

PRODUIT OFFICIEL DE FORMATION MICROSOFT

22742A

Identité avec Windows Server 2016

Les informations contenues dans ce document, notamment les URL et autres références aux sites Web, peuvent 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.

©2017 Microsoft Corporation. Tous droits réservés.

Microsoft et les marques commerciales figurant sur la page <http://www.microsoft.com/about/legal/fr/fr/IntellectualProperty/Trademarks/FR-FR.aspx> sont des marques commerciales du groupe de sociétés Microsoft. Toutes les autres marques sont la propriété de leurs propriétaires respectifs.

Numéro de produit : 22742A

Numéro de référence : X21-37335

Date de publication : 03/2017

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 Agrée » 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 Agrée 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,
- b. **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 reconnaisserez 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 reconnaise 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 reconnaîsse 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 interfaçer 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. RÈGLEMENTATION 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 connaît 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 d'avoir suivi notre formation! Nous avons travaillé en collaboration avec nos partenaires Microsoft certifiés pour des solutions d'apprentissage, ainsi qu'avec nos experts informatiques pour vous apporter une expérience de formation de classe mondiale —que vous soyez un professionnel qui cherche à perfectionner ses connaissances ou un stagiaire qui prépare une carrière en informatique.

- **Formateurs et instructeurs certifiés par Microsoft** — votre instructeur possède des compétences techniques et pédagogiques pointues qui répondent aux exigences actuelles en matière de certification. Et, si les instructeurs fournissent la formation à un de nos partenaires certifiés pour les solutions d'apprentissage, ils sont également évalués tout au long de l'année par les stagiaires et Microsoft.
- **Avantages de l'examen de certification** — Après formation, envisagez de passer un examen de certification Microsoft. Les certifications Microsoft confirment vos connaissances des technologies Microsoft et peuvent vous aider à vous démarquer lors de la recherche d'un emploi ou à promouvoir votre carrière. En effet, la recherche indépendante par IDC a conclu que 75% des gestionnaires croient que les certifications sont importantes pour la performance de l'équipe¹. Demandez à votre instructeur de vous renseigner sur les promotions de l'examen de certification Microsoft, ainsi que sur les remises qui peuvent être disponibles pour vous.
- **Garantie de satisfaction des clients** — nos partenaires certifiés pour les solutions d'apprentissage offrent une garantie de satisfaction des clients et nous leur attribuons toute responsabilité y afférente. À la fin du cours, nous vous demandons de bien vouloir remplir un formulaire d'évaluation sur l'expérience d'aujourd'hui. Vos commentaires sont les bienvenus !

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

Cordialement,

Microsoft Learning
www.microsoft.com/learning



¹IDC. \ telue 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 document 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 salle de classe.

Jason Hershey – Développeur de contenu

Jason Hershey est le propriétaire de Tellus Conseil et Tellus Project Management situé dans l'ouest de Washington. Il est un Microsoft Certified Professional (MCP), Project Management Professional (PMP) et Certified Scrum Master. Il est également titulaire d'une maîtrise (MBA) en finance. Avant de lancer sa propre entreprise, Jason a travaillé pendant près de 20 ans chez Microsoft avec presque toutes les équipes produits, y compris Microsoft Official Curriculum (MOC), Windows client et Windows Server, SQL Server et l'équipe des produits Office. Avec ces équipes, Jason a travaillé à la conception, au développement et au déploiement de solutions utilisant Microsoft SharePoint, à partir de SharePoint 2007 jusqu'à SharePoint 2013 et l'intégralité des technologies Microsoft.

Gary Dunlop - Développeur de contenu

Gary Dunlop est basé à Winnipeg au Canada et est consultant technique et formateur pour Broadview Networks. Il est l'auteur d'un certain nombre de contenus de formation de Microsoft et est un Microsoft Certified Trainer (MCT) depuis 1997.

Jamie Nelson - Développeur de contenu

Jamie Nelson est expert en matière de domaine et compte plus de 15 années d'expérience dans divers rôles de génie informatique et de leadership. Jamie possède une vaste expérience en conseil sur Active Directory, la stratégie de groupe, Exchange Server, System Center Configuration Manager, la gestion des identités et la virtualisation. Cependant, il a pour passion d'exploiter les capacités de Windows PowerShell pour l'automatisation de l'entreprise et de faire part à tous et à toute occasion opportune de son enthousiasme pour le sujet. Les clients de Jamie sont les organisations des secteurs publics et privés opérant dans les industries de l'énergie et de la santé et la United States Air Force. Jamie a travaillé en tant que professeur adjoint, dispensant des cours sur Windows Server et sur les Réseaux. Il est titulaire de plusieurs certifications dans l'industrie, en plus d'un Master en administration des affaires.

Jason Kellington – Développeur de contenu

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

Claus Jacob Wordenskjold - Développeur de contenu

Claus Jacob Wordenskjold est un consultant et formateur indépendant basé au Danemark. Il a fondé sa compagnie, Chinchilla Data, en 1995 et il compte plus de 25 ans d'expérience en informatique. Claus est MCT depuis 2002 et a dispensé des cours de formation dans toute l'Europe. Les cours sur les Clients et sur les Serveurs Windows sont sa spécialité, mais il assure de temps en temps des formations sur Microsoft SharePoint. Claus détient des certifications dans tous les systèmes d'exploitation Windows depuis Windows 2000 et fournit des services de conseil sur Windows Server, Active Directory Domain Services (AD DS) et sur la stratégie de groupe. Claus est intervenu lors d'événements Microsoft locaux au Danemark et est l'auteur de plusieurs cours sur Windows.

Damir Dizdarevic - Développeur de contenu

Damir Dizdarevic est MCSE, MCTS, MCITP et MCT. Il est le directeur exécutif des services de Logosoft d.o.o. à Sarajevo, en Bosnie-Herzégovine. Il travaille également à l'occasion en tant que consultant pour les clients de l'entreprise. Damir compte plus de 20 années d'expérience sur les plateformes Microsoft et se spécialise dans Windows Server, Exchange Server et des solutions de Cloud et de mobilité. Il a travaillé en tant que concepteur, expert technique (SME) et examinateur technique sur de nombreux cours officiels Microsoft sur Windows Server, Exchange Server, Office 365 et des sujets Microsoft Azure et a publié plus de 400 articles dans divers magazines informatiques, tels que Windows ITPro et INFO Magazine. Il officie également en tant que conférencier régulier et reconnu à la plupart des conférences de Microsoft en Europe orientale. En outre, Damir a été un MVP Microsoft pour la gestion du Cloud et du Datacenter pendant neuf années consécutives. Son blog technique est disponible à l'adresse : <http://dizdarevic.ba/ddamirblog>.

Clifton Leonard - Développeur de contenu

Clifton Leonard est un développeur de contenu et expert technique (SME) avec plus de 25 années d'expérience à son actif dans l'industrie des TI en tant qu'ingénieur, architecte, consultant, formateur et auteur. Clifton possède une vaste expérience de conseil sur Active Directory, Exchange Server, Lync Server, la gestion des identités et Office 365. Ses clients sont de grandes entreprises énergétiques, les écoles K-12, les universités, les fabricants de technologie, les institutions financières, la United States Air Force et le département de la Défense des États-Unis. Clifton a été expert technique (SME) pour plusieurs cours sur le Bureau de Windows, Windows Server, Exchange Server, Microsoft SharePoint Server, Hyper-V, la gestion des identités et Office 365.

Andrew Warren - Réviseur technique

Andrew Warren compte plus de 25 ans d'expérience dans l'industrie informatique, dont beaucoup passées dans l'enseignement et l'écriture. Il a été impliqué en tant qu'expert technique (SME) dans la conception de plusieurs cours sur Windows Server 2012 et a été le responsable technique de plusieurs autres cours. Il a également été impliqué dans le développement de sessions de TechNet sur Microsoft Exchange Server. Basé au Royaume-Uni, Andrew dirige son propre bureau de formation et conseil informatique.

Sommaire

Module 1 : Mise en œuvre et configuration de contrôleurs de domaine

| | |
|--|------|
| Vue d'ensemble du module | 1-1 |
| Leçon 1 : Vue d'ensemble de AD DS | 1-2 |
| Leçon 2 : Vue d'ensemble des contrôleurs de domaine AD DS | 1-15 |
| Leçon 3 : Déploiement d'un contrôleur de domaine | 1-24 |
| Atelier pratique : Déploiement et administration de AD DS | 1-36 |
| Révision du module et Takeaways | 1-41 |

Module 2 : Gestion d'objets dans AD DS

| | |
|--|------|
| Vue d'ensemble du module | 2-1 |
| Leçon 1 : Gestion des comptes d'utilisateurs | 2-2 |
| Lesson 2: Managing groups in AD DS | 2-12 |
| Leçon 3 : Gestion des objets ordinateur dans AD DS | 2-23 |
| Atelier pratique A : Gestion des objets AD DS | 2-29 |
| Leçon 4 : Utilisation de Windows PowerShell pour l'administration d'AD DS | 2-34 |
| Leçon 5 : Implémentation et gestion des UO | 2-49 |
| Atelier pratique B : Administration AD DS | 2-58 |
| Contrôle des acquis et éléments à retenir | 2-63 |

Module 3 : Gestion avancée de l'infrastructure AD DS

| | |
|--|------|
| Vue d'ensemble du module | 3-1 |
| Leçon 1 : Présentation des déploiements AD DS avancés | 3-2 |
| Leçon 2 : Déploiement d'un environnement AD DS distribué | 3-11 |
| Leçon 3 : Configuration approbations AD DS | 3-26 |
| Atelier pratique : Domaine et gestion des approbations dans AD DS | 3-32 |
| Révision du module et Takeaways | 3-35 |

Module 4 : Mise en œuvre et administration des sites AD DS et réPLICATION

| | |
|---|------|
| Vue d'ensemble du module | 4-1 |
| Leçon 1 : Vue d'ensemble de la réPLICATION AD DS | 4-2 |
| Leçon 2 : Configurer les sites AD DS | 4-11 |
| Leçon 3 : Configuration et surveillance de la réPLICATION AD DS | 4-20 |
| Atelier pratique : Implémentation des sites AD DS et réPLICATION | 4-27 |
| Contrôle des acquis et éléments à retenir | 4-33 |

Module 5 : Implémentation d'une stratégie de groupe

| | |
|--|------|
| Vue d'ensemble du module | 5-1 |
| Leçon 1 : Introduction d'une stratégie de groupe | 5-2 |
| Leçon 2 : Mise en œuvre et administration des GPO | 5-14 |
| Leçon 3 : Cadre et traitement de la stratégie de groupe | 5-22 |
| Atelier pratique A : Implémentation d'une infrastructure de stratégie de groupe | 5-38 |
| Leçon 4 : Résolution de problèmes de l'application des GPO | 5-42 |
| Atelier pratique B : Dépannage de l'infrastructure de stratégie de groupe | 5-50 |
| Révision du module et Takeaways | 5-56 |

Module 6 : Gestion des paramètres de l'utilisateur avec la stratégie de groupe

| | |
|--|------|
| Vue d'ensemble du module | 6-1 |
| Leçon 1 : Mise en œuvre des modèles d'administration | 6-2 |
| Leçon 2 : Configuration de la redirection de dossiers, de l'installation de logiciel et des scripts | 6-13 |
| Leçon 3 : Configuration des préférences de stratégie de groupe | 6-23 |
| Atelier pratique : Gestion des paramètres de l'utilisateur avec la stratégie de groupe | 6-30 |
| Révision du module et Takeaways | 6-39 |

Module 7 : Sécurisation des services de domaine Active Directory Domain Services

| | |
|--|------|
| Vue d'ensemble du module | 7-1 |
| Leçon 1 : Sécurisation des contrôleurs de domaine | 7-2 |
| Leçon 2 : Implémentation de la sécurité du compte | 7-16 |
| Leçon 3 : Mise en œuvre d'authentification d'audit | 7-37 |
| Leçon 4 : Configuration des comptes de services administrés | 7-42 |
| Atelier pratique : Sécurisation AD DS | 7-50 |
| Révision du module et Takeaways | 7-61 |

Module 8 : Déploiement et gestion AD CS

| | |
|---|------|
| Vue d'ensemble du module | 8-1 |
| Leçon 1 : Déploiement des AC | 8-2 |
| Leçon 2 : Administration des AC | 8-12 |
| Leçon 3 : Dépannage et maintien des AC | 8-23 |
| Atelier pratique : Déploiement et configuration d'une hiérarchie AC à deux niveaux | 8-31 |
| Contrôle des acquis et éléments à retenir | 8-35 |

Module 9 : Déploiement et gestion des certificats

| | |
|--|------|
| Vue d'ensemble du module | 9-1 |
| Leçon 1 : Déploiement et gestion de modèles de certificats | 9-2 |
| Leçon 2 : Gestion du déploiement, de la révocation et de la récupération de certificats | 9-9 |
| Leçon 3 : Utilisation de certificats dans un contexte commercial | 9-20 |
| Leçon 4 : Mise en œuvre et gestion des cartes à puce | 9-29 |
| Atelier pratique : Déploiement et utilisation de certificats | 9-36 |
| Révision du module et Takeaways | 9-43 |

Module 10 : Déploiement et administration d'AD FS

| | |
|--|-------|
| Présentation du module | 10-1 |
| Leçon 1 : Présentation de AD FS | 10-2 |
| Leçon 2 : Exigences et planification AD FS | 10-11 |
| Leçon 3 : Déploiement et configuration AD FS | 10-25 |
| Leçon 4 : Présentation du proxy d'application Web | 10-42 |
| Atelier pratique : Implémentation de AD FS | 10-53 |
| Module Review and Takeaways | 10-64 |

Module 11 : Implémentation et administration d'AD RMS

| | |
|--|-------|
| Présentation du module | 11-1 |
| Leçon 1 : Présentation de AD RMS | 11-2 |
| Leçon 2 : Déploiement et gestion d'une infrastructure AD RMS | 11-12 |
| Leçon 3 : Configurer la protection de contenu AD RMS | 11-22 |
| Atelier pratique : Implémentation d'une infrastructure AD RMS | 11-28 |
| Contrôle des acquis et éléments à retenir | 11-34 |

Module 12 : Mise en œuvre de la synchronisation AD DS avec Microsoft Azure AD

| | |
|--|-------|
| Vue d'ensemble du module | 12-1 |
| Leçon 1 : Planification et préparation pour la synchronisation de répertoires | 12-2 |
| Leçon 2 : Mise en œuvre de synchronisation de répertoires en utilisant Azure AD Connect | 12-13 |
| Leçon 3 : Gestion des identités avec la synchronisation de répertoires | 12-23 |
| Atelier pratique : Configuration de la synchronisation des annuaires | 12-38 |
| Contrôle des acquis et éléments à retenir | 12-44 |

Module 13 : Surveillance, gestion et récupération AD DS

| | |
|---|-------|
| Vue d'ensemble du module | 13-1 |
| Leçon 1 : Surveillance de AD DS | 13-2 |
| Leçon 2 : Gestion de la base de données Active Directory | 13-12 |
| Leçon 3 : Sauvegarde de Active Directory et options de récupération pour AD DS et autres solutions d'identité et d'accès | 13-19 |
| Atelier pratique : Récupération d'objets dans AD DS | 13-28 |
| Contrôle des acquis et éléments à retenir | 13-33 |

Corrigés des ateliers pratiques

| | |
|--|---------|
| Atelier du module 1 : Déploiement et administration d'AD DS | L1-1 |
| Atelier pratique A du module 2 : Gestion des objets AD DS | L2-7 |
| Atelier pratique B du module 2 : Administration AD DS | L2-11 |
| Atelier du module 3 : Domaine et gestion des approbations dans AD DS | L3-17 |
| Atelier du module 4 : Mise en œuvre des sites AD DS et réPLICATION | L4-23 |
| Atelier pratique A du module 5 : Implémentation d'une infrastructure de stratégie de groupe | L5-31 |
| Atelier pratique B du module 5 : Dépannage de l'infrastructure de stratégie de groupe | L5-35 |
| Atelier du module 6 : Gestion des paramètres de l'utilisateur avec la stratégie de groupe | L6-41 |
| Atelier du module 7 : Sécurisation AD DS | L7-51 |
| Atelier du module 8 : Déploiement et configuration d'une hiérarchie AC à deux niveaux | L8-65 |
| Atelier du module 9 : Déploiement et utilisation de certificats | L9-71 |
| Atelier du module 10 : Implémentation d'AD FS | L10-79 |
| Atelier du module 11 : Implémentation d'une infrastructure AD RMS | L11-91 |
| Atelier du module 12 : Configuration de la synchronisation des annuaires | L12-99 |
| Atelier du module 13 : Récupération d'objets dans AD DS | L13-105 |

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

 **Remarque :** Cette première version MOC du cours 22742A (version « A ») a été développée sur Windows Server 2016 Technical Preview 5. Microsoft Learning publiera une version « B » de ce cours avec des diapositives PowerPoint améliorées et le contenu d'accompagnement du cours sur le site de Microsoft Learning.

Ce cours d'une durée de cinq jours et dirigé par un instructeur apprend aux professionnels de l'informatique à déployer et à configurer AD DS (Active Directory Domain Services) dans un environnement distribué, à mettre en œuvre la stratégie de groupe, à effectuer une sauvegarde et une restauration, et à surveiller et résoudre les problèmes liés à Active Directory dans Windows Server 2016. En outre, il apprend aux stagiaires à déployer d'autres rôles de serveur Active Directory, comme les services AD FS (Active Directory Federation Services) et les AD CS (Active Directory Certificate Services).

Public visé

Ce cours s'adresse principalement aux professionnels de l'informatique en exercice qui disposent de connaissances et d'une expérience dans le domaine de AD DS, et qui souhaitent enrichir leurs connaissances sur les technologies d'identité et d'accès de Windows Server 2016. Cette audience comprend généralement des :

- Administrateurs de AD DS qui souhaitent se former aux technologies d'identité et d'accès de Windows Server 2016 ;
- Administrateurs système ou d'infrastructure qui disposent d'une expérience et de connaissances générales dans le domaine de AD DS et qui souhaitent se former aux technologies d'identité et d'accès de base et avancées de Windows Server 2016.

Ce cours s'adresse en deuxième lieu aux professionnels de l'informatique qui souhaitent renforcer leurs connaissances sur AD DS et les technologies connexes, ainsi qu'aux professionnels de l'informatique qui souhaitent se préparer à l'examen 70-742.

Connaissances préalables des stagiaires

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

- Expérience dans les concepts et technologies AD DS dans Windows Server 2012 ou Windows Server 2016 ;
- Expérience dans l'utilisation et la configuration de Windows Server 2012 ou Windows Server 2016 ;
- Expérience et compréhension des technologies de mise en réseau de base tels que l'adressage IP, la résolution de nom et Dynamic Host Configuration Protocol (DHCP) ;
- Expérience de l'utilisation et compréhension de Microsoft Hyper-V et des concepts de base de serveurs de virtualisation ;
- Sensibilité aux meilleures pratiques de sécurité de base ;
- Expérience pratique de l'utilisation de systèmes d'exploitation clients Windows tels que Windows 7, Windows 8, Windows 8.1 ou Windows 10 ;
- Expérience de base avec l'interface en ligne de commande Windows PowerShell.

Objectifs du cours

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

- Installer et configurer des contrôleurs de domaine ;
- Gérer des objets dans AD DS à l'aide d'outils graphiques et de Windows PowerShell ;
- Mettre en œuvre AD DS dans des environnements complexes ;
- Mettre en œuvre des sites AD DS, configurer et gérer la réPLICATION ;
- Implémenter et gérer des objets de stratégie de groupe (GPO) ;
- Configurer les paramètres d'utilisation à l'aide des GPO ;
- Sécuriser AD DS et les comptes d'utilisateurs ;
- Mettre en œuvre et gérer une hiérarchie d'autorités de certification (AC) avec AD CS ;
- Déployer et gérer des certificats ;
- Mettre en œuvre et administrer AD FS ;
- Mettre en œuvre et administrer Active Directory Rights Management Services (AD RMS) ;
- Mettre en œuvre la synchronisation entre AD DS et Azure AD ;
- Surveiller, dépanner et établir la continuité des activités pour les services AD DS.

Plan du cours

Le plan du cours est le suivant :

Le **module 1**, « Installation et configuration des contrôleurs de domaine », décrit les caractéristiques de AD DS et la démarche à suivre pour installer les contrôleurs de domaine (CD). Il couvre également les considérations relatives au déploiement des contrôleurs de domaine.

Le **module 2**, « Gestion des objets dans AD DS », décrit comment utiliser différentes techniques pour gérer les objets dans AD DS. Cela inclut la création et la configuration d'objets utilisateur, groupe et ordinateur.

Le **module 3**, « Gestion de l'infrastructure AD DS avancée », décrit comment planifier et mettre en œuvre un déploiement AD DS qui comprend de multiples domaines et forêts. Le module fournit un aperçu des composants dans un déploiement AD DS avancé, le processus de mise en œuvre d'un environnement AD DS distribué et la procédure de configuration des approbations AD DS.

Le **module 4**, « Mise en œuvre et administration des sites AD DS et de la réPLICATION », décrit comment planifier et mettre en œuvre un déploiement AD DS multi-sites. Le module explique comment fonctionne la réPLICATION dans un environnement AD DS avec un serveur Windows 2016.

Le **module 5**, « Mise en œuvre d'une stratégie de groupe », décrit comment mettre en place une infrastructure GPO. Le module fournit un aperçu des composants et des technologies qui constituent la structure de la stratégie de groupe.

Le **module 6**, « Gestion des paramètres de l'utilisateur avec la stratégie de groupe », décrit comment configurer les paramètres et les préférences de stratégie de groupe. Cela inclut la mise en œuvre des modèles d'administration, la configuration de la redirection de dossiers et des scripts, et la configuration des préférences de stratégie de groupe.

Le **module 7**, « Sécurisation des services de domaine Active Directory », décrit comment configurer la sécurité du contrôleur de domaine, la sécurité des comptes, la sécurité des mots de passe et les comptes de service gérés de groupe.

Le **module 8**, « Déploiement et gestion de AD CS », décrit comment mettre en œuvre un déploiement AD CS. Cela comprend le déploiement, l'administration et le dépannage des AC.

Le **module 9**, « Déploiement et gestion des certificats », décrit comment déployer et gérer les certificats dans un environnement AD DS. Cela implique le déploiement et la gestion des modèles de certificats, la gestion de la révocation et de la récupération des certificats, l'utilisation de certificats dans un environnement professionnel et la mise en œuvre des cartes à puce.

Le **module 10**, « Déploiement et administration de AD FS », décrit AD FS et la marche à suivre pour configurer AD FS dans un scénario d'organisation unique et dans un scénario avec organisation partenaire.

Le **module 11**, « Mise en œuvre et administration de AD RMS », décrit comment mettre en œuvre un déploiement AD RMS. Le module fournit un aperçu de AD RMS, explique comment déployer et gérer une infrastructure AD RMS, et comment configurer la protection du contenu de AD RMS.

Le **module 12**, « Mise en œuvre d'une synchronisation de AD DS avec Microsoft Azure AD », explique comment planifier et configurer une synchronisation de répertoires entre Microsoft Azure Active Directory (AD Azure) et AD DS sur site. Le module décrit différents scénarios de synchronisation, tels que Azure AD sync, AD FS, Azure AD et Azure AD Connect.

Le **module 13**, « Surveillance, gestion et récupération de AD DS », décrit comment surveiller, gérer et maintenir AD DS pour atteindre une haute disponibilité.

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** : Elles vous guident dans les objectifs de formation et fournissent les points clés essentiels pour un apprentissage en classe réussi.
 - **Ateliers pratiques** : Ils fournissent une plateforme pratique et ancrée dans la réalité qui vous permettra de mettre en application les connaissances et compétences acquises dans le module.
 - **Contrôle des acquis et éléments à retenir** : Ils fournissent une documentation de référence pratique qui favorise la mémorisation des connaissances et compétences.
 - **Corrigés des ateliers pratiques** : Ils fournissent des instructions pas à pas.



Lectures supplémentaires : Contenu d'accompagnement du cours sur le site

<http://www.microsoft.com/learning/fr/fr/companion-moc.aspx> : 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** : Ils incluent le contenu d'accompagnement du cours, tel que les questions et les réponses, les étapes détaillées de la démonstration et des liens de lectures supplémentaires 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, avec les questions et réponses de contrôle des acquis, les bonnes pratiques, des astuces et réponses sur les problèmes courants et la résolution des problèmes, des scénarios et problèmes concrets avec les réponses.
- **Ressources** : Elles incluent des ressources supplémentaires présentées par catégorie 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 mcspprt@microsoft.com. Pour obtenir des informations sur le programme MCP (Microsoft Certification Program), envoyez un message électronique à l'adresse mcphelp@microsoft.com.

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 Hyper-V pour réaliser les ateliers pratiques.

 **Remarque :** À la fin de chaque atelier pratique, vous devez rétablir l'instantané 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 |
|--------------------|---|
| 22742A-LON-DC1 | Contrôleur de domaine dans le domaine Adatum.com |
| 22742A-LON-DC2 | Contrôleur de domaine dans le domaine Adatum.com |
| 22742A-TOR-DC1 | Contrôleur de domaine dans le domaine Adatum.com (sur un autre site) |
| 22742A-TREY-DC1 | Contrôleur de domaine dans le domaine Treyresearch.com |
| 22742A-LON-SVR1 | Serveur membre dans le domaine Adatum.com |
| 22742A-LON-SVR2 | Serveur membre dans le domaine Adatum.com avec le rôle de serveur Web |
| 22742A-CA-SRV1 | Serveur hors domaine à utiliser AC racine hors ligne |
| 22742A-LON-CL1 | Windows 10 client avec Microsoft Office 2016 installé |
| 22742A-LON-CL2 | Windows 10 client avec Office 2016 installé |

Configuration logicielle

Les logiciels suivants sont installés sur chaque ordinateur virtuel :

- Windows Server 2016 TP5
- Windows 10 Entreprise
- Microsoft Office Professional 2016
- Microsoft Active Directory Replication Status Tool

Configuration de la classe

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

Niveau des éléments matériels du cours

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

- Processeur Intel VT (Intel Virtualization Technology) ou AMD-V (AMD Virtualization)
- Disque dur : Disques durs double SATA 7200 tr/min de 500 gigaoctets (Go) nommés disque C et disque D
- 16 Go de mémoire vive (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, avec 16 couleurs.

Module 1

Installation et configuration de contrôleurs de domaine

Sommaire :

| | |
|---|------|
| Vue d'ensemble du module | 1-1 |
| Leçon 1 : Vue d'ensemble de AD DS | 1-2 |
| Leçon 2 : Vue d'ensemble des contrôleurs de domaine AD DS | 1-15 |
| Leçon 3 : Déploiement d'un contrôleur de domaine | 1-24 |
| Atelier pratique : Déploiement et administration de AD DS | 1-36 |
| Révision du module et éléments à retenir | 1-41 |

Vue d'ensemble du module

Active Directory Domain Services (AD DS) et ses services connexes constituent les fondements de réseaux d'entreprises qui exécutent des systèmes d'exploitation Windows. La base de données AD DS est le magasin central de tous les objets de domaine tels que les comptes d'utilisateurs, les comptes d'ordinateurs et les groupes. AD DS fournit un répertoire hiérarchique consultable et une méthode pour appliquer des paramètres de configuration et de sécurité pour les objets dans l'entreprise. Ce module couvre la structure AD DS et ses divers composants tels que les forêts, les domaines et les unités d'organisation (UO).

Avec un intérêt croissant pour les environnements de cloud et hybrides, Windows Server 2016 inclut plusieurs nouvelles fonctionnalités AD DS qui facilitent la gestion de ces environnements. Ce module aborde les caractéristiques et les choix disponibles dans Windows Server 2016 pour installer AD DS sur un serveur avec un aperçu des contrôleurs de domaine.

Objectifs

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

- Décrire AD DS et ses principaux composants
- Décrire l'objectif des contrôleurs de domaine et des rôles correspondants
- Décrire les éléments à prendre en compte pour le déploiement des contrôleurs de domaine
- Déployer un contrôleur de domaine

Leçon 1

Vue d'ensemble de AD DS

La base de données AD DS stocke des informations sur l'identité des utilisateurs, des ordinateurs, des groupes, des services et des ressources dans une structure hiérarchique, appelée *annuaire*. Les contrôleurs de domaine AD DS hébergent également le service qui authentifie les comptes d'utilisateurs et d'ordinateurs lorsqu'ils se connectent au domaine. Parce que les services AD DS stocke des informations sur tous les objets dans le domaine et que tous les utilisateurs et les ordinateurs doivent se connecter aux contrôleurs de domaine AD DS lorsqu'ils se connectent au réseau, AD DS est le principal moyen par lequel vous pouvez configurer et gérer les comptes utilisateur et ordinateurs dans votre réseau.

Cette leçon porte sur les composants logiques de base et les composants physiques qui composent le déploiement d'un AD DS.

Objectifs de la leçon

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

- Décrire les composants de AD DS
- Décrire les domaines AD DS
- Décrire les UO et leur but
- Décrire les forêts et les arbres de AD DS et expliquer comment les déployer dans un réseau
- Expliquer comment un schéma AD DS fournit un ensemble de règles qui régissent les objets et les attributs qui sont stockés dans la base de données de domaine AD DS
- Décrire Microsoft Azure Active Directory (AD Azure)
- Identifier les outils disponibles pour administrer les services AD DS
- Décrire ce qui est nouveau pour Active Directory local dans Windows Server 2016

Vue d'ensemble de AD DS

Les services AD DS sont constitués de composants logiques et physiques. Vous devez comprendre la façon dont les composants AD DS travaillent ensemble afin que vous puissiez gérer efficacement votre infrastructure. En outre, vous pouvez utiliser de nombreuses autres options des services AD DS pour l'installation, la configuration et la mise à jour des applications, la gestion de l'infrastructure de sécurité, l'activation du service d'accès à distance et de DirectAccess, et l'émission ainsi que la gestion de certificats numériques.

AD DS est constitué de composants logiques et physiques

| Composants logiques | Composants physiques |
|---|--|
| <ul style="list-style-type: none">• Cloisons• Schéma• Domaines• Arborescences de domaine• Forêts• Sites• Unités d'organisation• Conteneurs | <ul style="list-style-type: none">• Les contrôleurs de domaine• Magasins de données• Serveurs de catalogue global• RODC |

L'une des fonctionnalités AD DS les plus utilisées est la stratégie de groupe qui vous permet de configurer des politiques centralisées que vous pouvez utiliser pour gérer la plupart des objets dans les services AD DS. Comprendre les différents composants AD DS est important pour utiliser la stratégie de groupe à bon escient.



Remarque : la stratégie de groupe est abordée plus en détail dans le module 5, « Mise en œuvre de la stratégie de groupe ».

Composants logiques

Les composants logiques AD DS sont des structures que vous utilisez pour mettre en œuvre une conception AD DS adéquate pour une organisation. Le tableau suivant décrit les types de structures logiques contenus dans une base de données AD DS.

| Composants logiques | Description |
|-------------------------|--|
| Partition | Une partition, appelée aussi contexte d'appellation, est une partie de la base de données AD DS. Bien que la base de données soit un fichier nommé Ndts.dit, différentes partitions contiennent des données différentes. Par exemple, la partition de schéma contient une copie du schéma de Active Directory. La partition de configuration contient les objets de configuration de la forêt et la partition de domaine contient les utilisateurs, les ordinateurs, les groupes et d'autres objets spécifiques au domaine. Des copies d'une partition peuvent être stockées sur plusieurs contrôleurs de domaine et mises à jour grâce à la réPLICATION d'annuaire. |
| Schéma | Un schéma est l'ensemble des définitions des types d'objets et des attributs que vous utilisez pour définir les objets créés dans les services AD DS. |
| Domaine | Un domaine est un conteneur administratif logique pour des objets tels que les utilisateurs et les ordinateurs. Un domaine mène à une partition spécifique et peut être organisé avec des relations parent-enfant avec d'autres domaines. |
| Arborescence de domaine | Un arbre de domaine est un ensemble hiérarchique de domaines qui partagent un domaine racine commun et un DNS (Domain Name System) contigu. |
| Forêt | Une forêt est un ensemble de domaines qui partagent une racine et un schéma AD DS communs et qui s'accordent une confiance mutuelle. |
| Site | Un site est un conteneur pour les objets AD DS tels que les ordinateurs et les services qui sont définis par leur emplacement physique. Ceci est en comparaison à un domaine qui représente la structure logique des objets tels que des utilisateurs et les groupes, en plus des ordinateurs. |
| Sous-réseau | Un sous-réseau est une partie des adresses IP du réseau d'une organisation affectée aux ordinateurs d'un site. Un site peut avoir plus d'un sous-réseau. |
| UO | Une UO est un objet conteneur pour les utilisateurs, les groupes et les ordinateurs qui fournit un cadre pour déléguer des droits d'administration et l'administration en liant les objets de stratégie de groupe (GPO). |
| Conteneur | Un conteneur est un objet qui fournit un cadre organisationnel pour une utilisation dans AD DS. Certains conteneurs sont créés par défaut ou vous pouvez créer des conteneurs personnalisés. Les conteneurs ne peuvent pas avoir de GPO liés à eux. |

Composants physiques

Le tableau suivant décrit certains des composants physiques AD DS.

| Composants physiques | Description |
|---|--|
| Contrôleur de domaine | Un contrôleur de domaine contient une copie de la base de données AD DS. Pour la plupart des opérations, chaque contrôleur de domaine peut traiter des changements et reproduire les modifications apportées à tous les autres contrôleurs de domaine dans le domaine. |
| Banque de données | Une copie de la banque de données existe sur chaque contrôleur de domaine. La base de données AD DS utilise la technologie de base de données Microsoft Jet et stocke les informations du répertoire dans le fichier Ntds.dit et les fichiers journaux associés. Ces fichiers sont stockés dans le dossier C:\Windows\NTDS par défaut. |
| Serveur de catalogue global | Un serveur de catalogue global est un contrôleur de domaine qui héberge le <i>catalogue global</i> qui est une copie partielle-en lecture seule de tous les objets dans une forêt à plusieurs domaines. Un catalogue global accélère les recherches pour les objets qui pourraient être stockés sur les contrôleurs de domaine dans un domaine différent de la forêt. |
| Contrôleur de domaine en lecture seule (RODC) | Un RODC est une installation spéciale, en lecture-seule de AD DS. Les RODC sont souvent utilisés dans les succursales où la sécurité physique ne peut pas être garantie ou dans lesquelles le support informatique est moins avancé que dans les principaux centres d'affaires. Il se peut aussi qu'il y ait des applications du cœur de métier qui doivent fonctionner dans un contrôleur de domaine. |



Lectures supplémentaires : Pour plus d'informations sur les domaines et les forêts, consultez le site suivant : « Vue d'ensemble des services de domaine Active Directory », à l'adresse <http://aka.ms/M2lr5a>

Qu'est-ce que le schéma AD DS ?

Le *schéma AD DS* est le composant qui définit toutes les classes d'objets et les attributs que AD DS utilise pour stocker des données. Tous les domaines d'une forêt contiennent une copie du schéma qui s'applique à cette forêt. Toute modification apportée au schéma est répliquée sur chaque contrôleur de domaine dans la forêt à partir du contrôleur de schéma qui est généralement le premier contrôleur de domaine dans la forêt.

Les services AD DS stockent et récupèrent des informations à partir d'une grande variété

d'applications et de services. Il le fait, en partie, en standardisant la façon dont les données sont stockées dans l'annuaire AD DS. En normalisant le stockage de données, les services AD DS peuvent récupérer, mettre à jour et reproduire des données tout en aidant à garantir le maintien de l'intégrité de celles-ci.

| Nom | Type | Système | Description | Classe Source |
|----------------------------|------------|---------|--------------------------------------|----------------------|
| cn | Facultatif | Oui | Common-Name | posixAccount |
| co | Facultatif | Oui | Text-Comment | organizationalPerson |
| l | Facultatif | Oui | Text-Country | organizationalPerson |
| o | Facultatif | Oui | Text-Organization | organizationalPerson |
| sn | Facultatif | Oui | Text-Surname | organizationalPerson |
| givenName | Facultatif | Oui | Text-GivenName | organizationalPerson |
| mail | Facultatif | Oui | Text-Email-Address | organizationalPerson |
| telephoneNumber | Facultatif | Oui | Text-TelNumber | organizationalPerson |
| facsimileTelephoneNumber | Facultatif | Oui | Text-FaxNumber | organizationalPerson |
| streetAddress | Facultatif | Oui | Text-Street-Address | organizationalPerson |
| postOfficeBox | Facultatif | Oui | Text-Post-Office-Box | organizationalPerson |
| registeredAddress | Facultatif | Oui | Text-Registered-Address | organizationalPerson |
| preferredDeliveryMethod | Facultatif | Oui | Text-Preferred-Delivery-Method | organizationalPerson |
| physicalDeliveryOfficeName | Facultatif | Oui | Text-Physical-Delivery-Office-Name | organizationalPerson |
| ipPhone | Facultatif | Oui | Text-Phone-Ip-Primary | organizationalPerson |
| pager | Facultatif | Oui | Text-Phone-Pager | organizationalPerson |
| mobile | Facultatif | Oui | Text-Phone-Mobile-Primary | organizationalPerson |
| cell | Facultatif | Oui | Text-Phone-Mobile-Other | organizationalPerson |
| otherTelephone | Facultatif | Oui | Text-Phone-Other | organizationalPerson |
| internationalISDNNumber | Facultatif | Oui | Text-Phone-International-ISDN-Number | organizationalPerson |
| telephoneNumber | Facultatif | Oui | Text-Phone-Primary | organizationalPerson |
| otherTelephone | Facultatif | Oui | Text-Phone-Other | organizationalPerson |

Objets

Les services AD DS utilisent des objets comme unités de stockage. Tous les types d'objet sont définis dans le schéma. Chaque fois que l'annuaire gère des données, celui-ci interroge le schéma pour une définition d'objet appropriée. Sur la base de la définition de l'objet dans le schéma, l'annuaire crée l'objet et stocke les données.

Les définitions de l'objet précisent à la fois les types de données que les objets peuvent stocker et la syntaxe des données. Vous pouvez uniquement créer des objets qui sont définis par le schéma. Parce que les données sont stockées dans un format rigide défini, les services AD DS peuvent stocker, extraire et valider les données qu'ils gèrent, quelle que soit l'application qui les fournit.

Les relations entre les objets, les règles, les attributs et les classes

Dans les services AD DS, le schéma définit les éléments suivants :

- Les objets qui stockent les données dans l'annuaire
- Les règles qui définissent la structure des objets
- La structure et le contenu de l'annuaire lui-même

Les objets du schéma AD DS se composent d'attributs qui sont regroupés en classes. Chaque classe a des règles qui définissent les attributs obligatoires et optionnels. Par exemple, la classe **utilisateur** se compose de plus de 400 attributs possibles, y compris **cn** (l'attribut nom commun), **prénom**, **afficher un nom**, **SID de l'objet** et **gestionnaire**. Parmi ces attributs, **cn** et **SID de l'objet** sont obligatoires. L'attribut **cn** est défini comme une chaîne unicode à valeur unique qui comprend 1 à 64 caractères et qui est reproduite dans le catalogue global.

Modification du schéma

Seuls les membres du groupe administrateurs du schéma peuvent modifier le schéma AD DS. Vous ne pouvez rien supprimer à partir du schéma AD DS. Vous ne pouvez qu'étendre le schéma AD DS en utilisant les extensions de schéma AD DS ou en modifiant les attributs des objets existants. Par exemple, lorsque vous vous apprêtez à installer Exchange Server 2016, vous devez appliquer les changements de schéma Exchange Server 2016 Active Directory. Ces changements ajoutent ou modifient des centaines de classes et attributs.

Vous devez modifier le schéma uniquement lorsque cela est nécessaire parce que le schéma dicte comment les informations sont stockées et les modifications apportées au schéma affectent chaque contrôleur de domaine. Avant de modifier le schéma, vous devez analyser les changements par le biais d'un processus minutieusement contrôlé et les mettre en œuvre uniquement après avoir effectué des tests pour veiller à ce que ceux-ci ne nuisent pas au reste de la forêt ou aux applications qui utilisent les services AD DS.

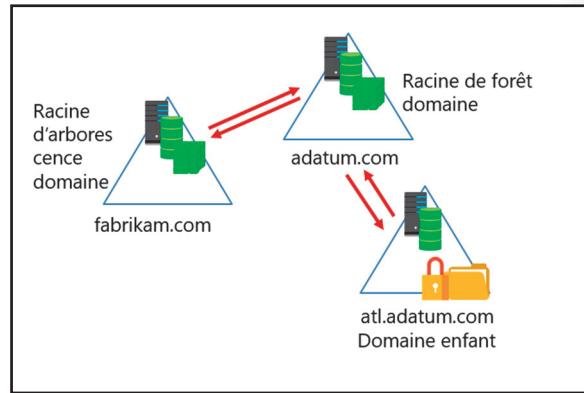
Le contrôleur de schéma est l'un des rôles de maître d'opérations qui est hébergé sur un seul contrôleur de domaine dans les services AD DS. Parce qu'il est un maître unique, vous devez apporter des modifications au schéma en ciblant le contrôleur de domaine qui héberge le contrôleur de schéma en utilisant le composant logiciel enfichable Active Directory Schema. Pour cibler le contrôleur de schéma dans une forêt distincte, vous aurez besoin de cibler la forêt appropriée au sein du composant logiciel enfichable.



Remarque : les rôles de maître d'opérations sont abordés en détail dans la rubrique « Que sont les contrôleurs d'opérations ? ».

Qu'est-ce qu'une forêt AD DS ?

Une forêt est un conteneur de niveau supérieur dans les services AD DS. Chaque *forêt* est un ensemble d'un ou plusieurs arbres de domaine qui partagent un schéma d'annuaire et un catalogue global communs. Un arbre de domaine est un ensemble d'un ou plusieurs domaines qui partagent un espace de noms contigu. Le premier domaine qui est créé dans la forêt est le *domaine racine de la forêt*. Le domaine racine de la forêt contient quelques objets qui n'existent pas dans d'autres domaines de la forêt. Parce que ces objets sont toujours conçus sur le premier contrôleur de domaine qui est créé, une forêt peut consister en un seul domaine avec un seul contrôleur de domaine ou elle peut être constituée de centaines de domaines à travers de multiples arbres de domaine. Les objets suivants existent uniquement dans le domaine racine de la forêt :



- Rôle de maître de schéma. Ceci est un rôle particulier de contrôleur de domaine à l'échelle de la forêt. Un seul maître de schéma existe dans toute la forêt. Le schéma ne peut être modifié que sur le contrôleur de domaine qui détient le maître de schéma.
- Le rôle de maître d'opérations des noms de domaine Ceci est également, un rôle particulier de contrôleur de domaine à l'échelle de la forêt. Un seul maître d'opérations des noms de domaine existe dans toute la forêt. Seul le maître d'opérations des noms de domaine peut ajouter de nouveaux noms de domaine dans l'annuaire
- Le groupe administrateurs de l'entreprise Par défaut, le groupe administrateurs de l'entreprise a le compte administrateur pour le domaine racine de la forêt en tant que membre. Le groupe administrateurs de l'entreprise est un membre du groupe administrateurs local dans chaque domaine de la forêt. Cela permet aux membres du groupe administrateurs de l'entreprise d'avoir des droits de contrôle administratifs complets pour chaque domaine dans la forêt
- Le schéma du groupe administrateurs Par défaut, ce groupe n'a pas de membres. Seuls les membres du groupe administrateurs de l'entreprise ou le groupe administrateurs du domaine (dans le domaine racine de la forêt) peuvent ajouter des membres au groupe administrateurs du schéma. Seuls les membres du groupe administrateurs du schéma peuvent apporter des modifications au schéma

Limite de sécurité

Une forêt AD DS est une limite de sécurité. Par défaut, aucun utilisateur de l'extérieur de la forêt ne peut accéder aux ressources à l'intérieur de la forêt. Généralement, une organisation ne crée qu'une seule forêt mais vous pouvez créer plusieurs forêts pour isoler des autorisations administratives entre les différentes parties de l'entreprise.

Par défaut, tous les domaines d'une forêt font automatiquement confiance aux autres domaines de la forêt. Cela contribue à faciliter l'accès aux ressources telles que les partages de fichiers et de sites Web pour tous les utilisateurs dans une forêt, quel que soit le domaine dans lequel un compte d'utilisateur se trouve.

Limite de réPLICATION

Une forêt AD DS est la limite de réPLICATION pour les partitions de configuration et de schéma dans la base de données AD DS. Par conséquent, tous les contrôleurs de domaine de la forêt doivent partager le même schéma. Pour cette raison, les organisations qui souhaitent déployer des applications avec des schémas incompatibles doivent déployer des forêts supplémentaires.

La forêt AD DS est aussi la limite de réPLICATION du catalogue global. Le catalogue global permet de trouver des objets de tout domaine dans la forêt. Par exemple, le catalogue global est sollicité à chaque

fois que des informations d'identification relatives au nom d'utilisateur principal (UPN) sont utilisées ou lors d'une recherche dans les carnets d'adresses Microsoft Exchange Server pour trouver des utilisateurs.

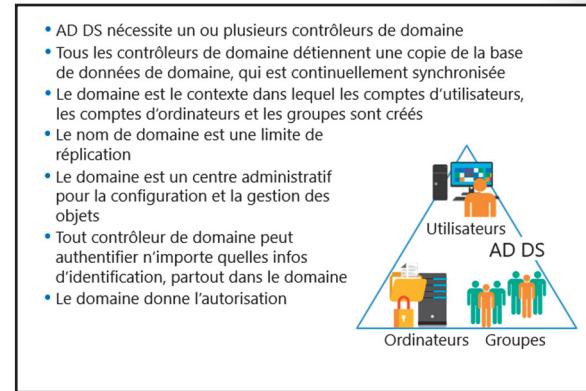
Qu'est-ce qu'un domaine AD DS ?

Domaine AD DS : un conteneur pour les utilisateurs, les ordinateurs, les groupes, etc.

Un domaine AD DS est un conteneur logique utilisé pour gérer l'utilisateur, l'ordinateur, le groupe et d'autres objets. Tous les objets du domaine sont stockés dans la base de données AD DS dont une copie se trouve sur chaque contrôleur de domaine.

De nombreux types d'objets existent dans la base de données AD DS. Vous travaillez le plus souvent avec des comptes d'utilisateurs, des comptes d'ordinateurs et des groupes. La liste suivante décrit brièvement ces trois types d'objets :

- Comptes d'utilisateurs Les comptes d'utilisateurs contiennent des informations sur les utilisateurs, y compris les informations requises pour authentifier un utilisateur pendant le processus-connexion et pour créer le jeton d'accès de l'utilisateur
- Les comptes d'ordinateurs Chaque ordinateur du domaine dispose d'un compte dans les services AD DS. Les comptes d'ordinateurs sont utilisés pour les ordinateurs appartenant à un domaine de la même manière que les comptes d'utilisateurs sont utilisés pour les utilisateurs
- Groupes Les groupes sont utilisés pour organiser les utilisateurs ou les ordinateurs afin de faciliter la gestion des autorisations et la stratégie de groupe dans le domaine



Le domaine AD DS est une limite de réPLICATION

Lorsque des modifications sont apportées à un objet quelconque dans le domaine, le contrôleur de domaine où le changement est survenu réplique ce changement à tous les autres contrôleurs de domaine dans le domaine. Si plusieurs domaines existent dans la forêt, seuls les sous-ensembles des modifications sont répliqués aux autres domaines. Les services AD DS utilisent un modèle de réPLICATION multimaître qui permet à chaque contrôleur de domaine d'apporter des modifications aux objets dans le domaine.

Les services AD DS permettent à un seul domaine de contenir près de 2 milliards d'objets. Avec une telle capacité, la plupart des organisations peuvent ne déployer qu'un seul domaine pour veiller à ce que tous les contrôleurs de domaine contiennent toutes les informations de domaine. Toutefois, les organisations qui ont décentralisé les structures administratives ou qui sont réparties sur plusieurs sites pourraient envisager déployer plusieurs domaines dans la même forêt pour répondre aux besoins administratifs de leurs environnements.

Le domaine AD DS est un centre administratif

Le domaine comporte un compte d'administrateur et un groupe administrateurs de domaine. Par défaut, le compte administrateur est un membre du groupe administrateurs de domaine et le groupe administrateurs de domaine est membre de chaque groupe d'administrateurs local des ordinateurs appartenant à un domaine. En outre, par défaut, les membres du groupe administrateurs du domaine ont un contrôle total sur tous les objets dans le domaine. Le compte administrateur dans le domaine racine de la forêt a des droits supplémentaires, comme détaillé dans la rubrique « Qu'est-ce qu'une forêt AD DS ? » plus loin dans ce module.

