercice, les stagiaires auront installé et configuré NLB et auront créé un enregistrement DNS pour leur adresse IP virtuelle à charge équilibrée.

Exercice 3 : Test de la configuration de la haute disponibilité

▶ Tâche 1 : Simuler une défaillance sur LON-CAS1 et vérifier la fonctionnalité Microsoft® Outlook Web Access

1. Basculez vers **LON-CAS1**, puis dans le Gestionnaire d'équilibrage de la charge réseau, dans le volet gauche, cliquez avec le bouton droit sur **LON-CAS1(Ethernet)**, cliquez sur **Hôte de contrôle**, puis sur **Arrêter**.
2. Basculez vers **LON-DC1**, ouvrez Internet Explorer, tapez sur **https://webmail.adatum.com/owa**, puis appuyez sur Entrée.
3. Connectez-vous à Outlook Web App en tant qu' **ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
4. Vous devez maintenant voir votre boîte de réception. Cela indique que LON-CAS2 sert actuellement de serveur d'accès au client.

▶ Tâche 2 : Activer LON-CAS1 et simuler une défaillance de LON-CAS2

1. Basculez vers le serveur virtuel LON-CAS1, et dans le Gestionnaire d'équilibrage de la charge réseau, dans le volet gauche, cliquez avec le bouton droit sur **LON-CAS1 (Ethernet)**, sur **Hôte de contrôle** et cliquez sur **Démarrer**.
2. Dans **Gestionnaire** d'équilibrage de la charge réseau, cliquez sur F5 jusqu'à ce que l'icône **LON-CAS1 (Ethernet)** devienne verte et que État indique **Activé**.
3. Basculez vers **Ordinateur hôte**, et dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22341B-LON-CAS2**, puis cliquez sur **Éteindre**. Cliquez sur **Éteindre**.
4. Basculez vers l'ordinateur virtuel LON-DC1. Dans Internet Explorer, cliquez sur **Actualiser (F5).**
5. Dans Outlook Web App, si la page de connexion apparaît, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
6. Dans Outlook Web App, dans le volet gauche, cliquez sur **Éléments envoyés** pour vérifier que Outlook Web App fonctionne toujours. Cela vérifie que LON-CAS1 a assumé le rôle serveur d'accès au client pour le client.

▶ Tâche 3 : Vérifier la haute disponibilité des copies de base de données

1. Basculez vers LON-CAS1 et, dans le Centre d'administration Exchange, cliquez sur **Serveurs**, puis, sur les onglets, sur **Bases de données**.
2. Dans l'affichage de liste, cliquez sur **Mailbox Database 1**, et dans le volet d'informations, vérifiez que la Mailbox Database 1\LON-MBX1 est Actif Monté et que la Mailbox Database 1\LON-MBX2 est Passif Sain.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Basculez vers **Ordinateur hôte**, et dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22341B-LON-MBX1**, puis cliquez sur **Éteindre**. Cliquez sur **Éteindre**.
4. Basculez vers l'ordinateur virtuel LON-CAS1. Dans Internet Explorer, cliquez sur **Actualiser (F5)**.

Remarque : Si une erreur s'affiche dans Internet Explorer, fermez le navigateur, rouvrez-le, puis reconnectez-vous au Centre d'administration Exchange.

5. Dans le Centre d'administration Exchange, si la page de connexion apparaît, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
6. Dans le Centre d'administration Exchange, dans le volet **Fonctionnalités**, cliquez sur **Serveurs**.
7. Sur les onglets, cliquez sur **Bases de données**, puis dans l'affichage de liste, cliquez sur **Mailbox Database 1**.
8. Vérifiez que, dans le volet d'informations, la Mailbox Database 1\LON-MBX1 est marquée comme Passif ServiceDown et que la Mailbox Database 1\LON-MBX2 est marquée comme Actif Monté.
9. Basculez vers l'ordinateur virtuel **LON-DC1**, et dans Internet Explorer et Outlook Web App, dans le volet gauche, cliquez sur **Boîte de réception**. Créez un message et envoyez-le pour vérifier que la boîte aux lettres est disponible et peut être utilisée.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-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 les ordinateurs **22341B-LON-CAS1**, **22341B-LON-CAS2**, **22341B-LON-MBX1** et **22341B-LON-MBX2**.

Remarque : Bien que certains serveurs ne soient pas en cours d'exécution, vous devez tout de même les rétablir.

Résultats : À la fin de cet exercice, les stagiaires auront testé leur configuration haute disponibilité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 7 : Planification et implémentation d'une solution de récupération d'urgence

Atelier pratique : Implémentation d'une solution de récupération d'urgence pour Exchange Server 2013

Exercice 1 : Sauvegarde d'Exchange 2013

▶ Tâche 1 : Remplir une boîte aux lettres avec Outlook Web App

1. Sur LON-CAS1, ouvrez Internet Explorer. Tapez **https://lon-cas1.Adatum.com/owa.**
2. Connectez-vous en tant qu'**Adatum\michael** avec le mot de passe **Pa$$w0rd**.
3. Dans la page relative à la langue et au fuseau horaire, cliquez sur **enregistrer**.
4. Cliquez sur **nouveau message**.
5. Dans la section **À**, tapez **Mark Bebbington**, sélectionnez **Rechercher dans les Contacts et le Répertoire**, puis tapez **Message avant la sauvegarde** dans la ligne Objet.
6. Cliquez sur **ENVOYER**.
7. Déconnectez-vous d'Outlook Web App.
8. Reconnectez-vous en tant qu'**Adatum\mark** avec le mot de passe **Pa$$w0rd**.
9. Dans la page relative à la langue et au fuseau horaire, cliquez sur **enregistrer**.
10. Vérifiez que le message est bien reçu.
11. Déconnectez-vous d'Outlook Web App.
12. Fermez Internet Explorer.
13. Basculez sur l'écran Accueil, et cliquez sur **Exchange Management Shell**.
14. Tapez la commande suivante, puis appuyez sur Entrée :

```
Get-Mailbox mark@ADatum.com |fl name,database,guid
```

    Notez le nom (Name) et le GUID (Guid) de la base de données de boîtes aux lettres. Cela est nécessaire pour la restauration.

15. Fermez Exchange Management Shell.

▶ Tâche 2 : Installer Sauvegarde Windows Server

1. Sur LON-MBX1, sur l'écran Accueil, cliquez sur **Gestionnaire de serveur**.
2. Dans le Tableau de bord, cliquez sur **Ajouter des rôles et des fonctionnalités**. L'**Assistant Ajout de rôles et de fonctionnalités** s'ouvre.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
4. Dans la page **Type d'installation**, sélectionnez **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
5. Dans la page **Sélection du serveur**, sélectionnez **Sélectionner un serveur du pool de serveurs**, dans **Pool de serveurs**, cliquez sur **LON-MBX1.Adatum.com**, puis sur **Suivant**.
6. Dans la page **Rôles de serveurs**, cliquez sur **Suivant**.
7. Dans la page **Fonctionnalités**, faites défiler la liste Fonctionnalités vers le bas, sélectionnez **Sauvegarde Windows Server**, puis cliquez sur **Suivant**.
8. Dans la page **Confirmation**, ne sélectionnez pas l'option **Redémarrer automatiquement le serveur de destination, si nécessaire**, puis cliquez sur **Installer**.
9. Dans la page **Résultats**, cliquez sur **Fermer**.

▶ Tâche 3 : Effectuer une sauvegarde d'une base de données de boîtes aux lettres à l'aide de Sauvegarde Windows Server

1. Sur LON-CAS1, ouvrez l'Explorateur de fichiers et créez un dossier nommé **Sauvegarde** sur le lecteur C:\.
2. Cliquez avec le bouton droit sur le dossier **Sauvegarde**, sélectionnez **Partager avec**, puis **Des personnes spécifiques**.
3. Vérifiez que le compte Administrateur a les autorisations en **Lecture/Écriture**, puis cliquez sur **Partager**. Cliquez sur **Terminé**.
4. Fermez l'Explorateur de fichiers.
5. Sur LON-MBX1, sur l'**écran Accueil**, cliquez sur **Outils d'administration**.
6. Faites défiler la liste des outils vers le bas et double-cliquez sur **Sauvegarde Windows Server**.
7. Dans le volet de navigation gauche, sélectionnez **Sauvegarde locale**.
8. À droite, dans le volet Actions, cliquez sur **Sauvegarde unique**.
9. Dans l'**Assistant Sauvegarde unique**, dans la page **Options de sauvegarde**, sélectionnez **Autres options**, puis cliquez sur **Suivant**.
10. Dans la page **Sélectionner la configuration de la sauvegarde**, sélectionnez **Serveur complet (recommandé)**, puis cliquez sur **Suivant**.
11. Dans la page **Spécifier le type de destination**, sélectionnez **Dossier partagé distant**, puis cliquez sur **Suivant**.
12. Dans la page **Spécifier un dossier distant**, sous **Emplacement**, tapez **\\LON-CAS1\Sauvegarde**, sous **Contrôle d'accès**, sélectionnez **Ne pas hériter**, puis cliquez sur **Suivant**.
13. Dans la fenêtre contextuelle de Sécurité de Windows, entrez **Administrateur** comme nom et **Pa$$w0rd** comme mot de passe, puis cliquez sur **OK**.
14. Dans la page **Confirmation**, cliquez sur **Sauvegarde**. Cette opération peut prendre 10 à 15 minutes.
15. Une fois la sauvegarde terminée, dans la page **Progression de la sauvegarde**, cliquez sur **Fermer**.
16. Fermez Sauvegarde Windows Server.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 4 : Supprimer un message d'une boîte aux lettres

1. Sur LON-CAS1, ouvrez Internet Explorer. Tapez **https://lon-cas1.ADatum.com/owa**.
2. Connectez-vous en tant qu'**Adatum\Mark** avec le mot de passe **Pa$$w0rd**.
3. Supprimez le message reçu de Michael.
4. Videz le dossier Éléments supprimés.
5. Cliquez avec le bouton droit sur le dossier **Éléments supprimés** et sélectionnez **récupérer les éléments supprimés**.
6. Dans la fenêtre **récupérer les éléments supprimés**, sélectionnez le message reçu de Michael, puis cliquez sur **vider**.
7. Cliquez sur **ok** pour confirmer l'action sur l'élément sélectionné.
8. Fermez la fenêtre **récupérer les éléments supprimés**.
9. Déconnectez-vous d'Outlook Web App.