Le domaine AD DS fournit une authentification

Chaque fois qu'un ordinateur appartenant au domaine démarre ou qu'un utilisateur se connecte à un ordinateur du domaine, les services AD DS l'authentifie. L'authentification permet de vérifier que l'ordinateur ou l'utilisateur dispose des informations d'identification appropriées pour un compte AD DS.

Le domaine AD DS fournit une autorisation

Les systèmes d'exploitation Windows utilisent les technologies d'autorisation et de contrôle d'accès pour permettre aux utilisateurs authentifiés d'accéder aux ressources. En règle générale, le processus d'autorisation est effectué localement au niveau de la ressource. Le contrôle d'accès dynamique sur la base du domaine permet d'avoir des règles d'accès central pour contrôler l'accès aux ressources. Les règles d'accès central ne remplacent pas la technologie de contrôle d'accès actuelle mais fournissent un niveau de contrôle supplémentaire.



Remarque : le contrôle d'accès dynamique (Dynamic Access Control ou DAC) est une fonctionnalité introduite dans Windows Server 2012 qui permet aux administrateurs de définir des règles qui contrôlent les autorisations d'accès. Le DAC est abordé plus en détail dans le cours 22744A, « Sécurisation de Windows Server 2016 », Module 11, « Mise en œuvre de l'accès aux données pour les utilisateurs et les périphériques », Leçon 3, « Comprendre le contrôle d'accès dynamique ».

Que sont les UO ?

Une *unité d'organisation* (UO) est un objet conteneur dans un domaine que vous pouvez utiliser pour consolider les utilisateurs, les ordinateurs, les groupes et d'autres objets. Vous pouvez lier des objets de stratégie de groupe (Group Policy Objects ou GPO) directement à une UO pour gérer les objets contenus dans l'unité d'organisation. Vous pouvez également attribuer un gestionnaire de UO et associer une partition COM+ avec une UO.

Vous pouvez créer de nouvelles UO dans les services AD DS à tout moment en utilisant le Centre d'administration Active Directory. Deux raisons existent pour créer une UO :

- Pour grouper des objets ensemble pour une gestion plus facile en appliquant des GPO à l'ensemble du groupe. Lorsque vous affectez des GPO à une UO, les paramètres s'appliquent à tous les objets de l'unité d'organisation. Les GPO sont des politiques créées par les administrateurs pour gérer et configurer les paramètres pour les ordinateurs et / ou les utilisateurs. Vous déployez les GPO en les reliant aux UO, domaines ou sites
- Pour déléguer le contrôle administratif des objets au sein de l'unité d'organisation. Vous pouvez attribuer des autorisations de gestion sur une UO, déléguant ainsi le contrôle de cette unité à un utilisateur ou un groupe au sein des services AD DS en plus du groupe administrateurs du domaine

- Utilisez des conteneurs pour regrouper les objets dans un domaine :
 - Vous ne pouvez pas appliquer les GPO aux conteneurs
 - Les conteneurs sont utilisés pour les objets du système et en tant que valeur par défaut pour les nouveaux objets
- Créez des UO pour :
 - Configurer les objets en leur attribuant les GPO ;
 - Déléguer les autorisations administratives.

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

Conteneurs génériques

Les services AD DS contiennent plusieurs conteneurs intégrés, appelés conteneurs génériques, tels que les utilisateurs et les ordinateurs. Ces conteneurs sont utilisés pour stocker les objets du système ou comme parents par défaut pour les nouveaux objets lors de leur création. Ces objets conteneurs génériques ne doivent pas être confondus avec les UO. La principale différence entre les UO et les conteneurs réside dans les capacités de gestion. Les conteneurs ont des capacités de gestion limitées. Par exemple, vous ne pouvez pas appliquer de GPO directement à un conteneur.

Lorsque vous installez les services AD DS, les UO contrôleurs de domaine et plusieurs objets conteneurs génériques sont créés par défaut. Certains objets par défaut sont utilisés principalement par les services AD DS et sont masqués par défaut. Les objets suivants sont visibles par défaut dans le Centre d'administration AD :

- Domaine Le niveau supérieur de la hiérarchie organisationnelle de domaine
- Conteneur intégré Un conteneur qui stocke plusieurs groupes par défaut
- Conteneur d'ordinateurs L'emplacement par défaut pour les nouveaux comptes d'ordinateur que vous créez dans le domaine
- Conteneur de principaux de sécurité externes L'emplacement par défaut pour les objets approuvés à partir de domaines en dehors de la forêt AD DS. En règle générale, ceux-ci sont créés quand un objet est ajouté à un groupe dans le domaine AD DS à partir d'un domaine externe
- Comptes de service administrés L'emplacement par défaut pour les comptes de services administrés. Les services AD DS fournissent la gestion automatique des mots de passe pour les comptes de services administrés
- Conteneur utilisateurs. L'emplacement par défaut pour les nouveaux comptes d'utilisateurs et les groupes que vous créez dans le domaine. Le conteneur utilisateurs contient également les comptes administrateur et invité pour le domaine et pour certains groupes par défaut
- UO contrôleurs de domaine L'emplacement par défaut pour les comptes d'ordinateurs contrôleurs de domaine. Il s'agit de la seule UO qui est présente dans une nouvelle installation AD DS

Plusieurs conteneurs existent. Vous ne pouvez les voir que lorsque vous cliquez sur **Fonctionnalités avancées** dans le menu **Affichage**. Les objets suivants sont masqués par défaut :

- Répertoire des fichiers perdus et trouvés. Ce conteneur contient des objets orphelins
- Données du programme. Ce conteneur contient des données Active Directory pour les applications Microsoft telles que les services ADFS (Active Directory Federation Services)
- Système Ce conteneur contient les paramètres intégrés du système
- Quotas NTDS Ce conteneur contient des données de quota de service d'annuaire
- Composants TPM Ce conteneur est nouveau avec Windows Server 2016. Il stocke les informations de récupération pour les périphériques de module de plateforme sécurisée (TPM, Trusted Platform Module)

 **Remarque :** les GPO ne peuvent pas être liés aux conteneurs dans un domaine AD DS. Pour lier les GPO afin d'appliquer des configurations et des restrictions, il faut créer une hiérarchie d'unité d'organisation puis lier les GPO à ces dernières.

Conception hiérarchique

La conception d'une hiérarchie d'unité d'organisation est dictée par les besoins administratifs de l'entreprise. La conception pourrait être basée sur les classifications géographiques, fonctionnelles, des ressources ou des utilisateurs. Quel que soit l'ordre, la hiérarchie devrait permettre d'administrer les

ressources des services AD DS aussi efficacement et avec autant de souplesse que possible. Par exemple, si tous les ordinateurs que les administrateurs informatiques utilisent doivent être configurés d'une certaine manière, vous pouvez regrouper tous les ordinateurs dans une unité d'organisation et puis attribuer un GPO pour gérer ces ordinateurs.

Vous pouvez également créer des UO dans les autres UO. Par exemple, votre organisation pourrait avoir plusieurs bureaux et chaque bureau pourrait avoir une équipe d'administrateurs informatiques qui sont responsables de la gestion des comptes d'utilisateurs et d'ordinateurs dans leur bureau. En outre, chaque bureau pourrait avoir différents départements avec des exigences de configuration d'ordinateur différentes. Dans cette situation, vous pouvez créer une unité d'organisation pour chaque bureau, puis au sein de chacune de ces UO, créer une unité d'organisation pour les administrateurs informatiques et une unité d'organisation pour chacun des autres départements.

Bien qu'il n'y ait pas de limite technique au nombre de niveaux dans votre structure d'unité d'organisation, pour faciliter sa gestion, limitez votre structure d'unité d'organisation à un maximum de 10 niveaux. La plupart des organisations utilisent 5 niveaux ou moins pour simplifier l'administration. Notez que les applications qui fonctionnent avec les services AD DS peuvent imposer des restrictions pour la profondeur de l'unité d'organisation dans la hiérarchie pour les parties de la hiérarchie qu'elles utilisent.

Nouveautés de AD DS dans Windows Server 2016

Windows Server 2016 comporte plusieurs nouvelles fonctionnalités dans le cadre des services AD DS lesquelles vous aident à sécuriser votre environnement AD DS et à migrer vers des environnements dans le cloud ou hybrides.

- PAM
- Azure AD Join
- Microsoft Passport

Gestion de l'accès privilégié

La gestion de l'accès privilégié (PAM) est basée sur le gestionnaire d'identité Microsoft. Le PAM vous permet de séparer les autorisations requises pour certaines activités administratives des autorisations des membres de l'environnement AD DS actuel. Avec le PAM, les utilisateurs

demandent l'autorisation d'effectuer des activités qui nécessitent un accès privilégié au lieu d'avoir l'accès accordé sur une base permanente. L'octroi de ces autorisations peut signifier que vous devez prévoir des étapes d'authentification supplémentaires telles que l'authentification multi-facteurs. Lorsque l'utilisateur reçoit l'accès, celui-ci est accordé à titre temporaire par un groupe d'ombres dans une *forêt bastion*. La forêt bastion est un environnement plus propre qui est destiné à être dépourvu de tout accès pour les pirates informatiques ou qui découle d'informations d'identification volées d'utilisateurs privilégiés. Parce que le compte professionnel personnel de l'utilisateur ne possède pas les autorisations requises sur une base permanente, les probabilités d'atteintes à la sécurité sont moindres. Il peut par exemple s'agir de l'accès illégal par un pirate malveillant qui a volé le mot de passe d'un administrateur.



Lectures supplémentaires : pour plus d'informations sur Azure AD Join, reportez-vous à : « Windows 10 pour l'entreprise : plusieurs manières d'utiliser des appareils professionnels » à l'adresse : <http://aka.ms/F7dfxe>

Azure AD Join

Azure Active Directory Join (AD Azure Join) prend en charge la connexion sur site des appareils appartenant à un domaine Azure AD pour l'amélioration des environnements du cloud uniquement et

hybrides. Pour les périphériques appartenant à l'entreprise, les utilisateurs ne doivent plus disposer d'un compte Microsoft personnel. Azure AD prend également en charge des dispositifs de connexion qui ne peuvent normalement pas appartenir à un domaine local tels que les appareils mobiles. Les utilisateurs peuvent accéder au Windows Store avec leurs comptes sur site et même avec leurs appareils personnels. Il existe aussi une prise en charge pour la gestion des périphériques mobiles (MDM), la mise en place des dispositifs partagés et l'imagerie des appareils appartenant à l'entreprise.

 **Documentation supplémentaire :** Pour plus d'informations sur Azure AD Join, reportez-vous à : « Windows 10 pour l'entreprise : plusieurs manières d'utiliser des appareils professionnels » à l'adresse : <http://aka.ms/F7dfxe>

Microsoft Passport

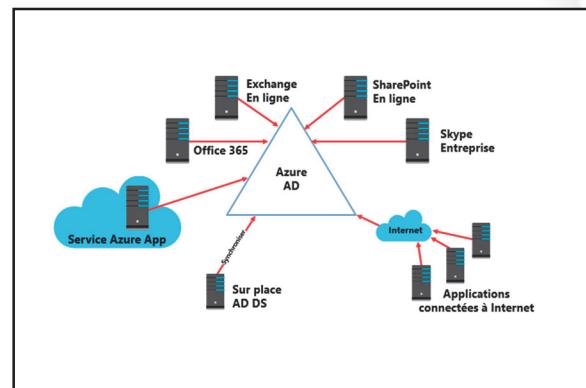
Les services AD DS dans Windows Server 2016 prennent en charge Microsoft Passport, qui fournit une approche d'authentification basée sur les certificats qui peuvent remplacer l'utilisation de mots de passe. Microsoft Passport permet aux utilisateurs de s'authentifier à un compte AD DS sur site, un compte Azure AD ou tout autre service qui prend en charge l'identité rapide en ligne (Fast Identity Online, FIDO). Microsoft Passport est abordé en détail dans le cours, 22744 : Sécurisation de Windows Server 2016.

 **Documentation supplémentaire :** Pour plus d'informations sur l'utilisation de Microsoft Passport avec AD DS dans Windows Server 2016, reportez-vous à : « Authentification des identités sans mot de passe avec Microsoft Passport » à l'adresse : <http://aka.ms/Nyrund>

 **Documentation supplémentaire :** Pour plus d'informations sur les nouvelles fonctionnalités de AD DS dans Windows Server 2016, reportez-vous à : « Quelles sont les nouveautés de la version d'évaluation technique des Services de domaine Active Directory » à l'adresse : <http://aka.ms/Nzrl6u>

Qu'est-ce que AD Azure ?

Azure AD est conçu pour fournir la gestion d'identité et d'accès pour vos applications cloud. Vous utilisez Azure AD lorsque vous vous abonnez à Microsoft Office 365, Microsoft SharePoint Online, Exchange Online ou Skype Entreprise. En outre, vous pouvez utiliser Azure AD avec les applications Azure ou les applications connectées à Internet qui nécessitent une authentification. Vous pouvez synchroniser votre AD DS local avec AD Azure pour permettre à vos utilisateurs d'utiliser la même identité pour des ressources internes et des ressources en cloud.



AD Azure ne comprend pas tous les services disponibles avec une-solution Active Directory locale qui utilise Windows Server 2016. Active Directory local dans Windows Server 2016 prend en charge cinq services :

- AD DS
- AD FS

- Services AD LDS (Active Directory Lightweight Directory Services)
- Services AD CS (Active Directory Certificate Services)
- Services AD RMS (Active Directory Rights Management Services)

Azure AD ne comprend que :

- Azure AD, qui prend en charge la gestion d'identité dans le cloud
- Le service de contrôle d'accès Azure, qui prend en charge la fédération avec les services de gestion d'identité externes, y compris votre instance de AD DS-locale

Azure AD ne prend pas en charge les applications qui sont intégrées à Active Directory local. Pour les applications à intégrer avec Azure AD, elles doivent être conçues pour Azure AD.



Remarque : vous ne pouvez pas créer de contrôleurs de domaine AD DS dans Azure AD.

Vous pouvez utiliser Azure AD en tant que service autonome ou l'intégrer à votre infrastructure locale Active Directory existante. Cependant, vous ne créez pas ni ne gérez les systèmes AD Azure. Au lieu de cela, vous gérez vos utilisateurs dans le service AD Azure.

Vue d'ensemble des outils d'administration AD DS

La gestion de l'environnement AD DS est l'une des tâches les plus communes pour un expert informatique. Vous gérez généralement vos contrôleurs de domaine à distance même si vous pouvez vous connecter à l'ordinateur soit directement ou en utilisant le bureau à distance. Le principal outil que vous allez utiliser est le centre d'administration Active Directory.

Centre d'administration Active Directory

Le Centre d'administration Active Directory fournit une interface utilisateur graphique (GUI) qui est construite sur Windows PowerShell. Cette interface améliorée vous permet de gérer les objets AD DS en utilisant la navigation orientée tâche. Elle remplace la fonctionnalité des utilisateurs et ordinateurs Active Directory. Les tâches que vous pouvez effectuer à l'aide du Centre d'administration Active Directory incluent :

- Création et gestion des comptes utilisateur, ordinateur et de groupes
- La création et la gestion d'unité d'organisation
- La connexion et la gestion de plusieurs domaines au sein d'une seule instance du Centre d'administration Active Directory
- La recherche et le filtrage de données AD DS par la construction de requêtes
- La création et la gestion de politiques de mot de passe à grains fins
- La récupération d'objets de la corbeille Active Directory
- La gestion d'objets nécessaires pour la fonction de contrôle d'accès dynamique

La gestion d'AD DS est généralement effectuée à l'aide des outils suivants :

- Centre d'administration Active Directory
- Utilisateurs et ordinateurs Active Directory
- Sites et services Active Directory
- Domaines et approbations Active Directory
- Schéma de composant logiciel enfichable Active Directory
- Module Active Directory pour Windows PowerShell

Vous pouvez installer le Centre administratif Active Directory uniquement sur des serveurs exécutant Windows Server 2008 R2 ou une version ultérieure ou sur des ordinateurs clients exécutant Windows 7 ou une version ultérieure.

D'autres outils de gestion que vous allez utiliser pour exécuter l'administration des services AD DS comprennent :

- Les utilisateurs et ordinateurs Active Directory

Les utilisateurs et ordinateurs Active Directory sont un composant logiciel enfichable MMC (MMC, console de gestion Microsoft) qui gère la plupart des ressources communes au jour le jour, y compris les utilisateurs, les groupes et les ordinateurs. Bien que ce composant logiciel enfichable soit bien connu de nombreux administrateurs, le Centre d'administration Active Directory le remplace et offre davantage de possibilités

- Sites et services Active Directory

Sites et services Active Directory est un composant logiciel enfichable MMC qui permet d'administrer la réPLICATION, la topologie du réseau et les services connexes.

- Domaines et approbations Active Directory

Domaines et approbations Active Directory est le composant logiciel enfichable MMC utilisé pour configurer et entretenir les relations d'approbation aux niveaux fonctionnels du domaine et de la forêt.

- Schéma de composant logiciel enfichable Active Directory

Schema Active Directory est un composant logiciel enfichable MMC qui examine et modifie les définitions des attributs et des classes d'objets AD DS. Le schéma fournit les définitions des objets et des attributs AD DS et vous ne l'affichez ou ne le modifiez généralement pas très souvent. Par conséquent, par défaut, le schéma de composant logiciel enfichable Active Directory n'est pas complètement installé

- Module Active Directory pour Windows PowerShell

Le module Active Directory pour Windows PowerShell prend en charge l'administration des services AD DS et est l'un des composants de gestion les plus importants. Le gestionnaire de serveur et le Centre d'administration Active Directory sont construits sur Windows PowerShell et utilisent des cmdlets pour exécuter leurs tâches.

Démonstration : Utilisation du Centre d'administration Active Directory pour administrer et gérer AD DS

Le Centre d'administration Active Directory est l'interface d'administration la plus puissante pour la gestion de votre environnement AD DS. Cette démonstration va vous montrer comment :

- Naviguer dans le Centre d'administration Active Directory
- Effectuer une tâche administrative dans le Centre d'administration Active Directory
- Créer des objets
- Voir tous les attributs de l'objet
- Utiliser la visionneuse de l'historique de Windows PowerShell dans le Centre d'administration Active Directory

Procédure de démonstration

Naviguer dans le Centre d'administration Active Directory

1. Sur **LON-DC1**, ouvrir le **Centre d'administration Active Directory**.
2. Sélectionner **Adatum (local)**, **Contrôle d'accès dynamique** et **Recherche globale** dans le volet de navigation.
3. Dans le volet de navigation, passer à l'arborescence puis développer **Adatum.com**.

Effectuer une tâche administrative au sein du Centre d'administration Active Directory

1. Aller à l'aperçu **Vue d'ensemble**.
2. Réinitialiser le mot de passe **Adatum \ Adam** en **Pa55w.rd** de sorte que l'utilisateur n'ait pas à changer le mot de passe à la prochaine connexion.
3. Utiliser la section **Recherche globale** pour trouver des objets qui correspondent à la chaîne de recherche **lon**.

Création d'un objet

- Créer un nouvel objet ordinateur nommé **LON-CL4** dans le conteneur **Ordinateurs**

Voir tous les attributs de l'objet

1. Ouvrez la page **Propriétés** pour **LON-CL4**, faites défiler jusqu'à la section **Extensions**, puis cliquez sur l'onglet **Éditeur d'attribut**.
2. Visualisez les attributs de l'objet AD DS.

Utiliser la visionneuse Windows PowerShell History

1. Ouvrez le volet **Historique de Windows PowerShell**.
2. Visualisez l'applet de commande Windows PowerShell que vous avez utilisé pour effectuer la tâche la plus récente.
3. Sur **LON-DC1**, fermez toutes les fenêtres actives.

Question : Quels sont les deux principaux objectifs des UO ?

Question : Pourquoi auriez-vous besoin de déployer un arbre supplémentaire dans la forêt AD DS ?

Leçon 2

Vue d'ensemble des contrôleurs de domaine AD DS

Parce que les contrôleurs de domaine authentifient tous les utilisateurs et les ordinateurs dans le domaine, le déploiement de contrôleurs de domaines est essentiel pour que le réseau fonctionne correctement.

Cette leçon aborde les contrôleurs de domaine, le processus de connexion et l'importance du DNS dans ce processus. En outre, cette leçon traite de l'objet du catalogue global.

Tous les contrôleurs de domaine sont essentiellement les mêmes, à deux exceptions près. Les RODC contiennent une copie-en lecture seule de la base de données AD DS alors que d'autres contrôleurs de domaine ont une copie de lecture / écriture. En outre, certaines opérations ne peuvent être effectuées que sur des contrôleurs de domaine spécifiques appelés maîtres d'opérations qui sont abordés à la fin de cette leçon.

Objectifs de la leçon

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

- Décrire l'objectif des contrôleurs de domaine
- Comprendre ce qui est contenu dans le dossier SYSVOL
- Décrire l'objectif du catalogue global
- Décrire le processus de connexion-AD DS et l'importance des enregistrements DNS et de service (enregistrements SRV) dans ce processus
- Expliquer les fonctions de maîtres d'opérations
- Décrire le transfert et la prise du rôle de maître d'opérations

Qu'est-ce qu'un contrôleur de domaine ?

Un *contrôleur de domaine* est un serveur qui est configuré pour stocker une copie de la base de données du répertoire AD DS (Ntds.dit) et une copie du dossier SYSVOL. Tous les contrôleurs de domaine, sauf les RODC, stockent une copie de lecture / écriture Ntds.dit et le dossier SYSVOL. Ntds.dit est la base de données elle-même et le dossier SYSVOL contient tous les paramètres du modèle et des fichiers pour les GPO.

Les contrôleurs de domaine utilisent un processus de réplication multimaître pour copier les données d'un contrôleur de domaine à un autre. Cela signifie que pour la plupart des opérations, les données peuvent être modifiées sur un contrôleur de domaine, sauf pour un RODC. Le service de réplication AD DS synchronise alors les modifications qui ont été apportées à la base de données AD DS avec tous les autres contrôleurs de domaine dans le domaine. Dans Windows Server 2016, vous pouvez uniquement utiliser le système de réplication de fichiers distribués (DFS) pour répliquer les dossiers SYSVOL. Les versions antérieures de Windows Server utilisaient le service de réplication de fichiers (FRS) pour répliquer les dossiers mais le FRS est obsolète pour plusieurs versions de Windows.

Contrôleurs de domaine :

- Sont des serveurs qui hébergent la base de données AD DS (Ntds.dit) et SYSVOL ;
- Hébergent le service d'authentification Kerberos et les services KDC pour effectuer une authentification.
- Avoir les bonnes pratiques pour :
 - La disponibilité :
 - Utilisez au moins deux contrôleurs de domaine dans un domaine ;
 - La sécurité :
 - Utilisez un RODC ou BitLocker.

Les contrôleurs de domaine hébergent plusieurs autres services liés aux services AD DS, y compris le service d'authentification Kerberos que les comptes d'utilisateurs et les ordinateurs utilisent pour l'authentification lors d'une ouverture de session et le Centre de distribution de clés (KDC) qui émet la permission d'octroi de tickets (TGT) à un compte qui se connecte au domaine AD DS. En option, vous pouvez configurer les contrôleurs de domaine pour héberger une copie du catalogue global.

Tous les utilisateurs d'un domaine AD DS existent dans la base de données AD DS. Si la base de données est indisponible pour une raison quelconque, toutes les opérations qui dépendent de l'authentification sur la base du domaine échoueront. Il est recommandé pour un domaine AD DS d'avoir au moins deux contrôleurs de domaine. Cela permet d'accroître la disponibilité de la base de données AD DS et de répartir la charge d'authentification pendant les pics de connexion.

Remarque : considérons deux contrôleurs de domaine comme le minimum absolu pour la plupart des entreprises afin d'assurer une grande disponibilité et une performance élevée.

Lorsque vous déployez un contrôleur de domaine dans une succursale où la sécurité physique est loin d'être optimale, vous pouvez utiliser des mesures supplémentaires pour réduire l'impact d'une violation de la sécurité. Une option consiste à déployer un RODC.

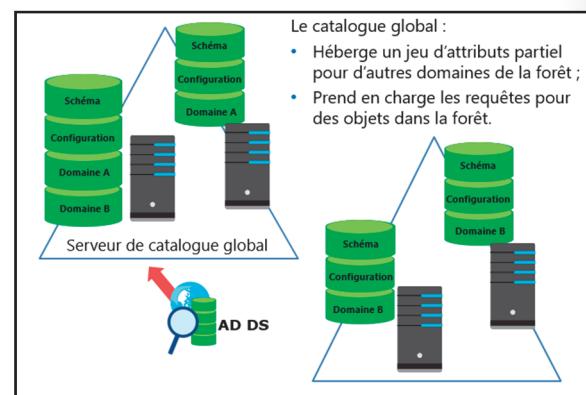
Le RODC contient une copie de la base de données AD DS en lecture-seule et par défaut, il ne met pas en cache les mots de passe de l'utilisateur. Vous pouvez configurer le RODC pour cacher les mots de passe des utilisateurs dans la succursale. Si un RODC est compromis, la perte potentielle de l'information est beaucoup plus faible qu'avec un contrôleur de domaine complet en lecture / écriture. Une autre option consiste à utiliser le chiffrement de lecteur BitLocker pour chiffrer le disque dur du contrôleur de domaine. Si le disque dur est volé, BitLocker aidera à veiller à ce qu'un pirate malveillant ait du mal à obtenir toute information utile de lui.

Remarque : bitLocker est une fonctionnalité de chiffrement de lecteur qui est disponible pour les systèmes d'exploitation Windows Server et certains systèmes d'exploitation client Windows. BitLocker crypte l'intégralité du lecteur pour empêcher l'ordinateur de démarrer à moins qu'il ne reçoive une clé privée et (éventuellement) passe un contrôle d'intégrité. Un disque dur reste crypté même si vous le transférez sur un autre ordinateur.

Qu'est-ce qu'un catalogue global ?

Un *catalogue global* est une copie partielle consultable en lecture-seule de tous les objets de la forêt. Il accélère les recherches pour les objets qui pourraient être stockés sur les contrôleurs de domaine dans un domaine différent dans la forêt.

Dans un seul domaine, la base de données AD DS sur chaque contrôleur de domaine contient toutes les informations sur chaque objet dans ce domaine. Toutefois, seul un sous-ensemble de ces informations est répliqué sur les serveurs de catalogue global dans d'autres domaines de la forêt. Dans un domaine particulier, une requête pour un objet est dirigée vers l'un des contrôleurs de domaine dans ce domaine mais cette requête ne comprend pas de résultats sur les objets dans d'autres domaines de la forêt. Pour qu'une requête comprenne les résultats d'autres domaines de la



forêt, vous devez interroger un contrôleur de domaine qui est un serveur de catalogue global. Par défaut, le premier contrôleur de domaine dans le domaine racine de la forêt est le seul serveur de catalogue global hébergé. Pour améliorer la recherche à travers des domaines dans une forêt, vous devez configurer des contrôleurs de domaine supplémentaires dont chacun dispose d'une copie du catalogue global.

Le catalogue global ne contient pas tous les attributs de chaque objet. Au lieu de cela, le catalogue global contient le sous-ensemble d'attributs qui sont les plus susceptibles d'être utiles dans les recherches inter-domaines. Ces attributs comprennent les **prénom**, **nom complet** et **courrier**. Vous pouvez modifier l'ensemble des attributs répliqués dans le catalogue global en modifiant l'ensemble d'attributs partiel (PAS) dans le schéma.

Pour diverses raisons, vous pouvez effectuer une recherche par rapport à un catalogue global plutôt qu'un contrôleur de domaine qui n'est pas un catalogue global. Par exemple, quand un serveur qui exécute Exchange Server reçoit un e-mail entrant, il doit rechercher le compte du destinataire afin qu'il puisse décider comment acheminer le message. En interrogeant automatiquement un catalogue global, le serveur qui exécute Exchange Server peut localiser le destinataire dans un environnement de domaine multiple.

Autre exemple, lorsque les utilisateurs se connectent à leur compte Active Directory, le contrôleur de domaine qui exécute l'authentification doit contacter un catalogue global pour vérifier les appartennances aux groupes universels avant que l'utilisateur soit authentifié.

Dans un domaine unique, tous les contrôleurs de domaine doivent être configurés pour contenir une copie du catalogue global. Cependant, dans un environnement à plusieurs domaines, le contrôleur d'infrastructure ne devrait pas être un serveur de catalogue global à moins que tous les contrôleurs de domaine du domaine soient également des serveurs de catalogue global. Lorsque vous avez plusieurs sites, vous devez également faire au moins un DC à chaque site avec un serveur de catalogue global, de sorte à ne pas être dépendant d'autres sites lorsque des requêtes de catalogue global sont nécessaires. Le trafic de réPLICATION et la bande passante du réseau détermineront quels contrôleurs de domaine doivent être configurés pour contenir une copie du catalogue global. De nombreuses organisations choisissent de faire de chaque contrôleur de domaine un serveur de catalogue global.

Vue d'ensemble du contrôleur de domaine des enregistrements SRV

Lorsque les utilisateurs se connectent aux services AD DS, leur ordinateur regarde dans le DNS pour les enregistrements SRV pour localiser le contrôleur de domaine le plus proche. Les enregistrements SRV contiennent des informations sur les services disponibles. Chaque contrôleur de domaine enregistre dynamiquement ses adresses dans le DNS au démarrage par l'enregistrement d'un SRV mis à jour dans le DNS.

Les clients peuvent localiser un contrôleur de domaine approprié pour exécuter leurs demandes de connexion à l'aide de requêtes DNS qui utilisent ces enregistrements SRV.

Les enregistrements SRV pour AD DS sont créés selon le schéma suivant.

`_Service._Protocol.DomainName`

- Les clients trouvent les contrôleurs de domaine par le biais de la recherche DNS
- Les contrôleurs de domaine enregistrent dynamiquement leurs adresses avec DNS
- Les résultats des requêtes DNS pour les contrôleurs de domaine sont retournés dans cet ordre :
 1. Une liste des contrôleurs de domaine du même site que le client ;
 2. Une liste des contrôleurs de domaine dans le prochain site le plus proche, si aucun n'est disponible sur le même site ;
 3. Une liste aléatoire de contrôleurs de domaine sur d'autres sites, si aucun contrôleur de domaine n'est disponible sur le site le plus proche.

Par exemple, si un client est à la recherche d'un serveur qui exécute le service (LDAP) Lightweight Directory Access Protocol dans le domaine Adatum.com, il demande `_ldap._tcp.Adatum.com`.

Sites et enregistrements SRV

Un client utilise des sites quand il faut contacter un contrôleur de domaine. Il commence par rechercher les enregistrements SRV dans le DNS. La réponse à la requête DNS comprend :

- Une liste des contrôleurs de domaine dans le même site que le client
- Une liste des contrôleurs de domaine du site suivant le plus proche qui ne comprend pas un RODC, si aucun contrôleur de domaine n'est disponible dans le même site et que la stratégie de groupe du site suivant le plus proche est activée
- Une liste aléatoire de contrôleurs de domaine disponibles, si aucun contrôleur de domaine n'est disponible sur le site suivant le plus proche

Les administrateurs peuvent définir les sites dans les services AD DS. Lorsque vous définissez les sites, vous devez réfléchir à quelles parties du réseau ont une bonne connectivité et une bonne bande passante. Par exemple, si un bureau d'une succursale est relié au centre de données principal par une liaison réseau étendu (WAN) non fiable, vous devez définir la succursale et le centre de données comme des sites distincts.

Le service Net Logon, qui fonctionne sur chaque contrôleur de domaine, enregistre les enregistrements SRV dans le DNS. Si les enregistrements SRV ne sont pas inscrits correctement dans le DNS, vous pouvez déclencher le contrôleur de domaine pour réenregistrer les données en redémarrant le service Net Logon sur ce contrôleur de domaine. Notez que ce processus ne réinscrit que les enregistrements SRV. Si vous souhaitez réenregistrer l'information de l'hôte (A) dans le DNS, vous devez exécuter **ipconfig /registerdns** à partir d'une invite de commande, comme vous le feriez pour tout autre ordinateur.

Démonstration : Affichage des enregistrements SRV dans DNS

Cette démonstration vous montre comment afficher les différents types d'enregistrements SRV que les contrôleurs de domaine inscrivent dans le DNS. Ces enregistrements sont essentiels pour la façon dont les services AD DS fonctionnent parce qu'ils sont utilisés pour rechercher des contrôleurs de domaine pour la connexion, la modification des mots de passe et la modification des GPO. Les contrôleurs de domaine utilisent également les enregistrements SRV pour trouver des partenaires de réplication.

Procédure de démonstration

Afficher les enregistrements SRV dans DNS

1. Sur **LON-DC1**, se connecter avec le nom d'utilisateur **Adatum\Administrateur** et le mot de passe **Pa55w.rd**.
2. Ouvrez la fenêtre du **Gestionnaire DNS**, puis explorez les domaines DNS qui commencent par un trait de soulignement (_).
3. Afficher les enregistrements SRV enregistrés par les contrôleurs de domaine.



Remarque : ces dossiers fournissent des chemins d'accès alternatifs afin que les clients puissent les découvrir.

Processus de connexion AD DS

Lorsqu'un utilisateur tente de se connecter à un ordinateur, l'ordinateur recherche d'abord un contrôleur de domaine pour authentifier l'utilisateur en utilisant la recherche DNS. L'ordinateur envoie ensuite le nom et le mot de passe de l'utilisateur au contrôleur de domaine pour l'authentification. L'autorité de sécurité locale (LSA) sur le contrôleur de domaine gère le processus d'authentification.

Si le processus de connexion fonctionne, la LSA crée un jeton d'accès pour l'utilisateur qui contient les ID de sécurité (SID) pour l'utilisateur et tous les groupes dont l'utilisateur est membre. Le jeton fournit les informations d'identification d'accès pour tout processus initié par l'utilisateur. Par exemple, disons qu'après s'être connecté aux services AD DS, un utilisateur exécute Microsoft Word et tente d'ouvrir un fichier. Word utilise alors les informations d'identification dans le jeton d'accès de l'utilisateur pour vérifier le niveau des autorisations de l'utilisateur pour ce fichier.

 **Remarque :** un SID est une chaîne unique sous la forme S-R-X-Y1-Y2-Yn-1-Yn. Par exemple, un SID de l'utilisateur peut être S-1-5-21-322346712-1256085132-1900709958-500.

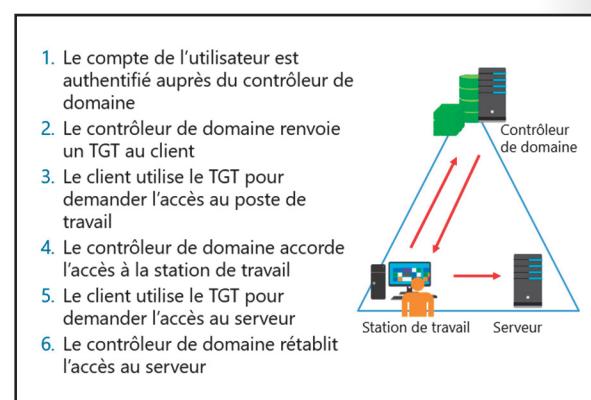
Le tableau suivant présente les différentes parties de ce SID.

| Composant | Définition | Dans l'exemple |
|------------|--|------------------------------------|
| S | Indique que la chaîne est un SID | S |
| R | Niveau de révision | 1 |
| X | Valeur de l'autorité de l'identificateur | 5 (Autorité NT) |
| Y1-Y2-Yn-1 | Identificateur de domaine | 21-322346712-1256085132-1900709958 |
| Yn | ID relatif (RID) | 500 |

Chaque compte d'utilisateur et d'ordinateur et chaque groupe que vous créez a un SID unique. Ils se distinguent les uns des autres uniquement en vertu du RID unique. Le SID dans l'exemple est un-SID connu pour le compte d'administrateur de domaine. Les comptes et groupes par défaut utilisent des-SID bien connus. Le SID du compte d'administrateur de domaine se termine toujours par 500.

Bien que le processus-de connexion apparaît à l'utilisateur comme un événement unique, il est en fait composé de deux parties :

- L'utilisateur fournit des informations d'identification, généralement un nom de compte d'utilisateur et un mot de passe qui sont vérifiés par rapport à la base de données AD DS. Si le nom du compte d'utilisateur et le mot de passe correspondent aux informations qui sont stockées dans la base de données AD DS, l'utilisateur devient un utilisateur authentifié et un TGT est émis par le contrôleur de domaine. À ce stade, l'utilisateur n'a pas accès aux ressources sur le réseau



- Un processus secondaire en arrière-plan soumet le TGT au contrôleur de domaine et demande l'accès à l'ordinateur local. Le contrôleur de domaine délivre un ticket de service à l'utilisateur qui peut alors interagir avec l'ordinateur local. À ce stade du processus, l'utilisateur est authentifié aux services AD DS et connecté à l'ordinateur local

Lorsqu'un utilisateur tente ensuite de se connecter à un autre ordinateur sur le réseau, le processus secondaire fonctionne à nouveau et le TGT est soumis au contrôleur de domaine le plus proche. Lorsque le contrôleur de domaine renvoie un ticket de service, l'utilisateur peut accéder à l'ordinateur sur le réseau, ce qui génère un événement d'ouverture de session sur l'ordinateur.



Remarque : un ordinateur-appartenant au domaine se connecte également aux services AD DS quand il démarre, un fait qui est souvent oublié. Vous ne voyez pas la transaction lorsque l'ordinateur utilise son nom de compte d'ordinateur et un mot de passe pour se connecter aux services AD DS. Après son authentification, l'ordinateur devient un membre du groupe utilisateurs authentifiés. Bien que l'événement d'ouverture de session d'ordinateur ne dispose pas d'une confirmation visuelle dans une interface graphique, il est enregistré dans le journal des événements. En outre, si l'audit est activé, d'autres événements sont enregistrés dans le journal de sécurité de l'Observateur d'événements.

Que sont les contrôleurs d'opérations ?

Certaines opérations ne peuvent être effectuées que par un rôle spécifique, sur un contrôleur de domaine spécifique. Un contrôleur de domaine qui détient l'un de ces rôles est appelé *maître d'opérations*. Un rôle de maître d'opérations est également connu en tant que *rôle d'opérations à maître unique flottant rôle (FSMO)*. Cinq rôles de maître d'opérations existent et tous les cinq peuvent être situés sur un seul contrôleur de domaine ou ils peuvent être répartis sur plusieurs contrôleurs de domaine. Par défaut, le premier contrôle de domaine installé dans une forêt

contient les cinq rôles. Cependant, ces rôles peuvent être déplacés après la construction de plusieurs contrôleurs de domaine. En permettant des modifications uniquement sur un contrôleur de domaine unique, les rôles de maître d'opérations aident à prévenir les conflits dans les services AD DS, qui sont causés par la latence de réPLICATION. Lors des modifications apportées aux données détenues sur l'un des maîtres d'opérations, vous devez vous connecter au contrôleur de domaine qui détient le rôle.

Les cinq rôles de maître d'opérations sont répartis comme suit :

- Chaque forêt possède un contrôleur de schéma et un maître d'opérations des noms de domaine
- Chaque domaine des services AD DS a un maître RID, un maître d'infrastructure et un émulateur de contrôleur de domaine principal (PDC)

Maîtres d'opérations des forêts

Une forêt contient les rôles individuels de base suivants :

- Maître d'opérations des noms de domaine C'est le contrôleur de domaine qui doit être contacté lorsque vous ajoutez ou supprimez un domaine ou faites des changements de noms de domaine.

- Dans le modèle de réPLICATION multimaître, certaines opérations doivent être des opérations à maître unique
- De nombreux termes sont utilisés pour les opérations à maître unique dans AD DS, notamment :
 - Maître d'opérations (ou rôle maître d'opérations) ;
 - Rôle de maître unique ;
 - Opérations à maître unique flottant (FSMO).

| Les cinq FSMO : | |
|---|--|
| Forêt : <ul style="list-style-type: none"> • Maître d'opérations des noms de domaine • Contrôleur de schéma | Domaine : <ul style="list-style-type: none"> • Maître RID • Maître d'infrastructure • Maître d'émulateur de contrôleur de domaine principal |

Si le maître d'opérations des noms de domaine est indisponible, vous ne serez pas en mesure d'ajouter des domaines à la forêt

- Contrôleur de schéma. C'est le contrôleur de domaine dans lequel vous faites tous les changements de schéma. Pour apporter des modifications, vous vous connectez généralement au contrôleur de schéma en tant que membre administrateur du schéma et du groupe administrateurs de l'entreprise. Un utilisateur qui est membre de ces deux groupes et qui a les autorisations appropriées peut également modifier le schéma à l'aide d'un script

Si le contrôleur de schéma est indisponible, vous ne serez pas en mesure d'apporter des modifications au schéma. Cela empêche l'installation d'applications qui nécessitent des changements de schéma, comme Exchange Server

 **Remarque :** la commande Windows PowerShell **Get-ADForest**, à partir du module Active Directory pour Windows PowerShell, montre les propriétés des forêts, y compris le maître d'opérations des noms de domaine et le contrôleur de schéma.

Maîtres d'opérations de domaine

Un domaine contient les rôles individuels de base suivants :

- Maître RID Chaque fois qu'un objet est créé dans les services AD DS, le contrôleur de domaine où l'objet est créé attribue à l'objet un numéro d'identification unique connu sous le nom de SID. Pour s'assurer que deux contrôleurs de domaine n'attribuent pas le même SID à deux objets différents, le maître RID alloue des blocs de RID à chaque contrôleur de domaine dans le domaine à utiliser lors de la création du SID

Si le maître RID est indisponible, vous risquez de rencontrer des difficultés pour ajouter de nouveaux objets au domaine. Alors que les contrôleurs de domaine utilisent leurs RID existants, ils ont fini par en manquer et sont incapables de créer de nouveaux objets.

- Maître d'infrastructure Ce rôle maintient les références d'objet interdomaines, comme quand un groupe d'un domaine contient un membre d'un autre domaine. Dans cette situation, le maître d'infrastructure est responsable du maintien de l'intégrité de cette référence. Par exemple, lorsque vous regardez l'onglet **Sécurité** d'un objet, le système regarde les SID qui sont répertoriés et les traduit en noms. Dans une forêt-à plusieurs domaines, le maître d'infrastructure regarde les SID d'autres domaines

Si le maître d'infrastructure est indisponible, les contrôleurs de domaine qui ne sont pas des catalogues globaux ne seront pas en mesure de vérifier les appartances au groupe universel ou d'authentifier les utilisateurs.

Le rôle de l'infrastructure ne doit pas résider sur un serveur de catalogue global, sauf si vous avez une forêt à domaine unique. À l'exception de lorsque vous suivez les meilleures pratiques et faites de tous les contrôleurs de domaine un catalogue global. Dans ce cas, le rôle de l'infrastructure n'est pas nécessaire car chaque contrôleur de domaine connaît chaque objet dans la forêt.

- Maître d'émetteur de contrôleur de domaine principal Le contrôleur de domaine qui détient le maître d'émetteur de contrôleur de domaine principal est la source de temps pour le domaine. Les maîtres d'émetteur de contrôleur de domaine principal dans chaque domaine dans une forêt synchronisent leur temps avec le maître d'émetteur de contrôleur de domaine principal dans le domaine racine de la forêt. Vous définissez le maître d'émetteur de contrôleur de domaine principal dans le domaine racine de la forêt pour qu'il se synchronise avec une source de temps externe fiable

Le maître d'émetteur de contrôleur de domaine principal est également le contrôleur de domaine qui reçoit les modifications de mot de passe urgentes. Si le mot de passe d'un utilisateur est modifié, l'information est immédiatement transmise au contrôleur de domaine qui détient le rôle de maître

d'émulateur de contrôleur de domaine principal. Cela signifie que si l'utilisateur tente de se connecter, même si l'utilisateur a été authentifié par un contrôleur de domaine à un autre endroit qui n'a pas encore reçu les nouvelles informations de mot de passe, le contrôleur de domaine dans l'emplacement actuel de l'utilisateur prendra contact avec le contrôleur de domaine qui contient le rôle de maître d'émulateur de contrôleur de domaine principal pour vérifier les changements récents.

Si le maître d'émulateur de contrôleur de domaine principal est indisponible, les utilisateurs pourraient avoir des problèmes de connexion jusqu'à ce que leurs changements de mot de passe soient répliqués sur tous les contrôleurs de domaine.

Le maître d'émulateur de contrôleur de domaine principal est également utilisé pour l'édition de GPO. Quand un GPO autre qu'un GPO local est ouvert pour l'édition, la copie éditée est stockée sur le maître d'émulateur de contrôleur de domaine principal. Cela évite les conflits si deux administrateurs tentent de modifier le même GPO en même temps sur différents contrôleurs de domaine. Cependant, vous pouvez choisir d'utiliser un contrôleur de domaine spécifique pour éditer les GPO. Ceci est particulièrement utile lors de l'édition de GPO dans un bureau à distance avec une connexion lente à l'émulateur PDC.



Remarque : la commande Windows PowerShell **Get-ADDomain** à partir du module Active Directory pour Windows PowerShell, montre les propriétés du domaine, y compris l'actuel maître RID, le maître d'infrastructure et le maître d'émulateur de contrôleur de domaine principal.



Remarque : le catalogue global n'est pas l'un des rôles de maître d'opérations.

Transfert et prise de rôles

Dans un environnement AD DS où les rôles FSMO sont répartis entre les contrôleurs de domaine, vous pourriez avoir besoin de déplacer un rôle d'un contrôleur de domaine à un autre. Lorsque vous planifiez ceci (par exemple, pour désengorger des serveurs ou équilibrer les charges de travail), ce mouvement est connu sous le nom de *transfert* de rôle. Si vous ne prévoyez pas de déplacement - par exemple dans le cas d'un problème matériel ou d'un échec du système, ce mouvement est connu sous le nom de *prise* de rôle.

- Le transfert est :
 - Planifié ;
 - Réalisé avec les dernières données ;
 - Effectué grâce à des composants logiciels enfichables Windows PowerShell ou ntdsutil.exe.
- La prise de rôle est :
 - Non planifiée et utilisée en dernier recours ;
 - Faite avec des données incomplètes ou obsolètes ;
 - Effectuée grâce à Windows PowerShell ou ntdsutil.exe.

Pour transférer un rôle, les dernières données du contrôleur de domaine dans ce rôle sont répliquées sur le serveur cible. Vous ne devez saisir un rôle qu'en dernier recours. Pour saisir un rôle, le contrôleur de domaine d'origine n'est pas disponible, les données disponibles pourraient donc être incomplètes ou obsolètes.

Transfert des rôles FSMO

Vous pouvez transférer des rôles FSMO par l'interface graphique en utilisant les composants logiciels enfichables AD DS qui sont répertoriés dans le tableau suivant.

| Rôle | Composant logiciel enfichable |
|---|--|
| Contrôleur de schéma | Schéma Active Directory |
| Maître d'opérations des noms de domaine | Domaines et approbations Active Directory |
| Maître d'infrastructure | Utilisateurs et ordinateurs Active Directory |
| Maître RID | Utilisateurs et ordinateurs Active Directory |
| Maître d'émulateur de contrôleur de domaine principal | Utilisateurs et ordinateurs Active Directory |

Prise des rôles FSMO

Vous ne pouvez pas utiliser les composants logiciels enfichables pour saisir les rôles FSMO. Au lieu de cela, vous devez utiliser l'outil de ligne de commande ntdsutil.exe ou Windows PowerShell pour saisir les rôles. Vous pouvez également utiliser ces outils pour transférer des rôles.

La syntaxe de transfert ou de prise d'un rôle est similaire au sein de Windows PowerShell, comme indiqué dans la ligne de syntaxe suivante.

```
Move-AddDirectoryServerOperationsMasterRole -Identity "<nomserveur>" -OperationsMasterRole <listenomsrôles> -Force
```

Pour la syntaxe précédente, les définitions remarquables sont les suivantes :

- <Servername> Le nom du contrôleur de domaine cible pour y transférer un ou plusieurs rôles
- <Rolenamelist> Une liste des noms de rôles AD DS séparés par des virgules pour passer au serveur cible
- - **Force**. Paramètre facultatif que vous incluez pour saisir un rôle au lieu de simplement le transférer



Documentation supplémentaire : Pour plus d'informations sur l'utilisation de Windows PowerShell pour le transfert ou la prise des rôles FSMO, reportez-vous à : « Déplacer (Transfert ou Prise) les rôles FSMO avec la commande AD-Powershell vers un autre contrôleur de domaine » à l'adresse : <http://aka.ms/Rn7kfi>



Lectures supplémentaires : Pour plus d'informations sur l'utilisation de ntdsutil.exe et sur le transfert ou la prise des rôles FSMO, reportez-vous à : « Utilisation de Ntdsutil.exe pour le transfert ou la prise des rôles FSMO vers un contrôleur de domaine » à l'adresse : <http://aka.ms/Npye86>

Question : Est-ce qu'un contrôleur de domaine doit être un catalogue global ?