Résultats : Après avoir terminé cet exercice, vous êtes parvenu à sauvegarder les bases de données de boîtes aux lettres.

Exercice 2 : Restauration de données Exchange Server 2013

▶ Tâche 1 : Restaurer la base de données à l'aide de la base de données Windows Server

1. Sur LON-MBX1, ouvrez l'Explorateur de fichiers et créez un dossier nommé **Restaurer** sur le lecteur C:\.
2. Sur l'écran Accueil, cliquez sur **Outils d'administration**.
3. Faites défiler la liste des outils vers le bas et double-cliquez sur **Sauvegarde Windows Server**.
4. Dans le volet **Actions**, cliquez sur **Récupérer**.
5. Dans l'**Assistant Récupération**, dans la page **Mise en route**, sélectionnez **Un autre emplacement**, puis cliquez sur **Suivant**.
6. Dans la page **Spécifier un type d'emplacement**, sélectionnez **Dossier partagé distant**, puis cliquez sur **Suivant**.
7. Dans la page **Spécifier un dossier distant**, tapez **\\LON-CAS1\Sauvegarde**, puis cliquez sur **Suivant**.
8. Dans la page **Sélectionner une date de sauvegarde**, sélectionnez la date et l'heure de la sauvegarde, et cliquez sur **Suivant**.
9. Dans la page **Sélectionner le type de récupération**, sélectionnez **Applications**, puis cliquez sur **Suivant**.
10. Dans la page **Sélectionner une application**, vérifiez que **Exchange** est sélectionné.

11. Sélectionnez **Ne pas exécuter une récupération de type restauration par progression des bases de données** et cliquez sur **Suivant**.
12. Dans la page **Spécifier les options de récupération**, sélectionnez **Restaurer à un autre emplacement**, puis cliquez sur **Parcourir**.
13. Dans la fenêtre **Rechercher un dossier**, sélectionnez le dossier **C:\Restaurer**, puis cliquez sur **OK**. Cliquez sur **Suivant**.
14. Dans la page **Confirmation**, cliquez sur **Récupérer**.
15. Dans la page **Statut de la récupération**, vérifiez que l'état de la récupération est **Terminé**, puis cliquez sur **Fermer**.
16. Fermez Sauvegarde Windows Server.

▶ Tâche 2 : Créer une base de données de récupération à l'aide de l'environnement de ligne de commande Exchange Management Shell

1. Sur LON-MBX1, cliquez sur l'écran Accueil, puis sur l'environnement de ligne de commande **Exchange Management Shell**.
2. Dans Exchange Management Shell, exécutez la commande suivante. Cette commande identifie le GUID de la base de données de boîtes aux lettres 1, ainsi que l'emplacement des fichiers journaux de base de données et de transactions.

```
Get-MailboxDatabase –ID “Mailbox Database 1” | fl name, guid, edbfilepath,
logfolderpath
```

3. Dans l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante pour créer la base de données de récupération, puis appuyez sur Entrée. Vérifiez que le GUID et les noms de journaux de base de données et de transactions correspondent au résultat de la commande précédente.

```
New-MailboxDatabase –Recovery –Name RecoveryDB –EdbFilePath “C:\Restaurer\3c32c739-
a0ce-43bc-a299-2f56f2bcb20c\C_\Program Files\Microsoft\Exchange
Server\V15\Mailbox\Mailbox Database 1808842331\Mailbox Database 1808842331.edb” –
LogFolderPath “C:\Restaurer\GUID\C_\Program Files\Microsoft\Exchange
Server\V15\Mailbox\Mailbox Database 1808842331” –Server LON-MBX1
```

4. À l'invite de commandes de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante, puis appuyez sur Entrée.

```
Restart-service msexchangeis
```

5. À l'invite de commandes de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante, puis appuyez sur Entrée.

```
CD “C:\Restaurer\3c32c739-a0ce-43bc-a299-2f56f2bcb20c\C_\Program
Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1808842331”
```

6. À l'invite de commandes de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante, puis appuyez sur Entrée.

```
Eseutil /r E00 /i /d
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. À l'invite de commandes de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante, puis appuyez sur Entrée.

```
Mount-Database RecoveryDB
```

8. À l'invite de commandes de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante, puis appuyez sur Entrée.

```
Get-MailboxStatistics -Database RecoveryDB
```

9. Cette applet de commande affiche toutes les boîtes aux lettres contenues dans la base de données de récupération. Vérifiez que la boîte aux lettres de Mark Bebbington fait bien partie de la liste.

▶ Tâche 3 : Récupérer une boîte aux lettres à partir de la base de données de récupération

1. À l'invite de commandes de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante, puis appuyez sur Entrée.

```
New-MailboxRestoreRequest –SourceDatabase RecoveryDB –SourceStoreMailbox “Mark
Bebbington” –TargetMailbox mark@adatum.com -SkipMerging StorageProviderForSource
```

2. À l'invite de commandes de l'environnement de ligne de commande Exchange Management Shell, tapez la commande suivante, puis appuyez sur Entrée.

```
Get-MailboxRestoreRequest
```

3. Répétez l'étape 2 jusqu'à ce que l'état soit **Completed**.
4. Sur LON-CAS1, démarrez Internet Explorer.
5. Tapez **https://lon-cas1.adatum.com/owa**.
6. Connectez-vous en tant qu'**Adatum\mark** avec le mot de passe **Pa$$w0rd**.
7. Vérifiez que le message a été restauré.
8. Déconnectez-vous d'Outlook Web App.
9. Fermez Internet Explorer.

Résultats : Après avoir terminé cet exercice, vous aurez restauré avec succès les éléments manquants dans les boîtes aux lettres des utilisateurs.

Exercice 3 : Récupération d'urgence dans Exchange Server 2013 (facultatif)

▶ Tâche 1 : Installation d'Exchange Server 2013 en mode de récupération de serveur

1. Sur LON-DC1, à partir du Gestionnaire de serveur, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console, cliquez sur **Computers**.
3. Dans le volet d'informations, cliquez avec le bouton droit sur le compte d'ordinateur LON-CAS2, puis cliquez sur **Réinitialiser le compte**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR ET UNIQUEMENT

4. Cliquez sur **Oui**, puis sur **OK**.
5. Sur votre hôte, dans le Gestionnaire Hyper-V, cliquez sur **22341B-LON-SVR1**, puis dans le volet Actions, cliquez sur **Démarrer**.
6. Dans le volet Actions, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
7. Connectez-vous en utilisant les informations d'identification suivantes :
   - Nom d'utilisateur : **Administrateur**
   - Mot de passe : **Pa$$w0rd**
8. Sur l'écran Accueil, cliquez sur **Gestionnaire de serveur**.
9. Dans l'arborescence de la console du **Gestionnaire de serveur**, cliquez sur **Serveur local**. En regard d'**Ethernet**, cliquez sur **172.16.0.30, Compatible IPv6**.
10. Cliquez avec le bouton droit sur **Ethernet**, puis cliquez sur **Propriétés**.
11. Cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur **Propriétés**.
12. Remplacez l'**Adresse IP** par **172.16.0.21** et le **Serveur DNS préféré** par **172.16.0.10**.
13. Cliquez sur **OK**, sur **Fermer**, puis fermez la fenêtre **Connexions réseau**.
14. Dans la vignette PROPRIÉTÉS, cliquez sur le lien en regard de **Nom de l'ordinateur**.
15. Dans la boîte de dialogue **Propriétés système**, dans l'onglet **Nom de l'ordinateur**, cliquez sur **Modifier**.
16. Dans **Nom de l'ordinateur**, tapez **LON-CAS2**. Sous **Membre d'un**, cliquez sur **Domaine**, puis tapez **adatum.com**. Cliquez sur **OK**.
17. Lorsque vous êtes invité à entrer un nom d'utilisateur et un mot de passe, tapez **Administrateur** et le mot de passe **Pa$$w0rd**, puis cliquez sur **OK**.
18. Lorsqu'une boîte de dialogue de bienvenue dans le domaine adatum.com, cliquez sur **OK**.
19. Lorsque le message vous invite à redémarrer votre ordinateur, cliquez sur **OK**.
20. Dans la boîte de dialogue **Propriétés système**, cliquez sur **Fermer**.
21. Lorsque vous êtes invité à redémarrer l'ordinateur, cliquez sur **Redémarrer maintenant**.
22. Toutes les étapes faisant référence à LON-CAS2 doivent être effectuées sur l'ordinateur virtuel renommé (précédemment LON-SVR1).
23. Ouvrez une session sur LON-CAS2 en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
24. Dans le Gestionnaire Hyper-V, ouvrez les paramètres de 22341B-LON-SVR1, et associez le fichier Exchange iso à partir de **D:\Programmes\Microsoft learning\22341\Drives\ ExchangeServer2013CU1.iso**.
25. Sur LON-CAS2, ouvrez une invite de commandes en tant qu'administrateur.
26. Tapez **D:** et appuyez sur Entrée.
27. Tapez la commande suivante, puis appuyez sur Entrée :