Question : Vérifiez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|--|---------|
| Dans une forêt à plusieurs domaines, une copie du catalogue global doit être enregistrée sur chaque contrôleur de domaine. | |

Leçon 3

Déploiement d'un contrôleur de domaine

Parfois, vous devez installer des contrôleurs de domaine supplémentaires dans votre domaine Windows Server 2016. Et ce, pour plusieurs raisons :

- Vous avez besoin de ressources supplémentaires sur un site parce que les contrôleurs de domaine existants sont surchargés de travail
- Vous ouvrez un nouveau bureau à distance qui vous oblige à déployer un ou plusieurs contrôleurs de domaine
- Vous créez un emplacement de reprise hors site après sinistre

La méthode d'installation que vous utilisez varie selon les circonstances.

Cette leçon aborde plusieurs façons d'installer des contrôleurs de domaine supplémentaires. Ceux-ci comprennent l'installation de AD DS sur un ordinateur local et sur un serveur distant à l'aide du Gestionnaire de serveur, l'installation de AD DS sur une installation Server Core et l'installation de AD DS en utilisant une capture instantanée de la base de données AD DS qui est stockée sur un support amovible. Cette leçon aborde également comment mettre à niveau un contrôleur de domaine à partir d'un ancien système d'exploitation Windows pour Windows Server 2016. Enfin, la leçon traite de Azure AD et de la façon d'installer un contrôleur de domaine dans Azure.

Objectifs de la leçon

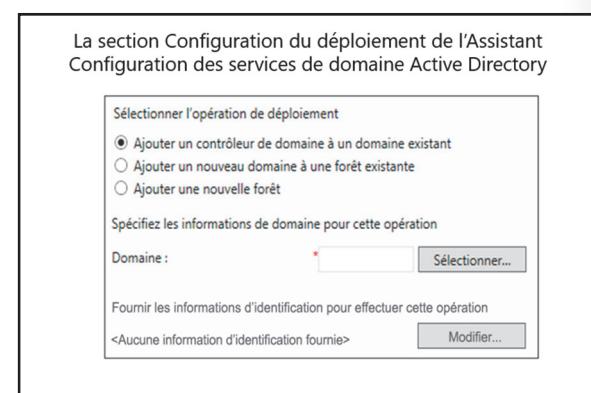
À la fin de cette leçon, vous devrez être capable de :

- Expliquer comment installer un contrôleur de domaine en utilisant l'interface graphique
- Expliquer comment installer un contrôleur de domaine sur une installation Server Core de Windows Server 2016
- Expliquer comment mettre à niveau un contrôleur de domaine à partir des médias
- Expliquer comment installer un contrôleur de domaine à partir des médias
- Décrire le processus de clonage des contrôleurs de domaine
- Expliquer les meilleures pratiques pour virtualiser les contrôleurs de domaine

Installation d'un contrôleur de domaine depuis le Gestionnaire de serveur

L'installation du contrôleur de domaine et la promotion comportent deux étapes. Tout d'abord, vous devez installer les fichiers que le rôle de contrôleur de domaine utilise. Vous faites cela en installant le rôle AD DS à l'aide du gestionnaire de serveur. À la fin du processus d'installation initial, les fichiers AD DS sont installés mais les services AD DS ne sont pas encore configurés sur le serveur.

Pour configurer les services AD DS, vous utilisez l'**Assistant de configuration Active Directory Domain Services**. Vous démarrez l'assistant en



cliquant sur le lien AD DS dans le Gestionnaire de serveur. L'assistant vous permet de faire l'une des actions suivantes :

- Ajouter un contrôleur de domaine à un domaine existant
- Créer un domaine dans une forêt existante
- Ajouter une nouvelle forêt

Avant d'installer un nouveau contrôleur de domaine, vous avez besoin de répondre aux questions posées dans le tableau suivant.

| Question | Commentaires |
|--|---|
| Installez-vous une nouvelle forêt, un nouvel arbre ou un contrôleur de domaine supplémentaire pour un domaine existant ? | Répondre à cette question permet de déterminer de quelles informations supplémentaires vous pourriez avoir besoin, comme le nom de domaine parent. |
| Quel est le nom DNS pour le domaine AD DS ? | Lorsque vous créez le premier contrôleur de domaine pour un domaine, vous devez spécifier le nom de domaine complet (FQDN). Lorsque vous ajoutez un contrôleur de domaine à une forêt ou un domaine existant, l'assistant fournit les informations de domaine existantes. |
| Comment définirez-vous le niveau fonctionnel de la forêt ? | Le niveau fonctionnel de la forêt détermine les caractéristiques de la forêt qui seront disponibles et système d'exploitation du contrôleur de domaine pris en charge. Ceci définit également le niveau fonctionnel minimum de domaine pour les domaines de la forêt. |
| Comment définirez-vous le niveau fonctionnel du domaine ? | Le niveau fonctionnel du domaine détermine les caractéristiques de domaine qui seront disponibles et le système d'exploitation du contrôleur de domaine pris en charge. |
| Est-ce que le contrôleur de domaine sera un serveur DNS ? | Votre DNS doit être fonctionnel pour prendre les services AD DS en charge. |
| Est-ce que le contrôleur de domaine hébergera le catalogue global ? | Cette option est sélectionnée par défaut pour le premier contrôleur de domaine dans une forêt et elle ne peut pas être changée. |
| Est-ce que le contrôleur de domaine sera un RODC ? | Cette option n'est pas disponible pour le premier contrôleur de domaine dans une forêt. |
| Quel sera le mot de passe du DSRM (Directory Services Restore Mode) ? | Cela est nécessaire pour récupérer la base de données AD DS à partir d'une sauvegarde. |
| Quel est le nom NetBIOS pour le domaine AD DS ? | Lorsque vous créez le premier contrôleur de domaine pour un domaine, vous devez spécifier le nom NetBIOS pour le domaine. |
| Où la base de données, les fichiers journaux et dossiers SYSVOL seront-ils créés ? | Par défaut, la base de données et le dossier de fichiers journaux sont dans C:\Windows\NTDS. Par défaut, le dossier SYSVOL est dans C:\Windows\SYSVOL. |



Remarque : si vous avez besoin de restaurer la base de données AD DS à partir d'une sauvegarde, redémarrez le contrôleur de domaine dans le DSRM. Le processus général pour entrer dans le DSRM est de redémarrer le contrôleur de domaine puis d'appuyer sur F8 lors du processus de démarrage initial. Lorsque le contrôleur de domaine démarre, il n'ouvre pas les services AD DS. Au lieu de cela, il fonctionne comme un serveur membre dans le domaine. Pour vous connecter à ce serveur en l'absence de AD DS, utilisez le mot de passe DSRM.



Remarque : windows Server 2016 prend en charge les serveurs AD DS clonés. Avant d'être cloné, un serveur AD DS doit être un membre du groupe des contrôleurs de domaine pouvant être clonés. En outre, le maître d'émulateur de contrôleur de domaine principal doit être en ligne, à la disposition du contrôleur de domaine cloné et doit exécuter Windows Server 2016.



Remarque : l'**Assistant d'installation Active Directory Domain Services (dcpromo.exe)**, communément utilisé pour installer les contrôleurs de domaine sur Windows Server 2008 et les versions antérieures est obsolète et ne fonctionne qu'à partir de Windows Server 2012.

Installer un contrôleur de domaine sur une installation Server Core de Windows Server 2016

Un serveur Windows Server 2016 qui exécute une installation Server Core ne dispose pas de l'interface graphique du Gestionnaire de serveur, vous devez donc utiliser des méthodes alternatives pour installer les fichiers pour le rôle de contrôleur de domaine et installer le rôle de contrôleur de domaine lui-même. Vous pouvez utiliser le Gestionnaire de serveur, Windows PowerShell ou des outils d'administration de serveur distant (RSAT) installés sur un client exécutant Windows 8.1 ou une version ultérieure.

- Utilisation du Gestionnaire de serveur :
 1. Installation du rôle AD DS
 2. Exécuter l'Assistant Configuration des services de domaine Active Directory
- Utilisation de Windows PowerShell :
 1. Installez les fichiers en exécutant la commande **Install-WindowsFeature AD-Domain-Services**
 2. Installer le rôle de contrôleur de domaine en exécutant la commande **Install-ADDSDomainController**

Pour installer les fichiers AD DS sur le serveur, vous pouvez effectuer l'un des éléments suivants :

- Utiliser le gestionnaire de serveur pour se connecter à distance au serveur exécutant l'installation Server Core, puis installer le rôle AD DS comme décrit dans la rubrique précédente
- Utiliser la commande Windows PowerShell **Install WindowsFeature AD Domain Services** pour installer les fichiers.

Après avoir installé les fichiers AD DS, vous pouvez tout terminer, sauf pour l'installation du matériel et la configuration de l'une des façons suivantes :

- Utilisez le gestionnaire de serveur pour démarrer l'assistant de configuration Active Directory Domain Services comme décrit dans la rubrique précédente
- Exécutez l'applet de commande Windows PowerShell **Install ADDSDomainController**, qui va fournir les informations requises sur la ligne de commande



Remarque : dans Windows Server 2016, l'exécution d'une cmdlet charge automatiquement le module cmdlets, si il est disponible. Par exemple, l'exécution de **Install-ADDSDomainController** cmdlet charge automatiquement le module **ADDSDeployment** dans votre session Windows PowerShell. Si un module n'est pas chargé ou n'est pas disponible, vous recevrez un message d'erreur lorsque vous exécutez la cmdlet qui dira qu'il est pas un cmdlet valide.

Vous pouvez toujours importer manuellement le module dont vous avez besoin. Cependant, vous ne devez pas faire cela dans Windows Server 2016, sauf si vous avez un besoin explicite de le faire, comme s'orienter vers une source particulière pour installer le module.



Lectures supplémentaires :

- Pour plus d'informations sur l'utilisation de l'applet de commande Windows PowerShell **Install ADDSDomainController**, reportez-vous à : « Installer les Services de domaine Active Directory (niveau 100) » à la page : <http://aka.ms/A9jlvk>
- Pour plus d'informations, consultez : « Déploiement d'applets de commandes AD DS dans Windows PowerShell » à l'adresse : <http://aka.ms/Lnxifx>

Mise à niveau d'un contrôleur de domaine

Le processus de mise à niveau d'un contrôleur de domaine est le même pour toute version de Windows Server de Windows Server 2008 à Windows Server 2016. Vous pouvez passer à un domaine de Windows Server 2016 de l'une des deux façons suivantes :

- Vous pouvez mettre à niveau le système d'exploitation sur les contrôleurs de domaine existants qui exécutent Windows Server 2008 ou une version ultérieure
- Vous pouvez ajouter des serveurs exécutant Windows Server 2016 comme contrôleurs de domaine dans un domaine qui a déjà des contrôleurs de domaine qui exécutent des versions antérieures de Windows Server

Options de mise à niveau d'AD DS pour Windows Server 2016 :

- Effectuer une mise à niveau sur place de Windows Server 2008 à Windows Server 2016.
 - Avantage : sauf pour les contrôles préalables, tous les fichiers et programmes restent en place et aucun travail supplémentaire n'est nécessaire
 - Risque : Il peut laisser des fichiers obsolètes et des bibliothèques de liaisons dynamiques (DLL)
- Introduire un nouveau serveur exécutant Windows Server 2016 dans le domaine, puis le promouvoir afin qu'il soit contrôleur de domaine (cette option est généralement préférée).
 - Avantage : le nouveau serveur n'a pas les fichiers et paramètres obsolètes
 - Risque : la migration des fichiers et des paramètres des administrateurs peut demander un travail supplémentaire

Parmi les deux méthodes, celle-ci est préférée parce que quand vous aurez terminé, vous aurez une installation propre du système d'exploitation Windows Server 2016 et de la base de données AD DS. Chaque fois qu'un nouveau contrôleur de domaine est ajouté, les enregistrements de domaine DNS sont mis à jour et les clients trouveront et utiliseront immédiatement ce contrôleur de domaine.

Mise à niveau vers Windows Server 2016

Pour mettre à niveau un domaine AD DS en cours d'exécution au niveau fonctionnel d'une version antérieure de Windows Server à un domaine AD DS en cours d'exécution au niveau fonctionnel de Windows Server 2016, vous devez d'abord mettre à niveau tous les contrôleurs de domaine vers le système d'exploitation Windows Server 2016. Vous pouvez effectuer cette mise à niveau en mettant à niveau tous les contrôleurs de domaine existants vers Windows Server 2016 ou en introduisant de nouveaux contrôleurs de domaine qui exécutent Windows Server 2016 et puis supprimer progressivement les contrôleurs de domaine existants.

Une mise à niveau du système d'exploitation en place n'engendre pas de schéma automatique et de préparation de domaine. Pour effectuer une mise à niveau d'un ordinateur qui a le rôle AD DS installé, vous devez d'abord utiliser les commandes de ligne de commande **adprep.exe /forestprep** et **adprep.exe /domainprep** pour préparer la forêt et le domaine. L'outil **adprep** est inclus sur le support d'installation dans le dossier \ Support \ Adprep. Aucune étape de configuration supplémentaire n'existe après ce point et vous pouvez continuer à exécuter la mise à niveau du système d'exploitation Windows Server 2016.

Lorsque vous souhaitez qu'un serveur exécutant Windows Server 2016 devienne un contrôleur de domaine dans un domaine existant et que vous êtes connecté en tant que membre des groupes administrateurs du schéma et administrateurs de l'entreprise, le schéma AD DS met automatiquement à jour vers Windows Server 2016. Dans ce scénario, vous ne devez pas exécuter la commande **adprep** avant de commencer l'installation.

Déploiement de contrôleurs de domaines Windows Server 2016

Pour mettre à niveau le système d'exploitation d'un contrôleur de domaine exécutant Windows Server 2008 ou une version ultérieure à Windows Server 2016, procédez comme suit :

1. Insérer le disque d'installation pour Windows Server 2016, puis lancer l'**Installation ; L'assistant d'installation Windows** s'ouvre.
2. Après l'apparition de la page de **Sélection de la langue**, cliquez sur **Installer maintenant**.
3. Après l'apparition des pages **Sélection du système d'exploitation** et **Acceptation de la licence**, sur la page **Quel type d'installation voulez-vous ?**, cliquez sur **Mise à niveau : Installer Windows et conserver les fichiers, les paramètres et les applications**.



Remarque : avec ce type de mise à niveau, vous ne devez pas conserver les paramètres des utilisateurs et réinstaller les applications ; tout est mis à jour en place. Rappelez-vous de vérifier la compatibilité matérielle et logicielle avant d'effectuer une mise à niveau.

Pour introduire une nouvelle installation de Windows Server 2016 en tant que contrôleur de domaine, procédez comme suit :

1. Déployez et configurez une nouvelle installation de Windows Server 2016, puis joignez-la au domaine.
2. Faites du nouveau serveur un contrôleur de domaine dans le domaine à l'aide du gestionnaire de serveur ou de l'une des autres méthodes décrites précédemment.
3. Mettez à jour les paramètres client DNS qui font référence aux anciens contrôleurs de domaine pour utiliser le nouveau contrôleur de domaine.

Installer un contrôleur de domaine en installant des médias

Si vous avez une connexion réseau entre les sites qui est lente, peu fiable ou coûteuse, vous trouverez peut-être nécessaire d'ajouter un autre contrôleur de domaine à un emplacement distant ou dans une succursale. Dans ce scénario, il est souvent préférable de déployer les services AD DS sur un serveur en l'installant à partir des médias plutôt que par le déploiement sur le réseau.

Par exemple, si vous vous connectez à un serveur qui se trouve dans un bureau distant et utilisez le Gestionnaire de serveur pour installer les services AD DS, la base de données AD DS et le dossier SYSVOL seront copiés sur le nouveau contrôleur de domaine via une connexion WAN potentiellement peu fiable. Comme alternative et pour réduire de manière significative la quantité de trafic sur la liaison WAN, vous pouvez créer une sauvegarde des services AD DS (peut-être sur une clé USB) et prendre cette sauvegarde à l'emplacement distant. Lorsque vous êtes à l'emplacement distant et exécutez le Gestionnaire de serveur pour installer les services AD DS, vous pouvez sélectionner l'option **Installation à partir des médias**.

à partir des médias. La plupart des copies sont ensuite effectuées au niveau local et la liaison WAN est utilisée uniquement pour le trafic lié à la sécurité et pour faire en sorte que le nouveau contrôleur de domaine reçoive toutes les modifications qui ont été apportées aux services AD DS centraux après avoir créé la sauvegarde **Installation à partir des médias**.

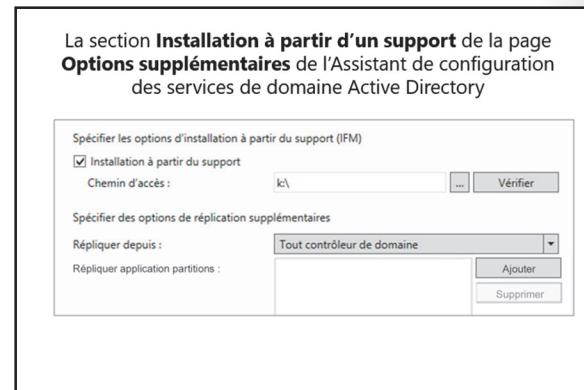
Pour installer un contrôleur de domaine à partir des médias, trouvez un contrôleur de domaine qui n'est pas un RODC. Utilisez l'outil de ligne de commande **ntdsutil** pour créer une capture instantanée de la base de données AD DS, puis copiez cette capture sur le serveur qui deviendra un contrôleur de domaine. Utilisez le Gestionnaire de serveur pour promouvoir le serveur à un contrôleur de domaine en sélectionnant l'option **Installation à partir des médias**, puis fournir le chemin d'accès local **Installation à partir des médias** au répertoire que vous avez déjà créé.

Le processus se déroule comme suit :

- Sur le contrôleur de domaine complet, au niveau d'une invite de commande d'administration, tapez les commandes suivantes (où C:\IFM est le répertoire de destination qui contiendra la capture instantanée de la base de données AD DS).

```
Ntdstil
Activate instance ntds
Ifm
create SYSVOL full C:\IFM
```

- Sur le serveur qui va devenir un contrôleur de domaine, procédez comme suit :
 - Utiliser le **Gestionnaire de serveur** pour ajouter le rôle AD DS.
 - Attendre que les fichiers AD DS s'installent.
 - Dans **Gestionnaire de serveur**, cliquez sur l'icône **Notification**, puis sous **Configuration post-déploiement**, cliquez sur **Promouvoir ce serveur en contrôleur de domaine**. Exécuter l'assistant de configuration des services de domaine Active Directory.
 - Sur la page correspondante de l'assistant, sélectionner l'option **Installation à partir des médias**, puis indiquer le chemin d'accès local vers le répertoire de la capture instantanée.
- AD DS s'installe à partir de la capture instantanée.



3. Notez que lors du redémarrage du contrôleur de domaine, il contacte les autres contrôleurs de domaine dans le domaine et met à jour les services AD DS avec toutes les modifications qui ont été faites après la création de la capture instantanée.



Documentation supplémentaire : Pour plus d'informations sur les étapes requises pour installer AD DS, reportez-vous à : « Installer les services de domaine Active Directory (niveau 100) » à : <http://aka.ms/Rvcwlz>

Cloner des contrôleurs de domaine

La façon la plus rapide de déployer plusieurs ordinateurs qui sont configurés de manière identique, en particulier lorsque ces ordinateurs fonctionnent dans un environnement virtualisé tel que Microsoft Hyper-V, est de cloner ces ordinateurs. Le clonage signifie que les disques durs virtuels des ordinateurs sont copiés et que les configurations mineures telles que les noms d'ordinateur et les adresses IP sont modifiées pour être uniques. Les ordinateurs sont alors immédiatement opérationnels. Ce processus, également appelé *approvisionnement* des ordinateurs, est une technologie principale des clouds privés. Avant Windows Server 2012, vous étiez en mesure de cloner les membres du domaine mais vous ne pouviez pas cloner les contrôleurs de domaine. Dans Windows Server 2016, comme dans Windows Server 2012, vous êtes en mesure de cloner les contrôleurs de domaine.

- Vous pouvez cloner des contrôleurs de domaine pour :
 - Un déploiement rapide ;
 - Les clouds privés ;
 - Les stratégies de récupération ;
- Pour cloner un contrôleur de domaine source :
 - Ajouter le contrôleur de domaine au groupe des Contrôleurs de domaine clonables ;
 - Vérifier la compatibilité des applications et des services ;
 - Créer un fichier DCCloneConfig.xml ;
 - Exporter une fois, puis créer autant de clones que nécessaire ;
 - Démarrer les clones.

Les scénarios suivants bénéficient du clonage de contrôleur de domaine virtuel :

- Déployer rapidement des contrôleurs de domaine supplémentaires dans un nouveau domaine
- Rétablir rapidement la continuité des activités au cours de la reprise après sinistre en rétablissant la capacité AD DS via le déploiement rapide des contrôleurs de domaine en utilisant le clonage
- L'optimisation des déploiements de cloud privé en tirant parti de l'approvisionnement flexible des contrôleurs de domaine pour répondre aux besoins accrus
- Fournir rapidement des environnements de test, ce qui permet le déploiement et le test de nouvelles fonctionnalités et capacités avant un déploiement de production
- Répondre rapidement aux besoins de capacité accrus dans les succursales, soit par le clonage de contrôleurs de domaine existants dans les succursales ou en les clonant dans le centre de données puis en les transférant aux succursales en utilisant Hyper-V

Le clonage de contrôleurs de domaine requiert la configuration suivante :

- Un hyperviseur qui prend en charge les identificateurs de génération d'ordinateurs virtuels, tels que Hyper-V dans Windows Server 2012 et les versions ultérieures
- Les contrôleurs de domaine en tant que systèmes d'exploitation invités basés sur Windows Server 2012 et les versions ultérieures
- Le contrôleur de domaine à cloner ou un contrôleur de domaine source qui doit fonctionner comme un ordinateur virtuel invité sur l'hyperviseur pris en charge

- Un maître d'émulateur de contrôleur de domaine principal qui fonctionne sur Windows Server 2012 ou une version ultérieure. Bien qu'il soit possible de cloner les contrôleurs de domaine exécutant Windows Server 2012 lorsqu'il existe des versions antérieures de contrôleurs de domaine, le contrôleur de domaine qui détient le rôle FSMO de maître d'émulateur de contrôleur de domaine principal doit prendre en charge le processus de clonage. L'émulateur PDC doit être en ligne lorsque les clones de contrôleur de domaine virtuels démarrent pour la première fois

Pour aider à s'assurer que le clonage des contrôleurs de domaine virtualisés est autorisé par les administrateurs AD DS, un membre du groupe administrateurs de domaine doit préparer un ordinateur à cloner. Les administrateurs de Hyper-V sont incapables de cloner un contrôleur de domaine sans les administrateurs AD DS et vice versa.

Préparer le contrôleur de domaine virtuel source

Pour préparer le déploiement de contrôleurs de domaine virtuels, procédez comme suit :

1. Ajouter le contrôleur de domaine source pour les groupes contrôleurs de domaine clonables.
2. Vérifier que les applications et services sur le contrôleur de domaine source prennent en charge le processus de clonage. Vous pouvez le voir en exécutant l'applet de commande Windows PowerShell suivant.

```
Get-ADDCCloneingExcludedApplicationList
```

Si des applications ou des services ne prennent pas le clonage en charge, vous devez les supprimer ou les tester d'abord. S'ils fonctionnent après le clonage, mettez les applications ou les services dans le fichier CustomDCCloneAllowList.xml. Vous pouvez créer CustomDCCloneAllowList.xml en utilisant la même cmdlet, annexant le paramètre *GenerateXML* et éventuellement le paramètre *-Force* si un fichier CustomDCCloneAllowList.xml existant doit être remplacé, comme indiqué dans la syntaxe suivante.

```
Get-ADDCCloneingExcludedApplicationList -GenerateXML [-Force]
```

3. Créez un fichier DCCloneConfig.xml. Vous devez créer ce fichier afin que le processus de clonage le reconnaisse et crée un nouveau contrôleur de domaine à partir du clone. En créant ce fichier, vous pouvez spécifier un nom d'ordinateur personnalisé, les paramètres d'adresse TCP / IP et le nom du site où le nouveau contrôleur de domaine doit se trouver. Si vous ne spécifiez pas un ou tous ces paramètres, un nom d'ordinateur est généré automatiquement et les paramètres de l'adresse IP sont fixés sur **dynamique**. Cela nécessite un serveur Dynamic Host Configuration Protocol (DHCP) sur le réseau et suppose que les clones de contrôleur de domaine se trouvent sur le même site que le contrôleur de domaine source. Vous pouvez utiliser Windows PowerShell pour créer le fichier DCCloneConfig.xml, comme indiqué dans la syntaxe suivante.

```
New-ADDCCloneConfigFile [-CloneComputerName <String>] [-IPv4DNSResolver <String[]>] [-Path <String>] [-SiteName <String>]
```

Si vous voulez créer plus d'un clone et que vous souhaitez spécifier des paramètres tels que les noms des ordinateurs et des informations d'adresse TCP / IP, vous devez modifier le fichier DCCloneConfig.xml ou en créer un nouveau, individuel pour chaque clone avant de le démarrer pour la première fois.

4. Exportez le contrôleur de domaine virtuel source.

Préparer des clones de contrôleur de domaine multiples

Si vous voulez préparer plusieurs clones de contrôleur de domaine, ne fournissez pas de paramètres supplémentaires et laissez le nom de l'ordinateur être généré automatiquement. En outre, utilisez le DHCP pour fournir les informations d'adresse TCP/IP.

Alternativement, vous pouvez personnaliser chaque clone en créant des fichiers DCCloneConfig.xml individuels. Pour ce faire, procédez comme suit :

1. Créer les disques durs virtuels clonés par l'exportation et l'importation de l'ordinateur virtuel.
2. Monter les disques durs virtuels nouvellement clonés en effectuant l'une des opérations suivantes :
 - o Double-cliquer sur ces derniers dans l'Explorateur de fichiers
 - o Utiliser **Diskpart.exe** avec la commande **attribuer** à une invite de commande à droits élevés
 - o Utiliser le cmdlet Windows PowerShell **Mount-DiskImage**
3. Utilisez les paramètres *-Offline* and *-Path* avec l'applet de commande **New-ADDCCloneConfigFile**. Remplacez **E** par la lettre de lecteur que vous avez utilisée lors du montage du fichier.vhdx à l'étape précédente, comme indiqué dans l'applet de commande suivante.

```
New-ADDCCloneConfigFile -CloneComputerName <LON-DC3> -offline -Path <E>:\Windows \ NTDS
```
4. Démonter les fichiers de disque dur virtuel en utilisant **Diskpart.exe** ou le cmdlet **Dismount-DiskImage** de Windows PowerShell.

Utilisation de noms d'ordinateurs affectés dynamiquement

Si vous ne configurez pas DCCloneConfig.xml avec un nom d'ordinateur statique par exemple pour créer plusieurs clones sans configurations individuelles, le nom de l'ordinateur du nouveau clone est généré automatiquement en fonction de l'algorithme suivant :

- Le préfixe comprend les huit premiers caractères du nom de l'ordinateur du contrôleur de domaine source. Par exemple, le nom de l'ordinateur source *SourceComputer* est l'abréviation dans le préfixe *SourceCo*
- Un suffixe de nom unique du format *-CLnnnn* est ajouté au préfixe, où *nnnn* est la prochaine valeur disponible de 0001 à 9999 que l'émulateur PDC détermine et qui n'est pas actuellement en cours d'utilisation

Création des clones de contrôleur de domaine virtuel

Pour créer les clones de contrôleur de domaine virtuel, procédez comme suit :

1. S'assurer que le contrôleur de domaine qui détient le rôle FSMO d'émulateur PDC, fonctionne sur Windows Server 2012 ou une version ultérieure.
2. S'assurer que l'émulateur PDC et un contrôleur de domaine qui héberge le catalogue global soient en ligne.
3. En utilisant les fichiers exportés à partir des étapes de préparation, utiliser la fonction **import** pour créer autant de clones que nécessaire ; En utilisant Hyper-V, sélectionnez **Copier les machines virtuelles (créer un nouvel identifiant unique)** pour vous permettre d'importer plusieurs instances individuelles du même ordinateur exporté.
4. Configurer individuellement les clones comme souhaité en suivant les étapes décrites précédemment.
5. Démarrer les clones.

Finalisation du clonage de contrôleur de domaine

Quand un nouveau clone de contrôleur de domaine démarre, les étapes suivantes sont exécutées automatiquement :

1. Le clone vérifie si un identificateur de génération d'ordinateur virtuel existe ; Ceci est nécessaire et s'il n'y a pas d'identifiant pour la génération de l'ordinateur virtuel, l'ordinateur démarre normalement en l'absence de DCCloneConfig ou alors il renomme DCCloneConfig et redémarre dans Mode

restauration des services d'annuaire (DSRM) ; Une sauvegarde est démarrée dans le DSRM et un administrateur de domaine a besoin de suivre de près le problème et de le résoudre pour faire fonctionner le contrôleur de domaine comme prévu.

2. Le clone vérifie si l'identificateur de génération d'ordinateur virtuel a changé et prend l'une des actions suivantes :
 - o S'il n'a pas changé, il est le contrôleur de domaine source d'origine ; Si DCCloneConfig existe, il est renommé ; Dans les deux cas, un démarrage normal se produit et le contrôleur de domaine est à nouveau fonctionnel
 - o S'il a changé, les sauvegardes de virtualisation se déclenchent et le processus continue
3. Le clone vérifie si DCCloneConfig existe ; Sinon, une vérification est effectuée pour savoir si une adresse IP existe en double et déterminer s'il faut démarrer normalement ou en DSRM ; Si le fichier DCCloneConfig existe, l'ordinateur obtient le nouveau nom de l'ordinateur et les paramètres de l'adresse IP à partir du fichier ; La base de données AD DS est modifiée et les étapes d'initialisation sont effectuées pour qu'un nouveau contrôleur de domaine soit créé.

Démonstration : Clonage un contrôleur de domaine

Dans cette démonstration, vous apprendrez à :

- Préparer un contrôleur de domaine source à cloner
- Exporter l'ordinateur virtuel source
- Créer et démarrer le contrôleur de domaine cloné

Procédure de démonstration

Préparer un contrôleur de domaine source à être cloné

1. Sur **LON-DC1** ouvrir le **Centre d'administration Active Directory**.
2. Ajouter le contrôleur de domaine **LON-DC1** au groupe de **Contrôleurs de domaine clonables**.
3. Vérifier que les applications et services sur **LON-DC1** prennent en charge le clonage.
4. Créer le fichier **DCCloneConfig.xml**, pour le clonage **LON-DC3**.
5. Fermer **LON-DC1**.

Exporter l'ordinateur virtuel source

1. Sur l'ordinateur hôte, dans le Gestionnaire Hyper-V, exporter **LON-DC1**.
2. Redémarrer **LON-DC1**.

Créer et démarrer le contrôleur de domaine cloné

1. Importer un nouvel ordinateur virtuel en utilisant les fichiers exportés.
2. Nommer le nouvel ordinateur virtuel **22742A-LON-DC3** puis sélectionner **Copier l'ordinateur virtuel (créer une nouvelle ID unique)**.
3. Dans le gestionnaire Hyper-V, démarrer **LON-DC3**.

Meilleures pratiques pour la virtualisation du contrôleur de domaine

La virtualisation offre de nombreux avantages, tels que l'indépendance matérielle, l'utilisation efficace des ressources et l'évolution pour les clouds privés. Elle fournit également une flexibilité lorsque vous déplacez des ordinateurs virtuels sur les infrastructures de virtualisation. Par le passé, la virtualisation des contrôleurs de domaine exigeait des administrateurs de l'infrastructure virtuelle de connaître les exigences spécifiques des services AD DS et de prendre des précautions pour éviter de prendre des risques pour l'infrastructure AD DS.

- Éviter les points de défaillance uniques
- Utiliser les services de temps
- Utiliser la technologie de virtualisation avec la fonction d'identification de génération d'ordinateur virtuel
- Utiliser Windows Server 2012 ou une version ultérieure en tant qu'invités de virtualisation
- Éviter ou désactiver les points de contrôle
- Penser à améliorer la sécurité
- Envisager de tirer profit du clonage dans votre déploiement ou dans votre stratégie de récupération
- Lancer au maximum 10 nouveaux clones en même temps
- Penser à utiliser les technologies de virtualisation qui permettent aux ordinateurs virtuels invités de se déplacer entre les sites
- Ajuster votre stratégie de nommage pour autoriser les clones de contrôleurs de domaine

Lorsque vous envisagez des contrôleurs de domaine virtuels, vous devez connaître les meilleures pratiques suivantes :

- Éviter les points de défaillance uniques. S'assurer que vous avez au moins deux contrôleurs de domaine virtualisés par domaine sur les différents hôtes de virtualisation, ce qui réduit le risque de perdre tous les contrôleurs de domaine si un hôte de virtualisation unique échoue. En outre, diversifier le matériel, les réseaux de stockage et les systèmes de stockage. S'assurer de maintenir les contrôleurs de domaine dans les différents centres de données ou les régions pour réduire l'impact des catastrophes
- Vérifier les services de temps. S'assurer que tous les ordinateurs, y compris l'hôte de l'hyperviseur et les contrôleurs de domaine invités, participent à la même infrastructure de services de temps. S'assurer aussi que le temps sur l'hôte et sur les invités ne diffère pas
- Utiliser la technologie de virtualisation qui permet les identificateurs de génération d'ordinateurs virtuels. Il n'y a que les infrastructures de virtualisation qui prennent en charge les nouveaux identifiants de génération d'ordinateurs virtuels qui prennent également en charge les sauvegardes et le clonage des contrôleurs de domaine virtuels
- Utiliser Windows Server 2012 ou une version ultérieure comme système d'exploitation invité pour les contrôleurs de domaine virtuels. Seules ces versions prennent en charge les sauvegardes pour les contrôleurs de domaine virtuels
- Éviter ou désactiver les points de contrôle. Si l'hôte de virtualisation ou les systèmes d'exploitation invités des contrôleurs de domaine ne prennent pas en charge les sauvegardes pour virtualiser les contrôleurs de domaine, désactiver la possibilité de créer des points de contrôle, par exemple, en utilisant un disque pass-through au lieu d'un disque dur virtuel. Lorsque les sauvegardes sont prises en charge, utiliser un disque dur virtuel pour prendre le clonage en charge mais éviter d'utiliser des points de contrôle
- Être conscient de l'amélioration de la sécurité et veiller à ce que les administrateurs de virtualisation soient aussi fiables que vos administrateurs de domaine
- Envisager de profiter du clonage. Le clonage peut être un déploiement ou une stratégie de récupération. Il permet de fournir un moyen simple et rapide pour créer de nombreux contrôleurs de domaine dans un court laps de temps
- Cloner par lots de 10 au maximum. Ne pas commencer plus de 10 nouveaux clones en même temps parce que la réplication de fichier utilisée pour SYSVOL permet seulement 10 connexions de réplication en même temps
- Penser à utiliser les technologies de virtualisation qui vous permettent de déplacer des ordinateurs virtuels au-delà des frontières du site. Cela peut s'avérer bénéfique pour vos stratégies de

déploiement et de récupération. Par exemple, vous pouvez créer 10 clones dans un emplacement central puis les déplacer vers les bureaux distants pendant les heures creuses

- Ajuster la stratégie de nommage pour permettre les clones de contrôleur de domaine. Il devrait être possible d'ajuster votre stratégie de nommage pour permettre aux contrôleurs de domaine clonés de conserver les huit premiers caractères du nom du contrôleur de domaine source et ensuite -CLnnnn attaché

 **Documentation supplémentaire :** Pour plus d'informations sur la virtualisation des contrôleurs de domaine, reportez-vous à : « Exécuter des contrôleurs de domaine dans Hyper-V » à : <http://aka.ms/Tjjl9g>

Question : Quel est le moyen le plus rapide pour répliquer des contrôleurs de domaine dans un environnement virtualisé ?

Question : Quelles sont les deux principales considérations pour le déploiement de contrôleurs de domaine pour Azure ?

Atelier pratique : Déploiement et administration de AD DS

Scénario

Vous êtes administrateur informatique à A. Datum Corporation. La société étend ses activités et possède plusieurs nouveaux emplacements. L'équipe d'administration AD DS évalue actuellement les méthodes disponibles dans Windows Server 2016 pour un déploiement rapide et à distance du contrôleur de domaine. En outre, l'équipe cherche un moyen d'automatiser certaines tâches administratives AD DS. L'équipe veut un déploiement rapide et transparent des nouveaux contrôleurs de domaine pour les nouveaux emplacements et elle veut faire la promotion de serveurs auprès de contrôleurs de domaine à partir d'un emplacement central.

Objectifs

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

- Déployer AD DS
- Déployer des contrôleurs de domaine en procédant à un clonage du contrôleur de domaine
- Administrer AD DS

Configuration de l'atelier pratique

Durée approximative : **45 minutes**

Ordinateurs virtuels : **22742A-LON-DC1**, **22742A-LON-DC2** et **22742A-LON-SVR1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquer sur **22742A-LON-DC1** et dans le volet **Actions** cliquer sur **Démarrer**.
3. Dans le volet d'**Actions**, cliquer sur **Se connecter** ; Attendre que l'ordinateur virtuel démarre.
4. Se connecter en utilisant les informations d'identification suivantes :
 - Nom d'utilisateur : **Adatum\Administrateur**
 - Mot de passe : **Pa55w.rd**
5. Répéter les étapes 2 à 4 pour les ordinateurs virtuels **22742A-LON-DC2** et **22742A-LON-SVR1**.

Exercice 1 : Déployer AD DS

Scénario

Dans le cadre de l'expansion de l'entreprise, A. Datum Corporation souhaite déployer de nouveaux contrôleurs de domaine sur des sites à distance avec un engagement minimal du personnel informatique distant. Vous allez utiliser Windows PowerShell pour déployer de nouveaux contrôleurs de domaine.

Les tâches principales de cet exercice sont les suivantes :

1. Installer des binaires AD DS.
2. Préparer l'installation d'AD DS et promouvoir un serveur distant.

3. Exécuter AD DS Best Practices Analyzer.

► **Tâche 1 : Installer des binaires AD DS**

1. Basculer vers **LON-DC1**.
2. Du **Gestionnaire de serveur**, ouvrir **Windows PowerShell**.
3. Utiliser le cmdlet **Installation-WindowsFeature** dans Windows PowerShell pour installer le rôle AD DS sur **LON-SVR1**.
4. Utiliser le cmdlet **Get-WindowsFeature** pour vérifier l'installation.
5. S'assurer que les cases à cocher pour **Active Directory Domain Services**, **Outils d'administration de serveur distant** et **Outils d'administration de rôles** sont cochées ; Pour le noeud **Outils AD DS et AD LDS**, il n'y a que le **Module Active Directory pour Windows PowerShell** qui doit être installé et non les outils graphiques, tels que le **Centre d'administration Active Directory**.

 **Remarque :** si vous gérez de manière centralisée vos serveurs, vous n'aurez généralement pas besoin d'outils de l'interface graphique sur chaque serveur. Si vous souhaitez les installer, vous devez spécifier les outils AD DS en exécutant le cmdlet **Add-WindowsFeature** avec le nom de commande **RSAT-ADDS**.

 **Remarque :** vous devrez peut-être patienter quelques instants une fois le processus d'installation terminé avant de vérifier que le rôle AD DS a été installé. Si les résultats attendus de la commande **Get-WindowsFeature** ne sont pas visibles, vous pouvez réessayer après quelques minutes.

► **Tâche 2 : Préparer l'installation d'AD DS et promouvoir un serveur distant**

Ajouter LON-SVR1 au Gestionnaire de serveur sur LON-DC1

- Sur **LON-DC1**, de **Gestionnaire de serveur**, sur le noeud de **tous les serveurs**, ajouter **LON-SVR1** comme serveur géré

Configurer AD DS à distance à l'aide du Gestionnaire de serveur

1. Sur **LON-DC1**, du **Gestionnaire de serveur**, configurer **LON-SVR1** en tant que contrôleur de domaine AD DS en utilisant les paramètres suivants :
 - Type : **Contrôleur de domaine supplémentaire pour le domaine existant**
 - Domaine : **Adatum.com**
 - Informations d'identification : **Adatum\Administrateur** avec le mot de passe **Pa55w.rd**
 - Mot de passe Directory Services Restore Mode (DSRM) : **Pa55w.rd**
 - Retirer les sélections pour le DNS et le catalogue global
2. Sur la page **Examiner les options** cliquer sur **Afficher le script**.
3. Dans le Bloc-notes Microsoft, modifier le script généré par Windows PowerShell.
 - Supprimer les lignes de commentaires qui commencent par le signe dièse (#)
 - Supprimer la ligne **Import-Module**
 - Supprimer les accents graves (`) à la fin de chaque ligne
 - Supprimer les sauts de ligne

4. Maintenant que la commande `Install-ADDSDomainController` et tous les paramètres sont sur une seule ligne, copier la commande.
5. Passer à l'**Assistant de configuration des services de domaine Active Directory**, puis cliquer sur **Annuler**.
6. Démarrer **Windows PowerShell** à l'invite de commande, taper la commande suivante :

```
Invoke-Command -ComputerName LON-SVR1 { }
```

7. Coller la commande copiée entre les accolades (`{ }`), puis appuyer sur entrée pour démarrer l'installation.
8. Utilisez les informations d'identification suivantes :
 - Nom d'utilisateur : **Adatum\Administrateur**
 - Mot de passe : **Pa55w.rd**
9. Taper et confirmer le **SafeModeAdministratorPassword** comme **Pa55w.rd**.
10. Après le redémarrage de **LON-SVR1**, sur **LON-DC1**, basculer vers **Gestionnaire de serveur** et sur le côté gauche, cliquer sur le nœud **AD DS** ; Noter que **LON-SVR1** a été ajouté en tant que serveur et que la notification d'avertissement a disparu ; Vous pourriez avoir à cliquer sur **Rafraîchir**.

► **Tâche 3 : Exécuter les services AD DS Best Practices Analyzer**

1. Sur **LON-DC1**, dans **Gestionnaire de serveur**, aller sur la vue du tableau de bord AD DS.
2. Commencer la recherche **BPA** pour **LON-DC1** et **LON-SVR1**.
3. Vérifier les résultats du BPA.

Résultats : Après cette opération, vous devriez avoir créé un nouveau contrôleur de domaine et vérifié les résultats de AD DS Best Practices Analyzer (BPA) pour ce contrôleur de domaine.

Exercice 2 : Déploiement de contrôleurs de domaine en procédant à un clonage du contrôleur de domaine

Scénario

Une équipe informatique de A. Datum Corporation souhaite déployer rapidement de nouveaux contrôleurs de domaine virtuel quand le besoin se fait sentir. Ils envisagent les clones de contrôleur de domaine dans Windows Server 2016. Vous devez effectuer une procédure de clonage de contrôleur de domaine pour vérifier que l'accélération du déploiement de contrôleurs de domaine est une option valide.

Les tâches principales de cet exercice sont les suivantes :

1. Vérifier les prérequis pour le clone du contrôleur de domaine.
2. Copier le contrôleur de domaine source.
3. Effectuer le clonage du contrôleur de domaine.

- ▶ **Tâche 1 : Vérifier les prérequis pour le clone du contrôleur de domaine**
 1. Basculez vers **LON-DC1**.
 2. Dans **Gestionnaire de serveur**, ouvrir le **Centre d'administration Active Directory** et ajouter **LON-DC1** au groupe **Contrôleurs de domaine clonable**.
 3. Ouvrir **Windows PowerShell** et utiliser **Get-ADDCCloningExcludedApplicationList** pour vérifier que les applications et services sur **LON-DC1** supportent le clonage.
 4. Utiliser les cmdlets **Get-ADDCCloningExcludedApplicationList -GenerateXML** et **New-ADDCCloneConfigFile** pour créer un fichier **DCCloneConfig.xml**.
- ▶ **Tâche 2 : Copier le contrôleur de domaine source**
 1. Arrêter **LON-DC1**.
 2. Sur l'ordinateur hôte, dans le gestionnaire Hyper-V, exporter **LON-DC1** à **D:\Program Files\Microsoft Learning\22742**.
 3. Démarrer **LON-DC1** et connecter-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
- ▶ **Tâche 3 : Effectuer le clonage du contrôleur de domaine**
 1. Sur l'ordinateur hôte, démarrer l'assistant **Import Virtual Machine** dans le gestionnaire Hyper-V.
 2. Sur la page **Localiser le dossier**, aller au dossier **D:\Program Files\Microsoft Learning\22742\22742A-LON-DC1**.
 3. Sur la page **Sélectionner un ordinateur virtuel**, sélectionnez **22742A-LON-DC1**.
 4. Sur la page **Choisir un type d'importation**, sélectionnez **Copier l'ordinateur virtuel (créer un nouvel ID unique)**.
 5. Sur la page **Choisir les dossiers pour les fichiers d'ordinateur virtuel**, activez la case à cocher **Stocker l'ordinateur virtuel dans un emplacement différent** ; Pour chaque emplacement de dossier, indiquez le chemin d'accès **D:\Program Files\Microsoft Learning\22742**.
 6. Sur la page **Choisir les dossiers pour stocker les disques durs virtuels**, indiquez le chemin d'accès **D:\Program Files\Microsoft Learning\22742**.
 7. Renommez le nouvel ordinateur virtuel **22742A-LON-DC3**.
 8. Dans l'assistant Hyper-V, démarrez et connectez-vous à **22742A-LON-DC3**.
 9. Pendant le démarrage du serveur, vous pouvez voir le message **Le clonage du contrôleur de domaine est achevé à X%**.

Résultats : Après avoir terminé cette opération, vous devez avoir déployé avec succès un contrôleur de domaine en le fermant dans Hyper-V.

Exercice 3 : Administration AD DS

Scénario

L'équipe informatique de A. Datum Corporation évalue les outils qui sont disponibles dans Windows Server 2016 pour l'administration AD DS. Vous devez évaluer l'utilisation à la fois du Centre d'administration Active Directory et Windows PowerShell pour l'administration et la gestion de AD DS.

Les tâches principales de cet exercice sont les suivantes :

1. Utiliser le Centre d'administration Active Directory.
2. Préparer le module suivant.

► Tâche 1 : Utiliser le Centre d'administration Active Directory

Naviguer dans le Centre d'administration Active Directory

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, ouvrez le **Centre administratif Active Directory**.
2. Passez à l'arborescence, puis développez **Adatum (local)**.

Effectuer une tâche administrative au sein du Centre d'administration Active Directory

1. Allez à l'aperçu **Vue d'ensemble**.
2. Réinitialisez le mot de passe pour **Adatum\Adam** en **Pa55w.rd** sans que l'utilisateur ne doive changer le mot de passe à la prochaine connexion.
3. Utilisez la section **Recherche globale** pour trouver des objets qui correspondent à la chaîne de recherche "Lon".

Créer des objets

- Créez un nouvel objet ordinateur nommé **LON-CL4** dans le conteneur **Computers**.

Voir tous les attributs de l'objet

- Ouvrez la page **Propriétés** pour **LON-CL4**, faites défiler jusqu'à la section **Extensions**, puis sélectionnez l'onglet **éditeur d'attribut**. Affichez les attributs des objets AD DS

Utiliser la visionneuse Windows PowerShell History

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

Résultats : Une fois cette opération terminée, vous devriez avoir utilisé avec succès le Centre d'administration Active Directory pour gérer AD DS et vérifié les applets de commande Windows PowerShell qui fonctionnent dans les coulisses.

► Tâche 2 : Préparer le module suivant

Une fois l'atelier terminé, rétablissez l'état initial de tous les ordinateurs virtuels :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-DC2** et **22742A-LON-SVR1**.

Révision du module et éléments à retenir

Dans ce module, vous avez reçu un aperçu de base de AD DS et appris les principales composantes. Vous pouvez maintenant décrire l'objectif d'un contrôleur de domaine et les différents rôles qu'il peut contenir. Vous êtes maintenant familiarisé avec les considérations pour le déploiement des contrôleurs de domaine et vous connaissez maintenant différentes méthodes de déploiement des contrôleurs de domaine.

Questions de contrôle des acquis

Question : Quelle méthode de déploiement utiliseriez-vous si vous deviez installer un contrôleur de domaine supplémentaire dans un emplacement éloigné qui avait une connexion WAN limitée ?

Question : Si vous avez besoin de promouvoir une installation Server Core de Windows Server 2016 pour être un contrôleur de domaine, quel(s) outil(s) pouvez-vous utiliser ?

Question : Si vous voulez exécuter un contrôleur de domaine dans le cloud, quel service devriez-vous envisager d'utiliser : AD Azure ou infrastructure en tant qu'ordinateurs virtuels d'un service (IaaS) Azure ?