```
Setup.exe /m:RecoverServer /Iacceptexchangeserverlicenseterms
```

28. Une fois la configuration terminée, redémarrez le serveur.

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 il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-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 **22341B-LON-CAS1**, **22341B-LON-SVR1** et **22341B-LON-MBX1**.

Résultats : À la fin de cet exercice, vous aurez correctement récupéré LON-CAS2.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 8 : Planification et configuration du transport des messages

Atelier pratique : Planification et configuration du transport des messages

Exercice 1 : Configuration du transport des messages

▶ Tâche 1 : Configurer un connecteur d'envoi vers Internet

1. Sur LON-CAS1, ouvrez **Internet Explorer**, tapez **https://lon-cas1.adatum.com/ecp**, puis appuyez sur Entrée.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans le CAE, dans le volet des fonctionnalités, cliquez sur **Flux de messagerie**.
4. Cliquez sur l'onglet **Connecteurs d'envoi**.
5. Cliquez sur le bouton **Nouveau**.
6. Dans la fenêtre **nouveau connecteur d'envoi**, tapez **Envoi Internet** dans la zone de texte **Nom**.
7. Sélectionnez **Internet (par exemple, pour envoyer du courrier Internet)**, puis cliquez sur **suivant**.
8. Dans la page suivante de l'assistant, vérifiez que **Enregistrement MX associé au domaine du destinataire** est sélectionné et cliquez sur **suivant**.
9. Dans la page suivante de l'assistant, cliquez sur **Ajouter**.
10. Dans la fenêtre Ajouter un domaine, dans la zone de texte ***Nom de domaine complet (FQDN)**, tapez *****, cliquez sur **enregistrer**, puis cliquez sur **suivant**.
11. Dans la page suivante de l'assistant, cliquez sur **Ajouter**.
12. Sélectionnez LON-MBX1, cliquez sur le bouton **ajouter->** et cliquez sur **ok**.
13. Cliquez sur **terminer**.

▶ Tâche 2 : Configurer un connecteur de réception pour accepter le relais

1. Dans le Centre d'administration Exchange, cliquez sur l'onglet **Connecteurs de réception**.
2. Cliquez sur **Nouveau**.
3. Dans la fenêtre **nouveau connecteur de réception**, tapez **AppClient** dans la zone **Nom**, puis sélectionnez **Client**. Cliquez sur **suivant**.
4. Dans la page suivante, cliquez sur **Supprimer** pour supprimer l'étendue 0.0.0.0 – 255.255.255.255. Cliquez sur **Ajouter**.
5. Dans la fenêtre **ajouter une adresse IP**, tapez **172.16.0.10** et cliquez sur **enregistrer**.
6. Cliquez sur **terminer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

7. Cliquez sur **AppClient**, puis sur **Modifier**.
8. Cliquez sur **Sécurité**.
9. Activez la case à cocher **Utilisateurs anonymes**, puis cliquez sur **enregistrer**.

Résultats : À la fin de cet exercice, les stagiaires auront configuré le transport des messages.

Exercice 2 : Résolution des problèmes liés à la remise de messages

▶ Tâche 1 : Vérifiez que les messages provenant d'Internet peuvent être reçus

1. Sur LON-DC1, ouvrez Windows PowerShell dans la barre des tâches.
2. À l'invite de commandes, tapez **telnet LON-CAS1 smtp** et appuyez sur Entrée.
3. Tapez **helo** et appuyez sur Entrée.
4. Tapez **mail from: info@internet.com** et appuyez sur Entrée.

   Vous devriez recevoir la réponse : **250 2.1.0 Sender OK**
5. Tapez **rcpt to: Aidan@adatum.com** et appuyez sur Entrée.

   Réponse : **250 2.1.5 Recipient OK**.
6. Tapez **data** et appuyez sur Entrée.

   Réponse : **354 Start mail input; end with <CRLF>.<CRLF>**
7. Tapez **Test à partir d'Internet** et appuyez sur Entrée.
8. Appuyez sur la touche point (**.**), puis sur **Entrée**.
9. Tapez **Quit** et appuyez sur **Entrée**.
10. Basculez vers LON-CL1, puis connectez-vous en tant qu'**Adatum\Aidan** avec le mot de passe **Pa$$w0rd**.
11. Sur l'écran d'accueil, cliquez avec le bouton droit, cliquez sur **Toutes les applications**, puis sur **Outlook 2013**.
12. Dans la boîte de dialogue Bienvenue dans **Bienvenue dans Microsoft Outlook 2013**, cliquez sur **Suivant** trois fois, puis cliquez sur **Terminer**.
13. Si une invite concernant un certificat s'affiche, dans la boîte de dialogue **Alerte de sécurité**, cliquez sur **Oui**.
14. Dans la boîte de dialogue **Commençons par le début**, cliquez sur **Me demander plus tard**, puis sur **Accepter**.
15. Vérifiez que vous avez reçu un nouveau message d'info@internet.com.
16. Répondez au message avec le texte de votre choix, puis cliquez sur **Envoyer**.

▶ Tâche 2 : Résoudre les problèmes liés au transport des messages

1. Sur LON-MBX1, dans l'écran **Accueil**, cliquez sur **Exchange Toolbox**.
2. Dans la fenêtre Exchange Toolbox, double-cliquez sur **Afficheur des files d'attente**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la fenêtre **Afficheur des files d'attente**, vérifiez que le domaine **internet.com** est répertorié avec un message dans la file d'attente.
4. Double-cliquez sur **internet.com**
5. Cliquez avec le bouton droit sur le message **Aidan@adatum.com** et sélectionnez **Supprimer (avec rapport de non-remise).**
6. Cliquez sur **OK** dans la fenêtre Action en bloc, puis cliquez sur **Oui**.
7. Basculez sur l'ordinateur LON-CL1 et vérifiez que vous êtes toujours connecté en tant qu'Aidan.
8. Dans la fenêtre **Outlook 2013**, vérifiez que vous avez reçu un rapport de non-remise pour le message que vous avez envoyé à info@internet.com.

Résultats : À la fin de cet exercice, les stagiaires auront résolu des problèmes SMTP.

Exercice 3 : Configuration des règles de transport et des stratégies de prévention des pertes de données

▶ Tâche 1 : Implémentation et test d'une règle de transport d'exclusion

1. Sur LON-CAS1, dans le Centre d'administration Exchange, cliquez sur **Flux de messagerie** dans le volet des fonctionnalités.
2. Cliquez sur l'onglet **Règles**.
3. Cliquez sur **Nouveau**, puis sur **Créer une règle**.
4. Dans la fenêtre Nouvelle règle, dans la zone de texte **Nom**, tapez **Exclusion de responsabilité d'Adatum**.
5. Dans la zone déroulante ***Appliquer cette règle si...**, sélectionnez l'option **L'expéditeur se situe...**, puis dans la fenêtre **Sélectionner l'emplacement de l'expéditeur**, sélectionnez **Dans l'organisation**, puis cliquez sur **ok**.
6. Dans la zone déroulante ***Procédez comme suit...**, sélectionnez **Ajouter une exclusion de responsabilité...**.
7. Cliquez sur ***Entrer du texte**.
8. Dans **Spécifier le texte de la clause d'exclusion de responsabilité**, tapez **Ceci est la clause d'exclusion de responsabilité d'Adatum**, puis cliquez sur **ok**.
9. Cliquez sur ***Sélectionner un...**, puis dans la zone **Spécifier l'action de secours**, sélectionnez **Inclure dans un wrapper** et cliquez sur **ok**.
10. Cliquez sur **Plus d'options**.
11. Cliquez sur le bouton **ajouter une exception**. Dans la zone déroulante **Sauf si**, pointez sur **L'expéditeur**, puis cliquez sur **est membre de ce groupe**.
12. Dans la fenêtre **Sélectionner les membres**, cliquez sur **Administrateur** et cliquez sur **ajouter->**. Cliquez ensuite sur **ok**.

13. Basculez vers LON-CL1 et dans **Outlook 2013**, cliquez sur **Nouveau message electronique**.
14. Dans le champ **À**, tapez **administrateur@adatum.com**.
15. Dans le champ **Objet**, tapez **test d'exclusion de responsabilité**.
16. Dans le corps du message, tapez **Test**, puis cliquez sur **Envoyer**.
17. Ouvrez **Internet Explorer** et tapez **https://lon-cas1.adatum.com/owa**.
18. Dans la fenêtre Outlook Web App, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
19. Dans **Outlook Web App**, assurez-vous que vous avez reçu un message électronique d'Aidan et que le texte de la clause d'exclusion de responsabilité est ajouté aux messages.
20. Répondez à ce message avec un texte de votre choix.
21. Basculez vers Outlook 2013, assurez-vous que vous avez reçu le message d'Administrateur, mais sans l'exclusion de responsabilité.

▶ Tâche 2 : Créer une stratégie de prévention des pertes de données

1. Sur LON-CAS1, dans le Centre d'administration Exchange, cliquez sur **Gestion de la conformité** dans le volet des fonctionnalités.
2. Cliquez sur l'onglet **Prévention des pertes de données**.
3. Cliquez sur une flèche à côté du signe **+**.
4. Sélectionnez **Nouvelle stratégie DLP personnalisée**.
5. Dans la fenêtre **Nouvelle stratégie DLP personnalisée**, dans la zone de texte **Nom**, tapez **Bloc d'adresses IP**.
6. Cliquez sur **Appliquer**, puis sur **enregistrer**.
7. Sélectionnez **Bloc d'adresses IP**, puis cliquez sur **Modifier**.
8. Dans la fenêtre Bloc d'adresses IP, cliquez sur **Règles**.
9. Cliquez sur une flèche en regard du signe **+**, puis sélectionnez **Bloquer les messages dont le contenu est sensible**.
10. Dans la fenêtre **Nouvelle règle**, cliquez sur **Hors de l'organisation**. Dans la fenêtre de sélection de l'emplacement du destinataire, sélectionnez **Dans l'organisation**, puis cliquez sur **ok**.
11. Cliquez sur **Sélectionner des types d'informations sensibles**.
12. Dans les fenêtres des types d'informations sensibles, cliquez sur **Ajouter**.
13. Faites défiler la liste et sélectionnez **Adresse IP**, puis cliquez sur **ajouter->**. Cliquez deux fois sur **ok**.
14. Dans la zone déroulante ***Procédez comme suit...**, sélectionnez **Générer un rapport d'incident et l'envoyer à**, puis cliquez sur ***Sélectionner un...**.
15. Dans la liste, sélectionnez **Administrateur** et cliquez sur **ok**.
16. Cliquez sur **Bloquer le message**.
17. Dans **notifier l'expéditeur à l'aide d'un Conseil de stratégie**, tapez **Le message est bloqué** dans la zone de texte **Saisissez le message d'échec de remise que les utilisateurs recevront**, puis cliquez sur **ok**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

18. Cliquez sur ***Inclure les propriétés du message**, puis dans la fenêtre **Inclure les propriétés du message**, activez la case à cocher **courrier original** et cliquez sur **ok**.
19. Dans **Bloc d'adresses IP**, cliquez sur **enregistrer**.

▶ Tâche 3 : Vérifier la fonctionnalité Stratégie de prévention des pertes de données

1. Basculez vers LON-CL1 et vers Outlook 2013.
2. Cliquez sur **Nouveau message électronique**.
3. Dans le champ **À**, tapez **amr@adatum.com**.
4. Dans le champ **Objet**, tapez **Test de bloc**.
5. Dans le corps du message, tapez **Voici mon adresse IP : 192.168.0.100** et cliquez sur **Envoyer**.
6. Attendez quelques instants et vérifiez si vous recevez un message électronique indiquant que votre message précédent à Arm Zaki n'a pas été remis. Assurez-vous également que le texte « Le message est bloqué » s'affiche. Examinez le contenu du message.
7. Basculez vers Internet Explorer, puis dans la fenêtre Outlook Web App, vérifiez que vous avez reçu un courrier électronique d'Aidan et que le message d'origine qu'Aidan a envoyé à Amr est attaché.
8. Déconnectez-vous d'**Outlook Web App**.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1, 22341B-LON-MBX1 et 22341B-LON-CL1**.

Résultats : À la fin de cet exercice, les stagiaires auront configuré des règles de transport et des stratégies de prévention de pertes de données.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR – MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 9 : Planification et configuration de l'hygiène des messages

Atelier pratique : Planification et configuration de la sécurité des messages

Exercice 1 : Configurer les options anti-programmes malveillants dans Exchange Server 2013

▶ Tâche 1 : Activer les fonctionnalités anti-programmes malveillants dans Exchange Server 2013

1. Sur LON-MBX1, sur l'écran Accueil, cliquez sur l'environnement de ligne de commande **Exchange Management Shell**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, passez du dossier actif au dossier **\Program Files\Microsoft\Exchange Server\V15\Scripts** en tapant l'applet de commande suivante, puis appuyez sur **Entrée**.

```
cd "\Program Files\Microsoft\Exchange Server\V15\Scripts"
```

3. Dans l'environnement de ligne de commande Exchange Management Shell, activez l'analyse anti-programmes malveillants en tapant le script suivant, puis appuyez sur Entrée.

```
.\Enable-AntimalwareScanning.ps1
```

4. Vérifiez que le message suivant apparaît : **Les moteurs anti-programmes malveillants sont en cours de mise à jour. Cette opération peut prendre quelques minutes**. Attendez la fin du processus de mise à jour.
5. Dans l'environnement de ligne de commande Exchange Management Shell, redémarrez le **service de Microsoft Exchange Transport** en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Restart-Service MSExchangeTransport
```

6. Dans l'environnement de ligne de commande Exchange Management Shell, répertoriez les agents de transport installés en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Get-TransportAgent
```

7. Vérifiez que l'agent anti-programmes malveillants suivant est répertorié : **Malware Agent**. Notez que l'état de l'agent anti-programmes malveillants est **Enabled True** si le script a été autorisé à s'exécuter.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Configurer la stratégie anti-programmes malveillants par défaut dans Exchange Server 2013

1. Basculez vers **LON-CAS1**.
2. Déplacez le pointeur de la souris vers le coin inférieur droit de la fenêtre, puis cliquez sur l'icône **Accueil**.
3. Sur l'écran **Accueil**, cliquez sur la vignette **Internet Explorer**.
4. Dans Internet Explorer, tapez l'adresse suivante dans la barre d'adresses, **https://lon-cas1.adatum.com/ecp**, puis appuyez sur Entrée.
5. Connectez-vous au CAE en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**, puis cliquez sur le bouton **Se connecter**.
6. Dans le CAE, dans le volet des fonctionnalités, cliquez sur **Protection**.
7. Dans la fenêtre du CAE, sur l'onglet **filtre anti-programme malveillant**, cliquez sur le bouton **Modifier** de la barre d'outils.
8. Dans la fenêtre **Default**, cliquez sur **Paramètres**.
9. Sous **Réponse à la détection de programmes malveillants**, sélectionnez **Supprimer toutes les pièces jointes et utiliser le texte d'avertissement personnalisé**.
10. Dans la zone **Texte d'avertissement personnalisé**, tapez le texte suivant : **La pièce jointe a été supprimée, car elle contenait des programmes malveillants. Contactez votre administrateur**.
11. Dans la section **Notifications**, activez les deux cases à cocher **Informer les expéditeurs internes** et **Informer les expéditeurs externes**.
12. Dans la section **Notifications de l'administrateur**, activez la case à cocher **Informer l'administrateur des messages d'expéditeurs internes non remis**.
13. Dans la zone **Adresse de messagerie de l'administrateur**, tapez **administrateur@adatum.com**.
14. Dans la section **Notifications de l'administrateur**, activez la case à cocher **Informer l'administrateur des messages d'expéditeurs externes non remis**.
15. Dans la zone **Adresse de messagerie de l'administrateur**, tapez **administrateur@adatum.com**.
16. Dans la fenêtre **Default**, cliquez sur le bouton **enregistrer**.

Exercice 2 : Configuration des options anti-courrier indésirable sur Exchange Server

▶ Tâche 1 : Activer les fonctionnalités anti-courrier indésirable sur LON-MBX1

1. Basculez vers **LON-MBX1**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, installez les agents anti-courrier indésirable en tapant le script suivant, puis appuyez sur Entrée.

```
.\Install-AntiSpamAgents.ps1
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans l'environnement de ligne de commande Exchange Management Shell, redémarrez le **service de Microsoft Exchange Transport** en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Restart-Service MSExchangeTransport
```

4. Dans l'environnement de ligne de commande Exchange Management Shell, spécifiez les adresses IP des serveurs SMTP internes, **LON-MBX1 et LON-MBX2**, qui doivent être ignorées par l'agent d'ID de l'expéditeur en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Set-TransportConfig -InternalSMTPServers @{Add="172.16.0.22","172.16.0.223"}
```

5. Dans l'environnement de ligne de commande Exchange Management Shell, répertoriez les agents de transport installés en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Get-TransportAgent
```

6. Vérifiez que les agents anti-courrier indésirable suivants sont présents : **Content Filter Agent, Sender ID Agent, Sender Filter Agent, Recipient Filter Agent, Protocol Analysis Agent.** Vérifiez que l'état des agents anti-courrier indésirable est **Enabled True**.

▶ Tâche 2 : Configurer le filtrage de contenu sur LON-MBX1

1. Dans l'environnement de ligne de commande Exchange Management Shell, vérifiez que le filtrage de contenu est activé en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Get-ContentFilterConfig | Format-List Enabled
```

2. Vérifiez que **Enabled:True** s'affiche.

3. Dans l'environnement de ligne de commande Exchange Management Shell, configurez l'expression bloquée **Poker results** en tapant l'applet de commande suivante, puis appuyez sur **Entrée**.

```
Add-ContentFilterPhrase -Influence BadWord -Phrase "Poker results"
```

4. Dans l'environnement de ligne de commande Exchange Management Shell, configurez l'expression autorisée **Report document** en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Add-ContentFilterPhrase -Influence GoodWord -Phrase "Report document"
```

5. Dans l'environnement de ligne de commande Exchange Management Shell, configurez la boîte aux lettres de quarantaine **quarantaine@adatum.com** en tapant l'applet de commande suivante, puis appuyez sur Entrée :

```
Set-ContentFilterConfig -QuarantineMailbox quarantaine@adatum.com
```

 **Remarque :** Dans un environnement de production, vous devez également créer une boîte aux lettres utilisateur et la configurer comme une boîte aux lettres de quarantaine.

UTILISATION PÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

6. Dans l'environnement de ligne de commande Exchange Management Shell, configurez les seuils SCL et activez la quarantaine en tapant l'applet de commande suivante, puis appuyez sur **Entrée**.