Problèmes courants et conseils de dépannage

| Problème courant | Conseils pour la résolution des problèmes |
|--|---|
| Erreurs de syntaxe | |
| Problèmes préalables | |
| Problème de configuration du réseau et de la forêt | |

Module 2

Gestion d'objets dans AD DS

Sommaire :

| | |
|--|------|
| Vue d'ensemble du module | 2-1 |
| Leçon 1 : Gestion des comptes d'utilisateurs | 2-2 |
| Leçon 2 : Gérer des groupes dans AD DS | 2-11 |
| Leçon 3 : Gestion des objets ordinateur dans AD DS | 2-22 |
| Atelier pratique A : Gestion des objets AD DS | 2-29 |
| Leçon 4 : Utilisation de Windows PowerShell pour l'administration d'AD DS | 2-33 |
| Leçon 5 : Implémentation et gestion des UO | 2-48 |
| Atelier pratique B : Administration AD DS | 2-57 |
| Contrôle des acquis et éléments à retenir | 2-62 |

Vue d'ensemble du module

Active Directory Domain Services (AD DS) peut vous aider à gérer plus efficacement votre réseau.

Par exemple, vous pouvez l'utiliser pour gérer les comptes d'utilisateurs et d'ordinateurs en groupes au lieu de le faire compte par compte. Il permet également de rassembler des objets dans des conteneurs appelés unités d'organisation (UO) et de déléguer des tâches administratives à certaines personnes pour vous aider à distribuer la charge de travail de manière efficace.

Gérer les identités des périphériques devient de plus en plus complexe puisque de plus en plus d'employés apportent leurs propres périphériques dans le lieu de travail. Avec l'expansion des programmes Bring Your Own Device (BYOD), vous devrez gérer les identités de différents types de périphériques personnels, ainsi que leurs systèmes d'exploitation respectifs. AD DS possède de nombreuses fonctionnalités qui peuvent rendre cela plus facile.

Ce module décrit comment utiliser les outils graphiques et Windows PowerShell pour gérer les comptes et les groupes d'utilisateurs et d'ordinateurs. Il explique comment gérer un réseau d'entreprise en effectuant des opérations en bloc dans le but de modifier les attributs d'objet.

Objectifs

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

- Gérer les comptes d'utilisateurs dans AD DS
- Gérez des groupes dans AD DS
- Gérer des objets ordinateur dans AD DS
- Utiliser Windows PowerShell pour l'administration AD DS
- Mettre en œuvre et gérer des UO
- Administre AD DS

Leçon 1

Gestion des comptes d'utilisateurs

Un objet utilisateur, dans AD DS, est beaucoup plus que des propriétés qui se rapportent à l'identificateur de sécurité ou au compte d'un utilisateur. Il constitue la pierre angulaire de l'identité et des accès dans AD DS. Par conséquent, des processus cohérents, efficaces et sûrs en ce qui concerne l'administration des comptes d'utilisateurs sont les pierres angulaires de la gestion de la sécurité de l'entreprise.

Dans cette leçon, vous apprendrez à gérer les comptes utilisateurs, ce qui est beaucoup plus complexe que leur simple création et suppression. Les comptes d'utilisateurs possèdent plusieurs attributs que vous pouvez utiliser à diverses fins, comme le stockage d'informations supplémentaires de contact utilisateur ou d'informations d'applications spécifiques pour les applications Active Directory. En outre, il y a des fichiers et des paramètres spécifiques à l'utilisateur qui ne sont pas dans Active Directory mais, à l'inverse, stockées généralement dans le profil de l'utilisateur. Enfin, vous apprendrez tout sur l'utilisation des modèles d'utilisateurs pour vous aider à créer plus facilement des comptes d'utilisateurs.

Objectifs des leçons

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

- Création de comptes d'utilisateurs
- Configuration des attributs de compte d'utilisateur
- Gestion des comptes d'utilisateurs
- Création de profils d'utilisateurs
- Gestion des comptes utilisateur inactifs et désactivés
- Modèles de compte d'utilisateur
- Utilisez des modèles de comptes utilisateur pour gérer les comptes

Création de comptes d'utilisateurs

Dans AD DS, vous devez fournir un compte d'utilisateur à tous les utilisateurs qui ont besoin d'accéder aux ressources du réseau. Avec ce compte utilisateur, les utilisateurs peuvent s'authentifier sur le domaine AD DS et accéder aux ressources du réseau.

Dans Windows Server 2017, un compte d'utilisateur est un objet qui contient toutes les informations définissant un utilisateur. Un compte utilisateur inclut le nom d'utilisateur, son mot de passe et ses appartennances à des groupes. Un compte d'utilisateur contient également de nombreux autres paramètres que vous pouvez configurer en fonction de la configuration requise de votre organisation. Avec un compte d'utilisateur, vous pouvez :

- Accorder ou refuser aux utilisateurs des autorisations d'ouverture de session sur un ordinateur en fonction de l'identité de leur compte d'utilisateur
- Autoriser les utilisateurs à accéder à des processus et à des services dans un contexte de sécurité spécifique

- Comptes d'utilisateur :
 - Autoriser ou refuser l'accès pour la connexion aux ordinateurs
 - Accorder l'accès aux processus et services
 - Gérer l'accès aux ressources réseau
- Les comptes d'utilisateur peuvent être créés en utilisant :
 - Utilisateurs et ordinateurs Active Directory
 - Centre d'administration Active Directory
 - Windows PowerShell
 - Outil de ligne de commande Directory **dsadd**
- Les considérations relatives à l'attribution de noms aux utilisateurs sont les suivantes :
 - Nommer les formats
 - Suffixes UPN



- Gérer l'accès des utilisateurs aux ressources, telles que les objets ad ds et leurs propriétés, les dossiers partagés, les fichiers, les annuaires et les files d'attente d'impression

Un compte d'utilisateur permet à un utilisateur d'ouvrir une session sur les ordinateurs et domaines avec une identité que le domaine peut authentifier. Lorsque vous créez un compte utilisateur, vous devez fournir un nom d'ouverture de session de l'utilisateur, qui doit être unique dans le domaine et dans la forêt sur lesquels le compte utilisateur est créé.

Pour optimiser la sécurité, vous devriez éviter que plusieurs utilisateurs partagent un même compte et vous assurer plutôt que chaque utilisateur qui se connecte au réseau a son propre compte d'utilisateur et mot de passe.

 **Remarque :** ce cours porte sur les comptes AD DS. Vous pouvez également stocker les comptes d'utilisateurs dans la base de données locale du Gestionnaire des comptes de sécurité de chaque ordinateur, permettant l'authentification locale et l'accès aux ressources locales. Les comptes d'utilisateurs locaux sont, pour la plupart, au-delà de la portée de ce cours.

Création de comptes d'utilisateurs

Un compte utilisateur inclut le nom d'utilisateur et le mot de passe. Ce sont les identifiants de l'utilisateur. Un objet utilisateur comprend également plusieurs autres attributs qui décrivent et gèrent l'utilisateur. Vous pouvez utiliser Utilisateurs et ordinateurs Active Directory, Centre d'administration de Active Directory, Windows PowerShell, ou l'outil de ligne de commande **dsadd** pour créer un objet utilisateur.

Éléments à prendre en compte pour l'attribution de noms aux utilisateurs

Votre convention de dénomination est un élément important. Avoir une convention de dénomination formalisée vous permettra de gérer les noms d'utilisateurs en double et les changements de nom de manière standardisée. Lorsque vous créez des comptes d'utilisateurs, tenez compte des éléments suivants :

- Attribut **Nom complet**. **Nom complet** est utilisé pour créer plusieurs attributs d'un objet utilisateur, notamment les attributs du nom commun et de l'affichage du nom. Le nom commun d'un utilisateur est le nom affiché dans le volet des détails du composant logiciel enfichable. Il doit être unique dans le conteneur ou dans l'UO. Si vous créez un objet utilisateur pour une personne qui a le même nom qu'un utilisateur existant déjà dans le conteneur or UO, vous devrez donner un autre Nom complet unique au nouvel objet utilisateur.
- **Ouverture de session UPN**. Les ouvertures de session Nom principal de l'utilisateur (UPN) suivent le format *ouverture de session utilisateur prénom@ (Suffixe UPN)*. Les noms d'utilisateurs dans AD DS peuvent contenir des caractères spéciaux, y compris les points, les traits d'union et les apostrophes. Ces caractères spéciaux permettent de générer les noms exacts des utilisateurs, tels que O'Hare et Smith-Bates. Cependant, certains programmes et applications pourraient avoir d'autres restrictions. Nous vous recommandons d'utiliser des lettres et des chiffres standards jusqu'à ce que vous puissiez tester si les applications de votre environnement d'entreprise sont complètement compatibles avec les caractères spéciaux

Vous pouvez gérer la liste des suffixes UPN disponibles en utilisant le composant logiciel enfichable Domaines et approbations Active Directory. Faites un clic droit sur la racine du composant logiciel enfichable, cliquez sur **Propriétés**, puis utilisez l'onglet **suffixes UPN** pour ajouter ou supprimer des suffixes. Le nom Domain Name System (DNS) de votre domaine AD DS est un suffixe toujours disponible. Vous ne pouvez pas le retirer. Dans un environnement multi-domaine, vous pouvez affecter différents suffixes UPN aux utilisateurs, par exemple pour les suffixes de domaines e-mail



Remarque : il est important de mettre en place une stratégie de dénomination de compte d'utilisateur, en particulier dans les grands réseaux dans lesquels certains utilisateurs pourraient avoir le même nom. La combinaison du nom et du prénom et, le cas échéant, des caractères supplémentaires, devrait générer un nom unique pour le compte utilisateur. Plus précisément, c'est seulement le nom UPN qui doit être unique au sein de votre forêt AD DS. La propriété nom complet doit être unique seulement au sein de l'unité d'organisation où elle réside. Le nom **SAMAccountName de l'utilisateur** doit être unique dans ce domaine.

Configuration des attributs de compte d'utilisateur

Lorsque vous créez un compte d'utilisateur dans AD DS, vous configurez également toutes les propriétés de compte associées. Vous devez définir les attributs qui permettent à l'utilisateur de se connecter avec le compte et quelques autres attributs. Comme il est possible d'associer un objet utilisateur avec de nombreux attributs, il est important que vous compreniez ce qu'ils sont et comment les utiliser dans votre organisation.

Vous pouvez configurer les attributs de l'utilisateur à l'aide de Centre d'administration Active Directory, Utilisateurs et ordinateurs Active Directory, Windows PowerShell, ou l'outil **dsmod**.

Les propriétés de l'utilisateur comprennent les catégories suivantes :

- Compte
- Organisation
- Membre de
- Paramètres de mot de passe
- Profil
- Stratégie
- Silo
- Extensions



Remarque : les attributs associés à un compte utilisateur sont définis dans le cadre du schéma AD DS, que les membres du groupe de sécurité Administrateurs du schéma peuvent modifier. En général, le schéma ne change pas souvent. Toutefois, lorsque vous introduisez un programme au niveau de l'entreprise (tels que Microsoft Exchange Server), de nombreux changements de schéma sont nécessaires. Ces changements permettront aux objets et aux objets utilisateurs d'avoir des attributs supplémentaires.

Catégories des attributs

Les attributs d'un objet utilisateur se répartissent en plusieurs grandes catégories. Ces catégories apparaissent dans le volet de navigation de la boîte de dialogue des **Propriétés de l'utilisateur**, dans le Centre d'administration Active Directory :

- **Compte.** En plus des propriétés du nom utilisateur de l'utilisateur (**Prénom**, **Initiale deuxième prénom**, **Nom**, **Nom complet**) et des divers noms d'ouverture de session de l'utilisateur (**Ouverture de session UPN de l'utilisateur**, **Ouverture de session SamAccountName de l'utilisateur**), vous pouvez configurer les propriétés supplémentaires suivantes :

- **Heures d'ouverture de session.** Cette propriété définit la période pendant laquelle le compte peut être utilisé pour accéder à des ordinateurs du domaine. Vous pouvez utiliser la vue hebdomadaire type calendrier pour définir les heures où la connexion est autorisée et les heures où elle est refusée
 - **Se connecter à.** Utilisez cette propriété pour définir les ordinateurs qu'un utilisateur peut utiliser pour se connecter au domaine. Indiquez le nom de l'ordinateur et ajoutez-le à la liste des ordinateurs autorisés
 - **Date d'expiration du compte.** Cette valeur est utile lorsque vous souhaitez créer des comptes utilisateur temporaires. Par exemple, vous pouvez créer des comptes d'utilisateurs pour des personnes en stage dans votre entreprise pendant un an. Vous pouvez définir la date d'expiration du compte à l'avance. Personne ne peut utiliser le compte après sa date d'expiration, jusqu'à la re-configuration manuelle d'un administrateur
 - **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session.** Cette propriété vous permet de forcer les utilisateurs à réinitialiser leur mot de passe la prochaine fois qu'ils se connecteront. C'est quelque chose que vous pouvez activer après la réinitialisation du mot de passe d'un utilisateur
 - **Une carte à puce est nécessaire pour ouvrir une session interactive.** Cette valeur réinitialise le mot de passe de l'utilisateur à une séquence aléatoire complexe de caractères et définit une propriété qui nécessite que l'utilisateur utilise une carte à puce pour s'authentifier et se connecter
 - **Le mot de passe n'expire jamais.** C'est une propriété à utiliser normalement avec les comptes de service ; c'est-à-dire des comptes qui ne sont pas utilisés par des utilisateurs réguliers, mais par des services. En définissant cette valeur, vous devez vous rappeler de mettre à jour manuellement le mot de passe de manière périodique. Cependant, vous n'êtes pas obligé de le faire à un intervalle prédéterminé. Par conséquent, le compte ne peut jamais être verrouillé en raison de l'expiration du mot de passe — une caractéristique particulièrement importante pour les comptes de service
 - **L'utilisateur ne peut pas changer le mot de passe.** Cette option est plus généralement utilisée pour les comptes de service
 - **Stocker le mot de passe en utilisant le chiffrage réversible.** Cette stratégie fournit un soutien pour les programmes qui utilisent des protocoles nécessitant la connaissance du mot de passe de l'utilisateur à des fins d'authentification. Le stockage des mots de passe en utilisant un chiffrage réversible est essentiellement la même chose que le stockage des versions textes simples des mots de passe. Pour cette raison, vous ne devriez jamais activer cette option à moins que les exigences du programme soient plus importantes que la nécessité de protéger les mots de passe. Cette politique est nécessaire lorsque vous utilisez l'authentification à distance Challenge Handshake Authentication Protocol (CHAP) ou un service d'authentification Internet (IAS). Il est également nécessaire si vous utilisez l'authentification Digest dans Internet Information Services (IIS)
 - **Le compte est approuvé pour la délégation.** Vous pouvez utiliser cette propriété pour permettre à un compte de service d'usurper l'identité d'un utilisateur standard pour accéder aux ressources du réseau à la place de cet utilisateur
- **Organisation.** Cela inclut des propriétés telles que le **Nom d'affichage** d'un utilisateur, son **Bureau**, son **Adresse e-mail**, divers numéros de téléphone de contact, noms de structure de gestion, noms de ministères et organismes, adresses, etc.
 - **Membre de.** Utilisez cette section pour définir les appartennances aux groupes pour l'utilisateur
 - **Paramètres du mot de passe.** Cette section comprend des paramètres de mot de passe appliqués directement à l'utilisateur

- **Profil.** Utilisez cette section pour configurer un emplacement pour les données personnelles de l'utilisateur et définir un emplacement dans lequel enregistrer le profil de bureau de l'utilisateur quand il ou elle se déconnecte
- **Stratégie.** Utilisez des stratégies d'authentification pour gérer la durée de vie des tickets Kerberos Ticket (TGT) et le contrôle d'accès d'authentification pour un compte spécifique, tels que les comptes administratifs de haut niveau
- **Silo.** Les silos de politique d'authentification sont des conteneurs auxquels vous pouvez affecter un compte d'utilisateur. Vous pouvez attribuer des politiques d'authentification à ces silos
- **Extensions.** Cette section expose de nombreuses propriétés d'utilisateurs supplémentaires, dont la plupart ne nécessitent pas généralement de configuration manuelle

Démonstration : Gestion des comptes d'utilisateurs

Dans cette démonstration, vous allez apprendre à utiliser le Centre administratif Active Directory en vue de :

- Créer un nouveau compte utilisateur
- Supprimer un compte utilisateur
- Déplacer un compte utilisateur
- Configurer les attributs de l'utilisateur :
 - Modifier le département
 - Modifier l'appartenance à un groupe

Procédure de démonstration

Créer un nouveau compte utilisateur

- Utilisez le **Centre d'administration Active Directory** pour créer un nouvel utilisateur comme suit :
 - Prénom : **Ventes**
 - Nom : **Gestionnaire**
 - Ouverture de la session UPN de l'utilisateur : **GestionnaireVentes**
 - Mot de passe : **Pa55w.rd**

Supprimer un compte utilisateur

- Supprimez le compte Art Odum

Déplacer un compte utilisateur

1. Déplacer le compte **Burton Bartels** de la UO **Managers** à la UO **Développement**.
2. Ouvrir l'UO **Développement** pour vérifier que le compte **Burton Bartels** est présent.

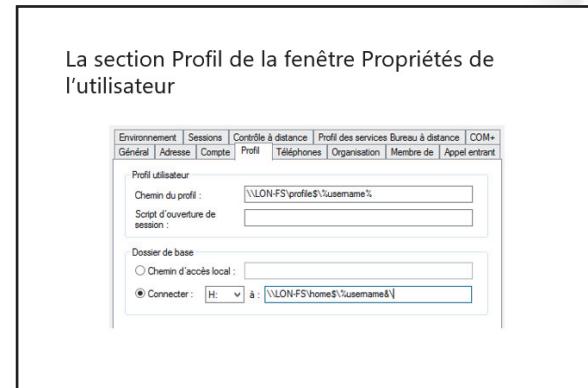
Configurer les attributs de l'utilisateur

- Modifiez le compte **Burton Bartels** comme suit :
 - Changer le champ **Département** de **Managers** à **Développement** ;
 - Supprimer le compte du groupe Managers
 - Ajouter le compte au groupe Développement

Création de profils d'utilisateurs

Lorsque les utilisateurs se déconnectent, leurs paramètres de bureau et d'applications sont enregistrés dans un sous-dossier qui correspond à leur nom d'utilisateur dans le répertoire C:\Users dossier sur le disque dur local. Ce dossier contient leur profil d'utilisateur. Dans ce dossier, des sous-dossiers contiennent des documents et des paramètres qui représentent le profil de l'utilisateur, avec ses **Documents, Vidéos, Photos, Téléchargements** et ses données d'applications.

Si un utilisateur est susceptible de se connecter de manière interactive à plus d'un poste de travail client, il est préférable que ses paramètres et documents soient disponibles sur les autres postes clients. Il y a différentes manières de faire en sorte que les utilisateurs puissent accéder à leurs profils à partir de plusieurs postes de travail.



Configuration des propriétés de compte utilisateur pour gérer les profils

Vous pouvez configurer les propriétés suivantes du profil de bureau d'un utilisateur en allant dans les paramètres du compte d'utilisateur dans le Centre d'administration Active Directory :

- Chemin du profil. Ce chemin est soit local, soit, plus généralement, un chemin d'accès Universal Naming Convention (UNC). Les paramètres de bureau de l'utilisateur sont stockés dans le profil. Si un profil utilisateur a un chemin UNC, l'utilisateur aura accès à ses paramètres de bureau indépendamment de l'ordinateur de domaine auquel il se connecte. C'est un profil itinérant
- Script d'ouverture de session. Ceci est un fichier de commandes qui contient des commandes qui s'exécutent lorsque l'utilisateur ouvre une session. En général, on utilise ces commandes pour créer des mappages de lecteur. Si vous utilisez un script d'ouverture de session, le nom du script ne peut être qu'un nom de fichier (avec extension). Les scripts doivent être stockés dans le dossier du répertoire C:\Windows\SYSVOL\domain\scripts sur tous les contrôleurs de domaine. Plutôt que d'utiliser un fichier de commandes de script d'ouverture de session, vous activerez généralement les scripts d'ouverture de session à l'aide des objets de stratégie de groupe (GPO) ou des préférences de stratégie de groupe
- Dossier de base. Ceci est une zone de stockage dans lequel les utilisateurs peuvent enregistrer leurs documents personnels. Vous pouvez spécifier un chemin d'accès local ou, plus généralement, un chemin UNC vers le dossier de l'utilisateur. Vous devez également spécifier la lettre du lecteur qui est utilisé pour mapper un lecteur réseau sur le chemin UNC spécifié. Vous pouvez ensuite faire en sorte que les documents personnels d'un utilisateur s'enregistrent dans ce dossier redirigé

 **Remarque :** lorsque vous créez des comptes d'utilisateurs destinés à être des modèles et que vous utilisez un même emplacement pour le chemin de profil et le dossier de base, il faut utiliser la variable %Nom d'utilisateur% dans le chemin d'accès, de telle sorte que AD DS puisse créer les dossiers automatiquement lorsque le compte est utilisé comme modèle. Par exemple, vous pouvez utiliser les chemins d'accès où le serveur de fichiers est nommé LON-FS et où des partitions ont été créées pour les profils et les dossiers d'origine. Respectivement profile\$ et home\$:

- Chemin du profil : \\LON-FS\profile\$\%Nom d'utilisateur%
- Dossier de base Connect H : à \\LON-FS\home\$\%Nom d'utilisateur%

Utilisation des groupes pour gérer les profils

En tant qu'alternative à l'utilisation des paramètres individuels du compte utilisateur, vous pouvez utiliser des GPO pour gérer ces paramètres. Vous pouvez configurer les paramètres de redirection des dossiers en utilisant l'éditeur de gestion des stratégies de groupe pour ouvrir un GPO pour l'édition. Puis, développez **Configuration utilisateur, Politiques et Paramètres Windows**. Paramètres Windows contient les sous-noeuds répertoriés dans le tableau suivant.

| Sous-noeuds dans le nœud Paramètres Windows | | |
|---|--|---|
| <ul style="list-style-type: none">▫ AppData (Roaming)▫ Bureau▫ Menu Démarrer▫ Document | <ul style="list-style-type: none">▫ Images▫ Musique▫ Vidéos▫ Favoris▫ Contacts | <ul style="list-style-type: none">▫ Téléchargements▫ Liens▫ Recherches▫ Parties enregistrées |

Vous pouvez utiliser ces sous-noeuds pour configurer tous les aspects des paramètres de profil de bureau et des applications d'un utilisateur. Pour un sous-nœud donné, tels que Documents, vous pouvez choisir entre la redirection de base ou avancée. Dans la redirection de base, tous les utilisateurs concernés par le GPO ont leur dossier Documents redirigé vers un sous-dossier nommé individuellement hors d'un dossier racine commun défini par un nom UNC. Par exemple, \\LON-SVR1\Utilisateurs\. Avec la redirection avancée, vous pouvez utiliser l'appartenance à un groupe de sécurité pour spécifier l'endroit où les paramètres et les documents d'un utilisateur seront stockés. Par exemple, vous pouvez stocker les documents de l'utilisateur Recherche et développement sur un serveur hautement sécurisé.

Gestion des comptes utilisateur inactifs et désactivés

Les comptes d'utilisateurs peuvent devenir inactifs pour différentes raisons. Les utilisateurs quittent l'entreprise, partent en congés maternité ou paternité, ou prennent des congés sabbatiques. Dans les cas mentionnés, si un utilisateur n'a pas besoin d'avoir accès à son compte pendant une période donnée, il convient de le désactiver, plutôt que de le supprimer. Même si un utilisateur a quitté l'organisation, il est recommandé de désactiver le compte de l'utilisateur jusqu'à ce que vous soyez sûr que ce compte utilisateur n'a plus aucune utilité. Cela est particulièrement applicable si un utilisateur possède une boîte aux lettres sur votre serveur Microsoft Exchange Server. Si vous supprimez l'utilisateur de AD DS, vous supprimez également la boîte aux lettres de l'utilisateur. Il y a plusieurs raisons pour lesquelles vous pourriez avoir intérêt à conserver le courrier de l'utilisateur. D'autant plus que la restauration d'un compte d'utilisateur et de sa boîte aux lettres associée prend du temps.

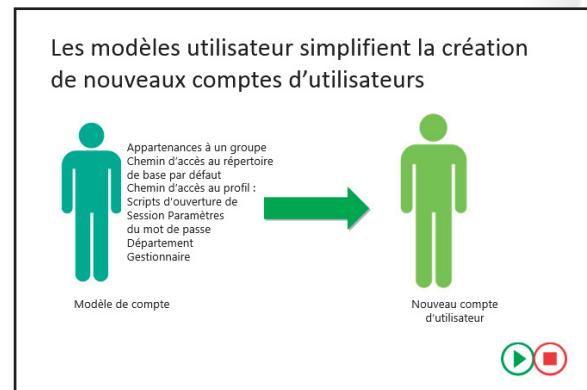
Pour désactiver un compte d'utilisateur, recherchez et sélectionnez le compte dans le Centre d'administration Active Directory. Puis, dans le volet **Tâches**, cliquez sur **Désactiver**. Pour activer un compte, cliquez sur **Activer** dans le volet **Tâches**.

- Les comptes utilisateur qui seront inactifs pendant un certain temps doivent être désactivés plutôt que supprimés
- Pour désactiver un compte dans Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur le compte et cliquez sur Désactiver le compte dans le menu

Modèles de compte utilisateur

Créer de nouveaux utilisateurs implique généralement le paramétrage de plusieurs attributs pour l'utilisateur. Cela peut être long et fastidieux, surtout si vous créez plusieurs utilisateurs. Les modèles d'utilisateur peuvent réduire l'effort requis pour créer de nouveaux comptes d'utilisateurs. Ils réduisent également les risques d'erreurs lors de la configuration des propriétés pour les utilisateurs.

La plupart des utilisateurs d'un département donné, business unit ou unité d'organisation, partageront de nombreux attributs communs, tels que les appartences aux groupes et l'emplacement du répertoire d'origine. Dans AD DS, un modèle d'utilisateur est tout simplement un compte que vous configurez avec toutes les propriétés communes propres à cet emploi ou à ce département. Par exemple, vous pouvez créer un compte d'utilisateur nommé Modèle_Ventes qui a tous les attributs qui correspondent à vos vendeurs. Lorsqu'un nouveau vendeur est embauché, vous pouvez copier le modèle pour créer le nouveau compte.



Remarque : les meilleures pratiques indiquent de désactiver le compte modèle afin qu'il ne puisse pas être utilisé pour se connecter et de mettre un trait de soulignement au début du nom afin que le compte modèle soit toujours au sommet de la liste des utilisateurs, ainsi plus facile à localiser.

Seuls les attributs les plus couramment utilisés sont copiés à partir du modèle vers le nouveau compte d'utilisateur. Il s'agit notamment des types suivants :

- Appartenances à un groupe
- Répertoires d'origine
- Paramètres du profil
- Scripts d'ouverture de session
- Horaires d'ouverture de session
- Paramètres du mot de passe
- Nom du département
- Gestionnaire

Lorsque vous copiez un compte, vous devez fournir les informations suivantes pour le nouveau compte :

- Prénom
- Nom
- Nom complet
- Nom de connexion d'utilisateur
- Mot de passe

Les champs d'attributs qui ne sont pas copiés à partir du modèle comprennent :

- Bureau

- Numéros de téléphone
- Nom de rue
- Dénomination du poste

Démonstration : Utiliser des modèles pour gérer les comptes

Dans cette démonstration, vous verrez comment créer un compte modèle et comment créer un nouvel utilisateur sur la base de ce compte modèle.

Procédure de démonstration

Créer un modèle utilisateur

1. Utilisez **Utilisateurs et ordinateurs Active Directory** pour créer un nouvel utilisateur comme suit :
 - Prénom : **_ventes**
 - Nom : **Modèle**
 - Nom de connexion d'utilisateur : **salestemplate**
 - Mot de passe : **Pa55w.rd**
2. Décochez la case **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**.
3. Paramétrez le mot de passe pour qu'il n'expire jamais.
4. Désactivez le compte.

Configurer les propriétés du modèle

- Double-cliquez sur le modèle de compte **_Ventes**, puis définissez les attributs suivants :
 - Membre de : **Ventes**
 - Département : **Ventes**
 - Gestionnaire : **Erin Bull**
 - Script d'ouverture de session : **\\\lon-dc1\Netlogon\Logon.bat**

Créer un nouvel utilisateur depuis le modèle

1. Cliquez avec le bouton droit sur le compte **_modèle ventes**, puis cliquez sur **Copier**.
2. Créer un nouvel utilisateur nommé **Utilisateur ventes** avec le mot de passe **Pa55w.rd**.
3. Activer le compte et effacer l'attribut **Le mot de passe n'expire jamais**.
4. Exigez que le compte change de mot de passe la prochaine fois que l'utilisateur ouvre une session.
5. Consulter les propriétés du niveau compte **Utilisateur ventes** et vérifier que les propriétés du modèle sont bien présentes.
6. Fermer la fenêtre **Utilisateurs et ordinateurs Active Directory**.

Question : Quelle est l'utilité d'un profil itinérant ?

Question : Quelle est la différence entre la désactivation d'un compte et un compte verrouillé ?

Leçon 2

Gérer des groupes dans AD DS

Bien qu'il puisse être pratique d'attribuer des autorisations et des capacités à des comptes d'utilisateurs individuels dans les petits réseaux, cela devient peu pratique et inefficace dans les grands réseaux d'entreprise. Par exemple, si de nombreux utilisateurs ont besoin du même niveau d'accès à un dossier, il est plus efficace de créer un groupe qui contient les comptes d'utilisateurs concernés, puis d'attribuer les autorisations spécifiques au groupe. Ceci a l'avantage de vous permettre de modifier les autorisations de fichiers d'un utilisateur en l'ajoutant ou en le retirant du groupe, plutôt que d'éditer directement les autorisations de fichiers. Avant d'implémenter des groupes dans votre organisation, vous devez connaître l'étendue des différents types de groupes Windows Server et la meilleure façon de les utiliser pour gérer l'accès aux ressources ou attribuer des droits et des capacités de gestion.

Objectifs des leçons

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

- Décrire les types de groupes
- Décrire les stratégies de groupes
- Expliquer comment implémenter la gestion des groupes
- Gérer les membres des groupes à l'aide de la Politique de Groupe
- Décrire les groupes définis par défaut
- Décrire les identités particulières
- Gérer les groupes dans Windows Server

Types de groupes

Dans un réseau d'entreprise Windows Server 2016, il existe deux types de groupes : la sécurité et la distribution. Lorsque vous créez un groupe, vous choisissez le type de groupe et sa portée. Le type de groupe détermine les capacités du groupe.

Les applications de messagerie électronique utilisent principalement les groupes de distribution, qui ne sont pas sécurisés. Les groupes de sécurité sont sécurisés et on les utilise pour attribuer des autorisations à diverses ressources. Vous pouvez utiliser des groupes de sécurité dans les entrées d'autorisation dans les listes de contrôle d'accès (ACL) pour sécuriser l'accès aux ressources. Vous pouvez également utiliser des groupes de sécurité comme un service de distribution pour les applications de messagerie. Si vous souhaitez utiliser un groupe pour gérer la sécurité, ce doit être un groupe de sécurité.

- Groupes de distribution
 - Utilisé uniquement avec des applications de messagerie
 - Sécurité pas activée (pas de SID)
 - Impossible d'accorder les autorisations



- Groupes de sécurité
 - Principal de sécurité avec un SID
 - Peut recevoir des autorisations
 - Peut également être activé pour le courrier électronique



Les groupes de sécurité et les groupes de distribution peuvent être convertis en un autre type de groupe



Remarque : le type de groupe par défaut pour les groupes nouvellement créés est sécurité.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR UNIQUEMENT

Puisqu'il est possible d'utiliser les groupes de sécurité à la fois pour l'accès aux ressources et pour la distribution du courrier électronique, de nombreuses organisations utilisent uniquement les groupes de sécurité. Cependant, il est préférable de créer un groupe de type distribution si vous n'utilisez celui-ci que pour la distribution de courrier électronique. Sinon, le groupe est associé à un SID, et le SID est ajouté au jeton d'accès de sécurité de l'utilisateur, ce qui peut rendre le jeton inutilement lourd.

Vous pouvez convertir un groupe de sécurité en un groupe de distribution à tout moment. Lorsque vous faites cela, l'attribut **type de groupe** change. Un groupe de sécurité qui a été converti en un groupe de distribution perd donc toutes les autorisations qui lui sont assignées, même si les ACLs contiennent toujours le SID. Si un groupe de distribution est converti en un groupe de sécurité, l'inverse se produit, l'attribut **type de groupe** change et on peut lui attribuer des autorisations aux ressources.

 **Remarque :** sachez que lorsque vous ajoutez un utilisateur à un groupe de sécurité, le jeton d'accès de l'utilisateur — qui authentifie les procédés utilisateurs — ne se met à jour que lorsque l'utilisateur ouvre une session. Par conséquent, si l'utilisateur est actuellement connecté, il devra se déconnecter et se reconnecter pour mettre à jour son jeton d'accès et prendre en compte les appartennances aux groupes modifiées.

 **Remarque :** l'avantage d'utiliser des groupes de distribution devient plus visible dans les déploiements Exchange Server à grande échelle, surtout quand il y a besoin d'imbriquer ces groupes de distribution dans toute l'entreprise.

Étendues des groupes

Windows Server 2017 prend en charge l'étendue de groupe. L'étendue d'un groupe détermine à la fois la gamme des capacités ou des autorisations d'un groupe et l'appartenance au groupe.

Il y a quatre étendues de groupes :

- Local. Ce type de groupe est adapté aux serveurs ou aux postes de travail autonomes, sur les serveurs membres de domaine qui ne sont pas contrôleurs de domaine, ou sur les postes de travail de membres du domaine. Les groupes locaux sont vraiment locaux, ce qui signifie qu'ils ne sont disponibles que sur l'ordinateur où ils existent. Les caractéristiques importantes d'un groupe local sont :
 - Vous pouvez affecter les capacités et les autorisations seulement sur les ressources locales, c'est-à-dire sur l'ordinateur local
 - Les membres peuvent être situés partout dans la forêt AD DS et peuvent inclure :
 - Tous les principaux de sécurité du domaine : les utilisateurs, les ordinateurs, les groupes globaux ou des groupes du domaine local
 - Les utilisateurs, les ordinateurs et les groupes globaux de tout domaine de la forêt
 - Les utilisateurs, les ordinateurs et les groupes globaux de tout domaine approuvé
 - Les groupes universels définis dans tout domaine de la forêt

- Les groupes locaux peuvent contenir des utilisateurs, des ordinateurs, des groupes globaux, des groupes locaux de domaine et des groupes universels du même domaine, des domaines de la même forêt et un autre domaine approuvé et peuvent recevoir les autorisations d'accès aux ressources uniquement sur l'ordinateur local
- Les groupes locaux de domaine ont les mêmes possibilités d'adhésion, mais ils peuvent recevoir l'autorisation d'accès aux ressources de n'importe où dans le domaine
- Les groupes universels peuvent contenir des utilisateurs, des ordinateurs, des groupes globaux et d'autres groupes universels du même domaine ou de domaines de la même forêt et peuvent recevoir des autorisations d'accès à n'importe quelle ressource de la forêt
- Les groupes globaux ne peuvent contenir que des utilisateurs, des ordinateurs et d'autres groupes globaux du même domaine et peuvent être autorisés à accéder aux ressources du domaine ou de n'importe quel domaine approuvé

- Domaine local. Ce type de groupe est adapté principalement pour gérer l'accès aux ressources ou pour attribuer des responsabilités de gestion (droits). Les groupes Domaine local existent sur les contrôleurs de domaines dans une forêt AD DS, et par conséquent, la portée du groupe est locale au domaine dans lequel ils résident. Les caractéristiques importantes de groupes Domaine local sont :
 - Vous pouvez affecter les capacités et les autorisations sur les ressources Domaine local uniquement, c'est-à-dire sur tous les ordinateurs dans le domaine local
 - Les membres peuvent être situés partout dans la forêt AD DS et peuvent inclure :
 - Tous les principaux de sécurité du domaine : les utilisateurs, les ordinateurs, les groupes globaux ou des groupes du domaine local
 - Les utilisateurs, les ordinateurs et les groupes globaux de tout domaine de la forêt
 - Les utilisateurs, les ordinateurs et les groupes globaux de tout domaine approuvé
 - Les groupes universels définis dans tout domaine de la forêt
- Global. Ce type de groupe est principalement utilisé pour regrouper les utilisateurs aux caractéristiques similaires. Par exemple, les groupes globaux sont souvent utilisés pour regrouper les utilisateurs qui font partie d'un département ou par emplacement géographique. Les caractéristiques importantes des groupes globaux sont :
 - Vous pouvez attribuer des capacités et des autorisations partout dans la forêt
 - Les membres peuvent être du Domaine local uniquement et peuvent comprendre des utilisateurs, des ordinateurs et des groupes globaux du domaine local
- Universel. Ce type de groupe est le plus souvent utilisé dans les réseaux multidomaines car il combine les caractéristiques des groupes de domaine local et des groupes globaux. Plus précisément, les caractéristiques importantes des groupes universels sont les suivantes :
 - Vous pouvez attribuer des capacités et des autorisations partout dans la forêt, comme avec les groupes globaux
 - Les membres peuvent être situés partout dans la forêt AD DS et peuvent inclure :
 - Les utilisateurs, les ordinateurs et les groupes globaux de tout domaine de la forêt
 - Les groupes universels définis dans tout domaine de la forêt
 - Les propriétés des groupes universels sont propagées dans le catalogue global et sont disponibles à travers le réseau de l'entreprise sur tous les contrôleurs de domaine qui hébergent le rôle du catalogue global. Cela rend l'adhésion aux listes des groupes universels plus accessible, ce qui est utile dans les scénarios multidomaines. Par exemple, si un groupe universel est utilisé pour la distribution de courrier électronique, le processus de détermination de la liste des membres est généralement plus rapide dans les réseaux multidomaines distribués

Le tableau suivant résume et compare les propriétés de base des quatre étendues de groupe.

| Étendues des groupes | Peut inclure les membres de | Peut posséder des autorisations pour | Peut être converti en |
|----------------------|---|--|-----------------------|
| Local | Les utilisateurs du domaine, les ordinateurs du domaine, des groupes globaux et les groupes universels de tout domaine dans la forêt Les groupes de domaine local du même domaine Les utilisateurs locaux de l'ordinateur | Les ressources de l'ordinateur local seulement | Non applicable |

| Étendues des groupes | Peut inclure les membres de | Peut posséder des autorisations pour | Peut être converti en |
|----------------------|--|---|--|
| Domaine local | Les utilisateurs du domaine, les ordinateurs du domaine, des groupes globaux et les groupes universels de tout domaine dans la forêt Les groupes de domaine local du même domaine | Les ressources de domaine local seulement | Les groupes universels (tant qu'aucun autre groupe de domaine local n'existe en tant que membre) |
| Global | Les utilisateurs du domaine, les ordinateurs de domaine et les groupes globaux du même domaine | Toute ressource du domaine dans la forêt | Les groupes universels (tant qu'ils ne sont pas membres d'un des autres groupes globaux) |
| Universel | Les utilisateurs du domaine, les ordinateurs du domaine, des groupes globaux et les groupes universels de tout domaine dans la forêt | toute ressource du domaine dans la forêt | Groupes de domaine local et groupes globaux (tant qu'aucun autre groupe universel n'existe en tant que membre) |

Implémentation d'une gestion de groupe

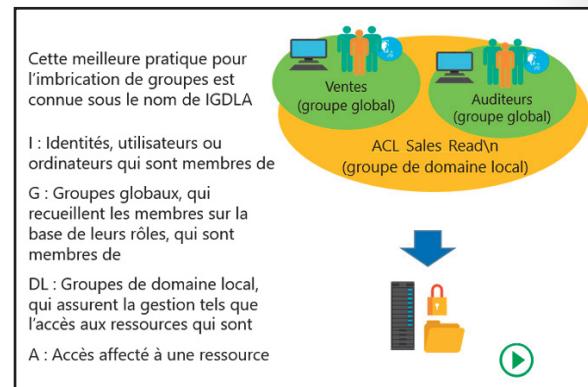
L'ajout de groupes à d'autres groupes est un processus appelé imbrication. L'imbrication crée une hiérarchie de groupes qui prend en charge vos rôles d'entreprise et vos règles de gestion.

Pour l'imbrication de groupes, une des meilleures pratiques se nomme IGDLA, qui est un acronyme pour ce qui suit :

- Identités
- Groupes globaux
- Groupes de domaine local
- Accès

Ces parties de IGDLA sont liées de la façon suivante :

- Les identités (comptes utilisateurs et ordinateurs) sont membres de groupes globaux, qui représentent les rôles d'entreprise
- Les groupes globaux (également appelés groupes de rôles) sont membres de groupes de domaine local, qui représentent les règles de gestion. Par exemple, ils déterminent qui a l'autorisation de lecture sur un ensemble spécifique de dossiers
- Les groupes de domaine local (également appelés groupes de règles) bénéficient d'un accès aux ressources. Dans le cas d'un dossier partagé, l'accès est accordé en ajoutant le groupe de domaine local à l'ACL du dossier, avec une autorisation qui fournit le niveau d'accès approprié



Dans une forêt multidomaine, la meilleure pratique pour l'imbrication de groupes s'appelle IGDLA. Le U supplémentaire représente les groupes universels :

- Identités
- Groupes globaux
- Groupes universels
- Groupes de domaine local
- Accès

Dans ce cas de figure, les groupes globaux de plusieurs domaines sont membres d'un groupe universel unique. Ce groupe universel est membre des groupes de domaine local dans de multiples domaines.

Exemple IGDLA

La figure sur la diapositive représente la mise en œuvre d'un groupe qui reflète l'aspect technique des meilleures pratiques de gestion de groupe (IGDLA) et le point de vue de l'entreprise d'une gestion basée sur les rôles et les règles. Prenez le scénario suivant.

La force de vente de Contoso Ltd vient de terminer son exercice. Les fichiers de vente de l'année précédente sont dans un dossier appelé Ventes. L'équipe des ventes a besoin d'avoir accès en lecture seule au dossier de vente. En outre, une équipe d'auditeurs de Woodgrove Bank, un investisseur potentiel, nécessite l'accès en lecture seule au dossier de vente pour effectuer la vérification. Vous pouvez mettre en place la sécurité pour ce scénario en suivant ces étapes :

1. Affecter des utilisateurs ayant des responsabilités professionnelles ou d'autres caractéristiques d'entreprises communes à des groupes de rôle, implémentés en tant que groupes de sécurité globaux. Effectuer cela séparément pour chaque domaine. Les vendeurs de Contoso Ltd. sont ajoutés à un groupe de rôle Ventes ; les auditeurs à Woodgrove Bank sont ajoutés à un groupe de rôle Auditeurs.
2. Créer un groupe pour gérer l'accès aux dossiers de vente en lecture seule. Implémentez cela dans le domaine qui contient la ressource qui est gérée. Dans ce cas, le dossier Ventes est dans le domaine Contoso. Par conséquent, vous devez créer le groupe de règles de gestion de l'accès aux ressources comme un groupe de domaine local nommé ACL_Sales_Eead.
3. Ajouter les groupes de rôle au groupe de règles de gestion d'accès aux ressources pour représenter la règle de gestion. Ces groupes peuvent provenir de tout domaine dans la forêt ou d'un domaine approuvé, comme Woodgrove Bank. Les groupes globaux des domaines externes approuvés, ou de tout domaine dans la même forêt, peuvent être membres d'un groupe de domaine local.
4. Attribuer l'autorisation qui implémente le niveau d'accès requis. Dans ce cas, accorder l'autorisation en lecture seule au groupe de domaine local.

Cette stratégie se traduit par deux points uniques de gestion, réduisant ainsi les contraintes propres à la gestion. Un point de gestion définit qui est en Ventes, et l'autre point de gestion définit qui est Auditeur. Comme ces rôles sont susceptibles d'avoir accès à une variété de ressources s'étendant au-delà du dossier Ventes, il y a un autre point de gestion unique pour déterminer qui a accès en lecture seule au dossier Ventes. Par ailleurs, le dossier Ventes ne consiste pas forcément en un seul dossier sur un seul serveur. Il peut être un ensemble de dossiers sur plusieurs serveurs, chacun de ces derniers attribuant l'autorisation de lecture au groupe de domaine local unique.

Configuration d'un gestionnaire de groupe

La page des propriétés d'un groupe a un onglet **Dirigé par**. Utilisez cette option pour fournir des informations sur le gestionnaire responsable de ce groupe. En ajoutant un utilisateur ou un groupe dans le champ **Nom**, des informations sur cet utilisateur — telles que son bureau, son adresse et numéro de téléphone — seront récupérées de AD DS et s'afficheront. Il y a aussi une case à cocher appelée

Le gestionnaire peut mettre à jour la liste des membres. Elle permet au gestionnaire du groupe de gérer l'appartenance au groupe. Ceci est utile dans les environnements administratifs répartis, dans lequel les Managers sont chargés de contrôler leurs propres départements.

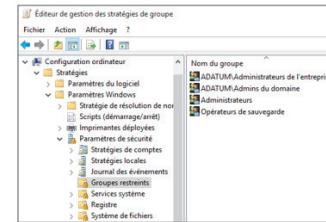
Gestion de membres de groupes à l'aide de la stratégie de groupe

La gestion de l'appartenance à un groupe peut être une tâche de longue haleine ; surtout si vous devez modifier la composition des groupes sur les postes de travail ou sur des serveurs répartis dans toute l'entreprise. Par exemple, vous devrez peut-être ajouter un utilisateur ou un groupe global au groupe Administrateurs local sur les ordinateurs clients ou ajouter un groupe global au groupe Opérateurs de sauvegarde sur les serveurs.

La stratégie de groupe fournit un paramètre appelé **Groupes restreints** qui vous permet de contrôler la composition des groupes locaux sur des ordinateurs appartenant à un domaine et celle des groupes AD DS en configurant un GPO et en attribuant ce GPO à l'unité d'organisation qui contient ces comptes d'ordinateurs.

Le paramètre **Groupes restreints** se trouve dans la Stratégie de configuration ordinateur, sous **Paramètres Windows**, puis sous **Paramètres de sécurité**. Il ne contient aucun groupe par défaut.

- Les groupes restreints peuvent simplifier la gestion de groupes
- Les groupes locaux et AD DS peuvent être gérés



Remarque : pour configurer l'appartenance aux groupes AD DS, vous devez attribuer le GPO à l'unité d'organisation qui contient les comptes d'ordinateur des contrôleurs de domaine.

Vous pouvez également configurer l'imbrication des groupes en utilisant le paramètre **Groupes restreints**. Par exemple, vous pourriez utiliser le paramètre **Groupes restreints** pour imbriquer des groupes globaux dans des groupes universels. Toutes les règles régissant l'imbrication de groupe s'appliquent même lors de l'utilisation de **Groupes restreints**.

Remarque : le paramètre **Groupes restreints** est disponible uniquement dans les politiques de groupes au niveau du domaine. Il n'existe pas dans les politiques de groupes locaux sur le client Windows et dans les systèmes d'exploitation serveur.

Suppression de membres non désignés

L'un des avantages du paramètre **Groupes restreints** est qu'il supprimera également tout utilisateur (ou groupe) du groupe concerné s'ils ne sont pas sur la liste des utilisateurs ou des groupes que le paramètre désigne. C'est utile pour contrôler l'appartenance à des groupes administratifs de haut niveau, tels que les administrateurs de l'entreprise, les administrateurs du domaine et les groupes d'administrateurs locaux sur les serveurs et les ordinateurs clients. Si un utilisateur est ajouté manuellement à un groupe contrôlé, il sera supprimé la prochaine fois qu'il réactualisera la stratégie de groupe.

Remarque : la seule exception à cette règle est que le compte Administrateur local par défaut ne peut jamais être supprimé du groupe Administrateurs local.

Suppression de la stratégie

Si la stratégie de groupe qui a été utilisée pour configurer l'appartenance à un groupe restreint est dissociée du conteneur qui détient les comptes d'ordinateur, ou si l'entrée du groupe restreint est supprimée du GPO, les appartances aux groupes qu'elle a attribuées ne seront pas supprimées. Ces adhésions aux groupes doivent être modifiées manuellement.

Groupes par défaut

Windows Server 2017 crée certains groupes automatiquement. Ceux-ci sont appelés groupes locaux par défaut, et ils incluent des groupes habituels, tels que les Administrateurs, les Opérateurs de sauvegarde, et les Utilisateurs de bureau à distance. Certains groupes supplémentaires sont créés automatiquement dans un domaine, à la fois dans le conteneur intégré et dans le conteneur Utilisateurs. Entre autres, Administrateurs de domaine, Administrateurs de l'entreprise et Administrateurs du schéma.