```
Set-ContentFilterConfig -SCLRejectEnabled $true -SCLRejectThreshold 8 -
SCLQuarantineEnabled $true -SCLQuarantineThreshold 7
```

7. Dans l'environnement de ligne de commande Exchange Management Shell, configurez une réponse de rejet personnalisée en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Set-ContentFilterConfig -RejectionResponse "Your message was rejected by our spam
filter. Contact your administrator."
```

8. Dans l'environnement de ligne de commande Exchange Management Shell, configurez le **seuil SCL du dossier Courrier indésirable** avec la valeur **6** pour toutes les boîtes aux lettres de votre organisation en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Set-OrganizationConfig -SCLJunkThreshold 6
```

▶ Tâche 3 : Configurer le filtrage des expéditeurs et des destinataires sur LON-MBX1

1. Sur LON-MBX1, dans l'environnement de ligne de commande Exchange Management Shell, configurez le filtrage des expéditeurs pour bloquer les messages en provenance de **marketing@contoso.com** en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Set-SenderFilterConfig -BlockedSenders marketing@contoso.com
```

2. Dans l'environnement de ligne de commande Exchange Management Shell, configurez le filtrage des destinataires pour bloquer les messages envoyés à **helpdesk@adatum.com** en tapant l'applet de commande suivante, puis appuyez sur Entrée.

```
Set-RecipientFilterConfig -BlockListEnabled $true -BlockedRecipients
helpdesk@adatum.com
```

Remarque : Dans ce scénario nous supposons que l'adresse de messagerie helpdesk@adatum.com est à utilisation interne uniquement et qu'elle ne doit recevoir aucun message électronique d'expéditeurs externes.

Exercice 3 : Validation de la configuration des logiciels anti-courrier indésirable et anti-programmes malveillants

▶ Tâche 1 : Valider la configuration anti-programmes malveillants

1. Basculez vers **LON-CAS1**.
2. Modifiez le fichier **E:\Labfiles\Mod09\Eicar.txt** et supprimez les sauts de ligne entre la première ligne et la ligne de texte suivante. La totalité du texte doit se trouver sur une ligne. Enregistrez le fichier.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Si Internet Explorer est actuellement ouvert, fermez-le.
4. Ouvrez Internet Explorer et tapez **https://lon-cas1.adatum.com/owa**.
5. Connectez-vous en tant qu'**ADATUM \Michael** avec le mot de passe **Pa$$w0rd**.
6. Dans la page **Langue et Fuseau horaire**, ne modifiez pas le fuseau horaire, puis cliquez sur **enregistrer**.
7. Dans la fenêtre Outlook Web App, cliquez sur **nouveau message**.
8. Tapez **mark@adatum.com** dans le champ **À**.
9. Cliquez dans le champ **Objet**, puis tapez **Message de test**.
10. Dans le corps du message, tapez **Rapport quotidien**, cliquez sur **INSÉRER**, puis sur **pièce jointe**.
11. Dans la fenêtre **Choisir un fichier à télécharger**, dans le volet de navigation, accédez à **E:\Labfiles\Mod09**, double-cliquez sur le fichier **Eicar.txt**, puis cliquez sur **ENVOYER**.
12. Dans la fenêtre **Outlook Web App**, cliquez sur **Michael Allen**, puis sur **Se déconnecter**.
13. Dans Internet Explorer, dans la page de connexion **Outlook Web App**, connectez-vous en tant qu'**ADATUM\Mark** avec le mot de passe **Pa$$w0rd**. Cliquez sur **enregistrer**.
14. Dans la fenêtre **Outlook Web App**, ouvrez le nouveau message en provenance de **Michael Allen**. Double-cliquez sur la pièce jointe, cliquez sur **Ouvrir**, puis sur **Ouvrir** une nouvelle fois.
15. Vérifiez que le code présent dans le fichier a été supprimé et remplacé par le texte personnalisé que vous avez configuré.
16. Dans la fenêtre **Outlook Web App**, cliquez sur **Mark Bebbington**, puis sur **Se déconnecter**.

▶ Tâche 2 : Valider la configuration anti-courrier indésirable

1. Basculez vers **LON-DC1**
2. Sur **LON-DC1**, ouvrez Windows PowerShell dans la barre des tâches.
3. À l'invite de commandes, tapez **telnet LON-CAS1 smtp** et appuyez sur Entrée.
4. Tapez **helo** et appuyez sur Entrée.
5. Tapez **mail from: info@internet.com** et appuyez sur Entrée.

   Vous devriez recevoir la réponse : **250 2.1.0 Sender OK**
6. Tapez **rcpt to: michael@adatum.com** et appuyez sur Entrée.

   Réponse : **250 2.1.5 Recipient OK**.
7. Tapez **data** et appuyez sur Entrée.

   Réponse : **354 Start mail input; end with <CRLF>.<CRLF>**
8. Tapez **Subject: Information for you**, puis appuyez deux fois sur Entrée.
9. Tapez **Please find below poker results**, puis appuyez sur Entrée.
10. Appuyez sur la touche point (**.**), puis sur **Entrée**.
11. Vérifiez que le message suivant s'affiche : **Your message was rejected by our spam filter. Contact your administrator**. Tapez **Quit**, puis appuyez sur **Entrée**.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels en procédant comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V®**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-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 **22341B-LON-CAS1** et **22341B-LON-MBX1**.

Résultats : À la fin de cet exercice, vous aurez validé l'analyse anti-programmes malveillants lors de l'envoi d'un message de test avec une pièce jointe de simulation de programmes malveillants, dans laquelle la pièce jointe sera supprimée par la fonctionnalité anti-programmes malveillants d'Exchange Server 2013. Vous aurez également validé le filtrage de contenu anti-courrier indésirable lors de l'envoi d'une simulation de message indésirable dans laquelle le message sera stocké dans le dossier Courrier indésirable du destinataire par la fonctionnalité de filtrage de contenu d'Exchange Server 2013.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 10 : Planification et configuration de la sécurité et de l'audit administratifs

Atelier pratique : Configuration de la sécurité et de l'audit administratifs

Exercice 1 : Configuration des autorisations Exchange Server

▶ Tâche 1 : Configurer des autorisations Exchange Server pour le groupe Administrateurs informatiques

1. Sur LON-MBX1, ouvrez le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans le volet gauche, développez Adatum.com, cliquez sur **Microsoft Exchange Security Groups**, puis dans le volet droit, double-cliquez sur **Server Management**.
3. Dans Propriétés de : Server Management, cliquez sur l'onglet **Membres**, puis cliquez sur **Ajouter**.
4. Dans le champ **Entrez les noms des objets à sélectionner**, tapez **IT**, puis cliquez sur **OK** à deux reprises.
5. Fermez la fenêtre Utilisateurs et ordinateurs Active Directory.

▶ Tâche 2 : Configurer les autorisations pour les groupes SupportDesk et HelpDeskAdmins

1. Sur LON-MBX1, cliquez sur l'écran Accueil, puis sur **Exchange Management Shell**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, à l'invite PS, tapez la commande suivante et appuyez sur Entrée :

```
New-RoleGroup -Name HelpDeskAdmins -roles "Mail Recipients"
```

3. À l'invite PS, tapez la commande suivante et appuyez sur Entrée :

```
New-RoleGroup -Name SupportDesk -roles "Mail Recipients", "Mail Recipient Creation",
"Distribution Groups"
```

4. Cliquez sur l'écran Accueil, puis sur **Internet Explorer**, connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
5. Dans le CAE, dans le volet des fonctionnalités, cliquez sur **Autorisations**.
6. Sur les onglets, cliquez sur **Rôles d'administrateur**, puis double-cliquez sur **SupportDesk** dans l'affichage de liste.
7. Dans la fenêtre **Groupe de rôles**, sous **Membres**, cliquez sur **Ajouter**.
8. Dans la page Sélectionner les membres, sélectionnez **Ryan Spanton**, cliquez sur **ajouter**, puis sur **ok**.
9. Dans la fenêtre **Groupe de rôles**, cliquez sur **enregistrer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Dans l'affichage de liste, double-cliquez sur **HelpDeskAdmins**.
11. Dans la fenêtre **Groupe de rôles**, sous **Membres**, cliquez sur **Ajouter**.
12. Dans la page **Sélectionner les membres**, sélectionnez **Carol Troup**, cliquez sur **ajouter**, puis cliquez sur **ok**.
13. Dans la fenêtre Groupe de rôles, cliquez sur **enregistrer**.
14. Fermez Internet Explorer.