Gérez soigneusement les groupes par défaut qui accordent des priviléges d'administration, car ces groupes :

- Ont généralement plus de priviléges que nécessaire pour la plupart des environnements délégués
- Offrent souvent une protection à leurs membres

| Groupe | Emplacement |
|---------------------------------|--|
| Administrateurs de l'entreprise | Conteneur Utilisateurs du domaine racine de la forêt |
| Administrateurs du schéma | Conteneur Utilisateurs du domaine racine de la forêt |
| Administrateurs | Conteneur intégré de chaque domaine |
| Administrateurs du domaine | Conteneur Utilisateurs de chaque domaine |
| Opérateurs de serveur | Conteneur intégré de chaque domaine |
| Opérateurs de compte | Conteneur intégré de chaque domaine |
| Opérateurs de sauvegarde | Conteneur intégré de chaque domaine |
| Opérateurs d'impression | Conteneur intégré de chaque domaine |
| Éditeurs de certificats | Conteneur Utilisateurs de chaque domaine |

Les groupes par défaut qui donnent des priviléges d'administration

Un sous-ensemble de groupes par défaut fournit d'importantes autorisations ainsi que des droits utilisateurs liés à la gestion de AD DS. En raison des droits que ces groupes détiennent, ces groupes sont protégés. Les groupes protégés sont décrits plus bas dans cette rubrique. La liste suivante résume les capacités de ces groupes :

- Administrateurs de l'entreprise (dans le conteneur Utilisateurs du domaine racine de la forêt). Ce groupe est un membre du groupe Administrateurs dans chaque domaine de la forêt, ce qui lui donne un accès complet à la configuration de tous les contrôleurs de domaine. Il possède également la partition de configuration du répertoire et a le plein contrôle sur le contexte de nommage de domaine dans tous les domaines de la forêt
- Administrateurs du schéma (conteneur Utilisateurs du domaine racine de la forêt). Ce groupe possède et a le plein contrôle du schéma Active Directory
- Administrateurs (Conteneur intégré de chaque domaine)/Les membres de ce groupe ont le plein contrôle sur tous les contrôleurs de domaine et sur les données dans le contexte de nommage de domaine. Ils peuvent changer la composition de tous les autres groupes administratifs dans le domaine et le groupe Administrateurs dans le domaine racine de la forêt peut changer la composition des Administrateurs de l'entreprise, Administrateurs du schéma et Administrateurs de domaine. Le groupe Administrateurs dans le domaine racine de la forêt est généralement considéré comme le plus puissant groupe d'administration de service de la forêt
- Administrateurs de domaine (conteneur Utilisateurs de chaque domaine). Ce groupe est ajouté au groupe Administrateurs de son domaine. Il hérite donc de toutes les capacités du groupe Administrateurs. Il est également, par défaut, ajouté au groupe Administrateurs local de chaque ordinateur membre du domaine, donnant ainsi aux administrateurs du domaine la propriété de tous les ordinateurs du domaine

- Opérateurs de serveur (Conteneur intégré de chaque domaine). Les membres de ce groupe peuvent effectuer des tâches de maintenance sur les contrôleurs de domaine. Ils ont le droit de se connecter localement, de démarrer et d'arrêter des services, d'effectuer des opérations de sauvegarde et de restauration, de formater des disques, de créer ou supprimer des partitions et d'éteindre les contrôleurs de domaine. Par défaut, ce groupe n'a pas de membres
- Opérateurs de compte (Conteneur intégré de chaque domaine). Les membres de ce groupe peuvent créer, modifier et supprimer des comptes d'utilisateurs, des groupes et des ordinateurs situés dans toute unité d'organisation dans le domaine (sauf les contrôleurs de domaine UO) et dans les conteneurs Utilisateurs et ordinateurs. Les membres du groupe de l'opérateur de compte ne peuvent pas modifier les comptes qui sont membres des groupes Administrateurs ou Administrateurs de domaine, ils ne peuvent pas non plus modifier ces groupes. Les membres du groupe de l'opérateur de compte peuvent également se connecter localement aux contrôleurs de domaine. Par défaut, ce groupe n'a pas de membres
- Opérateurs de sauvegarde (Conteneur intégré de chaque domaine). Les membres de ce groupe peuvent effectuer des opérations de sauvegarde et de restauration sur les contrôleurs de domaine, peuvent se connecter localement et éteindre les contrôleurs de domaine. Par défaut, ce groupe n'a pas de membres
- Opérateurs d'impression (Conteneur intégré de chaque domaine). Les membres de ce groupe peuvent maintenir des files d'attente d'impression sur les contrôleurs de domaine. Ils peuvent également se connecter localement et éteindre les contrôleurs de domaine. Par défaut, ce groupe n'a pas de membres
- Éditeurs de certificats (Conteneur Utilisateurs de chaque domaine). Les membres de ce groupe sont autorisés à publier des certificats dans le répertoire. Par défaut, ce groupe n'a pas de membres

Gestion des groupes qui offrent des privilèges d'administration

Il faut gérer soigneusement les groupes par défaut qui fournissent des privilèges d'administration car ils octroient généralement des privilèges plus larges que nécessaire dans la plupart des cas de délégations et parce qu'ils appliquent souvent une protection à leurs membres.

Le groupe Opérateurs de compte est un bon exemple. Si vous examinez les capacités du groupe Opérateurs de compte dans la liste précédente, vous pouvez voir que les membres de ce groupe disposent de beaucoup de droits. Ils peuvent même se connecter localement à un contrôleur de domaine. Dans de très petits réseaux, ces autorisations peuvent être affectées à une ou deux personnes qui sont généralement les administrateurs de domaine, de toute façon. Cependant, dans les grandes entreprises, les droits et les autorisations accordées aux opérateurs de compte sont généralement beaucoup trop larges. En outre, le groupe Opérateurs de compte est, comme les autres groupes administratifs, un groupe protégé.

Groupes protégés

Les groupes protégés sont définis par le système d'exploitation et ne peuvent pas être sans protection. Les membres d'un groupe protégé deviennent protégés par association et n'héritent plus des autorisations (ACL) de leur unité d'organisation mais reçoivent à la place une copie d'un ACL du groupe protégé. Cet ACL de groupe protégé offre une protection considérable aux membres. Par exemple, si vous ajoutez Jeff Ford au groupe Opérateurs de compte, son compte est protégé et le bureau d'aide, qui a l'autorisation de réinitialiser tous les mots de passe des utilisateurs dans l'UO Employés, est incapable de réinitialiser le mot de passe de Jeff Ford.

Les groupes protégés comprennent :

- Opérateurs de compte
- Administrateurs

- Opérateurs de sauvegarde
- Éditeurs de certificats
- Administrateurs du domaine
- Administrateurs de l'entreprise
- krbtgt
- Opérateurs d'impression
- Lecture seule des contrôleurs de domaine
- Duplateur
- Opérateurs de serveur

Groupes personnalisés

Il est préférable d'éviter l'ajout d'utilisateurs aux groupes qui ne possèdent pas de membres par défaut (Opérateurs de compte, Opérateurs de sauvegarde, Opérateurs de serveur et Opérateurs d'impression). Au lieu de cela, créez des groupes personnalisés auxquels vous pouvez attribuer des autorisations et des droits d'utilisateur qui conviennent aux exigences de votre entreprise et administration.

Par exemple, Scott Mitchell devrait être en mesure d'effectuer des opérations de sauvegarde sur un contrôleur de domaine, mais ne devrait pas pouvoir effectuer des opérations de restauration qui pourraient conduire à un rollback de la base de données ou à la corruption. En outre, Scott ne devrait pas être en mesure d'éteindre un contrôleur de domaine. Alors, il ne faut pas mettre Scott dans le groupe Opérateurs de sauvegarde. Au lieu de cela, créez un groupe local et assignez-lui seulement le droit de l'utilisateur de Sauvegarde des fichiers et des répertoires, puis créez un groupe global et ajoutez Scott en tant que membre. Ensuite, ajoutez ce groupe global au groupe local.

Identités spéciales

Windows et AD DS prennent également en charge les identités particulières. Ce sont des groupes où le système d'exploitation contrôle l'adhésion. Vous ne pouvez pas afficher les groupes dans une liste (dans Utilisateurs et ordinateurs Active Directory, par exemple), vous ne pouvez pas afficher ou modifier l'appartenance aux groupes de ces identités particulières et vous ne pouvez pas les ajouter à d'autres groupes. Vous pouvez toutefois utiliser ces groupes pour attribuer des droits et des autorisations.

Les plus importantes identités spéciales — souvent appelées *groupes* (pour plus de commodité) — sont décrites dans la liste suivante :

- Ouverture de session anonyme Cette identité représente les connexions à un ordinateur et ses ressources qui sont faites sans fournir un nom d'utilisateur et mot de passe. Avant Windows Server 2003, ce groupe était un membre du groupe Tout le monde. À partir de Windows Server 2003, ce groupe n'est plus un membre par défaut du groupe Tout le monde

Utilisateurs authentifiés. Cette identité représente les identités qui sont authentifiés. Ce groupe n'inclut pas l'utilisateur Invité, même si le compte Invité a un mot de passe.

- Tout le monde Cette identité inclut les Utilisateurs authentifiés et le compte Invité

• Identités spéciales :

- Ce sont des groupes pour lesquels l'adhésion est contrôlée par le système d'exploitation
- Elles peuvent être utilisées par le système d'exploitation Windows Server pour fournir un accès aux ressources en fonction du type d'authentification ou de connexion et non en fonction du compte utilisateur

• Les principales identités spéciales comprennent :

- | | |
|--------------------------------|-------------------------|
| • Ouverture de session anonyme | • Interactive |
| • Utilisateurs authentifiés | • Réseau |
| • Tout le monde | • Propriétaire créateur |

- Interactif. Cette identité représente les utilisateurs qui accèdent à une ressource tout en étant connecté localement sur l'ordinateur qui héberge la ressource et non en train d'accéder à la ressource sur le réseau. Lorsqu'un utilisateur accède à une ressource spécifique sur un ordinateur sur lequel l'utilisateur est connecté localement, l'utilisateur est automatiquement ajouté au groupe Interactif pour cette ressource. Interactif inclut également les utilisateurs qui se connectent à travers une connexion Bureau à distance (RDC)
- Réseau. Cette identité représente les utilisateurs qui accèdent à une ressource sur le réseau, par opposition aux utilisateurs connectés localement à l'ordinateur qui héberge la ressource. Lorsqu'un utilisateur accède à une ressource spécifique sur le réseau, l'utilisateur est automatiquement ajouté au groupe de réseau pour cette ressource
- Créeur propriétaire. Cette identité représente l'entité de sécurité qui a créé un objet. Le Créeur propriétaire a automatiquement l'autorisation de contrôle total sur l'objet en vertu d'être l'entité qui a créé l'objet

L'importance de ces identités spéciales est que vous pouvez les utiliser pour fournir un accès à des ressources en fonction du type d'authentification ou de connexion, plutôt que le compte d'utilisateur. Par exemple, vous pouvez créer un dossier sur un système qui permet aux utilisateurs de visualiser son contenu quand ils sont connectés localement sur le système, mais qui ne permet pas les mêmes utilisateurs de visualiser le contenu d'un lecteur mappé sur le réseau. Vous pouvez y parvenir en attribuant des autorisations à l'identité spéciale Interactif.

Un cas de figure commun pour le groupe Créeur propriétaire est lorsque les autorisations NTFS sont définies sur un dossier racine pour permettre aux utilisateurs de créer des sous-dossiers, tels que les répertoires personnels. Le groupe Créeur propriétaire accorde aux utilisateurs l'autorisation de contrôle total sur les répertoires d'origine parce que l'utilisateur a créé le sous-dossier.

Démonstration : Gestion des groupes dans Windows Server

Dans cette démonstration, vous allez apprendre à créer un nouveau groupe et à ajouter des membres à ce groupe. En outre, vous apprendrez à ajouter des utilisateurs au groupe, à modifier le type et l'étendue du groupe et à configurer un gestionnaire en charge du groupe.

Procédure de démonstration

Créer un nouveau groupe et ajouter des membres

1. Utilisez **Centre d'administration Active Directory** pour créer un nouveau groupe de sécurité globale nommé **Managers informatiques** dans l'UO IT de Adatum.com.
2. Ajoutez les membres suivants au groupe :
 - **Beth Burke**
 - **Logan Boyle**

Ajouter un utilisateur au groupe

- Recherchez l'utilisateur **Maj Hojski** puis ajoutez l'utilisateur au groupe **Managers informatiques**

Modifier le type et l'étendue du groupe

- Accédez aux propriétés du groupe **Managers informatiques**, changez le type de **Groupe Distribution**, puis changez l'étendue du **Groupe Universel**

Configurez un gestionnaire pour le groupe

1. Modifier la section **Dirigé par** pour ajouter **Parsha Schoonen** en tant que gestionnaire du groupe.
2. Permettre à **Parsha** de mettre à jour la liste des membres du groupe.
3. Fermer les propriétés des **Managers informatiques**.
4. Fermer le **Centre d'administration Active Directory**.

Leçon 3

Gestion des objets ordinateur dans AD DS

Ordinateurs, comme les utilisateurs, sont des principaux de sécurité :

- Ils ont un compte avec un nom d'utilisateur et mot de passe que Windows Server change automatiquement sur une base périodique
- Ils s'authentifient sur le domaine
- Ils peuvent appartenir à des groupes, avoir accès à des ressources et vous pouvez les configurer en utilisant la stratégie de groupe

Un compte d'ordinateur commence son cycle de vie lorsqu'il est créé et ajouté à votre domaine. Par la suite, l'exécution-journalière des tâches administratives incluent :

- La configuration des propriétés de l'ordinateur
- Le déplacement de l'ordinateur entre les UO
- La gestion de l'ordinateur lui-même
- Le renommage, la réinitialisation, la désactivation, le fonctionnement et finalement la suppression de l'objet ordinateur

Si vous savez comment effectuer ces tâches de gestion de l'ordinateur-, vous pouvez configurer et maintenir les objets ordinateurs au sein de votre organisation.

Objectifs des leçons

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

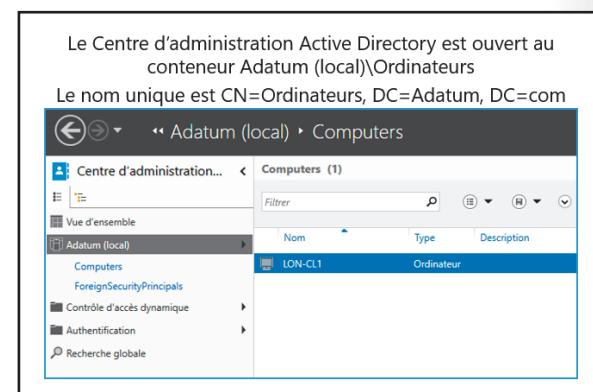
- Expliquer le but du conteneur Ordinateurs
- Décrire comment configurer l'emplacement des comptes d'ordinateurs
- Expliquer comment contrôler qui a la permission de créer des comptes d'ordinateur
- Expliquer comment ajouter un ordinateur à un domaine
- Décrire les comptes ordinateurs et les canaux sécurisés
- Expliquer comment réinitialiser le canal sécurisé
- Expliquer comment effectuer un ajout sur un domaine non-connecté

Quel est le conteneur Ordinateurs ?

Avant de créer un objet ordinateur dans les AD DS, vous devez avoir un endroit où le mettre.

Lorsque vous créez un domaine, le conteneur Ordinateurs est créé par défaut. Ce conteneur est l'emplacement par défaut pour les comptes d'ordinateur lorsqu'un ordinateur rejoint le domaine.

Ce conteneur n'est pas une unité d'organisation ; au contraire, il est un objet de type conteneur. Son nom commun est CN = Ordinateurs. Il existe des différences subtiles mais importantes entre un



conteneur et une unité d'organisation. Vous ne pouvez pas créer une unité d'organisation dans un conteneur, de sorte que vous ne pouvez pas diviser le conteneur Ordinateurs. Vous ne pouvez également pas lier un GPO à un conteneur. Par conséquent, nous vous recommandons de créer des UO personnalisées pour héberger des objets ordinateurs, au lieu d'utiliser le conteneur Ordinateurs.

Spécifier l'emplacement des comptes d'ordinateur

La plupart des organisations créent au moins deux unités d'organisation pour les objets ordinateurs : une pour les serveurs et une autre pour héberger les comptes d'ordinateur pour les ordinateurs clients, tels que les ordinateurs de bureau, portables et d'autres dispositifs utilisateurs. Ces deux UO viennent s'ajouter à l'unité d'organisation des contrôleurs de domaine qui est créée par défaut lors de l'installation des services AD DS.

Vous pouvez créer des objets ordinateurs dans n'importe quelle unité d'organisation dans votre domaine. Il n'y a pas de différence technique entre un objet ordinateur dans une UO cliente, un objet ordinateur dans une UO serveur, un objet ordinateur dans l'UO contrôleur de domaine, ou même un objet ordinateur dans une unité d'organisation destinée aux utilisateurs. Toutefois, les administrateurs créent généralement différentes UO pour créer des étendues uniques de gestion, de sorte qu'ils puissent déléguer la gestion d'objets client à une seule équipe et la gestion des objets serveur à une autre.

Votre modèle administratif pourrait vous amener à diviser vos UO clientes et UO serveurs en petits groupes. De nombreuses organisations créent des sous-UO sous une UO serveur pour classer et gérer les types spécifiques de serveurs. Par exemple, vous pouvez créer une UO pour les serveurs de fichiers et d'impression, une UO pour les serveurs de base de données, ou n'importe quel nombre de UO qui catégorise les types de serveurs de votre organisation. Ce faisant, vous pouvez donner les autorisations pour gérer les objets ordinateurs d'une UO à l'équipe d'administrateurs pour chaque type de serveur. De même, les organisations distribuées géographiquement avec des équipes locales de support technique divisent souvent une UO mère pour les clients en sous-OU pour chaque site. Cette approche permet à l'équipe technique de chaque site de créer des objets ordinateurs sur place pour les ordinateurs clients et à ajouter des ordinateurs dans le domaine en utilisant ces objets ordinateurs.

Votre structure d'unité d'organisation doit correspondre à votre modèle administratif afin que vos UO puissent fournir des points uniques de gestion pour la délégation de l'administration.

En outre, en utilisant des UO séparées, vous pouvez créer différentes configurations de base en utilisant les différents GPO qui sont liés aux UO cliente et serveur. Avec la stratégie de groupe, vous pouvez spécifier la configuration pour les ensembles d'ordinateurs en reliant les GPO qui contiennent des instructions de configuration aux UO. Il est commun pour les organismes de séparer les clients en UO d'ordinateurs de bureau et UO d'ordinateurs portables. Vous pouvez ensuite lier les GPO qui spécifient la configuration d'ordinateurs de bureau ou d'ordinateurs portables à l'UO correspondante.

 **Remarque :** vous pouvez utiliser l'outil de ligne de commande redircmp pour reconfigurer le conteneur par défaut pour les ordinateurs. Par exemple, si vous voulez changer le conteneur par défaut des ordinateurs par une unité d'organisation appelée MyComputers, utilisez la syntaxe suivante : redircmp ou=MyComputers,DC=contoso,dc=com.



Contrôler les autorisations pour créer des comptes d'ordinateur

Avant d'ajouter un ordinateur à un domaine, vous devez d'abord créer un objet ordinateur dans l'unité d'organisation appropriée. Pour ajouter un ordinateur à un domaine AD DS, trois conditions doivent être respectées :

- Vous devez disposer des autorisations appropriées sur l'objet ordinateur qui vous permettent d'ajouter un ordinateur physique du même nom au domaine
- Vous devez être membre du groupe Administrateurs local sur l'ordinateur. Cela vous permet de changer de domaine ou l'appartenance aux groupes de travail de l'ordinateur
- Vous ne devez pas avoir dépassé le nombre maximum de comptes d'ordinateurs que vous pouvez ajouter au domaine. Par défaut, les utilisateurs peuvent ajouter un maximum de dix ordinateurs au domaine ; cette valeur est connue sous le nom de *quota compte machine* et est commandée par la valeur MS-DS-MachineQuota. Vous pouvez modifier cette valeur en utilisant le composant logiciel enfichable de l'éditeur d'interfaces de service Active Directory (ADSI Edit)

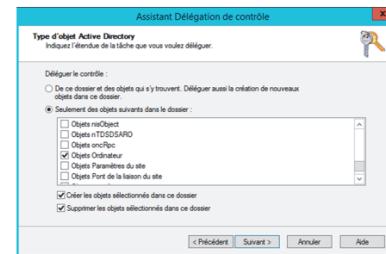
 **Remarque :** il est recommandé de pré-créer le compte d'ordinateur dans l'unité d'organisation appropriée avant d'ajouter l'ordinateur au domaine. Cela permet à l'ordinateur de recevoir immédiatement les stratégies de groupe qui conviennent. Si vous ne pré-creez pas le compte d'ordinateur, il sera créé dans le conteneur Ordinateurs.

Déléguer des autorisations

Par défaut, les groupes Administrateurs de l'entreprise, Administrateurs du domaine, Administrateurs et Opérateurs de compte ont la permission de créer des objets ordinateurs dans toute nouvelle UO. Cependant, comme indiqué plus haut, nous vous recommandons fortement de limiter les adhésions dans les trois premiers groupes et de ne pas ajouter des utilisateurs qui sont membres des groupes Administrateurs de l'entreprise, Administrateurs de domaine, ou Administrateurs au groupe Opérateurs de compte. Au lieu de cela, nous vous conseillons de déléguer l'autorisation de créer des objets ordinateurs aux administrateurs appropriés ou au personnel de soutien technique. Cette autorisation, qui est affectée au groupe auquel vous délégez l'administration, permet aux membres du groupe de créer des objets d'ordinateur dans une unité d'organisation spécifiée. Par exemple, vous pourriez permettre à votre équipe de support technique de créer des objets ordinateurs dans les UO clientes et autoriser vos administrateurs de serveur de fichiers à créer des objets ordinateurs dans l'UO serveur de fichiers.

Pour déléguer les autorisations pour créer des comptes d'ordinateur, vous pouvez utiliser l'**Assistant Délégation de contrôle** et choisir une tâche personnalisée à déléguer. Lorsque vous délégez des autorisations pour gérer les comptes d'ordinateur, vous pourriez envisager d'accorder des autorisations supplémentaires au-delà de celles qui sont nécessaires pour créer des comptes d'ordinateur. Par exemple, vous pourriez décider d'autoriser un administrateur délégué à gérer les propriétés des comptes d'ordinateurs existants, à supprimer le compte d'ordinateur, ou à le déplacer.

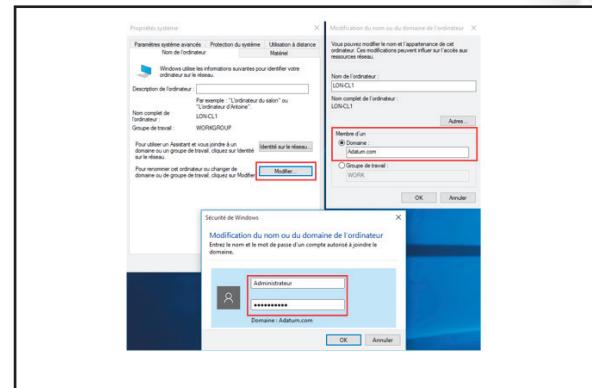
Dans la fenêtre Assistant Délégation de contrôle, l'administrateur crée une délégation personnalisée pour les objets ordinateur



Ajouter un ordinateur à un domaine

Le réel ajout de l'ordinateur au domaine se produit sur l'ordinateur client. Dans les systèmes d'exploitation Windows, cela a lieu dans l'onglet **Nom de l'ordinateur** des Paramètres système avancés dans l'applet Système du Panneau de configuration.

Tout utilisateur peut accéder à l'onglet Nom de l'ordinateur ; cependant, pour rejoindre le domaine, vous devez connaître le nom du domaine et fournir les informations d'identification d'un utilisateur de domaine qui possède les autorisations requises pour ajouter un ordinateur au domaine.



Quitter un domaine est un processus similaire. Entrez le nom du groupe de travail ou du domaine que vous souhaitez rejoindre, et fournissez les informations d'identification appropriées.



Remarque : si vous supprimez un ordinateur du domaine d'un groupe de travail, assurez-vous que vous connaissez les informations d'identification d'un compte local qui a des droits d'administrateur sur l'ordinateur local.

L'ordinateur nécessite un redémarrage après avoir rejoint ou quitté un domaine.

Les comptes d'ordinateurs et des canaux sécurisés

Chaque ordinateur membre dans un domaine AD DS maintient un compte d'ordinateur avec un nom d'utilisateur (SAMAccountName) et un mot de passe, tout comme un compte d'utilisateur.

L'ordinateur stocke son mot de passe sous la forme d'un secret autorité de sécurité local (LSA) et le modifie pour le domaine tous les 30 jours environ. Le service Net Logon utilise les identifiants pour se connecter au domaine, qui établit le canal sécurisé avec un contrôleur de domaine.

Les comptes d'ordinateurs et les relations sécurisées entre les ordinateurs et leur domaine

sont robustes. Néanmoins, il existe certains scénarios dans lesquels un ordinateur ne peut s'authentifier au domaine. Lorsque cela se produit, les utilisateurs sont incapables de se connecter et l'ordinateur ne peut pas accéder aux ressources, telles que la stratégie de groupe. Quelques exemples de cas où cela peut se produire :

- Après la réinstallation du système d'exploitation sur un poste de travail, le poste de travail ne peut pas s'authentifier alors que le technicien a utilisé le même nom d'ordinateur utilisé dans l'installation précédente. Parce que la nouvelle installation a généré un nouveau SID et parce que le nouvel ordinateur ne connaît le mot de passe original du compte d'ordinateur dans le domaine, il ne fait pas partie du domaine et ne peut pas authentifier au domaine

- Les ordinateurs ont des comptes :
 - SAMAccountName et mot de passe
 - Utilisés pour créer un canal sécurisé entre l'ordinateur et un contrôleur de domaine
- Les scénarios dans lesquels un canal sécurisé peut être rompu :
 - La réinstallation d'un ordinateur, même avec le même nom, génère un nouveau SID et mot de passe
 - La restauration d'un ordinateur à partir d'une ancienne sauvegarde ou la restauration d'un ordinateur vers une ancienne capture instantanée
 - Le désaccord entre l'ordinateur et le domaine sur le mot de passe

- Cet ordinateur n'a pas été utilisé pendant une longue période, peut-être parce que l'utilisateur travaille à distance ou parce que l'ordinateur a été pré-construit en tant que pièce de rechange et n'a pas servi pendant une longue période. Au cours de cette période, un administrateur peut avoir réinitialisé ou supprimé le compte d'ordinateur
- Le secret LSA de l'ordinateur n'est plus synchronisé avec le mot de passe que le domaine utilise. Comme si l'ordinateur oubliait son mot de passe. En fait, l'ordinateur n'a pas oublié son mot de passe : il est simplement en désaccord avec le domaine par rapport au mot de passe. Lorsque cela se produit, l'ordinateur ne peut pas s'authentifier et le canal sécurisé ne peut pas être créé

Le sujet suivant décrit les étapes à suivre lorsque l'un de ces scénarios se produit.

Remettre à zéro le canal sécurisé

De temps en temps, la relation de sécurité entre un compte d'ordinateur et son domaine est rompue. Cela se traduit par de nombreux symptômes et des erreurs potentielles. Les signes les plus courants de problèmes sur un compte d'ordinateur sont les suivants :

- Des messages à l'ouverture de session indiquent qu'un contrôleur de domaine ne peut pas être contacté, que le compte d'ordinateur est peut être manquant, que le mot de passe sur le compte d'ordinateur est incorrect ou que la relation de confiance (également appelée la relation sécurisée) entre l'ordinateur et le domaine a été corrompue
- Les messages d'erreur ou les événements dans le journal des événements indiquent des problèmes similaires ou suggèrent que les mots de passe, les approbations, les canaux sécurisés ou les relations avec le domaine ou un contrôleur de domaine ont échoué. Une telle erreur se nomme l'événement 3210 NETLOGON : Échec de l'authentification qui apparaît dans le journal des événements de l'ordinateur
- Le compte d'ordinateur est absent dans AD DS

- Ne pas supprimer un ordinateur du domaine avant de le rejoindre ; cela crée un nouveau compte, ce qui entraîne un nouveau SID et la perte des appartances aux groupes
- Options pour réinitialiser le canal sécurisé :
 - **nltest**
 - **netdom**
 - Utilisateurs et ordinateurs Active Directory
 - Centre d'administration Active Directory
 - Windows PowerShell
 - **dsmod**

Lorsque le canal sécurisé échoue, vous devez le réinitialiser. De nombreux administrateurs font cela en supprimant l'ordinateur du domaine, en le mettant dans un groupe de travail, puis en ré-ajoutant l'ordinateur au domaine. Lorsque vous supprimez l'ordinateur du domaine, le compte d'ordinateur dans AD DS est désactivé. Lorsque vous ré-ajoutez l'ordinateur au domaine, le même compte d'ordinateur est réutilisé et activé, mais les adhésions du groupe sont perdues. Ne renommez pas l'ordinateur lorsque vous le ré-ajoutez au domaine.

Vous pouvez également réinitialiser le canal sécurisé entre un membre de domaine et le domaine en utilisant :

- Utilisateurs et ordinateurs Active Directory
- Centre d'administration Active Directory
- L'outil en ligne de commande dsmod
- L'outil en ligne de commande dsmod
- L'outil en ligne de commande dsmod

Si vous réinitialisez le compte, le SID de l'ordinateur reste le même, et l'ordinateur maintient ses appartenances aux groupes.

Pour réinitialiser le canal sécurisé en utilisant Utilisateurs et ordinateurs Active Directory ou <Centre Administratif Active Directory>, suivez cette procédure :

1. Cliquez avec le bouton droit sur l'ordinateur, puis cliquez sur **Réinitialiser le compte**.
2. Cliquez **Oui** pour confirmer votre choix.
3. Ré-ajoutez l'ordinateur au domaine, puis redémarrez l'ordinateur.

Pour réinitialiser le canal sécurisé en utilisant **dsmod**, suivez cette procédure :

1. À l'invite de commandes, tapez la commande suivante :

```
dsmod computer "ComputerDN" -reset
```

2. Ré-ajoutez l'ordinateur au domaine, puis redémarrez l'ordinateur.

Pour réinitialiser le canal sécurisé en utilisant **netdom**, Tapez la commande suivante à l'invite de commande. Les identifiants appartiennent au groupe Administrateurs local de l'ordinateur :

```
netdom reset MachineName /domain DomainName /User0 UserName /Password0 {Password | *}
```

Cette commande réinitialise le canal sécurisé en essayant de réinitialiser le mot de passe sur l'ordinateur et le domaine, de sorte qu'il n'y a pas besoin de le ré-ajouter ou de redémarrer.

Pour réinitialiser le canal sécurisé en utilisant **nlttest**, sur l'ordinateur qui a perdu son approbation, entrez la commande suivante à l'invite de commande :

```
nlttest /server:servername /sc_reset:domain\domaincontroller
```

Vous pouvez également utiliser le module Active Directory pour Windows PowerShell pour réinitialiser un compte d'ordinateur. Pour réinitialiser le canal sécurisé entre l'ordinateur local et le domaine auquel il est relié, exécutez cette commande sur l'ordinateur local :

```
Test-ComputerSecureChannel -Repair
```

Vous pouvez également utiliser cette commande :

```
invoke-command -computername Workstation1 -scriptblock {reset-computermachinepassword}
```

Exécuter une jonction de domaine hors ligne

En règle générale, lorsque vous souhaitez relier un ordinateur à un domaine, l'ordinateur doit être capable de communiquer avec un contrôleur de domaine en ligne. En commençant par le système d'exploitation Windows Server 2008 R2, Microsoft a introduit la *jonction de domaine hors ligne*, une fonctionnalité qui permet d'ajouter un ordinateur à un domaine sans communiquer directement avec un contrôleur de domaine en ligne. Les jonctions de domaine hors ligne fonctionnent avec les ordinateurs clients qui utilisent Windows 7 ou une version plus récente, et Windows Server 2008 R2 ou une version plus récente. Cette fonction est utile dans les situations où la connectivité est intermittente, par exemple lorsque vous déployez un serveur vers un site distant connecté par liaison satellite.

Utiliser le domaine hors ligne pour joindre des ordinateurs à un domaine lorsqu'ils ne peuvent pas contacter un contrôleur de domaine

- Créer un fichier de jonction de domaine en utilisant :

```
djoin.exe /Provision /Domain <DomainName>
/Machine <MachineName> /SaveFile <filepath>
```

- Importer le fichier de jonction de domaine en utilisant :

```
djoin.exe /requestODJ /LoadFile <filepath>
/WindowsPath <path to the Windows directory of
the offline image>
```

Utilisez l'outil de ligne de commande **djoin** pour effectuer une jonction de domaine hors ligne. Cela génère un fichier de jonction de domaine qui est importé à l'ordinateur client. Lorsque vous effectuez une jonction de domaine hors ligne, vous devez spécifier les informations suivantes :

- Le nom de domaine auquel vous souhaitez ajouter l'ordinateur
- Le nom de l'ordinateur que vous voulez joindre au domaine
- Le nom du savefile que vous transférez à la cible de la jonction de domaine hors ligne

Pour effectuer une jonction de domaine hors ligne, suivez cette procédure :

1. Pour ajouter un compte d'ordinateur à un domaine et créer le fichier de jonction de domaine, ouvrez une invite de commande aux autorisations élevées et utilisez la commande **djoin** avec l'option **/provision**. Le format de cette commande est :

```
djoin.exe /Provision /Domain <DomainName> /Machine <MachineName> /SaveFile <filepath>
```

Par exemple, pour relier l'ordinateur Canberra au domaine adatum.com en utilisant le Canberra-join.txt savefile, tapez la commande suivante :

```
djoin.exe /provision /domain adatum.com /machine canberra /savefile
c:\canberra-join.txt
```

Si le compte d'ordinateur n'est pas préconfiguré, il sera créé dans le conteneur Ordinateurs. Si l'ordinateur est préconfiguré, vous devez inclure l'option **/reuse** dans la commande **djoin**.

2. Pour transférer le savefile à l'ordinateur prévu, utilisez la commande **djoin** avec l'option **/requestODJ**. Le format de cette commande est :

```
djoin.exe /requestODJ /LoadFile <filepath> /WindowsPath <path to the Windows
directory of the offline image>
```

Facultatif : vous pouvez effectuer l'importation sur un système d'exploitation en ligne en utilisant l'option **/LocalOS**. Si vous utilisez l'option **/LocalOS**, réglez l'option **/Windowspath** en **%systemroot%** ou en **%windir%**. Par exemple, pour transférer le savefile Canberra-join.txt à l'ordinateur Canberra, entrez la commande suivante sur Canberra :

```
djoin.exe /requestODJ /loadfile canberra-join.txt /windowspath %systemroot% /localos
```

3. Démarrez ou redémarrez l'ordinateur pour terminer l'opération de jonction de domaine.

Question : Pour quelles raisons un ordinateur perd-il sa relation de confiance avec le domaine ?

Atelier pratique A : Gestion des objets AD DS

Scénario

Vous avez travaillé pour A. Datum Corporation en tant que spécialiste de support technique et êtes allé sur les ordinateurs de bureau pour résoudre les problèmes liés aux applications et au réseau. Vous avez récemment accordé une promotion à l'équipe du support de serveur. Une de vos premières missions est de configurer le service de l'infrastructure pour une nouvelle filiale.

Pour commencer le déploiement de la nouvelle filiale, vous préparez des objets AD DS. Dans le cadre de cette préparation, vous devez créer des utilisateurs et des groupes pour la nouvelle filiale qui abritera le département de recherche. Enfin, vous devez réinitialiser le canal sécurisé pour un compte d'ordinateur qui a perdu sa connectivité au domaine dans la succursale.

Objectifs

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

- Création et configuration des groupes dans AD DS
- Création et configuration de comptes d'utilisateurs dans AD DS
- Gérez les objets d'ordinateur dans AD DS

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels : **22742A-LON-DC1**, **22742A-LON-DC2** et **22742A-LON-CL1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-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'authentification suivantes :
 - Nom d'utilisateur : **Administrateur**
 - Mot de passe : **Pa55w.rd**
 - Domaine : **Adatum**
5. Répétez les étapes 1 à 4 pour **22742A-LON-DC2**.
6. Répétez les étapes 1 à 3 pour **22742A-LON-CL1**. Ne vous connectez pas à **LON-CL1** avant d'y être invité au cours des étapes de l'atelier.

Exercice 1 : Création et gestion des groupes dans AD DS

Scénario

Vous devez créer des groupes pour le département Research. Un groupe mondial de distribution est nécessaire pour faciliter l'envoi d'e-mails aux utilisateurs de Research. Ce groupe sera géré par Cai Chu. Vous allez également créer un groupe de directeurs de recherche et ajouter Cai Chu et Vera Pace en tant que membres du groupe. Vous devez également créer un groupe universel dans le groupe Managers UO qui contiendra tous les groupes mondiaux de directeurs de service. Après avoir créé le groupe de

distribution Research, on vous dit que le groupe a besoin d'accéder aux ressources du réseau ; vous devez donc convertir le groupe en un groupe de sécurité.

Les tâches principales de cet exercice sont les suivantes :

1. Créer des groupes et ajouter des membres ;
2. Configurer l'imbrication de groupes ;
3. Convertir un type de groupe de la distribution à la sécurité.

► **Tâche 1 : Créer des groupes et ajouter des membres**

1. Sur **LON-DC1** utilisez **Centre d'administration Active Directory** pour créer les groupes suivants :
 - Dans **Managers** UO, créez un groupe universel nommé **Managers de l'entreprise** ;
 - Dans **Research UO**, créez un groupe de distribution globale nommé **Research Mail**.
2. Configurez l'adresse e-mail du groupe **Research Mail** pour qu'elle soit **Research@adatum.com**.
3. Configurez le groupe **Research Mail** qui sera géré par **Louis Delor**.
4. Fournissez à **Louis Delor** le droit de mettre à jour la liste des membres du groupe.
5. Dans **Research UO**, créez un nouveau groupe de sécurité global nommé **Research Managers**.
6. Ajoutez **Louis Delor** et **Valérie Dupont** en tant que membres.

► **Tâche 2 : Configurer l'imbrication du groupe**

- Accédez à **Managers** UO, ajoutez le groupe global **Managers** et le groupe global **Research Managers** en tant que membres du groupe universel **Managers de l'entreprise**

► **Tâche 3 : Convertir un type de groupe de la distribution à la sécurité**

- Dans l'UO **Recherche**, changez le type de groupe **Research Mail** en un groupe de **Sécurité**

Résultats : À la fin de cet exercice, vous aurez réussi à :

- Créer des groupes et ajouter des membres
- Imbrication du groupe configurée
- Conversion d'un type de groupe effectuée

Exercice 2 : Crédation et configuration de comptes d'utilisateurs dans AD DS

Scénario

Vous avez reçu une liste de nouveaux utilisateurs à créer pour la filiale. Vous avez décidé de créer un modèle pour faciliter la création rapide des utilisateurs de la filiale. Vous validerez ce modèle en créant un nouvel utilisateur test et en vérifiant ses propriétés.

Les tâches principales de cet exercice sont les suivantes :

1. Créer et configurer un modèle utilisateur pour le département de recherche.
2. Créer de nouveaux utilisateurs pour la filiale de recherche en vous basant sur le modèle.
3. Valider le modèle.

► **Tâche 1 : Crédater et configurer un modèle utilisateur pour le département de recherche**

1. Créez un nouvel utilisateur dans Research UO avec les propriétés suivantes :

- Nom : **_Modèle Research**
 - Ouverture de la session UPN de l'utilisateur : **Modèle Research**
 - Mot de passe : **Pa55w.rd**
 - Département : **Recherche**
 - Société : **Adatum**
 - Gestionnaire : **Louis Delor**
 - Membre de : **Research**
 - Script d'ouverture de session : **\LON-DC1\Netlogon\Logon.bat**
 - Désactivez le compte
2. Fermez le Centre d'administration Active Directory.
- **Tâche 2 : Créer de nouveaux utilisateurs pour la succursale de recherche basés sur le modèle**
1. Utilisez **Utilisateurs et ordinateurs Active Directory** pour copier le compte **_Modèle Research** compte.
 2. Créez le nouvel utilisateur à partir du modèle avec les propriétés suivantes :
 - Prénom : **Research**
 - Nom : **Utilisateur**
 - Mot de passe : **Pa55w.rd**
 - Statut du compte : **Activé**
- **Tâche 3 : Valider le modèle**
- Inspectez les propriétés de l'utilisateur Recherche et veillez à ce que les propriétés soient les suivantes :
 - Script d'ouverture de session : **\LON-DC1\Netlogon\Logon.bat**
 - Département : **Recherche**
 - Société : **Adatum**
 - Membre de : **Research**

Résultats : À la fin de cet exercice, vous aurez réussi à :

- Créer et configurer un modèle utilisateur pour les utilisateurs Research
- Créer trois nouveaux utilisateurs sur base du modèle
- Effectuer l'authentification pour vérifier que les comptes fonctionnent comme prévu

Exercice 3 : Gestion des objets ordinateur dans AD DS

Scénario

Un utilisateur est incapable de signer sur un poste de travail, a perdu sa connectivité au domaine et ne peut pas authentifier les utilisateurs correctement. Lorsque les utilisateurs tentent d'accéder aux ressources de ce poste de travail, leur accès est refusé. Vous devez réparer la relation de confiance entre l'ordinateur et le domaine.

Les tâches principales de cet exercice sont les suivantes :

1. Réinitialiser un compte d'ordinateur.
2. Observer le comportement lorsqu'un client tente de se s'authentifier.
3. Résoudre le problème de l'ordinateur.

► **Tâche 1 : Réinitialiser un compte d'ordinateur**

- Cliquez avec le bouton droit sur **LON-CL1** dans le conteneur ordinateurs et réinitialisez le compte
- **Tâche 2 : Observer le comportement lorsqu'un client tente de se s'authentifier**
- Redémarrez **LON-CL1** et connectez-vous en tant qu'**Adatum\Adam** avec le mot de passe **Pa55w.rd**

Question : Quel message s'affiche ?

Réponse : La relation d'approbation entre ce poste de travail et le domaine principal a échoué.

► **Tâche 3 : Résoudre le problème de l'ordinateur**

1. Connectez-vous à **LON-CL1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Démarrer une session de Windows PowerShell avec élévation de priviléges et exécutez la commande suivante :

```
Test-ComputerSecureChannel -Repair
```

3. Déconnectez-vous de **LON-CL1**, puis tentez de vous reconnecter en tant qu'**Adatum\Adam**. La connexion va s'effectuer maintenant.
4. Déconnectez-vous de **LON-CL1**.
5. Laissez les ordinateurs virtuels en cours d'exécution pour la démonstration suivante.

Résultats : À la fin de cet exercice, vous aurez réussi à :

- Réinitialiser un compte d'ordinateur
- Observer le comportement lorsqu'un client s'authentifie
- Résoudre le problème de l'ordinateur

Question : Quels types d'objets peuvent être membres des groupes globaux ?

Question : Quelles références sont nécessaires pour joindre un ordinateur à un domaine ?

Leçon 4

Utilisation de Windows PowerShell pour l'administration d'AD DS

Vous pouvez utiliser Windows PowerShell pour automatiser l'administration AD DS. Automatiser l'administration accélère les processus que vous pourriez autrement effectuer manuellement. Windows PowerShell comprend applets de commande pour effectuer l'administration AD DS et pour effectuer des opérations en bloc. Vous pouvez utiliser des opérations en bloc pour modifier de nombreux objets AD DS en une seule étape plutôt que de mettre à jour chaque objet manuellement.

Objectifs de la leçon

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

- Utiliser Windows powershell pour gérer des comptes d'utilisateurs
- Utiliser Windows powershell pour gérer les groupes
- Utiliser Windows powershell pour gérer les comptes d'ordinateur
- Utiliser Windows powershell pour gérer des UO
- Décrire les opérations en bloc
- Utiliser des outils graphiques pour effectuer des opérations en bloc
- Utiliser Windows powershell pour une requête d'objets
- Utiliser Windows Server powershell pour modifier des objets
- Travailler avec des fichiers de valeurs séparées par des virgules (CSV)
- Utiliser Windows powershell pour effectuer des opérations en bloc

Utilisation de cmdlets Windows PowerShell pour gérer des comptes d'utilisateurs

Vous pouvez utiliser les applets de commande Windows PowerShell pour créer, modifier et supprimer des comptes d'utilisateurs. Vous pouvez utiliser ces applets pour les opérations individuelles ou dans le cadre d'un script pour effectuer des opérations groupées. Le tableau ci-dessous présente quelques-uns des applets couramment utilisés pour la gestion des comptes d'utilisateurs.

| Applet de commande | Description |
|--|--|
| New-ADUser | Crée des comptes d'utilisateurs |
| Set-ADUser | Modifie les propriétés des comptes d'utilisateurs |
| Remove-ADUser | Supprime les comptes d'utilisateurs |
| Set-ADAccountPassword | Réinitialise le mot de passe d'un compte d'utilisateur |
| Set-ADAccountExpiration | Modifie la date d'expiration d'un compte d'utilisateur |
| Unlock-ADAccount | Débloque un compte d'utilisateur après que ce dernier ait été verrouillé suite à un trop grand nombre de tentatives de connexion incorrectes |
| Enable-ADAccount | Active un compte d'utilisateur |
| Disable-ADAccount | Désactive un compte d'utilisateur |
| New-ADUser "Sten Faerch" -AccountPassword (Read-Host -AsSecureString "Enter password") -Department IT | |

| Applet de commande | Description |
|----------------------|--|
| New-ADUser | Crée des comptes d'utilisateurs. |
| Set-ADUser | Modifie les propriétés des comptes d'utilisateurs. |
| Remove-ADUser | Supprime les comptes d'utilisateurs. |

| Applet de commande | Description |
|--------------------------------|---|
| Set-ADAccountPassword | Réinitialise le mot de passe d'un compte d'utilisateur. |
| Set-ADAccountExpiration | Modifie la date d'expiration d'un compte d'utilisateur. |
| Unlock-ADAccount | Débloque un compte d'utilisateur lorsqu'il est verrouillé après avoir dépassé le nombre accepté de tentatives de connexion incorrectes. |
| Enable-ADAccount | Active un compte d'utilisateur. |
| Disable-ADAccount | Désactive un compte d'utilisateur. |

Créer de nouveaux comptes d'utilisateurs

Lorsque vous utilisez l'applet de commande **New-ADUser** pour créer de nouveaux comptes d'utilisateurs, vous pouvez définir la plupart des propriétés de l'utilisateur, y compris un mot de passe. Par exemple :

- Si vous n'utilisez le paramètre **-AccountPassword**, aucun mot de passe n'est défini et le compte d'utilisateur est désactivé. Le paramètre **-Enabled** ne peut pas être défini comme **\$true** quand aucun mot de passe n'est défini.
- Si vous utilisez le paramètre **-AccountPassword (Mot de passe du compte)** pour spécifier un mot de passe, vous devez spécifier une variable qui contient le mot de passe en tant que chaîne sécurisée ou choisir de recevoir une invite pour le mot de passe. Une chaîne sécurisée est chiffrée dans la mémoire. Si vous définissez un mot de passe, vous pouvez activer le compte d'utilisateur en réglant le paramètre **-Enabled (Activé)** sur **\$true**.