▶ Tâche 3 : Vérifier les autorisations pour les trois groupes de rôles créés

1. Sur LON-MBX1, ouvrez **Internet Explorer**, puis connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Tony** avec le mot de passe **Pa$$w0rd**.
2. Dans le volet de fonctionnalités, cliquez sur **Serveurs**.
3. Dans les onglets, cliquez sur **Bases de données**.
4. Dans l'affichage de liste, double-cliquez sur **Research**.
5. Dans la boîte de dialogue de **Base de données de boîtes aux lettres**, dans le volet gauche, cliquez sur **Limites**, puis sur la liste déroulante **Émettre un avertissement à (Go)**, sélectionnez **unlimited**, puis cliquez sur **enregistrer**.
6. Dans le volet de fonctionnalités, cliquez sur **Messagerie unifiée**. Vérifiez que vous pouvez voir l'onglet domaine accepté, mais que vous l'option pour ajouter un domaine accepté ne s'affiche pas. Double-cliquez sur **Adatum.com** (domaine par défaut) et vérifiez que vous ne pouvez pas apporter de modifications. Cliquez sur **Fermer**. Rappelez-vous que Tony fait partie du groupe informatique, et peut donc modifier les propriétés de serveur mais pas les paramètres du flux de messages organisationnels.
7. Fermez Internet Explorer.
8. Ouvrez **Internet Explorer**, puis connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Ryan** avec le mot de passe **Pa$$w0rd**. Constatez que, dans le volet de fonctionnalités, il n'y a aucun serveur. Cela est dû au fait que Ryan n'est pas autorisé à gérer les serveurs.
9. Dans le volet de fonctionnalités, cliquez sur **Destinataires**.
10. Dans l'affichage de liste, double-cliquez sur **Alan Steiner**.
11. Dans la fenêtre **Boîte aux lettres d'utilisateur**, dans le volet gauche, cliquez sur **Organisation**.
12. Dans le champ **Service**, tapez **informatique**, puis cliquez sur **enregistrer**.
13. Dans les onglets, cliquez sur **Groupes**.
14. Dans l'affichage de liste, double-cliquez sur **Research**. Vérifiez que vous ne pouvez pas modifier les propriétés du groupe en tapant une description de groupe 'test', puis en cliquant sur **enregistrer**.
15. Une fenêtre d'erreurs apparaît indiquant que vous n'avez pas les autorisations suffisantes pour modifier le groupe, cliquez sur **ok**, puis dans la fenêtre **Groupe de sécurité**, cliquez sur **annuler**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

16. Dans les onglets, cliquez sur **Boîtes aux lettres**, puis sur **Nouveau** dans la barre d'outils, puis cliquez sur **Boîte aux lettres utilisateur**.
17. Dans la fenêtre **Boîte aux lettres utilisateur**, tapez **Test** dans le champ **Alias**, puis cliquez sur **Nouvel utilisateur**.
18. Tapez **Test** dans le champ **Prénom**, puis **Test** dans le champ **Nom**. Tapez **Test** dans le champ **Nom d'overture de session de l'utilisateur** et **Pa$$word** dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**, puis cliquez sur **enregistrer**. Ceci confirme que Ryan peut créer des boîtes aux lettres.
19. Fermez Internet Explorer.
20. Ouvrez **Internet Explorer**, puis connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Carol** avec le mot de passe **Pa$$w0rd**.
21. Dans le volet de fonctionnalités, cliquez sur **Destinataires**. Notez qu'il n'y a aucun bouton Nouvel utilisateur dans la barre d'outils.
22. Dans l'affichage de liste, double-cliquez sur **Alan Steiner**.
23. Dans la fenêtre **Boîte aux lettres utilisateur**, dans le volet gauche, cliquez sur **Organisation**.
24. Dans le champ **Service**, tapez **Service client**, puis cliquez sur **enregistrer**.
25. Vérifiez que les groupes ne sont pas disponibles dans les onglets, car Carol n'a pas l'autorisation de gérer les groupes.
26. Fermez Internet Explorer.

Résultats : À la fin de cet exercice, les stagiaires auront configuré des rôles RBAC et vérifié que les autorisations sont accordées en conséquence.

Exercice 2 : Configuration de la journalisation d'audit

▶ Tâche 1 : Configurer la journalisation d'audit sur la boîte aux lettres Info@Adatum.com

1. Sur LON-MBX1, cliquez sur l'écran Accueil, puis sur **Exchange Management Shell**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, à l'invite PS, tapez :

```
Set-Mailbox -Identity "Info" -AuditDelegate SendAs,SendOnBehalf -AuditEnabled $true
```

3. Réduisez l'environnement de ligne de commande Exchange Management Shell.

▶ Tâche 2 : Exercez l'activité SendAs sur la boîte aux lettres Info@Adatum.com

1. Basculez vers LON-CAS1, ouvrez Internet Explorer, tapez **https://LON-CAS1.adatum.com/owa**, puis appuyez sur Entrée.
2. Connectez-vous à l'application Outlook Web Access en tant qu'**ADATUM\Tony** avec le mot de passe **Pa$$w0rd**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Cliquez sur **nouveau message** pour créer un message, cliquez sur **plus d'options**, puis cliquez sur **afficher de**.
4. Cliquez avec le bouton droit sur De, cliquez sur modifier, dans le champ **De**, tapez **Info@adatum.com**, cliquez sur Utiliser ce address : Info@adatum.com et dans le champ **À**, tapez **Tony Smith**. puis cliquez sur **Rechercher dans les Contacts et le Répertoire**. Dans le champ **Objet**, tapez **Test de la journalisation Envoyer en tant que**.
5. Tapez du texte dans le corps du message, puis cliquez sur **ENVOYER**. Vérifiez que le message est envoyé.
6. Fermez Internet Explorer.

▶ Tâche 3 : Vérifier que l'activité est consignée

1. Sur LON-MBX1, ouvrez **Internet Explorer**, puis tapez **https://LON-CAS1.adatum.com/ecp.**
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans le CAE, dans le volet des fonctionnalités, cliquez sur **Gestion de la conformité**.
4. Sur les onglets, cliquez sur **Audit**.
5. Cliquez sur **Exécuter un rapport d'accès aux boîtes aux lettres par des non-propriétaires**.
6. Dans la fenêtre **Rechercher les boîtes aux lettres auxquelles des non-propriétaires ont accédé**, conservez la date de début et définissez la date de fin à demain.
7. Dans la zone déroulante **Rechercher les accès par**, sélectionnez **Tous les non-propriétaires**, puis cliquez sur **rechercher**.
8. Dans les résultats de recherche, cliquez sur **Info**, puis consultez le rapport qui montre que Tony Smith a accédé à la boîte aux lettres Info.
9. Cliquez sur **fermer**, puis fermez Internet Explorer.

Résultats : À la fin de cet exercice, les stagiaires auront configuré la journalisation d'audit de boîte aux lettres et vérifié que la journalisation d'audit fonctionne correctement.

Exercice 3 : Configuration des autorisations fractionnées RBAC sur Exchange Server 2013

▶ Tâche 1 : Créer un groupe de rôles appelé HRAdmins et attribuer des autorisations

1. Sur LON-MBX1 (si le Exchange Management Shell n'est pas encore ouvert), cliquez sur l'écran Accueil, puis sur **Exchange Management Shell**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, à l'invite PS, tapez les applets de commande suivantes et appuyez sur Entrée.

```
New-RoleGroup "HRAdmins" -Roles "Mail Recipient Creation", "Security Group Creation
and Membership"
New-ManagementRoleAssignment -Role "Mail Recipient Creation" -SecurityGroup
"HRAdmins" -Delegating
New-ManagementRoleAssignment -Role "Security Group Creation and Membership" -
SecurityGroup "HRAdmins" -Delegating
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans l'environnement de ligne de commande Exchange Management Shell, à l'invite PS, tapez la commande suivante et appuyez sur Entrée.

```
Add-RoleGroupMember "HRAdmins" -Member Tony
```

4. Ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
5. Dans le volet gauche, cliquez sur **Microsoft Exchange Security Groups**, puis double-cliquez sur **HRAdmins**.
6. Cliquez sur l'onglet **Géré par**, cliquez sur **Modifier** et tapez **HRAdmins**, puis cliquez sur **OK.**
7. Activez la case à cocher **Le gestionnaire peut mettre à jour la liste des membres**, puis cliquez sur **OK**.
8. Dans le volet droit, double-cliquez sur **Recipient Management**.
9. Cliquez sur l'onglet **Membres**, cliquez sur **Ajouter** et tapez **HRAdmins**, puis cliquez sur **OK**. Ceci est requis pour attribuer au groupe HRAdmins les autorisations nécessaires permettant de créer une boîte aux lettres. Cliquez sur **OK**.
10. Fermez la console **Utilisateurs et ordinateurs Active Directory**.

▶ Tâche 2 : Supprimer l'autorisation de création d'objets AD DS à partir d'autres groupes d'administrateurs Exchange Server

1. Sur LON-MBX1, ouvrez **Exchange Management Shell**.
2. Dans l'environnement de ligne de commande Exchange Management Shell, à l'invite PS, tapez :

```
Get-ManagementRoleAssignment -Role "Mail Recipient Creation" | Format-Table Name,
Role, RoleAssigneeName –Auto
```

3. Après avoir vu les groupes qui ont délégué les attributions de rôle pour ce rôle, exécutez l'applet de commande suivante pour supprimer tous les groupes excepté HRAdmins :