Le tableau suivant répertorie les paramètres couramment utilisés pour l'applet de commande **New-ADUser**.

| Paramètre | Description |
|--|--|
| AccountExpirationDate (Date d'expiration du compte) | Définit la date d'expiration pour le compte d'utilisateur. |
| AccountPassword (Mot de passe du compte) | Définit le mot de passe d'un compte d'utilisateur. |
| ChangePasswordAtLogon (Modifier le mot de passe lors de la connexion) | Requiert que le compte d'utilisateur modifie les mots de passe à la prochaine connexion. |
| Department (Département) | Définit le département pour le compte d'utilisateur. |
| HomeDirectory (Répertoire de base) | Définit l'emplacement du répertoire de base pour un compte d'utilisateur. |
| HomeDrive (Lecteur de base) | Définit les lettres de lecteur qui sont mappées dans le répertoire de base pour un compte d'utilisateur. |
| GivenName (Prénom) | Définit le prénom d'un utilisateur. |
| Surname (Nom) | Définit le nom d'un utilisateur. |
| Path (Chemin d'accès) | Définit l'UO ou le conteneur où le compte d'utilisateur est créé. |

La commande suivante est un exemple d'une commande que vous pouvez utiliser pour créer un compte d'utilisateur avec une invite pour un mot de passe :

```
New-ADUser "Sten Faerch" -AccountPassword (Read-Host -AsSecureString "Enter password")
-Department IT
```

Utilisation d'applets de commande Windows PowerShell pour gérer les groupes

Vous pouvez utiliser Windows PowerShell pour créer, modifier et supprimer des groupes comme vous le faites pour les utilisateurs. Vous pouvez utiliser ces applets pour les opérations individuelles ou dans le cadre d'un script pour effectuer des opérations groupées. Certains des applets de commande utilisés pour la gestion des groupes sont répertoriés dans le tableau suivant.

| Applet de commande | Description |
|-----------------------------------|--|
| New-ADGroup | Crée de nouveaux groupes |
| Set-ADGroup | Modifie les propriétés des groupes |
| Get-ADGroup | Affiche les propriétés des groupes |
| Remove-ADGroup | Supprime des groupes |
| Add-ADGroupMember | Ajoute des membres aux groupes |
| Get-ADGroupMember | Affiche l'appartenance des groupes |
| Remove-ADGroupMember | Supprime les membres des groupes |
| Add-ADPrincipalGroupMembership | Ajoute l'appartenance au groupe à des objets |
| Get-ADPrincipalGroupMembership | Affiche l'appartenance au groupe des objets |
| Remove-ADPrincipalGroupMembership | Supprime l'appartenance au groupe d'un objet |

```
New-ADGroup -Name "CustomerManagement" -Path
"ou=managers,dc=adatum,dc=com" -GroupScope Global
-GroupCategory Security
```

```
Add-ADGroupMember -Name "CustomerManagement"
-Members "Joe"
```

| Applet de commande | Description |
|--|---|
| New-ADGroup | Crée de nouveaux groupes. |
| Set-ADGroup | Modifie les propriétés des groupes. |
| Get-ADGroup | Affiche les propriétés des groupes. |
| Remove-ADGroup | Supprime des groupes. |
| Add-ADGroupMember | Ajoute des membres aux groupes. |
| Get-ADGroupMember | Affiche les membres des groupes. |
| Remove-ADGroupMember | Supprime les membres d'un groupe. |
| Add-ADPrincipalGroupMembership | Ajoute l'appartenance au groupe à des objets. |
| Get-ADPrincipalGroupMembership | Affiche l'appartenance au groupe des objets. |
| Remove-ADPrincipalGroupMembership | Supprime l'appartenance au groupe d'un objet. |

Création de groupes

Vous pouvez utiliser l'applet de commande **New-ADGroup** pour créer des groupes. Toutefois, lorsque vous créez des groupes en utilisant l'applet de commande **New-ADGroup**, vous devez utiliser le paramètre **GroupScope (Étendue du groupe)** en plus du nom de groupe. C'est le seul paramètre requis. Le tableau suivant répertorie les paramètres couramment utilisés pour **New-ADGroup**.

| Paramètre | Description |
|-------------------|---------------------------|
| Name (Nom) | Définit le nom du groupe. |

| Paramètre | Description |
|--|--|
| GroupScope (Étendue du groupe) | Définit l'étendue du groupe en tant que DomainLocal (Domaine local) , Global (Global) , ou Universal (Universel) . Vous devez fournir ce paramètre. |
| DisplayName (Nom d'affichage) | Définit le nom d'affichage du protocole LDAP (LDAP) pour l'objet. |
| GroupCategory (Catégorie de groupe) | Définit si c'est un groupe de sécurité ou un groupe de distribution. Si vous ne spécifiez pas lequel des deux, un groupe de sécurité est créé. |
| ManagedBy (Géré par) | Définit un utilisateur ou un groupe qui peut gérer le groupe. |
| Path (Chemin d'accès) | Définit l'UO ou le conteneur dans lequel le groupe est créé. |
| SamAccountName (Nom de compte SAM) | Définit un nom qui assure la compatibilité descendante avec les systèmes d'exploitation plus anciens. |

La commande suivante est un exemple de ce que vous pouvez saisir à l'invite Windows PowerShell pour créer un nouveau groupe :

```
New-ADGroup -Name "CustomerManagement" -Path "ou=managers,dc=adatum,dc=com" -GroupScope Global -GroupCategory Security
```

Gestion de l'appartenance au groupe

Il y a deux ensembles d'applets de commande que vous pouvez utiliser pour gérer l'appartenance au groupe : * **-ADGroupMember** et * **-ADPrincipalGroupMembership**. La distinction entre ces deux ensembles d'applets de commande est la perspective utilisée lors de la modification de l'appartenance au groupe :

- Les applets de commande * **-ADGroupMember** modifient l'appartenance à un groupe. Par exemple, vous ajoutez ou supprimez les membres d'un groupe
 - Vous ne pouvez pas utiliser les canaux pour transmettre une liste de membres à ces applets de commande
 - Vous pouvez transmettre une liste de groupes à ces applets de commande
- Les applets de commande * **-ADPrincipalGroupMembership** modifient l'appartenance au groupe d'un objet comme un utilisateur. Par exemple, vous pouvez modifier un compte d'utilisateur pour l'ajouter en tant que membre d'un groupe
 - Vous pouvez utiliser les canaux pour transmettre une liste de membres à ces applets de commande
 - Vous ne pouvez pas fournir une liste de groupes à ces applets de commande



Remarque : l'utilisation de canaux est un processus fréquent dans les langages de script qui vous permet d'utiliser la sortie d'un applet de commande en entrée pour le prochain applet de commande dans la commande. Par exemple, cette commande crée un compte d'utilisateur, puis active le compte :

```
New-ADUser -Name "Sten Faerch" -AccountPassword (Read-Host -AsSecureString "Enter password") | Enable-Account
```

Utilisation de cmdlets Windows PowerShell pour gérer les comptes d'ordinateur

Vous pouvez utiliser Windows PowerShell pour créer, modifier et supprimer des comptes d'ordinateurs. Vous pouvez utiliser ces applets pour les opérations individuelles ou dans le cadre d'un script pour effectuer des opérations groupées. Le tableau suivant répertorie les applets de commande que vous pouvez utiliser pour gérer des comptes d'ordinateurs.

| Applet de commande | Description |
|-------------------------------|---|
| New-ADComputer | Crée de nouveaux comptes d'ordinateurs |
| Set-ADComputer | Modifie les propriétés des comptes d'ordinateurs |
| Get-ADComputer | Modifie les propriétés des comptes d'ordinateurs |
| Remove-ADComputer | Supprime les comptes client |
| Test-ComputerSecureChannel | Vérifie ou répare la relation d'approbation entre un ordinateur et le domaine |
| Reset-ComputerMachinePassword | Réinitialise le mot de passe d'un compte d'ordinateur |

```
New-ADComputer -Name "LON-SVR8" -Path "ou=marketing,dc=adatum,dc=com" -Enabled $true
Test-ComputerSecureChannel -Repair
```

| Applet de commande | Description |
|-------------------------------|--|
| New-ADComputer | Crée un nouveau compte d'ordinateur. |
| Set-ADComputer | Modifie les propriétés d'un compte d'ordinateur. |
| Get-ADComputer | Modifie les propriétés d'un compte d'ordinateur |
| Remove-ADComputer | Supprime un compte d'ordinateur. |
| Test-ComputerSecureChannel | Vérifie ou répare la relation d'approbation entre un ordinateur et le domaine. |
| Reset-ComputerMachinePassword | Réinitialise le mot de passe d'un compte d'ordinateur. |

Création de nouveaux comptes d'ordinateurs

Vous pouvez utiliser l'applet de commande **New-ADComputer** pour créer un nouveau compte d'ordinateur avant de joindre l'ordinateur au domaine. Vous effectuez cette action afin de pouvoir créer le compte d'ordinateur dans la bonne UO avant de déployer l'ordinateur.

Le tableau suivant répertorie les paramètres couramment utilisés pour **New-ADComputer**.

| Paramètre | Description |
|------------------------------|---|
| Name (Nom) | Définit le nom du compte d'ordinateur. |
| Path (Chemin d'accès) | Définit l'unité d'organisation ou le conteneur où le compte d'ordinateur est créé. |
| Enabled (Activé) | Définit si le compte d'ordinateur est activé ou désactivé. Par défaut, le compte d'ordinateur est activé et un mot de passe aléatoire est généré. |

La commande suivante est un exemple d'une commande que vous pouvez utiliser pour créer un compte d'ordinateur :

```
New-ADComputer -Name LON-SVR8 -Path "ou=marketing,dc=adatum,dc=com" -Enabled $true
```

Réparation de la relation d'approbation pour un compte d'ordinateur

Vous pouvez utiliser l'applet de commande **Test-ComputerSecureChannel** avec le paramètre **-Repair** (**Réparer**) pour réparer une relation d'approbation perdue entre un ordinateur et le domaine. Vous devez exécuter l'applet de commande sur l'ordinateur avec la relation d'approbation perdue.

Utilisation de cmdlets Windows PowerShell pour gérer des UO

Vous pouvez utiliser les applets de commande Windows PowerShell pour créer, modifier et supprimer des UO. Vous pouvez utiliser ces applets pour les opérations individuelles ou dans le cadre d'un script pour effectuer des opérations groupées. Le tableau suivant décrit les applets de commande dont vous pouvez vous servir pour gérer les UO.

| Applet de commande | Description |
|------------------------------------|--|
| New-ADOrganizationalUnit | Crée des unités d'organisation |
| Set-ADOrganizationalUnit | Modifie les propriétés des unités d'organisation |
| Get-ADOrganizationalUnit | Affiche les propriétés des unités d'organisation |
| Remove-ADOrganizationalUnit | Supprime les unités d'organisation |

```
New-ADOrganizationalUnit -Name "Sales"
-Path "ou=marketing,dc=adatum,dc=com"
-ProtectedFromAccidentalDeletion $true
```

| Applet de commande | Description |
|------------------------------------|--------------------------------|
| New-ADOrganizationalUnit | Crée des UO. |
| Set-ADOrganizationalUnit | Modifie les propriétés des UO. |
| Get-ADOrganizationalUnit | Affiche les propriétés des UO. |
| Remove-ADOrganizationalUnit | Supprime des UO. |

Création de nouvelles UO

Vous pouvez utiliser l'applet de commande **New-ADOrganizationalUnit** pour créer une nouvelle UO pour représenter les départements ou les emplacements physiques au sein de votre organisation.

Le tableau suivant présente les paramètres couramment utilisés pour l'applet de commande **New-ADOrganizationalUnit**.

| Applet de commande | Description |
|--|---|
| Name | Définit le nom de la nouvelle UO. |
| Path | Définit l'emplacement de la nouvelle UO. |
| ProtectedFromAccidentalDeletion | Empêche la suppression accidentelle de l'UO. La valeur par défaut est \$true . |

La commande suivante est un exemple d'une commande que vous pouvez utiliser lorsque vous souhaitez créer une nouvelle UO :

```
New-ADOrganizationalUnit -Name Sales -Path "ou=marketing,dc=adatum,dc=com"
-ProtectedFromAccidentalDeletion $true
```

Quelles sont les opérations en bloc ?

Une *opération en bloc* est une seule action qui modifie plusieurs objets. Effectuer une opération en bloc est beaucoup plus rapide que de changer beaucoup d'objets individuellement. Ça pourrait également être plus précis, parce que la réalisation de nombreuses actions individuelles augmente la probabilité de faire une erreur typographique. Cependant, en raison de la nature des opérations en bloc, si vous introduisez une erreur, elle sera multipliée à chaque objet en cours de modification. Par conséquent, assurez-vous de tester votre opération en bloc sur un ensemble d'objets plus petit avant de l'exécuter sur tous les éléments que vous souhaitez modifier.

- Une opération en bloc est une action unique qui modifie plusieurs objets
- Exemple d'opérations en bloc :
 - Créer des comptes d'utilisateurs sur la base de données d'une feuille de calcul
 - Désactiver tous les comptes non utilisés depuis six mois
 - Renommer le service pour de nombreux utilisateurs
- Vous pouvez effectuer des opérations en bloc en utilisant :
 - Outils graphiques
 - Outils en ligne de commande
 - Scripts

Les opérations en bloc fréquentes dans un environnement Windows Server comprennent :

- Créer de nouveaux comptes d'utilisateurs basés sur les informations d'une feuille de calcul
- Désactiver tous les comptes d'utilisateurs qui n'ont pas été utilisés au cours des six derniers mois
- Changer le nom du département pour tous les utilisateurs appartenant à un département donné

Vous pouvez effectuer des opérations en bloc avec des outils graphiques, à l'invite de commandes ou en utilisant des scripts. Chaque méthode permettant d'effectuer des opérations en bloc a des fonctionnalités différentes. Par exemple :

- Les outils graphiques ont tendance à être limités dans les propriétés qu'ils peuvent modifier
- Les outils de ligne de commande ont tendance à être plus flexibles que les outils graphiques lors de la définition des requêtes et ils ont plus d'options pour modifier les propriétés des objets
- Les scripts peuvent combiner plusieurs actions de ligne de commande pour plus de complexité et de flexibilité

Démonstration : L'utilisation d'outils graphiques pour effectuer des opérations en bloc

Dans cette démonstration, vous verrez comment utiliser les Utilisateurs et ordinateurs Active Directory pour modifier l'attribut **Bureau** pour les utilisateurs dans l'UO Recherche en tant qu'opération en bloc.

Procédure de démonstration

1. Ouvrez **Utilisateurs et ordinateurs Active Directory**, puis sélectionnez l'UO **Recherche**.
2. Triez les objets par **Type**, puis sélectionnez tous les objets **USER**.
3. Modifiez les propriétés pour définir l'attribut **Bureau** sur **Winnipeg**.
4. Vérifier l'onglet **Général** dans les propriétés de l'un des utilisateurs pour vous assurer que la mise à jour a eu lieu.
5. Fermez la fenêtre **Utilisateurs et ordinateurs Active Directory**.

Interrogation d'objets avec Windows PowerShell

Dans Windows PowerShell, vous utilisez les applets de commande **Get-*** pour obtenir des listes d'objets, tels que les comptes d'utilisateurs. Vous pouvez également utiliser ces applets de commande pour générer des requêtes pour des objets sur lesquels vous pouvez effectuer des opérations en bloc. Le tableau suivant répertorie les paramètres qui sont communément utilisés avec les applets de commande **Get-AD ***.

| Paramètre | Description |
|-----------------------------|--|
| Base de recherche | Définit le chemin d'accès AD DS pour commencer la recherche |
| SearchScope | Définit à quel niveau en dessous de la base de données une recherche doit être effectuée |
| ResultSetSize | Définit le nombre d'objets à retourner en réponse à une requête |
| Propriétés | Définit les propriétés de l'objet à retourner et afficher |
| Filtre | Définit un filtre en utilisant la syntaxe PowerShell |
| LDAPFilter | Définit un filtre en utilisant la syntaxe de requête LDAP |
| Descriptions des opérateurs | |
| -eq | Égal à |
| -ne | Différent de |
| -lt | Inférieur à |
| -le | Inférieur ou égal à |
| -gt | Supérieur à |
| -ge | Supérieur ou égal à |
| -Comme | Utilise des caractères génériques pour les critères spéciaux |

| Paramètre | Description |
|--|---|
| SearchBase | Définit le chemin d'accès AD DS pour lancer la recherche : par exemple, le domaine ou une unité d'organisation. |
| SearchScope (Étendue de recherche) | Définit à quel niveau en dessous de la SearchBase la recherche doit être effectuée. Vous pouvez choisir de rechercher uniquement dans la base, un niveau en dessous ou dans l'ensemble de la sous-arborescence. |
| ResultPageSize (Taille de la plage de résultat) | Définit le nombre d'objets à retourner en réponse à une requête. Pour veiller à ce que tous les objets soient retournés, réglez ce paramètre sur \$null . |
| Properties (Propriétés) | Définit quelles propriétés de l'objet retourner et afficher. Pour retourner toutes les propriétés, saisissez un astérisque (*). Vous n'êtes pas obligés d'utiliser ce paramètre pour utiliser une propriété pour le filtrage. |

Création d'une requête

Vous pouvez utiliser le paramètre **Filter** ou le paramètre **LDAPFilter** pour créer des requêtes pour les objets avec les applets de commande **Get-AD ***. Utilisez le paramètre **Filter** pour les requêtes que vous écrivez dans Windows PowerShell, et utilisez le paramètre **LDAPFilter** pour les requêtes que vous écrivez en tant que chaînes de requête LDAP.

Windows PowerShell est préférable parce que :

- Il est plus facile d'écrire des requêtes dans Windows powershell
- Vous pouvez utiliser des variables dans les requêtes
- Il y a une conversion automatique des types de variables lorsque cela est nécessaire

Le tableau ci-dessous répertorie les opérateurs couramment utilisés dans Windows PowerShell.

| Opérateur | Description |
|------------|----------------------|
| -eq | Égal à. |
| -ne | Différent de. |
| -lt | Inférieur à. |
| -le | Inférieur ou égal à. |

| Opérateur | Description |
|--------------|---|
| -gt | Supérieur à. |
| -ge | Supérieur ou égal à. |
| -like | Utilise des caractères génériques et des critères spéciaux. |

Filter

Comme mentionné précédemment, vous pouvez utiliser le paramètre **Filter** pour filtrer les données récupérées par un applet de commande **Get-***. Le paramètre **Filter** utilise la même syntaxe que l'applet de commande **Where-Object** dans Windows PowerShell. À titre d'exemple, cette commande récupère tous les comptes d'utilisateurs qui ont Belisle comme nom, suivi par la sortie de la commande :

```
Get-ADUser -Filter {sn -eq "Bourgeoise"}
DistinguishedName : CN=Nathalie Bourgeoise,OU=Marketing,DC=Adatum,DC=com
Enabled           : True
GivenName         : Nathalie
Name              : Nathalie Bourgeoise
ObjectClass       : user
ObjectGUID        : 1ff1b2cb-38c1-4bc7-bda7-511e19744d2a
SamAccountName   : Nathalie
SID               : S-1-5-21-322346712-1256085132-1900709958-1407
Surname           : Bourgeoise
UserPrincipalName: Nathalie@adatum.com
DistinguishedName : CN=Olivier Bourgeoise,OU=IT,DC=Adatum,DC=com
Enabled           : True
GivenName         : Olivier
Name              : Olivier Bourgeoise
ObjectClass       : user
ObjectGUID        : ac7eb8db-3cf1-4e6d-91d3-7527e540c284
SamAccountName   : Olivier
SID               : S-1-5-21-322346712-1256085132-1900709958-1408
Surname           : Bourgeoise
UserPrincipalName: Olivier@adatum.com
```

L'une des caractéristiques des applets de commande **Get-*** que vous utilisez pour récupérer des données de AD DS est qu'ils ne retournent pas toujours toutes les propriétés des objets qu'ils récupèrent. Par exemple, en regardant la sortie ci-dessus, vous ne voyez que quelques-unes des propriétés d'un compte d'utilisateur dans AD DS. Par exemple, vous ne voyez pas la propriété **mail (courrier électronique)**. Vous pouvez utiliser le paramètre **-Properties (Propriétés)** pour récupérer les propriétés non retournées par défaut lorsque vous exécutez des applets de commande **Get-***. Par exemple, le code ci-dessous retourne la même liste d'utilisateurs, mais cette fois avec les propriétés **mail (courrier électronique)** et **PasswordLastSet (Dernier changement de mot de passe)** :

```
Get-ADUser -Filter {sn -eq "Bourgeoise"} -Properties mail, passwordlastset
DistinguishedName : CN = Nathalie Bourgeoise, OU = Marketing, DC = Adatum, DC = com
Enabled : True
GivenName : Nathalie
Name : Nathalie Bourgeoise
ObjectClass : user
ObjectGUID : 1ff1b2cb-38c1-4bc7-bda7-511e19744d2a
PasswordLastSet : 7/9/2016 12:51:30 PM
SamAccountName : Nathalie
SID : S-1-5-21-322346712-1256085132-1900709958-1407
Surname : Bourgeoise
UserPrincipalName : Nathalie@adatum.com
DistinguishedName : CN=Olivier Bourgeoise,OU=IT,DC=Adatum,DC=com
Enabled : True
GivenName : Olivier
Name : Olivier Bourgeoise
ObjectClass : user
ObjectGUID : ac7eb8db-3cf1-4e6d-91d3-7527e540c284
PasswordLastSet : 7/9/2016 12:51:30 PM
SamAccountName : Olivier
SID : S-1-5-21-322346712-1256085132-1900709958-1408
Surname : Bourgeoise
UserPrincipalName : Olivier@adatum.com
```

Utilisez la commande suivante pour afficher toutes les propriétés d'un compte d'utilisateur :

```
Get-ADUser -Name "Administrator" -Properties *
```

Utilisez la commande suivante pour renvoyer tous les comptes d'utilisateur dans l'unité d'organisation Marketing et tous ses UO enfants :

```
Get-ADUser -Filter * -SearchBase "ou=Marketing,dc=adatum,dc=com" -SearchScope subtree
```

Utilisez la commande suivante pour afficher tous les comptes d'utilisateurs dont la date de la dernière connexion est postérieure à une date spécifique :

```
Get-ADUser -Filter {lastlogondate -lt "January 1, 2016"}
```

Utilisez la commande suivante pour afficher tous les comptes d'utilisateurs dans le département Marketing dont la date de la dernière connexion est postérieure à une date spécifique :

```
Get-ADUser -Filter {((lastlogondate -lt "January 1, 2016") -and (department -eq "Marketing"))}
```



Lectures supplémentaires : Pour plus d'informations, consultez : « À propos des filtres Active Directory » à l'adresse : <http://aka.ms/Kv5dy3>

LDAPFilter (Filter LDAP)

Vous pouvez également utiliser le paramètre **LDAPFilter (Filter LDAP)** pour filtrer les données récupérées par un applet de commande **Get-***. Le paramètre **LDAPFilter (Filter LDAP)** prend une valeur de chaîne qui utilise la même syntaxe que vous utilisez pour générer une requête LDAP. Par exemple, cette commande récupère tous les utilisateurs dont le nom est Bourgeoise :

```
Get-ADUser -LDAPFilter "(sn=Bourgeoise)"
```

Search-ADAccount (Recherche compte AD)

Une des faiblesses des applets de commande **Get-AD *** est la manière dont ils gèrent la propriété **UserAccountControl (Contrôle de compte d'utilisateur)**. Cette propriété est un bitmap à 4 octets,

où chaque bit correspond à une propriété différente liée à un compte Active Directory. Le tableau ci-dessous montre quelques-uns des bits du bitmap.

| Valeur hexadécimale | Valeur décimale | Identificateur | Description |
|---------------------|-----------------|-------------------------|---|
| 0x00000001 | 1 | ADS_UF_SCRIPT | Le script d'ouverture de session est exécuté. |
| 0x00000002 | 2 | ADS_UF_ACCOUNTDISABLE | Le compte de l'utilisateur est désactivé. |
| 0x00000008 | 8 | ADS_UF_HOMEDIR_REQUIRED | Un dossier de base est requis. |
| 0x00000010 | 16 | ADS_UF_LOCKOUT | Le compte d'utilisateur est verrouillé. |

 **Lectures supplémentaires :** Pour plus d'informations, consultez : « Comment utiliser les indicateurs UserAccountControl pour manipuler propriétés du compte d'utilisateur » à l'adresse : <http://aka.ms/Mxt8a1>

Quand vous lisez le UserAccountControl, vous recevez une valeur numérique et non un groupe de valeurs true/false par indicateur individuel. Par exemple, le code ci-dessous montre la propriété

UserAccountControl (Contrôle de compte d'utilisateur) pour tous les utilisateurs dont le nom commence par *Bo* :

```
Get-ADUser -Filter {sn -like "Bo*"} -Properties userAccountControl |Select Name,
userAccountControl|FT -AutoSize
Nom           userAccountControl
-----
Nathalie      Bourgeoise
Olivier       Bourgeoise
```

Imaginez que vous avez besoin de récupérer une liste de tous les comptes désactivés dans AD DS. Pour ce faire, vous devez récupérer tous les comptes dans lesquels les bits sont activés du deuxième au dernier pour la propriété **UserAccountControl (Contrôle de compte d'utilisateur)**. Vous pouvez y parvenir en utilisant ce code :

```
Get-ADUser -LDAPFilter "(userAccountControl:1.2.840.113556.1.4.803:=2)" |Select Name
```

La mémorisation ou même la consultation des indicateurs dans la propriété **UserAccountControl (Contrôle de compte d'utilisateur)** est un travail de longue haleine. Bien sûr, vous pouvez créer des scripts dans lesquels le code est déjà intégré et simplement les réutiliser. Cependant, il est bien mieux d'avoir une commande qui résume tout ce travail pour vous, ce que fait l'applet de commande **Search-ADAccount**. Vous pouvez récupérer une liste des comptes désactivés en utilisant l'applet de commande **Search-ADAccount** comme suit :

```
Search-ADAccount -AccountDisabled | Select name
```

C'est bien plus facile que d'utiliser **Get-ADUser**. Le tableau suivant répertorie les paramètres qu'utilise l'applet de commande **Search-ADAccount**.

| Paramètre | Description |
|------------------------|--|
| AccountDisabled | Récupère une liste des comptes désactivés. |

| Paramètre | Description |
|---|--|
| (Compte désactivé) | |
| AuthType (Type d'authentification) | Indique le type d'authentification utilisé lors de l'exécution de cette commande. |
| AccountExpired (Compte périmé) | Récupère une liste des comptes qui ont expiré. |
| AccountExpiring (Compte se périment) | Récupère une liste de comptes qui expirent dans une période donnée. |
| AccountInactive (Compte inactif) | Récupère une liste des comptes qui seront inactifs dans une période donnée. |
| LockedOut (Verrouillé) | Récupère une liste des comptes qui sont verrouillés. |
| PasswordExpired (Mot de passe périmé) | Récupère une liste de comptes dont les mots de passe ont expiré. |
| PasswordExpiring (Mot de passe se périment) | Récupère une liste des comptes dont les mots de passe expireront dans un délai donné. |
| PasswordNeverExpires (Mot de passe ne périme jamais) | Récupère une liste des comptes dont les mots de passe n'expirent jamais. |
| ComputersOnly (Ordinateurs uniquement) | Récupère les comptes d'ordinateurs. |
| UsersOnly (Utilisateurs uniquement) | Récupère des comptes d'utilisateurs. |
| TimeSpan (Période donnée) | Utilisé conjointement à PasswordExpiring , AccountExpiring et AccountInactive pour spécifier la période pour ces paramètres. |
| DateTime (Date heure) | Utilisé conjointement à PasswordExpiring , AccountExpiring et AccountInactive pour préciser la date d'expiration de ces paramètres. |
| SearchBase | Spécifie le conteneur LDAP de base pour la recherche. |
| SearchScope | Indique l'étendue de la recherche. |
| Serveur | Indique le serveur auquel se connecter. |

Voici quelques exemples de l'applet de commande **Search-ADAccount** :

```
# Récupérer tous les comptes d'utilisateurs désactivés
Search-ADAccount -AccountDisabled -UsersOnly
# Récupérer tous les comptes d'utilisateurs inactifs ces 5 derniers jours
Search-ADAccount -AccountInactive -TimeSpan -5 -UsersOnly
# Récupérer tous les comptes d'utilisateurs dont le mot de passe expirera le 04/07/2016
Search-ADAccount -AccountExpiring -DateTime "4/7/2016" -UsersOnly
# Récupérer tous les comptes d'ordinateurs qui sont verrouillés
Search-ADAccount -ComputersOnly -LockedOut
```

Modification des objets avec Windows PowerShell

Pour effectuer une opération en bloc, vous devez transmettre la liste des objets que vous avez interrogés à un autre applet de commande pour modifier les objets. Dans la plupart des cas, vous utilisez les applets de commande **Set-AD*** pour modifier les objets.

Pour transmettre la liste des objets interrogés à un autre applet de commande pour un traitement ultérieur, vous utilisez la barre verticale (|). La barre verticale transmet chaque objet de la requête à un deuxième applet de commande, qui effectue ensuite une opération spécifiée sur chaque objet.

Vous pouvez utiliser la commande suivante pour ces comptes dont l'attribut **Entreprise** n'est pas défini : Elle génère une liste des comptes d'utilisateurs et définit l'attribut **Entreprise** sur A. Datum.

```
Get-ADUser -Filter {company -notlike "*"} | Set-ADUser -Company "A. Datum"
```

Utilisez la barre verticale (|) pour passer une liste d'objets à une applet de commande pour la poursuite du traitement

```
Get-ADUser -Filter {company -notlike "*"} | Set-ADUser -Company "A. Datum"
```

```
Get-ADUser -Filter {lastlogondate -lt "January 1, 2016"} | Disable-ADAccount
```

```
Get-Content C:\users.txt | Disable-ADAccount
```

 **Lectures supplémentaires :** Pour plus d'informations, consultez : « Set-ADUser » à l'adresse : <http://aka.ms/K34c8d>

Vous pouvez utiliser beaucoup de commandes. Voici quelques exemples. Pour générer une liste de comptes d'utilisateurs qui ne se sont pas connectés depuis une date spécifique, puis les désactiver, vous pouvez utiliser la commande suivante :

```
Get-ADUser -Filter {lastlogondate -lt "January 1, 2012"} | Disable-ADAccount
```

Utilisation d'objets à partir d'un fichier texte

Au lieu d'utiliser une liste d'objets à partir d'une requête pour effectuer une opération en bloc, vous pouvez utiliser une liste d'objets dans un fichier texte. C'est utile quand vous avez une liste des objets à modifier ou supprimer et qu'il est impossible de la générer en utilisant une requête. Par exemple, le département RH peut générer une liste de comptes d'utilisateurs à désactiver. Il n'y a aucune requête qui permet d'identifier une liste d'utilisateurs qui ont quitté l'organisation.

Quand vous utilisez un fichier texte pour spécifier une liste d'objets, le fichier texte doit avoir le nom de chaque objet sur une seule ligne.

C'est une commande que vous pouvez utiliser pour désactiver les comptes d'utilisateurs qui sont répertoriés dans un fichier texte :

```
Get-Content C:\users.txt | Disable-ADAccount
```

Utilisation de fichiers CSV

Un fichier.csv peut contenir beaucoup plus d'informations qu'une simple liste. Semblable à une feuille de calcul, un fichier.csv peut avoir plusieurs lignes et colonnes d'informations. Chaque ligne du fichier.csv représente un objet unique et chaque colonne dans le fichier.csv représente une propriété de l'objet. C'est utile pour les opérations en bloc telles que la création de comptes d'utilisateurs lorsque plusieurs éléments d'information sur chaque objet sont nécessaires.

Vous pouvez utiliser l'applet de commande

Import-Csv pour lire le contenu d'un fichier.csv dans une variable puis travailler avec les données. Une fois les données importées dans la variable, vous pouvez vous reporter à chaque ligne individuelle de données et chaque colonne individuelle des données. Chaque colonne de données a un nom basé sur la ligne d'en-tête (la première ligne) du fichier.csv et vous pouvez vous référer à chaque colonne par son nom.

Voici un exemple d'un fichier.csv avec une ligne d'en-tête :

```
Prénom, Nom, Département
Grégoire, Carlson, IT
Robert, Paquet, Recherche
Théo, Faure, Marketing
```

Utilisez **foreach** pour traiter les données CSV.

Dans de nombreux cas, vous allez créer des scripts que vous réutilisez pour plusieurs fichiers.csv et vous ne savez pas combien de lignes il y a dans chaque fichier.csv. Dans ces cas, vous pouvez utiliser une boucle **foreach** pour traiter chaque ligne dans un fichier.csv. Vous n'avez pas besoin de savoir combien de lignes il contient. Pendant chaque itération de la boucle **foreach**, une ligne du fichier.csv est importée dans une variable qui est ensuite traitée.

Utilisez cette commande pour importer un fichier.csv dans une variable et utilisez une boucle **foreach** pour afficher le premier nom de chaque ligne dans un fichier.csv :

```
$users=Import-CSV -LiteralPath "C:\users.csv"
foreach ($user in $users)
{
    Write-Host "The first name is:" $user.FirstName
}
```

Démonstration : Exécution d'opérations en bloc avec Windows PowerShell

Vous pouvez utiliser un script pour combiner plusieurs commandes Windows PowerShell pour effectuer des tâches plus complexes. Dans un script, vous utilisez souvent des variables et des boucles pour traiter les données. Les scripts Windows PowerShell ont une extension.ps1.

La stratégie d'exécution sur un serveur détermine si les scripts sont en mesure de s'exécuter. La stratégie d'exécution par défaut sur Windows Server 2016 est **RemoteSigned**. Cela signifie que les scripts locaux peuvent s'exécuter sans être signés numériquement. Vous pouvez contrôler la stratégie d'exécution en utilisant l'applet de commande **Set-ExecutionPolicy**.

La première ligne d'un fichier .csv définit les noms des colonnes

```
FirstName,LastName,Department
Greg,Guzik,IT
Robin,Young,Research
Qiong,Wu,Marketing
```

Une boucle **foreach** traite le contenu d'un fichier .csv qui a été importé dans une variable

```
$users=Import-CSV -LiteralPath "C:\users.csv"
foreach ($user in $users) {
    Write-Host "The first name is:"
    $user.FirstName
}
```

Procédure de démonstration

Créer un nouveau groupe global dans le département IT

- Sur **LON-DC1**, démarrez une session **Windows PowerShell** avec des autorisations élevées.
- Exécutez la commande suivante :

```
New-ADGroup -Name Helpdesk -Path "ou=IT,dc=Adatum,dc=com" -GroupScope Global
```

Ajouter tous les utilisateurs dans le service informatique pour le groupe Helpdesk

- Dans la fenêtre Administrateur : Dans la fenêtre Windows PowerShell, exécutez la commande suivante :

```
Get-ADUser -Filter "Department -eq 'IT'" | Foreach {Add-ADGroupMember "Helpdesk" -members $_}
```

Définir l'adresse pour tous les utilisateurs dans le département de recherche

- Dans la fenêtre Administrateur : Dans la fenêtre Windows PowerShell, exécutez la commande suivante :

```
Get-ADUser -Filter {Department -eq "Recherche"} | Set-ADUser -StreetAddress "1530 Taylor Ave." -City "Winnipeg" -State "Manitoba" -Country "CA"
```

 **Remarque :** notez que cette commande utilise des parenthèses plutôt que de citations et utilise le cmdlet **Set-ADUser** plutôt qu'une boucle **foreach**.

Créer une unité d'organisation

- Dans la fenêtre Administrateur : Dans la fenêtre Windows PowerShell, exécutez la commande suivante :

```
New-ADOrganizationalUnit London -Path "dc=Adatum,dc=com"
```

Exécuter un script pour créer de nouveaux utilisateurs à partir d'un fichier.csv

- Ouvrez **E:\Labfiles\Mod02**, puis utilisez le Bloc-notes pour ouvrir **DemoUtilisateurs.csv**. Décrivez la composition du fichier.csv.
- Fermez le fichier.
- Dans Windows PowerShell, accédez au répertoire racine **E:\Labfiles\Mod02**.
- Exécutez le script **DemoUsers.ps1**.

Vérifier que les comptes d'utilisateurs ont été créés et que les comptes ont été modifiés

- Dans **Utilisateurs et ordinateurs Active Directory**, vérifiez que :
 - L'uo **Londres** existe
 - Il y a trois utilisateurs dans l'uo Londres
 - Le groupe **Support technique** existe dans l'uo **IT** et qu'il est peuplé avec les utilisateurs IT
 - Les utilisateurs de l'uo **Recherche** ont leurs champs d'adresses peuplés

Question : Qu'est-ce que l'environnement de script intégré Windows PowerShell ?

Leçon 5

Implémentation et gestion des UO

Lors de la conception de votre structure d'unité d'organisation, la planification du modèle de délégation des tâches d'administration Active Directory est essentielle. Bien qu'il soit possible d'utiliser les UO pour appliquer des stratégies de groupe, séparer des objets ou représenter la structure d'entreprise de votre organisation, la considération de conception de la structure de l'UO est le modèle de délégation des tâches administratives, qui dépend des processus et des exigences administratives dans votre organisation. Dans cette leçon, vous allez en apprendre davantage sur la planification et les considérations de la structure de l'UO, comment les autorisations fonctionnent pour l'UO et comment déléguer des autorisations pour les tâches administratives.

Objectifs de la leçon

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

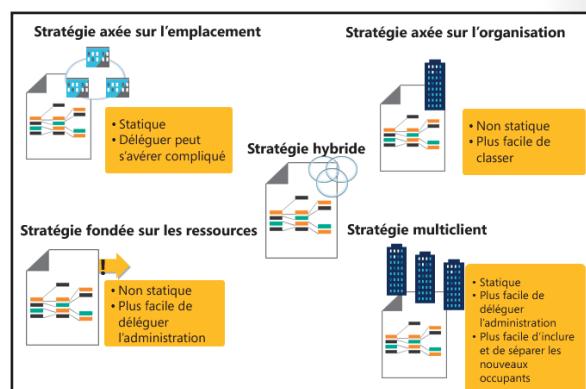
- Planifier les UO
- Décrire les considérations hiérarchiques de l'uo
- Décrire les considérations pour l'utilisation des UO
- Expliquer les autorisations AD DS
- Déléguer des autorisations AD DS
- Déléguer des autorisations administratives sur une UO

Planification d'UO

En tant qu'un des composants administratifs les plus importants dans votre domaine

Active Directory, les UO vous permettent de séparer et d'organiser tous les objets du domaine dans une structure hiérarchique. Les UO peuvent vous aider à :

- Déléguer des droits à des groupes administratifs, leur permettant d'administrer certains objets ou attributs des objets en dessous de cette UO
- Appliquer des stratégies de groupe pour des objets utilisateur et ordinateur en dessous de cette UO
- créer une hiérarchie qui vous permet d'administrer les objets du domaine rapidement.



Il existe plusieurs stratégies pour la conception de structures d'unité d'organisation. Les stratégies de conception d'unité d'organisation suivantes sont les plus courantes :

Stratégie axée sur l'emplacement

Cette stratégie utilise des emplacements pour chaque UO de haut niveau dans la racine du domaine. Ces UO basés sur l'emplacement sont les principaux éléments organisationnels de la structure d'unité d'organisation. Par exemple, A. Datum Corporation peut utiliser une stratégie basée sur l'emplacement pour créer des UO pour chacun de ses sites physiques (Londres, Toronto et Sydney) et ensuite créer

d'autres UO pour les centres de distribution de leurs filiales. Chaque ressource AD DS (comme les utilisateurs, les groupes et les ordinateurs) est située dans l'UO qui correspond à l'emplacement où réside la ressource.

La stratégie basée sur l'emplacement est couramment utilisée lorsque chaque emplacement fonctionne de façon relativement indépendante ou lorsque de nombreuses tâches sont déléguées à des administrateurs décentralisés. Par exemple, le personnel administratif à Londres peut effectuer les principales tâches administratives. Les administrateurs à Sydney ou à Toronto qui ont des droits délégués peuvent accéder rapidement à leurs utilisateurs, leurs groupes et leurs ordinateurs. C'est un avantage pour le personnel local pour remplir certaines fonctions administratives pour différents types d'objets dans la même filiale. En outre, vous ne devez pas déplacer des objets fréquemment entre les UO de haut niveau, à moins que les objets ne se déplacent vers un autre emplacement physique. Cela nécessite probablement le déplacement des dossiers de base ou des boîtes aux lettres de Microsoft Exchange Server. La stratégie basée sur l'emplacement fonctionne aussi bien pour les organisations qui s'attendent à se développer sur de nouveaux sites, parce que vous pouvez facilement ajouter de nouveaux sites à la structure de l'UO.

Stratégie fondée sur les ressources

Cette stratégie est construite autour des fonctions des ressources qui résident dans la structure de l'UO. En règle générale, vous séparez les ressources par fonction (ou les objets par type) et vous créez des UO pour représenter ces fonctions. Par exemple, certaines UO de haut niveau communes sont des Serveurs, des Stations de travail, des Groupes et des Utilisateurs. La stratégie fondée sur les ressources est généralement utilisée dans les petites organisations, dans les organisations dont la maintenance se fait de manière centralisée par le même personnel administratif et où la délégation administrative est basée sur le type d'objet plutôt que sur l'emplacement ou le département. Des exemples de ces groupes administratifs comprennent Support technique des clients, Prise en charge des clients, Administration de visualisation et prise en charge spécifique à une application. Dans les grandes organisations, il est probable que ces UO de haut niveau soient plus définies que dans le niveau subordonné suivant. Par exemple, les Serveurs UO peuvent contenir des UO enfants nommées d'après leurs applications, telles que Microsoft Exchange Server ou Microsoft SQL Server.

Stratégie basée sur l'organisation. Cette stratégie reflète la structure de la logique commerciale d'une organisation. Les UO de haut niveau représentent les départements au sein de l'organisation, tels que les départements Ventes, Recherche ou Finance. Cette stratégie fonctionne bien si les ressources se déplacent fréquemment ou si elles ne sont pas affiliées à un emplacement physique et s'il y a peu de changements d'employés entre les départements. Vous devriez envisager cette stratégie lorsque les tâches administratives sont déléguées par département plutôt que par emplacement. Par exemple, une organisation avec des équipes commerciales itinérantes et d'autres unités qui ne sont pas liées à un emplacement bénéficient d'une stratégie fondée sur l'organisation. Cependant, cette stratégie n'est pas un bon choix pour les organisations qui réalignent souvent leur modèle économique ou qui encouragent les employés à changer de rôle.

Stratégie basée sur des domaines multiples

Cette stratégie est adaptée aux organisations qui fournissent l'infrastructure Active Directory comme service (IaaS) à d'autres organisations. Cela pourrait être un groupe d'organisations affiliées qui partagent le même domaine, un environnement hébergé, un environnement externalisé ou même un fournisseur de cloud privé ou public. Cette stratégie est appropriée quand une organisation est responsable de la maintenance de l'infrastructure Active Directory tandis qu'une autre organisation est déléguée à la gestion de certains objets Active Directory ou si la première organisation repose entièrement sur l'administration de l'organisation hôte. Par exemple, A. Datum peut assurer la maintenance de AD DS pour Trey Research et Contoso, Ltd. Trey Research peut vouloir administrer leurs UO Utilisateurs, Groupes et Ordinateurs indépendamment, mais peut ne pas vouloir gérer la réPLICATION et le DNS Active Directory, tandis que Contoso, Ltd. repose entièrement sur le personnel informatique de A. Datum pour l'ensemble de ces tâches. Dans ce scénario, A. Datum crée une UO de haut niveau pour Services informatiques, où ils

effectuent la maintenance de tous les comptes et groupes administratifs et des UO de haut niveau nommés ADatum, Contoso, Ltd. et TreyResearch pour chacune des organisations gérées. Sous ces UO, les utilisateurs, groupes, stations de travail réguliers et peut-être les comptes de serveur sont représentés comme des niveaux plus profonds. Le personnel informatique de Trey Research est délégué pour effectuer la maintenance de leurs propres comptes comme prévu. Dans la stratégie basée sur des domaines multiples, il est possible d'autoriser différents locataires à fonctionner ensemble ou à créer des paramètres de confidentialité afin que chaque organisation ne voie que ses propres ressources. Dans cette stratégie, un processus plus simple pour inclure ou séparer de nouvelles organisations est également possible.

Stratégie hybride

Cette stratégie utilise une combinaison d'unité d'organisation basée sur l'emplacement, l'organisation et les ressources. La stratégie basée sur des domaines multiples est aussi une stratégie hybride. D'autres stratégies hybrides peuvent attribuer l'emplacement au niveau supérieur et séparer les types d'objets au niveau suivant. Les stratégies hybrides peuvent être complètement mélangées, en fonction des impératifs organisationnels. Par exemple, l'UO Serveurs peut contenir des UO pour FileServers, IIS, SQL Server, Exchange Server et d'autres serveurs d'applications. Les UO Utilisateurs peuvent contenir l'emplacement ou l'UO du service, les UO Stations de travail peuvent faire la distinction entre Bureaux et Ordinateurs portables et les UO Groupes peuvent incorporer des groupes de service, d'emplacement, de projet ou spécifiques à une application.

Quelle que soit la stratégie que vous utilisez pour concevoir votre structure d'unité d'organisation, rappelez-vous toujours que le but principal est de permettre la mise en œuvre d'un modèle modèle de tâches administratives Active Directory, tandis que les stratégies de groupe peuvent être la seconde priorité. Nous recommandons également de séparer les comptes et groupes administratifs des comptes d'utilisateurs et des groupes réguliers qui peuvent être administrés par les administrateurs délégués.

Considérations hiérarchiques UO

Lors de la planification de la fonctionnalité Active Directory, vous devriez envisager les aspects de la conception de UO de haut niveau suivants :

- Fins administratives. La structure UO doit s'aligner essentiellement sur les fins administratives, tel que votre modèle de délégation des tâches Active Directory et vos GPO. Évitez d'imiter votre schéma organisationnel, à moins qu'il ne bénéficie au modèle administratif. Les schémas organisationnels changent fréquemment et il

est peu pratique de modifier aussi souvent votre structure UO. Si vous avez des requêtes concernant des GPO spécifiques à un département, il peut être préférable de refléter ces départements dans un niveau inférieur de la structure UO. Cependant, il est également probable qu'un groupe de sécurité et de distribution reflète les utilisateurs et vous pouvez plutôt utiliser le filtrage de sécurité à cette fin. Les utilisateurs et les Managers ne voient généralement pas la structure UO, donc il n'y a aucun avantage à avoir des hiérarchies au sein de l'entreprise répertoriées à cet endroit. Si vous voulez permettre aux utilisateurs de parcourir la structure organisationnelle, assurez-vous que vous remplissez l'attribut **Gestionnaire** des objets utilisateur, ce qui permet aux utilisateurs d'utiliser les versions actuelles et précédentes de Microsoft Office Outlook en combinaison avec une infrastructure

Aligner la stratégie UO sur les exigences administratives et non sur l'organigramme car les ceux-ci sont plus sujets au changement que votre modèle d'administration informatique

L'héritage de comportement AD DS peut simplifier l'administration de stratégie de groupe car il permet de définir des stratégies de groupe sur une UO et de redescendre vers d'autres UO dans la hiérarchie

Prévoir d'aménager les changements dans le modèle d'administration informatique

de messagerie Exchange Server, Microsoft Office 365 ou Microsoft SharePoint Server pour naviguer dans la structure organisationnelle. L'UO sert à des fins purement administratives

- Héritage. L'héritage est un aspect important de la fonctionnalité UO, tant pour la délégation du contrôle que pour l'application de GPO. Vous devez concevoir la structure UO pour inclure des objets qui nécessitent le même contrôle administratif ou les mêmes paramètres de stratégie de groupe au sein de la même structure UO. De cette façon, vous ne pouvez attribuer la délégation du contrôle ou le paramètre de GPO qu'une seule fois à un niveau supérieur dans la structure UO, plutôt qu'individuellement à chaque niveau enfant. Rappelez-vous que vous pouvez bloquer l'héritage pour certaines UO enfants si vous ne voulez pas que AD DS applique les paramètres pour un niveau UO plus élevé à certaines UO enfants
- Modification. Concevez votre structure d'unité d'organisation pour intégrer la modification. Après avoir mis en œuvre une structure d'unité d'organisation, il peut être difficile de la modifier, surtout si vous modifiez également les stratégies de conception, telles que la modification d'une stratégie basée sur l'organisation à une stratégie fondée sur les ressources. Assurez-vous que votre structure d'unité d'organisation laisse place à la croissance organisationnelle et un niveau raisonnable de changement structurel

Éléments à prendre en compte pour l'utilisation des UO

Lorsque AD DS est d'abord mis en œuvre, il n'y a qu'une seule UO : l'UO des contrôleur de domaine. Vous devez créer toutes les autres UO.

Création d'unité d'organisation

Vous pouvez créer des UO en utilisant des outils graphiques tels que les Utilisateurs et ordinateurs Active Directory ou le Centre d'administration Active Directory. Vous pouvez également créer des UO en utilisant des outils de ligne de commande comme Windows PowerShell.

- Les unités d'organisation peuvent être créées en utilisant les outils graphiques AD DS ou des outils en ligne de commande
- Les nouvelles unités d'organisation sont par défaut protégées contre toute suppression accidentelle
- Quand des objets sont déplacés entre des unités d'organisation :
 - Les autorisations directement assignées restent en place
 - Les autorisations héritées changent
- Les autorisations appropriées sont nécessaires pour déplacer des objets entre des unités d'organisation



Remarque : vous devez créer toute nouvelle UO en utilisant un outil administratif. Il n'y a pas de mécanisme pour copier des UO existantes pour en créer de nouvelles.

Dans la plupart des cas, vous utilisez un outil graphique ou un script pour accomplir cette tâche.

Prévention contre la suppression accidentelle

La suppression accidentelle est l'une des principales causes des récupérations de Active Directory. Par conséquent, Windows Server 2016 prend en charge la fonctionnalité Protéger les UO contre la suppression accidentelle de AD DS. Les UO qui sont protégées contre la suppression accidentelle partagent les avantages suivants :

- Les UO ne peuvent pas être accidentellement supprimées. Si les administrateurs souhaitent supprimer délibérément une UO, ils doivent retirer la protection avant de la supprimer
- Les UO ne peuvent pas être déplacées accidentellement
- Les UO nouvellement créées en utilisant le Centre d'administration Active Directory ou Utilisateurs et ordinateurs Active Directory dans Windows Server 2008 ou une version plus récente sont protégées automatiquement contre la suppression accidentelle

Vous pouvez activer ou désactiver la protection contre la suppression accidentelle dans le Centre d'administration Active Directory dans les propriétés de l'UO. Vous pouvez également utiliser Utilisateurs et ordinateurs Active Directory pour activer ou désactiver la protection contre la suppression accidentelle sur l'onglet **Objet** dans la boîte de dialogue **Propriétés UO**



Remarque : vous devez activer l'affichage avancé dans Utilisateurs et ordinateurs Active Directory avant de pouvoir voir l'onglet **Objet** dans les propriétés de l'UO.