```
Get-ManagementRoleAssignment -Role "Mail Recipient Creation" | Where {
$_.RoleAssigneeName -NE "HRAdmins" } | Remove-ManagementRoleAssignment
```

4. À l'invite de commandes, tapez **T**, puis appuyez sur Entrée.
5. Dans l'environnement de ligne de commande Exchange Management Shell, à l'invite PS, tapez :

```
Get-ManagementRoleAssignment -Role "Security Group Creation and Membership" | Where {
$_.RoleAssigneeName -NE "HRAdmins" } | Remove-ManagementRoleAssignment
```

6. À l'invite de commandes, tapez **T**, puis appuyez sur Entrée.
7. Fermez l'environnement de ligne de commande Exchange Management Shell.

▶ Tâche 3 : Valider la fonctionnalité d'autorisations fractionnées RBAC

1. Sur LON-MBX1, ouvrez **Internet Explorer**, connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le volet des fonctionnalités, cliquez sur **Destinataires**.

3. Cliquez sur l'onglet **Boîtes aux lettres**, sur **Nouvelle** dans la barre d'outils, puis sur **Boîte aux lettres utilisateur**.
4. Dans la fenêtre **Boîte aux lettres utilisateur**, tapez **Nouveau** dans le champ **Alias**, puis cliquez sur **Nouvel utilisateur**. Notez que tous les champs requis pour créer un nouvel utilisateur sont grisés. Cela est dû au fait que vous n'avez pas l'autorisation de créer un compte d'utilisateur dans AD DS.
5. Cliquez sur annuler, puis fermez Internet Explorer.
6. Ouvrez **Internet Explorer**, connectez-vous à **https://LON-CAS1.adatum.com/ecp**. Connectez-vous en tant qu'**Adatum\Tony** avec le mot de passe **Pa$$w0rd**.
7. Cliquez sur l'onglet **Boîtes aux lettres**, sur **Nouveau** dans la barre d'outils, puis sur **Boîte aux lettres utilisateur**.
8. Dans la fenêtre **Boîte aux lettres utilisateur**, tapez **Test2** dans le champ **Alias**, puis cliquez sur **Nouvel utilisateur**.
9. Tapez **Test2** dans le champ **Prénom**, puis **Test2** dans le champ **Nom**. Tapez **Test2** dans le champ **Nom d'overture de session de l'utilisateur** et **Pa$$word** dans les champs **Nouveau mot de passe et Confirmer le mot de passe**, puis cliquez sur **enregistrer**. Ceci confirme que Tony peut créer des comptes d'utilisateurs pour les nouvelles boîtes aux lettres.
10. Fermez Internet Explorer.

▶ Pour préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme il est indiqué ci-dessous.

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22341B-LON-DC1**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22341B-LON-CAS1** et **22341B-LON-MBX1**.

Résultats : À la fin de cet exercice, les stagiaires auront créé un groupe de rôles, configuré des autorisations fractionnées RBAC et validé que les autorisations fractionnées RBAC fonctionnent comme prévu.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Module 11 : Analyse et résolution des problèmes de Microsoft® Exchange Server 2013

Atelier pratique : Analyse et résolution des problèmes d'Exchange Server 2013

Exercice 1 : Analyse d'Exchange Server

▶ Tâche 1 : Créer un ensemble de collecteurs de données nommé Analyse Exchange

1. Sur LON-MBX1, cliquez sur la vignette **Gestionnaire de serveur**.
2. Dans la fenêtre Gestionnaire de serveur, cliquez sur le menu **Outils**, puis cliquez sur **Analyseur de performances**.
3. Dans la fenêtre Analyseur de performances, dans le volet de navigation, développez **Ensembles de collecteurs de données**, puis cliquez sur **Définis par l'utilisateur**.
4. Cliquez sur le menu **Action**, sur **Nouveau**, puis sur **Ensemble de collecteurs de données**.
5. Dans l'Assistant Créer un nouvel ensemble de collecteurs de données, dans la zone **Nom**, tapez **Analyse Exchange**, sélectionnez **Créer manuellement (avancé)**, puis cliquez sur **Suivant**.
6. Cochez la case **Compteur de performance**, puis cliquez sur **Terminer**.

▶ Tâche 2 : Créer un ensemble de collecteurs de données de compteur de performances pour analyser les performances de base du serveur Exchange

1. Dans le volet de navigation de l'Analyseur de performances, développez successivement **Ensembles de collecteurs de données** puis **Défini par l'utilisateur**, cliquez sur **Analyse Exchange**, sur le menu **Action**, sur **Nouveau**, puis sur **Collecteur de données**.
2. Dans l'Assistant Créer un nouveau collecteur de données, dans la zone **Nom,** tapez **Analyse Exchange de base**, sélectionnez **Collecteur de données de compteur de performance**, cliquez sur **Suivant**, puis sur **Ajouter**.
3. Dans la liste d'objets **Compteurs disponibles**, développez **Processeur**, puis cliquez sur **% temps processeur**. Appuyez sur la touche Ctrl et maintenez-la enfoncée, cliquez sur **% temps utilisateur**, sur **% temps privilégié**, puis sur **Ajouter**.
4. Dans la liste d'objets **Compteurs disponibles**, développez **Mémoire**, puis cliquez sur **Mégaoctets disponibles**. Maintenez la touche Ctrl enfoncée, cliquez sur les éléments suivants, puis cliquez sur **Ajouter** :
   - **Lectures de pages/s**
   - **Pages en entrée/s**
   - **Pages/s**
   - **Pages en sortie/s**
   - **Octets de réserve paginée**
   - **Pages de transition avec nouvel objet/s**

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

5. Dans la liste d'objets **Compteurs disponibles**, développez **Contrôleurs de domaine MSExchange ADAccess**, puis cliquez sur **Durée de lecture LDAP**. Maintenez la touche Ctrl enfoncée, cliquez sur les éléments suivants, puis cliquez sur **Ajouter** :
   - **Durée de recherche LDAP**
   - **Délai de recherche LDAP dépassé par minute**
   - **Opérations LDAP longues/min**
6. Dans la liste d'objets **Compteurs disponibles,** développez **Système**, cliquez sur **Longueur de la file du processeur**, sur **Ajouter**, puis sur**OK**.
7. Dans l'Assistant Créer un nouveau collecteur de données, dans la zone **Intervalle d'échantillonnage,** tapez **1**, dans le menu déroulant **Unités,** sélectionnez **Minutes** puis cliquez sur **Terminer** pour créer le collecteur de données.

▶ Tâche 3 : Créer un ensemble de collecteurs de données de compteur de performances pour analyser les performances du rôle serveur de boîtes aux lettres

1. Dans le volet de navigation de l'Analyseur de performances, cliquez sur **Analyse Exchange**, sur le menu **Action**, sur **Nouveau**, puis sur **Collecteur de données**.
2. Dans l'Assistant Créer un nouveau collecteur de données, dans la zone **Nom,**tapez **Analyse de rôle serveur de boîte aux lettres**, sélectionnez **Collecteur de données de compteur de performance**, cliquez sur **Suivant**, puis sur **Ajouter**.
3. Dans la liste d'objets **Compteurs disponibles**, développez **Disque logique**, puis cliquez sur **Moyenne disque s/lecture**. Maintenez la touche Ctrl enfoncée, cliquez sur les éléments suivants, puis cliquez sur **Ajouter** :
   - **Moyenne disque s/transfert**
   - **Moyenne disque s/écriture**
4. Dans la liste d'objets **Compteurs disponibles**, développez **MSExchangeIS Store**, puis cliquez sur **RPC Average Latency**. Maintenez la touche Ctrl enfoncée, cliquez sur les éléments suivants, puis cliquez sur **Ajouter** :
   - **RPC Operations/sec**
   - **RPC Requests**
   - **Messages Delivered/sec**
5. Cliquez sur **OK**.
6. Dans l'Assistant Créer un nouveau collecteur de données, dans la zone **Intervalle d'échantillonnage,** tapez **1**, dans la liste déroulante **Unités,** sélectionnez **Minutes**, puis cliquez sur **Terminer** pour créer le collecteur de données.

▶ Tâche 4 : Vérifier que l'ensemble de collecteurs de données fonctionne correctement

1. Dans l'Analyseur de performances, dans le volet de navigation, cliquez sur **Analyse Exchange**, sur le menu **Action,** puis cliquez sur **Démarrer**.
2. Attendez au moins cinq minutes, cliquez sur le menu **Action**, puis sur **Arrêter**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans le volet de navigation, développez successivement **Rapports**, **Définis par l'utilisateur**, **Analyse Exchange**, cliquez sur **LON-MBX1_DateTime-Number**, puis examinez le rapport.
4. Fermez l'Analyseur de performances.

Résultats : À la fin de cet exercice, vous aurez créé un ensemble de collecteurs de données pour l'analyse de LON-MBX1 en utilisant les compteurs de performances recommandés.

Exercice 2 : Résolution des problèmes liés à la disponibilité des bases de données

▶ Tâche 1 : Identifier l'étendue du problème

Avant de commencer cet exercice, procédez comme suit :

1. Sur LON-MBX1, ouvrez Exchange Management Shell. À l'invite, tapez **c:\scripts\Lab11Prep1.ps1**, puis appuyez sur Entrée. Ce script simulera une défaillance de base de données.
2. Sur LON-MBX1, si l'écran **Accueil** ne s'affiche pas, placez la souris dans l'angle inférieur droit de l'écran et cliquez sur **Accueil**.
3. Sur l'écran d'accueil, ouvrez **Internet Explorer**.
4. Dans la fenêtre Internet Explorer, tapez https://lon-cas1.adatum.com/ecp, puis appuyez sur Entrée.
5. Dans la page Web d'Outlook Web App, dans la zone **Nom d'utilisateur**, tapez **ADATUM\Administrateur**. Dans la zone **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **se connecter**.
6. Dans le Centre d'administration Exchange, dans le volet des fonctionnalités, cliquez sur **Serveurs**, puis sur l'onglet **Bases de données**.
7. Dans l'affichage liste, cliquez sur la base de données **MailboxDB100**, puis dans le volet d'informations, vérifiez que son état est **Démonté**.
8. Dans la barre d'outils, cliquez sur **Plus**, puis sur **Monter**.
9. Dans la fenêtre **avertissement**, cliquez sur le bouton **oui**.
10. Une autre fenêtre **avertissement** s'affiche, avec un message indiquant qu'au moins une base de données est manquante. Dans la fenêtre **avertissement**, cliquez sur **annuler**.

▶ Tâche 2 : Examiner les journaux des événements

1. Sur LON-MBX1, cliquez sur **Gestionnaire de serveur**.
2. Dans le Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur **Observateur d'événements**.
3. Dans le volet de navigation de l'Observateur d'événements, développez **Journaux Windows**, cliquez sur **Application**, puis dans le volet **Contenu,** examinez les événements récents. Cliquez sur les événements récents dont la source provient d'un des services MSExchange, puis examinez les détails de l'erreur dans la partie inférieure du volet **Contenu**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Dans le volet de navigation, cliquez sur **Système**, puis dans le volet **Contenu**, examinez les événements récents. Notez la présence d'événements notables.
5. Fermez l'Observateur d'événements.

▶ Tâche 3 : Répertorier les causes probables du problème et classer les solutions possibles, si plusieurs options existent

- Répertoriez les problèmes et les solutions possibles :

Problème	Solution suggérée
Des erreurs de disque empêchent l'accès à la base de données.	Remplacez les disques et restaurez à partir de la sauvegarde.
Le chemin d'accès de la base de données est incorrect à cause des modifications apportées au stockage.	Modifiez la configuration du stockage ou de la base de données.

▶ Tâche 4 : Vérifier la configuration de la base de données

1. Sur LON-MBX1, dans le Centre d'administration Exchange, dans l'affichage liste, vérifiez que la base de données MailboxDB100 est sélectionnée, puis dans la barre d'outils, cliquez sur le bouton **Modifier**.
2. Notez le Chemin d'accès à la base de données.
3. Cliquez sur l'icône **Explorateur de fichiers** dans la barre des tâches puis, dans le volet de navigation, développez successivement **Ordinateur**, **Disque local (C:)**, **Programmes**, **Microsoft**, **Exchange Server**, **V15**, **Mailbox**, puis vérifiez que le dossier **MailboxDB100-newpath** n'existe pas. C'est l'emplacement spécifié pour **MailboxDB100.edb**.
4. Dans le volet de navigation, cliquez sur le dossier **MailboxDB100**, puis localisez le fichier de la base de données **MailboxDB100.edb**. C'est l'emplacement réel des fichiers de bases de données et des journaux de transaction. La configuration pointe vers un chemin d'accès incorrect.
5. Fermez la fenêtre de l'Explorateur de fichiers.

▶ Tâche 5 : Reconfigurer et monter la base de données

1. Dans LON-MBX1, basculez vers Exchange Management Shell, tapez l'applet de commande ci-dessous et appuyez sur Entrée.