Vous pouvez également utiliser Windows PowerShell pour activer ou désactiver la protection. Par exemple, vous pouvez rechercher des UO qui ne sont pas protégées et activer la protection avec la commande suivante :

```
Get-ADOrganizationalUnit -filter * -properties ProtectedFromAccidentalDeletion | where {$_.ProtectedFromAccidentalDeletion -eq $false} | Set-ADOrganizationalUnit -protectedFromAccidentalDeletion $true
```

Déplacement des objets entre UO

Si les fonctions principales changent ou si les ordinateurs sont réaffectés, parfois les objets dans AD DS doivent être déplacés vers des UO différentes. Déplacer des objets entre UO dans le même domaine est une tâche simple. Vous pouvez cliquer avec le bouton droit sur l'objet et le déplacer ou vous pouvez cliquer et faire glisser l'objet vers la nouvelle UO. Déplacer des objets a les effets suivants sur les autorisations des objets :

- Les autorisations attribuées directement à l'objet perdurent après le déplacement de l'objet
- L'objet hérite de nouvelles autorisations à partir de sa nouvelle UO et perd toutes les autorisations héritées de l'UO précédente

Autorisations requises pour déplacer des objets

Les autorisations suivantes sont nécessaires pour déplacer des objets AD DS :

- L'autorisation Supprimer_Enfant sur l'UO source (ou l'autorisation Supprimer sur l'objet déplacé)
- L'autorisation Écrire_Propriété sur l'objet pour les propriétés du nom unique relatif (RDN), du nom unique (DN) et du nom commun (CN)
- L'autorisation Créer_enfant sur l'UO cible

Autorisations de AD DS

Vous mettez en œuvre le modèle de délégation administrative Active Directory en fusionnant la conception d'unité d'organisation avec les autorisations sur les UO. Cela permet aux administrateurs délégués de remplir des tâches administratives. Pour créer le modèle de tâche administrative et concevoir la structure d'unité d'organisation pour le prendre en charge, vous devez comprendre comment fonctionnent la délégation administrative de Active Directory fonctionne et les options pour déléguer le contrôle administratif.

- Les utilisateurs reçoivent leur jeton (liste de SID) lors de la connexion
- Les objets ont un descripteur de sécurité, qui décrit :
 - Qui (SID) a eu ou non l'autorisation d'accès
 - Les autorisations (lecture, écriture, créer ou supprimer enfant)
 - Le genre d'objets
 - Les sous-niveaux
- Quand les utilisateurs parcourent la structure Active Directory, leur jeton est comparé au descripteur de sécurité pour évaluer leurs droits d'accès

Comment les utilisateurs obtiennent-ils des autorisations ?

Lorsque les utilisateurs se connectent à un domaine Active Directory, ils reçoivent un jeton, qui est une liste des identificateurs de sécurité (SID) de leur compte individuel, de leurs comptes d'historique, s'ils ont été migrés, et chaque groupe auquel ils appartiennent (même de manière récursive). Si un groupe a été migré d'un autre domaine, il est probable qu'il reçoit également les historiques d'identificateurs de sécurité (SID) de ces groupes dans le domaine précédent.

Dans les systèmes d'exploitation Windows, de nombreux objets (tels que les fichiers, les dossiers, les clés de Registre, les processus et les objets Active Directory) contiennent un descripteur de sécurité. Basé sur le SID, le descripteur de sécurité définit quels droits sont accordés ou refusés et à qui ils le sont.

Lorsqu'un utilisateur accède aux fichiers, aux dossiers ou aux clés de Registre ou navigue à travers la structure du domaine Active Directory, la liste des SID dans le jeton est comparée à la liste des SID dans le descripteur de sécurité. S'il y a des SID correspondants, le système valide le type d'accès et permet ou interdit l'opération en cours.

Autorisations d'unité d'organisation de Active Directory

Dans Active Directory, le modèle d'autorisation est plus complexe que dans la plupart des autres services du système d'exploitation Windows. Les paramètres de sécurité sur le domaine Active Directory sont hérités hiérarchiquement dans la structure d'unité d'organisation de ce domaine. À tout point de la structure, vous pouvez configurer des paramètres de sécurité supplémentaires qui pourraient être hérités dans toute la hiérarchie en fonction de l'étendue de l'héritage qui est définie dans le paramètre de sécurité et du fait que l'héritage est bloqué ou non à un niveau inférieur. Les nouveaux objets obtiennent les paramètres de sécurité par défaut (qui sont définis dans la classe de schéma) et héritent des paramètres de sécurité de leurs parents. Par exemple, dans la définition du schéma UO, tous les droits sont accordés aux Opérateurs de compte pour créer et supprimer des objets des comptes d'ordinateur, des comptes d'utilisateurs, des objets de groupe et des objets **inetOrgPerson**. Par conséquent, si vous supprimez le groupe Opérateurs de compte par défaut des autorisations de sécurité d'une UO, puis créez un enfant UO, l'UO enfant conserve les paramètres de sécurité explicites des Opérateurs de compte.

Descripteurs de sécurité de l'objet Active Directory

Le descripteur de sécurité d'un objet Active Directory contient les éléments suivants :

- Le propriétaire de l'objet. Le propriétaire peut réinitialiser les paramètres de sécurité, même s'il les a accidentellement configurés pour n'avoir aucune autorisation sur l'objet
- Le groupe principal du propriétaire (SID)
- Un champ de contrôle qui spécifie si la liste de contrôle d'accès discrétionnaire (dacl) ou la liste de contrôle d'accès de sécurité (sacl) est présente et/ou bloque l'héritage
- Une dacl en option. L'option dacl contient des autorisations pour accorder ou refuser l'accès
- Une sacl en option. L'option sacl contient les autorisations d'audit lorsque l'audit des réussites ou des échecs est activé

La dacl et la sacl sont des conteneurs qui contiennent une ou plusieurs entrées du contrôle d'accès (aces). Une ace stocke les informations suivantes :

- A qui (quelle entité de sécurité, comme un utilisateur ou un groupe) l'accès est autorisé ou refusé
- Quelles sont les autorisations accordées à l'entité de sécurité. Lire, écrire, créer ou supprimer
- Sur quels objets ou attributs de l'objet l'action peut être effectuée
- A quel sous-niveaux (seulement au niveau de l'uo, seulement sur les objets dans l'uo ou les objets dans n'importe quelle sous-uo)

Dans les propriétés UO, vous utilisez l'onglet **Sécurité** et plus précisément, la boîte de dialogue **Sécurité avancée** pour vérifier ou ajuster les paramètres de sécurité. L'**Assistant Délégation de sécurité** aide à effectuer certaines tâches courantes, mais vous ne pouvez pas l'utiliser pour reviser les paramètres de sécurité.

Déléguer les autorisations AD DS

Les administrateurs de domaine ont tous les droits sur tous les objets du domaine. D'autres groupes prédéfinis par défaut ont des droits limités sur les objets dans le domaine. Par exemple, le groupe Opérateurs de compte a tous les droits sur les Utilisateurs, les Ordinateurs et les Objets de groupe, mais pas sur d'autres types d'objets. Si vous voulez que certains utilisateurs ou groupes aient l'autorisation de n'effectuer que des tâches spécifiques dans des zones spécifiques de l'annuaire, vous devez déléguer ces tâches.

- Les autorisations sur les objets AD DS peuvent être accordées aux utilisateurs ou aux groupes
- Les modèles d'autorisation sont généralement basés sur des objets ou des rôles
- L'Assistant Délégation de contrôle peut simplifier l'attribution de tâches administratives communes
- Les propriétés de sécurité avancées des unités d'organisation permettent d'accorder des autorisations granulaires

Méthodes de contrôle de la délégation

Lorsque vous délégez le contrôle des objets dans votre UO Active Directory, vous devez tenir compte de deux facteurs : à qui vous accordez des autorisations et à quel emplacement de la hiérarchie d'annuaire. Dans AD DS, vous pouvez accorder des droits spécifiques sur les ressources. Vous pouvez autoriser la création ou la suppression de certains types d'objets seulement ou vous pouvez sélectionner les individus qui ont des droits sur un attribut particulier d'un type d'objet spécifique, tels que les descriptions de compte de groupe ou de leurs membres. Sauf dans de rares cas (comme les comptes de service), vous devez toujours accorder le contrôle administratif aux groupes plutôt qu'aux utilisateurs. Même si le groupe ne contient qu'un seul utilisateur, cet individu peut quitter l'organisation et il est plus difficile de déterminer où cet individu avait des autorisations que de modifier l'appartenance aux groupes appropriés.

Il existe deux méthodes pour déléguer le contrôle administratif sur les ressources de domaine Active Directory :

- La délégation type-objet. Dans ce modèle de délégation, vous pouvez déléguer différents niveaux de contrôle à des groupes basés sur les objets que les groupes contrôlent. Un exemple d'une délégation type-objet serait si vous avez délégué le contrôle au groupe Administrateurs de Toronto pour les objets de l'UO Toronto. Dans ce cas, le groupe Administrateurs de Toronto est probablement responsable de la majorité des tâches administratives au sein de l'UO de Toronto

Vous utilisez généralement la délégation type-objet s'il n'y a que peu d'administrateurs ou si une délégation mineure est nécessaire. Ce type de délégation fonctionne bien également si de nombreux administrateurs exigent le même niveau de contrôle, généralement sur la majorité de la structure de domaine.

Nous ne recommandons pas la délégation type-objet dans un environnement où différents utilisateurs exigent différents niveaux de contrôle sur différents objets, car il peut être difficile de déterminer quel niveau de contrôle est accordé à quels utilisateurs pour un objet spécifique.

- Délégation basée sur les rôles. Ce modèle de délégation consiste à créer plusieurs groupes spécifiques auxquels vous délégez le contrôle administratif. Ces groupes se rapportent généralement à une ressource spécifique (ou des ressources spécifiques) et vous pouvez nommer des groupes pour le niveau de contrôle que vous leur attribuer. Contrairement à la délégation basée sur les objets, la délégation basée sur les rôles implique d'accorder des autorisations pour modifier seulement certains

attributs d'un objet. Par exemple, vous pouvez créer le groupe basé sur les rôles Modifier le mot de passe de l'utilisateur Finance, puis attribuer des autorisations à ce groupe pour modifier les mots de passe pour tous les utilisateurs dans l'UO Finance.

Pour vous assurer que votre délégation basée sur les rôles est efficace, toutes les fonctions ou tous les rôles au sein de la structure de domaine Active Directory doivent avoir un groupe associé. Ce niveau de spécificité peut vous aider à déterminer quel niveau de contrôle vous avez affecté à un utilisateur individuel, parce que vous examinez simplement les groupes basés sur les rôles auxquels l'utilisateur appartient.

La mise en œuvre de la délégation basée sur les rôles peut prendre plus de temps que la délégation type-objet. Toutefois, si vous concevez correctement la structure d'unité d'organisation et de groupe, la délégation basée sur les rôles permet d'épargner l'effort administratif et la frustration, en particulier pour les organisations plus grandes.

Assistant Délégation du contrôle

Cet outil peut être très utile pour déléguer des droits administratifs à des objets dans AD DS à des groupes ou à des individus. Il permet de simplifier les autorisations qui sont nécessaires pour effectuer des tâches administratives quotidiennes telles que la réinitialisation des mots de passe ou la modification de l'appartenance aux groupes.

L'assistant fournit une liste des tâches courantes que vous pouvez attribuer ou vous permet de créer une tâche personnalisée en fonction du type d'objet pour lequel vous souhaitez déléguer le contrôle.

Pour démarrer l'**Assistant Délégation du contrôle**, cliquez avec le bouton droit sur le conteneur, puis cliquez sur **Déléguer le contrôle**. Ensuite, sélectionnez l'utilisateur ou le groupe auquel vous souhaitez attribuer des droits et sélectionnez les tâches que vous voulez qu'ils effectuent.



Remarque : l'exécution de l'**Assistant Délégation du contrôle au** niveau du domaine fournit une tâche commune pour **Joindre l'ordinateur au domaine**. Cette tâche apparaît uniquement lorsque l'assistant s'exécute au niveau du domaine.

Attribution manuelle des autorisations

Les propriétés avancées de sécurité d'une UO vous permettent d'être très précis sur les autorisations accordées aux utilisateurs et aux groupes. Par exemple, vous pouvez vouloir accorder la possibilité de modifier uniquement certains attributs de l'utilisateur, tels que **Adresse (domicile)** et **Fonction** aux employés du département RH.

Démonstration : Délégation des autorisations administratives sur une unité d'organisation

Dans cette démonstration, vous verrez comment créer une nouvelle UO, utiliser l'**Assistant Délégation du contrôle** pour assigner une tâche et utiliser la sécurité avancée UO pour attribuer des autorisations précises au groupe Recherche.

Procédure de démonstration

Créer une unité d'organisation

- Utilisez **Utilisateurs et ordinateurs Active Directory** pour créer une nouvelle UO nommée **Ressources humaines** dans **Adatum.com**

Utiliser l'Assistant Délégation de contrôle pour assigner une tâche

1. Démarrez l'**Assistant Délégation du contrôle** au niveau **Adatum.com**.
2. Sélectionnez le groupe **Support technique** et assignez les tâches suivantes :
 - Réinitialiser les mots de passe des utilisateurs et forcer le changement de mot de passe à la prochaine ouverture de session
 - Joindre un ordinateur à un domaine

Attribuer au groupe de recherche le droit de modifier les adresses des utilisateurs et des titres d'emploi dans l'unité de recherche

1. Activez les **Fonctionnalités avancées**.
2. Ouvrez les propriétés de l'UO **Recherche**.
3. Dans la section de sécurité avancée, sélectionnez le groupe **Recherche**, puis attribuez les autorisations suivantes sur les objets **Descendant utilisateur** :
 - Écrire Adresse (domicile)
 - Écrire Fonction

Question : Quel est l'avantage d'utiliser l'**Assistant Délégation de contrôle** ?

Atelier pratique B : Administration AD DS

Scénario

Vous avez travaillé pour la Corporation A. Datum en tant que spécialiste de l'assistance de bureau et avoir effectué des tâches de dépannage sur les ordinateurs de bureau pour résoudre les problèmes d'application et réseau. Vous avez récemment accordé une promotion à l'équipe du support de serveur. Une de vos premières missions est de configurer le service de l'infrastructure pour une nouvelle filiale.

Pour commencer le déploiement de la nouvelle succursale, vous préparez les objets AD DS. Dans le cadre de cette préparation, vous devez créer une unité d'organisation pour la succursale et déléguer l'autorisation de la gérer. En outre, vous devez évaluer Windows PowerShell pour gérer AD DS plus efficacement.

Objectifs

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

- Déléguer l'administration des UO
- Utiliser Windows powershell pour gérer les objets AD DS

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateur virtuel : **22742A-LON-DC1**, **22742A-LON-DC2**, **22742A-LON-SVR1** et **22742A-LON-CL1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**.

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-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'authentification suivantes :
 - Nom d'utilisateur : **Administrateur**
 - Mot de passe : **Pa55w.rd**
 - Domaine : **Adatum**
5. Répétez les étapes 1 à 4 pour **22742A-LON-DC2** et **22742A-LON-SVR1**.
6. Répétez les étapes 1 à 3 pour **22742A-LON-CL1**. Ne vous connectez pas à **LON-CL1** avant d'y être invité au cours des étapes de l'atelier.

Exercice 1 : Déléguer l'administration pour les UO

Scénario

A. Datum Corporation délègue la gestion de chaque bureau de branche à un groupe spécifique. Cela permet aux employés informatiques qui travaillent sur place d'être configurés en tant qu'administrateurs de la branche. Chaque succursale a un groupe d'administrateurs de succursales qui peut prendre en charge l'administration complète au sein de l'unité d'organisation de la succursale. Il existe aussi un groupe d'assistance de la branche qui est en mesure de gérer les utilisateurs dans l'unité d'organisation de la succursale, mais pas d'autres objets. Vous devez créer l'unité d'organisation et des groupes pour les nouvelles succursales et de déléguer des autorisations aux groupes. Vous pourrez également valider les autorisations.

Les tâches principales de cet exercice sont les suivantes :

1. Créer une nouvelle UO pour la filiale.
2. Créer des groupes pour les administrateurs de la filiale et le personnel du Support technique de la filiale.
3. Ajouter des membres au groupe.
4. Déléguer des autorisations au groupe.
5. tester les permissions.

► Tâche 1 : Créer une nouvelle UO pour la succursale

- Sur **LON-DC1**, utilisez **Utilisateurs et ordinateurs Active Directory** pour créer une nouvelle UO nommée **Londres**

► Tâche 2 : Créer des groupes pour les administrateurs de succursales et le personnel du Help-desk de la succursale

- Dans l'UO **Londres**, créez les groupes de sécurité globaux suivants :
 - **Administrateurs Londres**
 - **Support technique Londres**

► Tâche 3 : Ajouter des membres au groupe

1. Sélectionnez l'UO **IT**.
2. Ajoutez **Beth Burke** au groupe **Administrateurs Londres**.
3. Ajoutez **Dante Dabney** au groupe **Support technique Londres**.

► Tâche 4 : Déléguer des autorisations au groupe

1. Dans **Utilisateurs et ordinateurs Active Directory**, activez l'affichage **Fonctionnalités avancées**.
2. Définissez des autorisations sur l'onglet **Sécurité** des propriétés de l'UO **Londres** pour donner au groupe **Administrateurs Londres** le **Contrôle total**.
3. Utilisez l'**Assistant Délégation du contrôle** pour accorder le **Contrôle total** des **objets USER** dans l'UO **Londres** au groupe **Support technique Londres**.

► **Tâche 5 : Tester les permissions**

- Sur **LON-SVR1**, utilisez l'**Assistant Ajout de rôles et de fonctionnalité** dans **Gestionnaire de serveur** pour installer la fonctionnalité **Outils AD DS**. Lorsque cette tâche est terminée, déconnectez-vous de **LON-SVR1**.

Tester les permissions pour Admins Londres

- Connectez-vous à **LON-SVR1** en tant qu'**Aurore** avec le mot de passe **Pa55w.rd**.
- Ouvrez **Utilisateurs et ordinateurs Active Directory**.
- Cliquez sur l'UO **Research**. Notez que les icônes de la barre d'outils pour créer des utilisateurs, des groupes ou des UO sont grises.
- Cliquez sur l'UO **Londres**, puis notez que ces icônes sont maintenant actifs.
- Créez une sous-UO dans l'UO **Londres** nommée **Ordinateurs portables**.
- Déconnectez-vous de **LON-SVR1**.

Tester les permissions pour le Support technique de Londres

- Connectez-vous à **LON-SVR1** en tant que **Dante** avec le mot de passe **Pa55w.rd**.
- Ouvrez **Utilisateurs et ordinateurs Active Directory**.
- Cochez l'UO **Londres**. Notez que la seule icône non griseée est l'icône créer un utilisateur.

Résultats : À la fin de cet exercice, vous aurez réussi à :

- Créer une nouvelle UO pour la succursale
- Créer des groupes pour les administrateurs de succursales et le personnel Help-desk de la succursale
- Ajouter des membres au groupe
- Déléguer des permissions aux groupes
- Installer des outils AD DS et tester les permissions

Exercice 2 : Création et modification d'objets AD DS dans Windows PowerShell

Scénario

La corporation A. Datum présente un certain nombre de scripts qui ont été utilisés dans le passé pour créer des comptes d'utilisateurs en utilisant des outils de ligne de commande. Toutefois, un mandat à l'échelle de l'entreprise spécifie que tous les scripts seront désormais créés en utilisant Windows PowerShell. En guise de première étape dans la création de scripts, vous devez identifier la syntaxe requise pour gérer les objets AD DS dans Windows PowerShell.

Vous disposez d'un fichier.csv qui contient une grande liste de nouveaux utilisateurs pour la succursale. Il est inefficace de créer ces utilisateurs individuellement avec des outils graphiques, raison pour laquelle vous allez utiliser un script Windows PowerShell à la place. Un collègue qui a de l'expérience avec les scripts vous a donné un script qu'il a créé. Vous devez vous connecter en tant qu'administrateur de la branche et modifier le script pour correspondre au format de votre fichier.csv.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un compte d'utilisateur en utilisant Windows powershell.
2. Créer un nouveau groupe en utilisant Windows powershell.
3. Ajouter un membre au groupe en utilisant Windows powershell.
4. Modifier le fichier.csv.
- 5.Modifier le script.
6. Exécuter le script.
7. Préparer le module suivant.

► **Tâche 1 : Créer un compte utilisateur en utilisant Windows PowerShell**

1. Basculez vers **LON-DC1**.
2. Démarrez une session de Windows PowerShell avec élévation de privilèges.
3. Créez un compte d'utilisateur pour **Ty Carlson** dans l'UO **Londres** en exécutant la commande suivante :

```
New-ADUser -Name Ty -DisplayName "Ty Carlson" -GivenName Ty -Surname Carlson -Path "ou=Londres,dc=adatum,dc=com"
```

4. Exédez la commande suivante pour définir le mot de passe **Pa55w.rd** :

```
Set-ADAccountPassword Ty
```

Le mot de passe actuel est vide.

5. Exédez la commande suivante pour activer le compte :

```
Enable-ADAccount Ty
```

6. Testez le compte en optant pour **LON-CL1**, puis connectez-vous en tant que **Ty** avec un mot de passe **Pa55w.rd**.

► **Tâche 2 : Créer un nouveau groupe en utilisant Windows PowerShell**

- Sur **LON-DC1**, dans l'**Administrateur** : Dans la fenêtre **Windows PowerShell**, exédez la commande suivante :

```
New-ADGroup LondonBranchUsers -Path "ou=Londres,dc=adatum,dc=com" -GroupScope Global -GroupCategory Security
```

► **Tâche 3 : Ajouter un membre au groupe en utilisant Windows PowerShell**

1. Dans la fenêtre **Administrateur** : Dans la fenêtre **Windows PowerShell**, exédez la commande suivante :

```
Add-ADGroupMember LondonBranchUsers -Members Ty
```

2. Confirmer que l'utilisateur est dans le groupe en exédez la commande suivante :

```
Get-ADGroupMember LondonBranchUsers
```

► Tâche 4 : Modifier le fichier.csv

- Utilisez le Bloc-notes pour modifier le fichier.csv en ajoutant l'en-tête suivant :

Prénom, Nom, Département, MotdepasseparDéfaut

- Enregistrez et fermez le fichier.

► Tâche 5 :Modifier le script

- Dans la fenêtre **Administrateur : Windows PowerShell (ISE)**, remplacez ces variables :

C:\path\file.csv par **E:\Labfiles\Mod02\LabUsers.csv**
"uo = orgUnit, dc = domain, dc = com" par **"uo = Londres, dc = adatum, dc = com"**

- Sauvegardez le fichier, puis fermez l'**Administrateur : Fenêtre Windows PowerShell (ISE)**.

► Tâche 6 : Exécuter le script

- Passer à l'**Administrateur : Fenêtre Windows PowerShell**.
- Modifiez le répertoire racine **E:\Labfiles\Mod02**.
- Saisissez **.\\LabUsers.ps1** pour exécuter le script.
- Exécutez la commande suivante pour vous assurer que les utilisateurs ont été créés :

```
Get-ADUser -Filter * -SearchBase "ou=Londres,dc=adatum,dc=com"
```

► Tâche 7 : Préparer le module suivant

Une fois l'atelier terminé, rétablissez l'état initial de tous les ordinateurs virtuels.

- Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
- Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
- Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
- Répétez les étapes 2 et 3 pour **22742A-LON-DC2**, **22742A-LON-SVR1** et **22742A-LON-CL1**.

Résultats : À la fin de cet exercice, vous aurez réussi à :

- Créé un compte utilisateur en utilisant Windows powershell
- Créé un groupe en utilisant Windows powershell
- Un utilisateur ajouté à un groupe en utilisant Windows powershell
- Fichier.csv modifié
- Script modifié
- Exécuté le script

Question : Pourquoi les utilisateurs créés par ce script sont activés ?

Question : Quel est l'état des comptes créés par le cmdlet **New-ADUser** ?

Contrôle des acquis et éléments à retenir

Enjeux et scénarios du monde réel

De nombreuses organisations vont créer des comptes d'utilisateurs basés sur le rôle de l'emploi plutôt que ce soit à l'utilisateur de remplir le rôle. Par exemple, l'organisation aura toujours un réceptionniste. Pour assurer la continuité, la personne qui remplit ce rôle utilise un compte générique appelé la réception. Ainsi, quand une nouvelle personne occupe le poste, tout ce qui est nécessaire est de changer le mot de passe de l'utilisateur concerné. Les applications, paramètres, documents, mails et autres resteront compatibles.

Outils

Le tableau suivant répertorie les outils référencés par ce module :

| Outil | Utilisé pour | Emplacement |
|--|---|--|
| Windows PowerShell | Ligne de commande et script de toutes les tâches administratives. | Natif du système d'exploitation. |
| Centre d'administration Active Directory | Effectuer des tâches administratives au jour le jour dans AD DS. | Dans le Gestionnaire de serveur, sous Outils ou dans Panneau de contrôle dans Outils administratifs . |
| Utilisateurs et ordinateurs Active Directory | Exécution journalière des tâches administratives dans AD DS. | Dans le Gestionnaire de serveur, sous Outils ou dans Panneau de contrôle dans Outils administratifs . |
| Assistant Délégation de contrôle | Affectation des autorisations d'effectuer des tâches administratives. | Faites un clic droit sur une unité d'organisation dans Utilisateurs et ordinateurs Active Directory. |

Meilleures pratiques

Retenez les meilleures pratiques suivantes pour administration AD DS :

- Évitez d'utiliser les groupes intégrés afin de déléguer l'accès administratif à moins que vous comprenez toutes les autorisations accordées par l'appartenance au groupe
- Créer des groupes administratifs spécialisés et leur affecter seulement les droits et autorisations requis pour exécuter les tâches assignées
- Développer des scripts Windows PowerShell pour effectuer des tâches répétitives
- Ne pas vous connecter avec votre compte administratif pour les activités au jour le jour. Ne l'utilisez que lorsque vous avez besoin d'effectuer une tâche administrative

Problèmes courants et conseils de dépannage

| Problème courant | Conseil pour la résolution du problème |
|--|--|
| Les utilisateurs ne peuvent pas accéder aux ressources réseau. | |
| Vous avez affecté à un utilisateur des droits d'administration dans AD DS, mais il dit qu'il n'a pas d'outil pour effectuer la tâche | |

Module 3

Gestion avancée de l'infrastructure AD DS

Sommaire :

| | |
|---|------|
| Vue d'ensemble du module | 3-1 |
| Leçon 1 : Vue d'ensemble des déploiements AD DS avancés | 3-2 |
| Leçon 2 : Déploiement d'un environnement AD DS distribué | 3-11 |
| Leçon 3 : Configuration d'approbations AD DS | 3-26 |
| Atelier pratique : Domaine et gestion des approbations dans AD DS | 3-32 |
| Révision du module et éléments à retenir | 3-35 |

Vue d'ensemble du module

Pour la plupart des organisations, le déploiement des services de domaine Active Directory (AD DS) peut être l'élément le plus important dans l'infrastructure des TI. Lorsque les organisations déplacent des services AD DS ou d'autres services liés au Active directory au sein du système d'exploitation Windows Server 2016, elles mettent en place un service d'authentification et d'autorisation central qui fournit un accès à autorisation unique (SSO) à de nombreux autres services réseau et applications dans l'organisation. L'AD DS permet également une gestion basée sur les stratégies pour les comptes d'utilisateur et d'ordinateur.

La plupart des organisations déplacent un seul domaine AD DS. Cependant, certaines organisations ont également des exigences qui nécessitent un déploiement de AD DS plus complexe qui peut inclure plusieurs domaines ou forêts.

Ce module décrit les éléments clés d'un environnement AD DS avancé et explique comment installer et configurer un déploiement AD DS avancé.

Objectifs

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

- Décrire les composants de déploiements AD DS avancés ;
- Expliquer comment déployer un environnement AD DS distribué ;
- Expliquer comment configurer les approbations AD DS.

Leçon 1

Vue d'ensemble des déploiements AD DS avancés

Avant de commencer à configurer un déploiement AD DS avancé, il est important de connaître les éléments qui constituent la structure AD DS et comment ils interagissent les uns avec les autres pour permettre d'offrir un environnement TI évolutif et sûr. La leçon commence par l'examen des différentes composantes d'un environnement AD DS, puis par l'exploration des raisons pour lesquelles une organisation peut choisir de déployer un environnement AD DS complexe.

Objectifs de la leçon

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

- Expliquer comment les domaines AD DS et les forêts forment des limites pour la sécurité et l'administration
- Décrire les raisons d'avoir plus d'un domaine dans un environnement AD DS ;
- Expliquer les raisons d'avoir plus d'une forêt dans un environnement AD DS ;
- Expliquer les scénarios et les facteurs à considérer pour déployer AD DS dans l'infrastructure Microsoft Azure en tant que service (IaaS) ;
- Expliquer comment gérer l'utilisateur, le groupe et les objets d'ordinateur dans les déploiements AD DS complexes.

Vue d'ensemble des limites de domaine et de forêt dans une structure AD DS

Les domaines AD DS et les forêts offrent différents types de frontières au sein d'un déploiement AD DS. Il est essentiel de bien comprendre les différents types de limites pour gérer un environnement AD DS complexe.

Limites de domaine AD DS

Le domaine AD DS fournit les limites suivantes :

- Limite de réplication pour la partition de domaine. Tous les objets AD DS qui existent dans un seul domaine sont stockés dans la partition de domaine dans la base de données AD DS sur chaque contrôleur de domaine dans le domaine. Le processus de réplication garantit que toutes les mises à jour qu'il produit sont répliquées à tous les autres contrôleurs de domaine dans le même domaine. Les données de la partition de domaine ne sont pas répliquées aux contrôleurs de domaine dans d'autres forêts.
- Limites liées à l'administration. Par défaut, un domaine AD DS comprend plusieurs groupes, comme le groupe des administrateurs du domaine. Le groupe des administrateurs du domaine a le contrôle administratif complet sur le domaine. Vous pouvez également attribuer des autorisations d'administration à des comptes d'utilisateur et à des groupes au sein de domaines. À l'exception du groupe des administrateurs de l'entreprise dans le domaine racine de forêt, les comptes administratifs ne disposent pas de droits d'administration dans d'autres domaines de la forêt ou dans d'autres forêts.

| Objet AD DS | Type de limite |
|-------------|---|
| Domaine | Réplication de partition de domaine |
| | Autorisations administratives |
| | Application de la stratégie de groupe |
| | Audit |
| Forêt | Stratégie de mot de passe et de compte |
| | Réplication de zone DNS de domaine |
| | Sécurité |
| | Réplication de partition de schéma |
| | Réplication de partition de configuration |
| | Réplication du catalogue global |
| | Réplication de zone DNS de forêt |

- Limite de l'application de la stratégie de groupe. Vous pouvez lier les stratégies de groupe aux niveaux suivants : local, site, domaine et unité d'organisation (UO). En dehors des stratégies de groupe au niveau du site, l'étendue des stratégies de groupe est le domaine AD DS. Il n'y a pas d'héritage pour les stratégies de groupe d'un domaine AD DS à l'autre, même si un domaine AD DS est plus bas dans la hiérarchie qu'un autre dans une arborescence de domaine.
- Limite liée à l'audit. L'audit est géré de manière centralisée à l'aide d'objets de stratégie de groupe (GPO). L'étendue maximale de ces paramètres est le domaine AD DS. Vous pouvez avoir les mêmes paramètres d'audit dans les différents domaines AD DS, mais vous devez les gérer séparément dans chaque domaine.
- Mot de passe et limites de la stratégie de compte. Par défaut, le mot de passe et les stratégies de compte sont définis au niveau du domaine et appliqués à tous les comptes de domaine. Bien qu'il soit possible de configurer des stratégies de mot de passe à granularité élevée pour configurer différentes stratégies pour des utilisateurs particuliers dans un domaine, vous ne pouvez pas appliquer le mot de passe et les stratégies de compte au-delà de l'étendue d'un seul domaine.
- Limite de réPLICATION pour les zones du système DNS (Domain Name System). L'une des options lorsque vous configurez des zones DNS dans un environnement AD DS est de configurer des zones intégrées au Active Directory. Cela signifie qu'au lieu de stocker localement les enregistrements DNS sur chaque serveur DNS dans des fichiers texte, ils sont stockés et reproduits dans la base de données AD DS. L'administrateur peut alors décider de répliquer les informations DNS à :
 - Tous les contrôleurs de domaine dans le domaine (peu importe s'il s'agit de serveurs DNS) ;
 - Tous les contrôleurs de domaine qui sont des serveurs DNS dans le domaine AD DS ;
 - Tous les contrôleurs de domaine qui sont des serveurs DNS dans la forêt.

Par défaut, lorsque vous déployez le premier contrôleur de domaine dans un domaine AD DS et que vous configurez ce serveur en tant que serveur DNS, vous créez deux partitions de réPLICATION distinctes appelées DomainDnsZones et ForestDNSZones. La partition DomainDnsZones contient les enregistrements DNS propres au domaine et est répliquée seulement à d'autres serveurs DNS qui sont également contrôleurs de domaine AD DS dans le domaine.

Limites de la forêt AD DS

La forêt AD DS présente les limites suivantes :

- Limite de sécurité ; La limite de la forêt est une limite de sécurité parce que, par défaut, aucun compte en dehors de la forêt n'a des autorisations d'administration à l'intérieur de la forêt.
- Limite de réPLICATION pour la partition de schéma ; La partition de schéma contient les règles et la syntaxe pour la base de données AD DS. Ceci est ensuite répliqué vers tous les contrôleurs de domaine dans la forêt AD DS.
- Limite de réPLICATION pour la partition de configuration ; La partition de configuration contient les détails de la structure du domaine AD DS, notamment : les domaines, les contrôleurs de domaine, les partenaires de réPLICATION, les informations sur le site et le sous-réseau et l'autorisation DHCP (Dynamic Host Configuration Protocol) ou la configuration de contrôle d'accès dynamique. La partition de configuration contient également des informations concernant les applications qui sont intégrées à la base de données AD DS. Un exemple d'une application est le serveur Exchange. La partition est répliquée vers tous les contrôleurs de domaine dans la forêt.
- Limite de réPLICATION pour le catalogue global ; Le catalogue global est la liste en lecture seule contenant chaque objet dans toute la forêt AD DS. Pour le maintenir à une taille gérable, le catalogue global ne contient que certains attributs de chaque objet. Le catalogue global est répliqué vers tous les contrôleurs de domaine dans toute la forêt qui sont également des serveurs du catalogue global.

- Limite de réPLICATION pour les zones DNS de la forêt ; La partition forestDnsZones est répliquée vers tous les contrôleurs de domaine dans la forêt entière qui sont également des serveurs DNS. Cette zone contient des enregistrements qui sont importants pour activer la résolution de noms DNS à l'échelle de la forêt.

Pourquoi implémenter plusieurs domaines ?

De nombreuses organisations peuvent fonctionner de manière adéquate avec un seul domaine AD DS. Cependant, d'autres organisations ont des besoins qui nécessitent le déploiement de plusieurs domaines. Parmi ces besoins, on retrouve les suivants :

- Besoins de réPLICATION de domaine. Dans certains cas, les organisations ont plusieurs grands bureaux qui sont reliés par des réseaux étendus (WAN) lents ou peu fiables. Les connexions réseau peuvent ne pas avoir suffisamment de bande passante pour prendre en charge la réPLICATION AD DS de la partition de domaine. Dans de tels cas, l'installation d'un domaine AD DS distinct dans chaque bureau est préférable.
- Exigences pour l'espace de noms DNS Certaines organisations exigent plus d'un espace de noms DNS dans une forêt AD DS. Cela est généralement le cas lorsqu'une société acquiert une autre société ou fusionne avec une autre organisation, et qu'il est nécessaire de préserver les noms de domaine de l'environnement existant. Il est possible de fournir plusieurs noms d'utilisateurs principaux (UPN) pour les utilisateurs dans un seul domaine, mais dans ce scénario, de nombreuses organisations choisissent de déployer plusieurs domaines.
- Exigences administratives distribuées Les organisations peuvent devoir se doter d'un modèle d'administration distribué pour des besoins de sécurité de l'entreprise ou politiques. Les organisations peuvent atteindre l'autonomie administrative en déployant un domaine distinct. Grâce à ce déploiement, les administrateurs de domaine ont un contrôle complet sur leurs domaines.

Les organisations peuvent choisir de déployer des domaines multiples pour répondre à :

- Des exigences de réPLICATION de domaine
- Des exigences de l'espace de noms DNS
- Des exigences administratives distribuées
- Des exigences de sécurité de groupe administratif de forêt
- Des exigences de domaine de ressources



Remarque : Le déploiement de domaines distincts fournit une autonomie administrative, mais non l'isolement administratif. La seule façon d'assurer l'isolement administratif est de déployer une forêt distincte.

- Exigences en matière de sécurité du groupe d'administration de la forêt. Certaines organisations peuvent choisir de déployer un domaine racine dédié ou vide. C'est un domaine qui ne possède pas de comptes d'utilisateurs autres que les comptes de domaine racine de la forêt par défaut. Le domaine racine de la forêt AD DS a deux groupes (le groupe des administrateurs du schéma et le groupe des administrateurs de l'entreprise), qui n'existent pas dans un autre domaine dans la forêt AD DS. Parce que ces groupes ont des droits étendus dans la forêt AD DS, vous pouvez décider de restreindre l'utilisation de ces groupes en utilisant uniquement le domaine racine de la forêt AD DS pour les stocker.

- Exigences pour le domaine ressource. Certaines organisations déploient des domaines de ressources pour déployer des applications spécifiques. Grâce à ce déploiement, tous les comptes d'utilisateurs sont situés dans un domaine, alors que les serveurs d'applications et les comptes d'administration de l'application sont déployés dans un domaine distinct. Cela permet aux administrateurs d'applications d'avoir des autorisations administratives complètes dans le domaine de ressources sans activer les autorisations dans le domaine qui contient les comptes d'utilisateur réguliers.

 **Remarque :** Il est conseillé de choisir la configuration la plus simple pour atteindre l'objectif requis; c'est moins coûteux à implémenter et plus facile à administrer.

Pourquoi implémenter plusieurs forêts ?

Les organisations peuvent parfois exiger que leur conception de AD DS contienne plus d'une forêt. Il y a plusieurs raisons pour lesquelles une seule forêt AD DS peut ne pas suffire :

- Exigences de l'isolement de sécurité Si une organisation nécessite l'isolement administratif entre deux ou plusieurs parties de l'organisation, il faut déployer plusieurs forêts AD DS. Des forêts AD DS distinctes sont souvent déployées par les fournisseurs qui travaillent pour la défense du gouvernement et pour d'autres organisations pour lesquelles l'isolement de la sécurité est une exigence. Dans Windows Server 2016, AD DS inclut une nouvelle fonctionnalité appelée Privileged Access Management (PAM), qui utilise une forêt bastion distincte pour isoler les comptes privilégiés afin de les protéger contre les techniques de vol d'informations d'identification.
- Exigences de schéma incompatibles. Certaines organisations peuvent exiger plusieurs forêts, car elles nécessitent des schémas incompatibles ou des procédures de modification de schéma incompatible. Tous les domaines d'une forêt partagent le schéma.
- Exigences multinationales. Certains pays ont des règles strictes concernant la propriété ou la gestion des entreprises dans le pays. Avoir une forêt AD DS distincte peut fournir l'isolement administratif requis par les lois.
- Exigences en matière de sécurité pour l'Extranet. Certaines organisations déploient plusieurs serveurs dans un réseau de périmètre. Ces serveurs peuvent avoir besoin de AD DS pour authentifier les comptes d'utilisateur ou ils peuvent utiliser AD DS pour appliquer des stratégies sur les serveurs du réseau de périmètre. Pour veiller à ce que les services AD DS extranet soient aussi sécurisés que possible, les organisations configurent souvent une forêt AD DS distincte dans le réseau de périmètre.
- Exigences en matière de fusion ou de cession d'entreprises. Les fusions d'entreprises sont parmi les raisons les plus courantes pour lesquelles les organisations se dotent de plusieurs forêts AD DS. Lorsque des organisations fusionnent ou qu'une organisation en achète une autre, elles doivent évaluer la nécessité de fusionner leurs forêts AD DS. La fusion des forêts AD DS offre les avantages d'une collaboration et d'une administration simplifiées. Toutefois, si les deux groupes différents dans l'organisation doivent être gérés séparément, et qu'une collaboration est peu nécessaire, cela ne vaut pas la peine d'engager des dépenses pour fusionner deux forêts. En particulier, si l'on planifie de vendre une partie de l'entreprise, il est préférable de conserver les deux organisations en tant que forêts distinctes.

Les entreprises peuvent choisir de déployer des forêts multiples pour répondre à :

- Des exigences d'isolement de sécurité :
 - PAM dans Windows Server 2016 AD DS utilise une forêt de bastion séparée pour isoler les comptes privilégiés afin de les protéger contre les techniques de vol d'informations d'identification.
- Des exigences de schéma incompatible
- Des exigences multinationales
- Des exigences de sécurité Extranet
- Des exigences de fusion ou de cession d'entreprise



Méthode conseillée : il est conseillé de choisir la configuration la plus simple pour atteindre l'objectif requis; cela est moins coûteux à implémenter et plus facile à administrer.

Le déploiement d'un contrôleur de domaine dans Azure IaaS

Microsoft Azure fournit l'infrastructure en tant que service (IaaS), qui est essentiellement la virtualisation dans l'infonuage. Tous les facteurs à considérer pour la virtualisation des applications et des serveurs dans une infrastructure sur site s'appliquent pour le déploiement des mêmes applications et serveurs à Azure. Lors du déploiement de Active Directory dans Azure, vous installez le contrôleur de domaine sur une machine virtuelle, de sorte que toutes les règles applicables à la virtualisation d'un contrôleur de domaine s'appliquent au déploiement de Active Directory dans Azure. Vous pouvez installer AD DS sur les ordinateurs virtuels Azure pour soutenir une variété de scénarios :

- Récupération d'urgence. Dans un scénario lors duquel vos contrôleurs de domaine sur site sont détruits ou indisponibles, des ordinateurs virtuels Azure fonctionnant en tant que répliques des contrôleurs de domaine feront une copie complète de votre base de données AD DS. Cela peut aider à accélérer la récupération et c'est une solution à faible coût pour les organisations qui ne disposent pas d'un site de récupération d'urgence physique.
- Contrôleurs de domaine géo-distribués. Si votre organisation est très décentralisée, les ordinateurs virtuels Azure fonctionnant en tant que répliques de contrôleurs de domaine peuvent fournir des connexions à faible latence pour améliorer les performances d'authentification. Vous pouvez réaliser cela en exécutant les contrôleurs de domaine dans différentes régions Azure qui correspondent aux endroits où il ne serait pas rentable pour votre organisation de déployer l'infrastructure physique.
- Authentification des utilisateurs pour des applications isolées. Si vous devez déployer une application avec une dépendance AD DS, mais que l'application ne nécessite pas la connectivité avec l'environnement AD DS de l'entreprise, vous pouvez déployer une forêt distincte sur les ordinateurs virtuels Azure.



Remarque : Bien que les serveurs sur site et les clients membres peuvent communiquer avec les contrôleurs de domaine Azure, ces contrôleurs de domaine ne devraient jamais être les seuls contrôleurs de domaine dans un environnement hybride. Une perte de connectivité à partir de votre environnement Azure sur site empêche le fonctionnement de l'authentification et d'autres domaines si vous n'exécutez pas aussi les services AD DS dans votre environnement sur site.

Lorsque vous implémentez AD DS dans Azure, prenez en considération les points suivants :

- Topologie du réseau. Pour répondre aux exigences de AD DS, vous devez créer un réseau virtuel Microsoft Azure et y joindre vos ordinateurs virtuels. Si vous avez l'intention de vous joindre à une infrastructure AD DS sur site existante, vous pouvez choisir d'étendre la connectivité réseau à votre environnement sur site. Ceci est réalisé soit par l'entremise d'un réseau privé virtuel (VPN) standard, soit par un circuit Azure ExpressRoute, en fonction de la vitesse, de la fiabilité et de la sécurité que votre organisation exige.



Remarque : Un circuit Azure ExpressRoute est une méthode pour connecter votre infrastructure sur site aux services infonuagiques de Microsoft par l'entremise d'un fournisseur de connectivité dédié qui n'utilise pas l'Internet public.

- Topologie du site. Comme pour un site physique, vous devez définir et configurer un site AD DS qui correspond à l'espace d'adressage IP de votre réseau virtuel Azure. Parce que l'utilisation d'un réseau virtuel Azure engage des frais de passerelle supplémentaires pour tout le trafic sortant de votre environnement local, vous devez soigneusement planifier vos sites AD DS et les liens de site pour minimiser les coûts. Parce que la transitivité des liens de site AD DS est activée par défaut, vous devriez envisager de désactiver l'option afin de créer un pont pour tous les liens de site si vous avez plus de 2 sites. Si vous laissez la fonction pontage de lien de site activée, AD DS présume que tous les sites de votre déploiement ont une connectivité directe les uns avec les autres, et cela peut faire que votre site AD DS Azure ait de nombreux partenaires de réPLICATION. Assurez-vous de ne pas activer la notification de modification des liens de sites que comprend votre site AD DS Azure. La raison est que cela remplace tous les intervalles de réPLICATION configurés sur le lien du site, ce qui entraîne une réPLICATION fréquente et souvent inutile. Si une copie inscriptible de AD DS n'est pas nécessaire, vous devriez envisager de déployer un contrôleur de domaine en lecture seule (RODC) afin de limiter davantage la quantité de trafic sortant créé par la réPLICATION de AD DS.



Remarque : Les sites AD DS, les liens de sites et la réPLICATION sont traités plus en détail dans un module ultérieur.

- Réparation de service. Bien que Azure ne fournit pas de services de restauration directement aux clients, les serveurs Azure peuvent être restaurés dans le cadre normal d'une maintenance lors de la récupération d'une défaillance de service. La réPLICATION du contrôleur de domaine dépend du numéro de séquence de la mise à jour : (USN) ; quand un système AD DS est restauré, il serait possible de créer un double du USN. Pour éviter cela, Windows Server 2012 AD DS a introduit un nouvel identifiant nommé *ID VM-Generation*. L'*ID VM-Generation* peut détecter une restauration et empêcher un contrôleur de domaine virtualisé de répliquer des modifications sortantes jusqu'à ce que les services AD DS virtualisés aient convergé avec les autres contrôleurs de domaine dans le domaine.



Remarque : Les ordinateurs virtuels Azure exécutant le rôle de contrôleur de domaine doivent toujours être fermés par l'entremise du système d'exploitation invité et jamais par le portail Azure. Initier un arrêt par l'intermédiaire du portail Azure libère l'ordinateur virtuel, ce qui entraîne une remise à zéro de l'identifiant ID VM-Generation.

- Adresses IP. Tous les ordinateurs virtuels Azure reçoivent des adresses DHCP par défaut, mais vous pouvez configurer des adresses statiques grâce à Azure PowerShell qui persisteront entre les redémarrages, les arrêts, et la réparation de service. Les ordinateurs virtuels Azure qui doivent être l'hôte du contrôleur de domaine ou du rôle de DNS en utilisant le cmdlet **Set-AzureStaticVNetIP**, afin que l'IP ne soit jamais libéré si l'ordinateur virtuel est arrêté. Vous devez d'abord configurer le réseau virtuel Azure avant de configurer les contrôleurs de domaine Azure.
- DNS Le système DNS intégré à Azure ne répond pas aux exigences de AD DS, comme le système DNS dynamique et les enregistrements de services (enregistrements SRV). Avant de pouvoir prolonger votre environnement AD DS sur site à un ordinateur virtuel Azure, vous devez approvisionner et configurer le réseau virtuel Azure à un serveur DNS sur site.

- Disques. Les ordinateurs virtuels Azure utilisent la mise en cache de l'hôte en lecture-écriture pour le système d'exploitation (OS) des disques durs virtuels. Bien que cela puisse améliorer la performance de l'ordinateur virtuel, si les composants AD DS sont installés sur le disque du système d'exploitation, la perte de données est possible dans le cas d'une défaillance de disque. La mise en cache peut être désactivée dans les disques durs Azure supplémentaires attachés à un ordinateur virtuel. Lorsque vous installez Active Directory dans Azure, vous devez localiser les dossiers NTDS.DIT et SYSVOL sur un disque de données supplémentaires dans l'ordinateur virtuel Azure avec le réglage **préférences de cache d'hôte** configuré à **AUCUN**. Cependant, gardez à l'esprit que les disques de données Azure ont une limite de taille à 1 téraoctet (To).

Gestion des objets dans les déploiements complexes de AD DS

Dans les petits déploiements de AD DS consistant en un seul domaine et forêt, des outils intégrés tels que la console de gestion **Centre d'administration Active Directory** ou **Utilisateurs et ordinateurs Active Directory** sont généralement suffisants pour gérer l'utilisateur, le groupe et les objets Ordinateur dans votre organisation. Cependant, à titre d'administrateur d'un environnement complexe de AD DS, vous gérerez des millions d'objets dans plusieurs forêts et domaines, ce qui rend les tâches beaucoup plus pénibles et difficiles si ce sont les seuls outils disponibles pour vous. Dans ces situations, vous pouvez avoir besoin d'implémenter des processus de gestion des identités de pointe pour gérer les différents problèmes associés à l'administration. Prenez les scénarios suivants :

- Les problèmes potentiels comprennent :
 - La gestion des utilisateurs et des groupes
 - Le libre-service de l'utilisateur
 - La gestion des certificats
 - La synchronisation d'identité
- Microsoft Identity Manager 2016 fournit :
 - Des identités prêtes au cloud pour Azure Active Directory
 - De puissantes fonctionnalités utilisateur en libre-service avec authentification multifacteurs
 - Gestion des accès à distance privilégiés

- Gestion de l'Utilisateur. Lors de déploiements complexes de AD DS, il n'est généralement pas possible pour un administrateur de tenir à jour les objets utilisateurs manuellement. Les tâches telles que la création de nouveaux comptes d'utilisateurs, la mise à jour du service d'un utilisateur ou la configuration d'une boîte aux lettres pour un serveur Microsoft Exchange doivent généralement être traitées par un workflow automatisé qui est entrepris par la source de données faisant autorité. Par exemple, vous pouvez décider de créer automatiquement des comptes d'utilisateurs AD DS dans un domaine spécifique pour les nouveaux employés, selon les données de la demande d'emploi des RH de votre organisation. Si le service de l'employé est modifié dans la demande d'emploi des RH, vous voudrez peut-être que cette même modification se reflète sur l'objet utilisateur AD DS correspondant. La manipulation de ces tâches à l'aide d'un workflow automatisé est généralement plus efficace et moins sujette à l'erreur humaine.
- Gestion des groupes. Comme pour la gestion des objets de l'utilisateur, la gestion manuelle des groupes dans des déploiements complexes de AD DS peut présenter plusieurs défis. Parce que les modifications d'appartenance à un groupe peuvent souvent exiger une autorisation, vous pouvez décider de déléguer la gestion des objets de groupe à une personne ou à un groupe de personnes désignées. Cependant, pour les non-administrateurs, la gestion des objets de groupe peut ne pas être un processus intuitif. Dans certains cas, déléguer la gestion des groupes peut encore entraîner de l'inefficacité qui pourrait être mieux traitée par l'automatisation. Par exemple, l'accès basé sur les rôles dans votre organisation peut dépendre du service auquel un objet utilisateur est assigné. Plutôt que de tenir à jour manuellement un groupe de sécurité pour chaque service dans l'organisation, il peut être plus efficace de tirer profit de l'automatisation pour mettre à jour l'appartenance à un groupe basée sur le service auquel est assigné l'utilisateur.

- Libre-service de l'utilisateur. L'implémentation du libre-service de l'utilisateur pour les tâches telles que le déverrouillage de comptes et la réinitialisation des mots de passe peut vous aider à soulager d'une grande partie des frais administratifs associés aux déploiements complexes de AD DS.
- Gestion des certificats. Dans un déploiement de AD DS typique, vous pouvez avoir une autorité de certification Active Directory (AD CS) par forêt. Par conséquent, dans les déploiements complexes de AD DS comprenant plusieurs forêts, vous pouvez avoir plusieurs autorités de certification à gérer. Dans cette situation, tenir à jour les modèles requis, les stratégies d'inscription automatique et la révocation des certificats d'utilisateurs mis hors service dans plusieurs forêts peut être un défi.
- Synchronisation d'identité. Alors que les organisations sont de plus en plus dans l'infonuage, vous pouvez avoir besoin de synchroniser les identités des utilisateurs avec des services infonuagiques tels que Azure Active Directory afin de tirer parti d'offres comme Office 365 ou l'authentification multifactorielle. Vous pouvez également avoir plusieurs banques d'authentification sur site ou des applications métier héritées nécessitant la synchronisation des données de l'utilisateur afin qu'elles soient cohérentes dans chaque source.

Microsoft Identity Manager 2016

Pour faire face à la plupart des scénarios ci-dessus, vous pouvez envisager le déploiement d'une plate-forme de gestion des identités et de l'accès comme Microsoft Identity Manager (MIM) 2016. MIM 2016 peut parfaitement préparer vos identités AD DS existantes pour l'infonuage; il offre également de puissantes capacités de libre-service pour l'utilisateur et des fonctionnalités de sécurité renforcée pour soutenir votre infrastructure sur site ou hybride :

- Identités prêtes pour l'infonuage. MIM 2016 peut préparer automatiquement les identités AD DS pour la synchronisation grâce à Azure Active Directory en normalisant les attributs et valeurs de l'utilisateur AD DS.
- Libre-service de l'utilisateur. MIM 2016 offre à vos utilisateurs des fonctions de déverrouillage de compte ou de réinitialisation de mot de passe en utilisant l'authentification multifacteurs. Il permet également aux utilisateurs de créer et de tenir à jour des groupes à l'aide de l'approbation des workflows et prend en charge la gestion des certificats dans des scénarios multiforest.
- Sécurité améliorée. PAM dans MIM 2016 tire parti d'une forêt AD DS distincte afin d'offrir une sécurité supplémentaire limitée dans le temps pour les comptes administrateur.

Testez vos connaissances

| Question | |
|--|---------------------------------------|
| Laquelle des conditions suivantes nécessite l'implémentation du déploiement de plusieurs forêts AD DS ? | |
| Sélectionnez la réponse correcte. | |
| | Exigences de l'isolement de sécurité |
| | Exigences de schéma |
| | Exigences de l'espace de noms DNS |
| | Fusions d'entreprises |
| | Exigences administratives distribuées |

Testez vos connaissances

| Question | |
|---|---|
| Avant de déployer un réplica de contrôleur de domaine AD DS sur un ordinateur virtuel Azure, quelles exigences de la liste ci-dessous doivent être remplies ? | |
| Sélectionnez la réponse correcte. | |
| | Créer un site AD DS pour contrôler la réplication de vos réseaux sur site au réseau virtuel Azure. |
| | Ajouter un disque dur supplémentaire à l'ordinateur virtuel pour lequel on a désactivé la mise en cache lecture-écriture. |
| | Créer et configurer un réseau virtuel Azure. |
| | Créer manuellement des enregistrements SRV requis dans une zone DNS Azure pour votre domaine. |
| | Configurer l'adresse IP dynamique initiale de l'ordinateur virtuel pour qu'il soit statique en utilisant le cmdlet Set-AzureStaticVNetIP . |

Leçon 2

Déploiement d'un environnement AD DS distribué

Certaines organisations doivent déployer plusieurs domaines ou même plusieurs forêts. Le déploiement de contrôleurs de domaine AD DS dans ce scénario est semblable au déploiement des contrôleurs de domaine dans un environnement de domaine unique, mais il y a des facteurs particuliers que vous devez considérer.

Dans cette leçon, vous apprendrez à déployer un environnement AD DS complexe, et vous verrez comment le mettre à niveau à partir d'une version antérieure de AD DS.

Objectifs de la leçon

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

- Décrire les niveaux fonctionnels du domaine AD DS ;
- Décrire les niveaux fonctionnels de la forêt AD DS ;
- Décrire le déploiement de nouveaux domaines AD DS ;
- Installer un contrôleur de domaine dans un nouveau domaine dans une forêt.
- Expliquer comment mettre à niveau une version précédente de AD DS vers Windows Server 2016 ;
- Expliquer comment migrer vers Windows Server 2016 AD DS à partir d'une version précédente ;
- Décrire les éléments dont il faut tenir compte pour l'implémentation d'un environnement AD DS complexe.

Domaine des niveaux fonctionnels AD DS

Les domaines AD DS peuvent fonctionner à différents niveaux fonctionnels. En règle générale, la mise à niveau du domaine à un niveau fonctionnel supérieur introduit des fonctionnalités supplémentaires. Le tableau suivant présente certains des niveaux fonctionnels de domaine.

- Une nouvelle fonctionnalité exige que les contrôleurs de domaine exécutent une version particulière de Windows :
 - Windows Server 2003
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
 - Aperçu technique Windows Server 2016
- Vous ne pouvez pas augmenter le niveau fonctionnel si les contrôleurs de domaine exécutent des versions précédentes de Windows Server.
- Vous ne pouvez pas ajouter de contrôleurs de domaine exécutant des versions précédentes de Windows Server après avoir augmenté le niveau fonctionnel.

| Niveau fonctionnel de domaine | Fonctionnalités |
|--|--|
| Natif de Microsoft Windows Server 2000 | <p>Les fonctionnalités comprennent :</p> <ul style="list-style-type: none"> • Groupes universels. • Imbrication de groupe. • Conversion du groupe, de la sécurité à la distribution ou vice versa. • Identificateur de sécurité (SID) - Historique. <p> Remarque : Vous ne pouvez pas installer les contrôleurs de domaine de Windows Server 2016 dans un domaine fonctionnant au niveau natif de Windows Server 2000.</p> |

| Niveau fonctionnel de domaine | Fonctionnalités |
|-------------------------------|--|
| Windows Server 2003 | <p>Les fonctionnalités comprennent :</p> <ul style="list-style-type: none"> • Netdom.exe. Cet outil de gestion de domaine permet de renommer les contrôleurs de domaine. • LastLogonTimestamp. Cet attribut se souvient du moment de la dernière connexion au domaine par les utilisateurs et le réplica vers les autres contrôleurs de domaine AD DS dans le domaine AD DS. • Prise en charge de l'objet InetOrgPerson. L'objet InetOrgPerson est défini dans Internet RFC 2798 et il est utilisé pour fédérer avec les services d'annuaire externes. • Redirection. Cette fonction vous offre la possibilité de rediriger l'emplacement par défaut pour les objets d'utilisateur et d'ordinateur. • Délégation contrainte. Cette fonctionnalité permet aux applications de tirer parti de la délégation sécurisée des informations d'identification d'utilisateurs en utilisant l'authentification Kerberos. • Authentification sélective. Cette fonction vous permet de préciser les utilisateurs et groupes qui sont autorisés à s'authentifier auprès de serveurs de ressources spécifiques dans une forêt d'approbation. • Partitions d'application. Elles sont utilisées pour stocker des informations pour les applications intégrées Active Directory. Le système DNS intégré à Active Directory utilise une partition d'application, ce qui permet à la partition de DNS d'être répliquée vers les contrôleurs de domaine qui sont également des serveurs DNS dans le domaine, ou même dans l'ensemble de la forêt. |
| Windows Server 2008 : | <p>Les fonctionnalités comprennent :</p> <ul style="list-style-type: none"> • La réPLICATION du système de fichiers DFS (Distributed File System) est disponible en tant que mécanisme de réPLICATION de fichiers qui est plus efficace et plus robuste que le service de réPLICATION de fichiers (FRS) utilisé pour les dossiers SYSVOL. • Les informations d'ouverture de session interactive supplémentaires sont stockées pour chaque utilisateur, au lieu de tout simplement pour la dernière ouverture de session. • Les réglages des mots de passe à granulométrie fine permettent de régler des stratégies de verrouillage de mot de passe pour les utilisateurs et les groupes, en remplaçant les paramètres de domaine par défaut pour ces utilisateurs ou membres du groupe. • Les bureaux virtuels personnels sont disponibles pour que les utilisateurs puissent se connecter à l'aide de RemoteApp et Bureau à distance. • La prise en charge des services avancés de chiffrement (AES 128 et 256) pour Kerberos est offerte. • RODC fournit un moyen sûr et économique d'offrir des services de connexion AD DS dans les sites éloignés, sans stocker des informations confidentielles (comme les mots de passe) dans des environnements non approuvés. |
| Windows Server 2008 R2 | <p>Les fonctionnalités comprennent :</p> <ul style="list-style-type: none"> • L'assurance du mécanisme d'authentification ; regroupe les informations sur la méthode de connexion d'un utilisateur et peut être utilisée en conjonction avec l'application d'authentification, par exemple, avec les services AD FS (Active Directory Federation Services). |

| Niveau fonctionnel de domaine | Fonctionnalités |
|--------------------------------------|--|
| | <p>Dans un autre exemple, vous pouvez autoriser les utilisateurs qui se connectent à l'aide d'un accès de carte à puce à accéder à plus de ressources que lorsqu'ils se connectent avec un nom d'utilisateur et un mot de passe.</p> <ul style="list-style-type: none"> La gestion automatisée du nom de principal du service (SPN) des comptes de services gérés est disponible. Les comptes de services gérés permettent de gérer les mots de passe par le système d'exploitation Windows. |
| Windows Server 2012 : | <p>Le niveau fonctionnel du domaine de Windows Server 2012 n'implémente pas de nouvelles fonctionnalités du niveau fonctionnel de Windows 2008 R2. Une exception prévaut toutefois. Si le Centre de distribution de clés (KDC) prend en charge les réclamations, l'authentification composée et le blindage Kerberos est configuré pour toujours fournir les réclamations ou faire rejeter les demandes d'authentification non blindées, ces fonctionnalités ne seront pas activées tant que le domaine est également réglé à Windows Server 2012.</p> |
| Windows Server 2012 R2 | <p>Les fonctionnalités comprennent :</p> <ul style="list-style-type: none"> Les protections du côté du contrôleur du domaine pour les utilisateurs protégés. Le groupe des utilisateurs protégés a été introduit dans Windows Server 2012 R2. Les membres du groupe des utilisateurs protégés ne peuvent plus : <ul style="list-style-type: none"> S'authentifier avec l'authentification NTLM, l'authentification Digest, ou CredSSP. Les périphériques de Windows 8.1 ne cachent pas les mots de passe des utilisateurs protégés. Utiliser le Data Encryption Standard (DES) ou les suites de chiffrement Rivest Cipher 4 (RC4) dans la préauthentification Kerberos. Les domaines doivent être configurés pour prendre en charge au moins la suite de chiffrement AES. Être délégués avec la délégation contrainte ou non contrainte. Les connexions pour les utilisateurs protégés à d'autres systèmes peuvent échouer. Renouveler les tickets d'utilisateur (TGT) au-delà de la durée de vie initiale de quatre heures. Au bout de quatre heures, les utilisateurs protégés doivent s'authentifier à nouveau. Les stratégies d'authentification peuvent être appliquées à des comptes dans les domaines Windows R2 2012. La stratégie d'authentification Silos est utilisée pour créer une relation entre les comptes d'utilisateurs, les comptes de services gérés et les comptes d'ordinateur pour les stratégies d'authentification. |
| Aperçu technique Windows Server 2016 | <p>Les fonctionnalités comprennent :</p> <ul style="list-style-type: none"> La gestion de l'accès privilégié est une fonction pour les liens qui arrivent à expiration. Il permet l'adhésion de durée limitée à un groupe de sécurité qui est exprimée en valeur de durée de vie (TTL) liée au ticket de durée de vie Kerberos. Les liens arrivant à expiration sont disponibles sur tous les attributs liés et ne sont pas limités à la relation membre/membre de. |

| Niveau fonctionnel de domaine | Fonctionnalités |
|-------------------------------|---|
| | <ul style="list-style-type: none"> Azure Active Directory améliore l'expérience de l'identité pour le client d'affaires en améliorant les capacités qui s'étendent aux périphériques des sociétés et personnels. Le Microsoft Passport est une nouvelle fonctionnalité d'authentification permettant une connexion biométrique ou avec NIP. Parce que Windows Server 2003 n'est plus pris en charge, nous recommandons d'augmenter les niveaux fonctionnels de votre domaine et forêt au minimum à Windows Server 2008 afin d'assurer la cohérence de la réPLICATION SYSVOL. |

 **Remarque :** Généralement, vous ne pouvez pas restaurer le niveau fonctionnel AD DS de domaine après qu'il a été configuré. Si vous avez implémenté une fonctionnalité qui est disponible uniquement dans un niveau fonctionnel de domaine supérieur, vous ne pouvez pas revenir à un état antérieur. Vous ne pouvez abaisser le niveau fonctionnel de domaine qu'en utilisant le cmdlet PowerShell **Set-ADDomainMode**.

 **Lectures supplémentaires :** Pour plus d'informations sur la publication de la version d'évaluation des fonctionnalités de AD DS dans Windows Server 2016, reportez-vous à : <http://aka.ms/Bxg2z0>

 **Lectures supplémentaires :** Pour plus d'informations sur le domaine des niveaux fonctionnels AD DS, reportez-vous à l'adresse : <http://aka.ms/Ynmvma>

Les niveaux fonctionnels de la forêt AD DS

La forêt AD DS peut fonctionner à différents niveaux fonctionnels et parfois élever le niveau fonctionnel AD DS de la forêt rend disponibles des fonctionnalités supplémentaires. Les caractéristiques supplémentaires les plus notables viennent avec la mise à niveau vers un nouveau niveau fonctionnel de forêt Windows Server. Lorsque vous augmentez le niveau fonctionnel de la forêt, l'ajout de nouveaux domaines est limité par le niveau fonctionnel de la forêt. Les contrôleurs de domaine doivent utiliser des domaines fonctionnels des niveaux qui sont les mêmes que le niveau fonctionnel de la forêt. Par exemple, si le niveau fonctionnel de la forêt est Windows Server 2012 R2, vous ne pouvez pas ajouter un nouveau domaine basé sur les contrôleurs de domaine de Windows Server 2008 R2. Les fonctionnalités supplémentaires qui sont disponibles avec les versions de Windows Server, à partir de Windows Server 2003, comprennent :

- | | |
|--|---|
| Windows Server 2003 : <ul style="list-style-type: none"> Approbation de forêt Renommer un domaine Réplication de valeur liée Amélioration du vérificateur de cohérence des données | Windows Server 2008 : <ul style="list-style-type: none"> Prise en charge RODC Conversion d'objets inetOrgPerson en objets utilisateur Désactivation et redéfinition de classes d'attributs et d'objets |
| Windows Server 2008 R2 : <ul style="list-style-type: none"> Aucune nouvelle fonctionnalité ; définit le niveau minimum pour tous les nouveaux domaines. | Windows Server 2012 R2 : <ul style="list-style-type: none"> Activer la Corbeille d'Active Directory |
| Windows Server 2012 et Windows Server 2012 R2 : <ul style="list-style-type: none"> Aucune nouvelle fonctionnalité ; définit le niveau minimum pour tous les nouveaux domaines. | Windows Server 2016 : <ul style="list-style-type: none"> Aucune nouvelle fonctionnalité ; définit le niveau minimum pour tous les nouveaux domaines. |

- Approbations. La caractéristique fondamentale des forêts est que toutes les approbations de domaine sont des approbations transitives, de sorte que, après avoir reçu l'autorisation, tout utilisateur d'un domaine dans la forêt peut accéder à toutes les ressources de la forêt.

- Approbations de forêt. Il est possible de mettre en place des approbations entre les forêts AD DS pour permettre le partage des ressources. Il y a des approbations complètes et des approbations sélectives.
- RéPLICATION de valeurs liées. Cela présente une réPLICATION améliorée de Windows Server 2000 et la gestion de l'appartenance au groupe. Dans les versions précédentes de AD DS, l'attribut d'appartenance à un groupe pour un groupe a été répliqué en une seule valeur. Cela signifie que si deux administrateurs ont modifié les membres du même groupe dans deux instances différentes de AD DS au cours de la même période de réPLICATION, la dernière écriture a gagné. Les premières modifications apportées seraient perdues parce que la nouvelle version de l'attribut d'appartenance au groupe a entièrement remplacé la précédente. Avec la réPLICATION validée par un lien, l'appartenance à un groupe est traitée au niveau de la valeur ; par conséquent, toutes les mises à jour sont fusionnées. Cela réduit aussi grandement le trafic de réPLICATION. Un avantage supplémentaire de cette fonction est la suppression de la restriction de l'appartenance à un groupe précédent qui limitait le nombre maximal de membres à 5000.
- Amélioration des algorithmes de calcul de réPLICATION AD DS. Le vérificateur de cohérence des données (KCC) et le générateur de topologie intersite (ISTG) utilisent des algorithmes améliorés pour accélérer le calcul de l'infrastructure de réPLICATION AD DS et fournissent beaucoup plus rapidement les calculs de liens de site.
- Prise en charge des contrôleurs de domaine en lecture seule (RODC). Les RODC sont pris en charge au niveau fonctionnel de la forêt de Windows Server 2003. Le RODC doit fonctionner avec Windows Server 2008, ou une version plus récente, et nécessite au moins un contrôleur de domaine complet Windows Server 2008, ou une version plus récente, en tant que partenaire de réPLICATION.
- Conversion des objets inetOrgPerson à objets utilisateur. Vous pouvez convertir une instance d'un objet inetOrgPerson (utilisé pour assurer la compatibilité avec certains services de répertoires qui ne sont pas de Microsoft) en une instance de l'objet utilisateur de la classe inetOrgPerson. Vous pouvez également convertir un objet utilisateur à un objet inetOrgPerson.
- Désactivation et redéfinition des attributs et classes d'objets. Bien que vous ne puissiez pas supprimer un attribut ou une classe d'objets dans le schéma au niveau fonctionnel de Windows Server 2003, vous pouvez désactiver ou redéfinir les attributs ou classes d'objets.

Le niveau fonctionnel de la forêt de Windows Server 2008 n'ajoute pas de nouvelles fonctionnalités à l'échelle de la forêt. Le niveau fonctionnel de la forêt de Windows Server 2008 R2 ajoute la possibilité d'activer les fonctionnalités de Active Directory, telles que la fonction corbeille d'Active Directory. Cette fonction permet de restaurer des objets Active Directory supprimés. Vous ne pouvez pas restaurer le niveau fonctionnel de la forêt si les fonctionnalités nécessitant un certain niveau de forêt, comme la fonction corbeille d'Active Directory, ont été activées.

Bien que le niveau fonctionnel de la forêt de Windows Server 2008 R2 AD DS ait introduit la corbeille Active Directory, la corbeille devait être gérée avec Windows PowerShell. Cependant, la version des outils d'administration de serveur distant (RSAT) qui vient avec Windows Server 2012 a la capacité de gérer la corbeille d'Active Directory en utilisant les outils de l'interface graphique utilisateur (GUI).

Le niveau fonctionnel de la forêt de Windows Server 2012 ne fournit pas de nouvelles fonctionnalités à l'échelle de la forêt. Par exemple, si vous élévez le niveau fonctionnel de la forêt à Windows Server 2012, vous ne pouvez pas ajouter un nouveau domaine fonctionnant au niveau fonctionnel du domaine de Windows Server 2008 R2.

Le niveau fonctionnel de la forêt de Windows Server 2012 R2 n'offre pas de nouvelles fonctionnalités à l'échelle de la forêt. Tous les domaines ajoutés à la forêt fonctionnent au niveau fonctionnel du domaine Windows Server 2012 R2.

Au moment de la rédaction de ce cours, la Technical Preview du niveau fonctionnel de la forêt de Windows Server 2016 n'a pas fourni de nouvelles fonctionnalités à l'échelle de la forêt. Tous les domaines ajoutés à la forêt fonctionneront au niveau fonctionnel du domaine de Windows Server 2016 Technical Preview.

Déploiement de nouveaux domaines AD DS

Lorsque vous créez une nouvelle forêt dans AD DS, un nouveau domaine appelé le domaine racine de la forêt est automatiquement créé et forme la base de votre infrastructure AD DS. Les contrôleurs de domaine dans le domaine racine de la forêt détiennent le contrôleur de schéma et les rôles de maître d'opérations des noms de domaine de FSMO (Flexible Single Master Operation) pour la forêt en plus des rôles FSMO de domaine. Si votre organisation ne nécessite qu'un seul domaine, le domaine racine de la forêt contiendra également tous les objets utilisateurs, groupes et ordinateurs utilisés par votre organisation. Si vous déployez plusieurs domaines en raison de la réPLICATION, l'espace de noms DNS, ou les exigences administratives, votre domaine racine de la forêt ne peut contenir que des objets administratifs nécessaires à la forêt. Vous pouvez choisir de créer des domaines supplémentaires de l'une des deux manières suivantes :

- Créer un domaine enfant. Les domaines d'enfants partagent un espace de noms commun avec un domaine parent. Ils sont fréquents dans les scénarios où vous pouvez décider de déployer plusieurs domaines qui correspondent aux services ou aux régions spécifiques au sein de votre organisation. Par exemple, si vous êtes l'administrateur de la forêt pour la forêt adatum.com, vous pouvez déployer des domaines enfants nommés europe.adatum.com et asia.adatum.com qui s'alignent avec les continents où A. Datum exerce ses activités. Les domaines enfants peuvent aussi être les parents d'autres domaines enfants tels que sales.europe.adatum.com ou test.asia.adatum.com
- Créer un domaine de l'arborescence ; Les domaines de l'arborescence sont des domaines qui établissent un nouvel espace de noms qui diffère du domaine racine de la forêt. Les domaines de l'arborescence sont courants dans les scénarios de fusions et d'acquisitions ou dans des organisations qui ont plusieurs filiales. Par exemple, si vous êtes l'administrateur de la forêt pour la forêt adatum.com, vous pouvez déployer des domaines de l'arborescence treyresearch.net et tailspintoys.com qui s'alignent sur les entreprises autonomes appartenant à A. Datum. Les domaines de l'arborescence peuvent également contenir des domaines enfants tels que europe.treyresearch.net ou asia.tailspintoys.com.

- Le domaine racine de forêt :
 - Est automatiquement créé avec une nouvelle forêt.
 - Est la base d'une infrastructure AD DS.
 - Peut être l'unique domaine dans un déploiement AD DS.
- Le domaine enfant :
 - Est l'un enfant d'un domaine parent.
 - Partage le même espace de noms que le domaine parent.
- Le domaine de l'arborescence :
 - Crée une nouvelle arborescence de domaine et un nouvel espace de noms.
 - Est couramment utilisé dans les scénarios de fusions et acquisitions.

Démonstration : Installation d'un contrôleur de domaine dans un nouveau domaine dans une forêt existante

Dans cette démonstration, vous allez apprendre à :

- Installer les binaires de AD DS sur TOR-DC1
- Configurer TOR-DC1 en tant que contrôleur de domaine AD DS à l'aide de l'Assistant de configuration des services de domaine Active Directory

Procédure de démonstration

Installer les binaires de AD DS sur TOR-DC1

- Sur **TOR-DC1**, dans le **Gestionnaire de serveur**, utilisez **l'assistant ajouter des rôles et fonctionnalités** pour installer les binaires des services de domaine Active Directory.
- Suivez l'**Assistant Ajouter des rôles et des fonctionnalités** d'AD DS en utilisant les paramètres par défaut.

Configurer TOR-DC1 en tant que contrôleur de domaine AD DS à l'aide de l'assistant de configuration des services de domaine Active Directory

- Utilisez **promouvoir ce serveur à un contrôleur de domaine** pour démarrer l'**assistant de configuration des services de domaine Active Directory**.
- Utilisez l'**assistant de configuration des services de domaine Active Directory** pour configurer AD DS sur **TOR-DC1** avec les paramètres suivants :
 - Opération de déploiement : **Ajouter un nouveau domaine à une forêt existante**
 - Nouveau nom de domaine : **NA**
 - Mot de passe du mode restauration des services d'annuaire (DSRM) : **Pa55w.rd**
- Suivez l'**assistant de configuration des services de domaine Active Directory** avec les paramètres par défaut.
- Redémarrez, puis connectez-vous comme **NA\Administrateur** avec le mot de passe **Pa55w.rd**, sur le contrôleur de domaine AD DS nouvellement créé **TOR-DC1**.

Mise à niveau d'une version précédente de AD DS vers Windows Server 2016

Pour mettre à niveau une version précédente de AD DS à Windows Server 2016 AD DS, vous pouvez utiliser l'une des deux méthodes suivantes :

- Mise à niveau du système d'exploitation sur les contrôleurs de domaine existants Windows Server 2016.
- Introduire les serveurs de Windows Server 2016 en tant que contrôleurs de domaine dans le domaine existant. Vous pouvez ensuite désaffecter les contrôleurs de domaine AD DS qui exécutent des versions antérieures de AD DS.

Méthodes de mise à niveau AD DS pour Windows Server 2016 :

- Mise à niveau sur place de Windows Server 2012 R2 ou de Windows Server 2012
- Introduire un nouveau serveur Windows Server 2016 dans le domaine et en faire un contrôleur de domaine (méthode recommandée)
- Ces deux méthodes nécessitent que le schéma soit au niveau de Windows Server 2016 :
 - L'Assistant Installation d'Active Directory Domain Services met à niveau le schéma automatiquement lorsqu'il est exécuté avec les autorisations appropriées
 - Adprep est disponible

De ces deux méthodes, la seconde est préférable parce que la mise à niveau des systèmes (surtout sur les serveurs qui fonctionnent depuis plusieurs années) est souvent difficile en raison de tous les changements apportés au fil des ans. En installant de nouveaux contrôleurs de domaine exécutant Windows Server 2016, vous aurez une nouvelle installation de Windows Server 2016.

Vous pouvez déployer les serveurs de Windows Server 2016 en tant que serveurs membres dans un domaine ayant des contrôleurs de domaine exécutant Windows Server 2008 ou des versions plus récentes. Cependant, avant de pouvoir installer le premier contrôleur de domaine qui exécute Windows Server 2016, vous devez mettre à niveau le schéma. Dans les versions de AD DS antérieures

à Windows Server 2012 R2, vous avez exécuté l'outil Adprep.exe pour effectuer les mises à jour de schéma. Toutefois, lorsque vous déployez de nouveaux contrôleurs de domaine de Windows Server 2016 dans un domaine existant et si vous êtes connecté avec un compte qui est un membre des groupes des administrateurs du schéma et des administrateurs de l'entreprise, l'assistant pour l'installation des services de domaine Active Directory met à jour automatiquement le schéma de la forêt AD DS.

 **Remarque :** Windows Server 2016 fournit encore une version 64 bits de Adprep, de sorte que vous pouvez exécuter Adprep.exe séparément. Par exemple, si l'administrateur qui installe le premier contrôleur de domaine Windows Server 2016 n'est pas un membre du groupe Administrateurs de l'entreprise et groupe Administrateurs du schéma, vous pourriez avoir à exécuter la commande séparément. Vous avez seulement à exécuter adprep.exe si vous planifiez une mise à niveau sur place pour le premier contrôleur de domaine Windows Server 2016 dans le domaine.

Le processus de mise à niveau

Pour mettre à niveau le système d'exploitation d'un contrôleur de domaine Windows Server 2012 vers Windows Server 2016, procédez comme suit :

1. Insérez le support d'installation pour Windows Server 2016, puis exécutez **installation** ;
2. Après la page **sélection de la langue**, cliquez sur **installer maintenant** ;
3. Après la fenêtre de **sélection du système d'exploitation** et la page **Acceptation de la licence**, dans la fenêtre **Quel type d'installation voulez-vous effectuer ?**, cliquez sur **Mise à niveau : installer Windows et conserver les fichiers, les paramètres et les applications**.

Avec ce type de mise à niveau, AD DS sur le contrôleur de domaine est mis à niveau vers Windows Server 2016 AD DS. Nous vous conseillons de vérifier la compatibilité matérielle et logicielle avant d'effectuer une mise à niveau. Après avoir effectué la mise à niveau du système d'exploitation, n'oubliez pas de mettre à jour vos pilotes et autres services (comme les agents de surveillance) et de vérifier les mises à jour pour les applications Microsoft et les logiciels non Microsoft.

 **Remarque :** Vous pouvez mettre à jour directement à partir de Windows Server 2012 et Windows Server 2012 R2 vers Windows Server 2016. Pour mettre à niveau les serveurs qui exécutent une version de Windows Server qui est plus ancienne que Windows Server 2012, vous devez soit effectuer une mise à niveau intermédiaire vers Windows Server 2012 ou Windows Server 2012 R2, soit exécuter une nouvelle installation. Notez que les contrôleurs de domaine de Windows Server 2016 AD DS peuvent coexister en tant que contrôleurs de domaine dans le même domaine que les contrôleurs de domaine de Windows Server 2008 ou plus récent.

Le processus pour une nouvelle installation

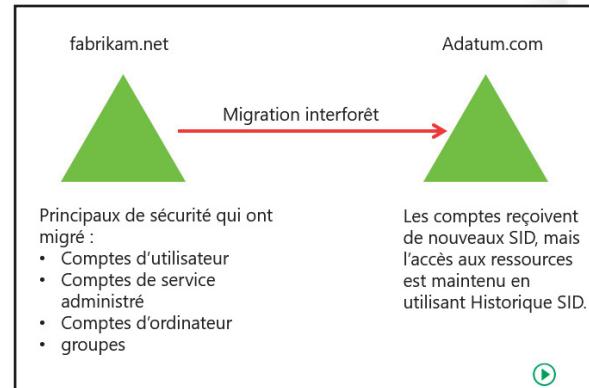
Pour une nouvelle installation de Windows Server 2016 en tant que membre de domaine, procédez comme suit :

1. Déployer et configurer une nouvelle installation de Windows Server 2016, puis joignez-la au domaine.
2. Promouvoir le nouveau serveur pour qu'il soit un contrôleur de domaine dans le domaine à l'aide du gestionnaire de serveur.

Migration vers Windows Server 2016 AD DS à partir d'une version précédente

Dans le cadre du déploiement AD DS, vous pouvez choisir de restructurer votre environnement pour les raisons suivantes :

- Pour optimiser la structure logique de AD DS. Dans certaines organisations, l'entreprise peut avoir changé de façon importante depuis que AD DS a été déployé. En conséquence, le domaine AD DS ou la structure de la forêt ne peut plus répondre aux besoins de l'entreprise.
- Pour aider à compléter une fusion, l'acquisition ou la cession de l'entreprise.



La restructuration implique la migration des ressources entre les domaines AD DS soit dans la même forêt, soit dans des forêts différentes. Il n'y a aucune option disponible dans AD DS pour détacher un domaine d'une forêt, puis l'attacher à une autre forêt. Dans certaines circonstances, vous pouvez renommer et réorganiser les domaines dans une forêt, mais il n'y a aucun moyen de fusionner facilement les domaines à l'intérieur ou entre les forêts. La seule option pour restructurer un domaine de cette manière est de déplacer tous les comptes et les ressources d'un domaine à un autre.

Vous pouvez utiliser l'outil de migration Active Directory (ADMT) pour déplacer les comptes d'utilisateur, de groupe et d'ordinateur d'un domaine à l'autre et pour faire migrer les ressources du serveur. Si elle est bien gérée, la migration peut être effectuée sans perturber l'accès des utilisateurs aux ressources dont ils ont besoin pour faire leur travail. L'ADMT fournit à la fois une interface graphique et une interface de script et prend en charge les tâches suivantes pour compléter la migration de domaine :

- Migration du compte d'utilisateur
- Migration du compte de groupe
- Migration du compte d'ordinateur
- Compte de service
- Migration de l'approbation
- Migration de l'annuaire Exchange Server
- Conversion de la sécurité sur les comptes d'ordinateurs migrés
- Fonctionnalités de rapports pour l'affichage des résultats de la migration
- Fonction de rapport pour annuler la dernière migration et relancer la dernière migration

Étapes de prémigration

Avant d'effectuer la migration, vous devez effectuer plusieurs tâches pour préparer les domaines sources et cibles. Ces tâches comprennent :

- Pour les ordinateurs membres du domaine qui sont pré-Windows Vista Service Pack 1 (SP1) ou Windows Server 2008 R2, configurer une clé de Registre sur le contrôleur de domaine AD DS cible pour autoriser des algorithmes de cryptographie qui sont compatibles avec le système d'exploitation Microsoft Windows NT Server 4.0.
- Activer les règles de pare-feu sur les contrôleurs de domaine AD DS source et cible pour permettre le partage de fichiers et d'imprimantes.

- Préparer les domaines AD DS sources et cibles pour gérer la façon dont les utilisateurs, les groupes, et les profils d'utilisateurs seront traités.
- Créer une planification de restauration.
- Établir les relations d'approbation qui sont nécessaires pour la migration.
- Configurer les domaines AD DS source et cible pour permettre la migration de l'historique SID.
- Préciser les comptes de service qui seront migrés.
- Effectuer un test de migration et corriger les erreurs qui sont signalées.

Restructuration interforêts avec ADMT

Une restructuration interforêts implique des ressources mobiles de domaines sources qui se trouvent dans des forêts différentes que le domaine cible. Pour utiliser ADMT pour effectuer une restructuration interforêts, procédez comme suit :

1. Créez un plan de restauration. Un plan adéquat est essentiel à la réussite du processus de restructuration. Effectuez les étapes suivantes pour créer votre plan de restructuration :
 - a. Déterminez le processus compte-migration.
 - b. Assignez les emplacements d'objets et le mappage d'emplacement.
 - c. Élaborez un plan de test.
 - d. Créer une planification de restauration.
 - e. Créer un plan de communication.
2. Préparer les domaines sources et cibles. Vous devez préparer à la fois les domaines sources et cibles pour le processus de restructuration en effectuant les tâches suivantes :
 - a. Assurer le cryptage 128 bits pour tous les contrôleurs de domaine. Windows Server 2000 SP3 et les versions plus récentes prennent nécessairement en charge le cryptage 128 bits. Pour les systèmes d'exploitation plus anciens, vous devez télécharger et installer un pack de cryptage distinct.
 - b. Mettre en place les approbations nécessaires. Vous devez configurer au moins une approbation à sens unique entre les domaines sources et cibles.
 - c. Mettez en place des comptes de migration. L'ADMT utilise des comptes de migration pour faire migrer des objets entre les domaines sources et cibles. Assurez-vous que ces comptes aient des autorisations pour déplacer et modifier des objets sur les domaines sources et cibles.
 - d. Déterminer si l'ADMT traitera l'historique SID automatiquement ou s'il faut configurer manuellement les domaines cibles et sources.
 - e. Assurez-vous que la structure OU du domaine cible soit bien configurée. Assurez-vous de configurer les droits d'administration appropriés et l'administration déléguée dans le domaine cible.
 - f. Installer l'outil de migration (ADMT) dans le domaine cible.
 - g. Activer le mot de passe de la migration.
 - h. Effectuer une migration d'essai avec un petit groupe de compte test.

3. Migrer les comptes. Pour faire migrer les comptes, procédez comme suit :
 - a. Faire la transition des comptes de service ;
 - b. Faire migrer les groupes globaux ;
 - c. Faire migrer les comptes. Faire migrer des comptes d'utilisateurs et d'ordinateurs par lots pour surveiller la progression de la migration. Si vous faites migrer des profils locaux dans le cadre du processus, faites migrer les ordinateurs touchés d'abord, puis les comptes d'utilisateurs associés.
4. Faire migrer les ressources. Faire migrer les dernières ressources dans le domaine en effectuant les étapes suivantes :
 - a. Faire migrer les postes de travail et les serveurs membres ;
 - b. Faire migrer les groupes de domaine locaux ;
 - c. Faire migrer les contrôleurs de domaine ;
5. Achever la migration. Achever la migration et effectuer le nettoyage en exécutant les étapes suivantes :
 - a. Transférer le processus d'administration vers le domaine cible ;
 - b. Veiller à ce qu'au moins deux contrôleurs de domaine exécutables existent dans le domaine cible ; Sauvegarder ces contrôleurs de domaine ;
 - c. Désactiver le domaine source.

L'attribut de l'historique SID

Durant la migration, vous avez peut-être déplacé des comptes d'utilisateur et de groupe vers le nouveau domaine, mais les ressources auxquelles les utilisateurs doivent accéder peuvent encore être dans l'ancien domaine. Lorsque vous faites migrer un compte d'utilisateur, AD DS lui attribue un nouveau SID. Parce que la ressource dans le domaine source autorise l'accès en fonction du SID de l'utilisateur du domaine source, l'utilisateur ne peut pas utiliser le nouveau SID pour accéder à la ressource jusqu'à ce que la ressource soit déplacée vers le nouveau domaine.

Pour remédier à cette situation, vous pouvez configurer l'outil de migration Active Directory (ADMT) pour faire migrer le SID à partir du domaine source, puis stocker le SID dans un attribut appelé **historique SID**. Quand l'attribut **historique-SID** est peuplé, le SID précédent de l'utilisateur est utilisé pour accorder l'accès aux ressources dans le domaine source.

L'historique SID augmente la taille du jeton d'accès de l'utilisateur. Après la migration des utilisateurs vers le nouveau domaine, les listes de contrôle d'accès (ACL) dans votre environnement devraient être examinées et vous devriez également faire migrer les ACL. Après qu'une migration est terminée et que le domaine d'origine a été supprimé, vous devez nettoyer l'attribut de l'historique SID de vos utilisateurs. Vous pouvez mieux accomplir cette tâche en utilisant les cmdlets **Get-SIDHistory** et **Remove-SIDHistory** de **Windows PowerShell**. Vous devriez soigneusement planifier et exécuter ces activités parce que la suppression de l'historique SID avant que l'environnement soit correctement préparé pourrait provoquer l'interruption de vos affaires.

 **Lectures supplémentaires :** Pour plus d'informations sur l'utilisation de l'outil de migration Active Directory (ADMT, Active Directory Migration Tool), consultez : <http://aka.ms/Jiauyg>

Éléments à prendre en compte pour l'implémentation d'environnements AD DS complexes

Dans un environnement AD DS à forêt unique et à un seul domaine, lorsque vous installez AD DS et DNS avec les paramètres par défaut, la configuration fonctionne de manière appropriée dans la plupart des scénarios. Cependant, à mesure que votre organisation s'agrandit et que votre environnement AD DS devient plus complexe, il y a plusieurs choix que vous pourriez avoir à faire afin de faciliter une résolution de nom et avoir une connexion d'utilisateur efficace dans l'environnement AD DS.

- Éléments DNS à prendre en compte :

- Centralisé vs décentralisé
- Vérifier la configuration du client DNS et la résolution de noms
- Optimiser la résolution de nom DNS :
 - Redirecteur conditionnel et zones de relais
 - Dévolution DNS et ordre de recherche de suffixe DNS
- Déployer une zone GlobalNames
- Utiliser des zones AD DS intégrées
- Étendre AD DS à Azure

- Considérations UPN :

- Suffixes UPN
- Catalogue global
- Scénarios d'authentification fédérée

Éléments DNS à prendre en compte

Dans un environnement multidomaines ou multiforêts, les ordinateurs clients peuvent devoir trouver une variété de services entre les forêts, y compris les serveurs gestionnaires de clés pour l'activation de Windows, les serveurs de gestion de licences Terminal Services, les serveurs de gestion de licences pour des applications spécifiques, et les contrôleurs de domaine dans un domaine pour valider les approbations lors de l'accès aux ressources dans un autre domaine. Lorsque les organisations déplacent de multiples arborescences dans une forêt AD DS ou quand ils déplacent plusieurs forêts, la résolution de noms est plus compliquée parce que vous devez gérer plusieurs espaces de noms de domaine. Dans ces scénarios, tenez compte des points suivants :

- Opter pour un modèle centralisé ou décentralisé. Dans un modèle centralisé, vous pouvez configurer toutes les zones DNS pour la réPLICATION à l'échelle des forêts, ce qui les rend disponibles localement sur chaque contrôleur de domaine dans la forêt. Bien que ce soit facile à réaliser et que cela assure la résolution de noms entre les domaines, vous devez tenir compte des répercussions que cela peut avoir sur la réPLICATION du contrôleur de domaine dans tout votre environnement AD DS. Dans un modèle décentralisé, les zones sont configurées pour la réPLICATION à l'échelle du domaine, ce qui les rend disponibles sur chaque contrôleur de domaine dans le domaine. Pour implémenter la résolution de nom entre les domaines, vous créez des délégations dans le domaine parent et les transitaires dans les domaines enfants. Un modèle décentralisé est plus difficile à tenir à jour, mais il vous permet de mieux contrôler la réPLICATION et la flexibilité dans l'administration des domaines enfants.
- Vérifier la configuration DNS du client. Configurez tous les ordinateurs dans le domaine AD DS avec au moins deux adresses de serveurs DNS fonctionnels. Tous les ordinateurs doivent avoir une bonne connectivité réseau avec les serveurs DNS.
- Vérifier et surveiller la résolution de noms DNS. Assurez-vous que tous vos ordinateurs, y compris les contrôleurs de domaine, sont en mesure d'effectuer des recherches DNS fructueuses pour tous les contrôleurs de domaine dans la forêt. Les contrôleurs de domaine doivent être en mesure de se connecter à d'autres contrôleurs de domaine pour répliquer avec succès les modifications à AD DS. Les ordinateurs clients doivent être en mesure de localiser les contrôleurs de domaine en utilisant des enregistrements de ressource SRV, et ils doivent pouvoir résoudre les noms des contrôleurs de domaine en adresses IP.
- Optimiser la résolution de nom DNS entre plusieurs espaces de noms :
 - Utilisez les fonctions DNS comme les zones de transfert conditionnelles et les zones de stub afin d'optimiser le processus de résolution des noms d'ordinateur dans tous les espaces de noms. En utilisant une zone de transfert conditionnelle ou une zone stub, vous créez un raccourci efficace qui vous évite de recourir à des requêtes récursives à l'arborescence de domaine ou à la racine de forêt. Bien qu'une zone de transfert conditionnelle ou une zone de stub ne soit pas nécessaire

pour que la résolution de nom fonctionne correctement, elle peut réduire considérablement la latence lorsque la résolution de noms entre les domaines ou entre les forêts se produit fréquemment. Lorsque vous configurez une approbation entre les deux forêts, vous utilisez généralement un redirecteur conditionnel dans chaque forêt pour faciliter la résolution des noms des deux côtés de l'approbation.

- Envisager la dévolution DNS et l'ordre de recherche des suffixes DNS. La dévolution DNS est une fonctionnalité du client DNS de Windows qui permet à un client dans un espace de noms enfant de résoudre l'adresse IP d'un hôte dans un espace de noms parent sans spécifier un nom de domaine complet (FQDN). Le processus de dévolution tente automatiquement de résoudre un nom en une partie en ajoutant le suffixe DNS principal. Si un résultat est introuvable, la dévolution ajoute récursivement le suffixe DNS parent jusqu'à ce que le nom soit résolu ou que le niveau de dévolution soit atteint. Le niveau de dévolution est déterminé automatiquement en comparant le domaine racine de la forêt au suffixe DNS principal, mais il peut également être configuré manuellement lorsqu'un contrôle précis est nécessaire. Dans des environnements AD DS complexes où vous pourriez avoir un arbre de domaine profond avec de nombreux niveaux dans l'espace de noms, se fier à la dévolution DNS pour la résolution de nom peut ne pas être efficace. Dans ces cas, vous pouvez configurer l'ordre de recherche des suffixes DNS afin de spécifier manuellement les suffixes DNS à annexer et l'ordre dans lequel les annexer. Lorsque l'ordre de recherche des suffixes DNS est spécifié soit manuellement, soit grâce à la stratégie de groupe, le processus de dévolution DNS est automatiquement désactivé.
- Déployer une zone GlobalNames. Une zone GlobalNames vous permet de configurer la résolution de noms unique pour les noms DNS de votre forêt. Ceci permet la résolution de noms en utilisant un nom plus court qui est plus facile à retenir qu'un nom de domaine complet public (FQDN). Auparavant, le service WINS (Windows Internet Name Service) était configuré dans un domaine pour prendre en charge la résolution pour un seul nom. Vous pouvez utiliser une zone GlobalNames pour remplacer WINS dans votre environnement, particulièrement si vous déployez Internet Protocol version 6 (IPv6), parce que WINS ne prend pas en charge l'adressage IPv6. En outre, vous pouvez utiliser une zone GlobalNames lorsque compter sur les listes de recherche des suffixes DNS n'est pas efficace en raison du nombre de domaines qui doivent être recherchés.
- Utiliser des zones DNS intégrées à AD DS. Lorsque vous configurez une zone DNS intégrée à AD DS, les informations DNS sont stockées dans AD DS et répliquées grâce au processus normal de réPLICATION AD DS. Cela permet d'optimiser le processus de réPLICATION des modifications dans l'ensemble de la forêt. Vous pouvez également configurer l'étendue de la réPLICATION pour les zones DNS. Par défaut, les enregistrements DNS propres au domaine sont répliqués vers d'