```
Move-DatabasePath MailboxDB100 –LogFolderPath "C:\Program Files\Microsoft\Exchange
Server\V15\Mailbox\MailboxDB100" –EdbFilePath "C:\Program Files\Microsoft\Exchange
Server\V15\Mailbox\MailboxDB100\MailboxDB100.edb" –ConfigurationOnly –force
```

2. Tapez **O**, puis appuyez sur Entrée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Dans la fenêtre de l'environnement de ligne de commande Exchange Management Shell, tapez l'applet de commande suivante :

```
Mount-Database MailboxDB100
```

4. Appuyez sur Entrée.
5. Dans le CAE, dans le volet des fonctionnalités, cliquez sur **Serveurs**, puis sur l'onglet **Bases de données**.
6. Dans l'affichage liste, actualisez la page et cliquez sur la base de données **MailboxDB100**, puis dans le volet d'informations, vérifiez que son état est **Monté**.

Résultats : À la fin de cet exercice, vous aurez utilisé une technique de résolution des problèmes pour identifier et résoudre un problème de serveur de boîtes aux lettres.

Exercice 3 : Résolution des problèmes liés aux serveurs d'accès au client

▶ Tâche 1 : Utiliser les applets de commande Test pour vérifier l'intégrité du serveur

Avant de commencer cet exercice, procédez comme suit :

1. Sur LON-MBX1, dans Exchange Management Shell, tapez **c:\scripts\Lab11Prep2.ps1** et appuyez sur Entrée.
2. Fermez l'environnement de ligne de commande Exchange Management Shell.
3. Sur LON-MBX1, si l'écran **Accueil** ne s'affiche pas, placez la souris dans l'angle inférieur droit de l'écran et cliquez sur **Accueil**.
4. Sur l'écran d'accueil, cliquez sur l'environnement de ligne de commande **Exchange Management Shell**.
5. Dans la fenêtre de l'environnement de ligne de commande **Exchange Management Shell**, tapez l'applet de commande de test suivante :

```
Test-ServiceHealth
```

6. Appuyez sur Entrée. Vérifiez que le résultat ne renvoie aucune erreur.
7. Dans l'environnement de ligne de commande Exchange Management Shell, tapez l'applet de commande ci-dessous et appuyez sur Entrée :

```
Test-OwaConnectivity –URL https://LON-MBX1.adatum.com/OWA -TrustAnySSLCertificate
```

8. Notez les erreurs d'authentification.
9. Fermez Exchange Management Shell.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

▶ Tâche 2 : Répertorier les causes probables du problème et classer les solutions possibles si plusieurs options existent

- Répertoriez les problèmes et les solutions possibles :

Problème	Solution suggérée
La configuration Internet Information Server (IIS) n'est pas configurée correctement.	Modifier la configuration IIS.
L'authentification de l'application Microsoft Outlook Web App n'est pas configurée correctement.	Modifier la configuration de l'authentification de l'application Outlook Web App.

▶ Tâche 3 : Vérifier la configuration d'Outlook Web App

1. Sur LON-MBX1, si l'écran **Accueil** ne s'affiche pas, placez la souris dans l'angle inférieur droit de l'écran et cliquez sur **Accueil**.
2. Sur l'écran d'accueil, ouvrez **Internet Explorer**.
3. Dans la fenêtre Internet Explorer, tapez **https://lon-cas1.adatum.com/ecp**, puis appuyez sur Entrée.
4. Dans la page Web d'Outlook Web App, dans la zone Nom d'utilisateur, tapez **ADATUM\Administrateur,** dans la zone de mot de passe, tapez **Pa$$w0rd**, puis cliquez sur le bouton **se connecter**.
5. Vérifiez que vous ne pouvez pas vous connecter au CAE.
6. Dans **Exchange Management Shell**, tapez l'applet de commande suivante puis appuyez sur Entrée.

```
Get-OwaVirtualDirectory –Identity "lon-cas1\owa (Default Web Site)" | ft name,
*authentication
```

7. Vérifiez que toutes les méthodes d'authentification sont définies sur **False**.
8. Dans l'environnement de ligne de commande **Exchange Management Shell**, tapez l'applet de commande suivante puis appuyez sur Entrée.

```
Set-OwaVirtualDirectory –Identity "lon-cas1\owa (Default Web Site)" –
FormsAuthentication $true
```

9. Dans l'environnement de ligne de commande **Exchange Management Shell**, tapez la commande suivante et appuyez sur Entrée.

```
iisreset
```

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

10. Dans la fenêtre Internet Explorer, tapez **https://lon-cas1.adatum.com/ecp**, puis appuyez sur Entrée.
11. Dans la page Web d'Outlook Web App, dans la zone Nom d'utilisateur, tapez **ADATUM\Administrateur**, ans la zone de mot de passe, tapez **Pa$$w0rd**, puis cliquez sur le bouton **se connecter**.
12. Vérifiez que vous pouvez maintenant vous connecter au CAE. Si une erreur de navigation s'affiche dans Internet Explorer, fermez le navigateur, rouvrez-le, puis répétez le processus à partir de l'étape 10.

Remarque : Si vous recevez une erreur qui indique que le service n'a pas démarré, démarrez le service de publication World Wide Web dans la console de gestion des services.

▶ Tâche 4 : Vérifier que vous avez résolu le problème

1. Ouvrez Internet Explorer et connectez-vous à **https://LON-CAS1.adatum.com/owa**.
2. Ouvrez une session Outlook Web App en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Confirmez qu'Administrateur peut maintenant accéder à l'application Outlook Web App, puis fermez Internet Explorer.

Résultats : À la fin de cet exercice, vous aurez utilisé une technique de résolution des problèmes pour identifier et résoudre un problème de serveur d'accès au client.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT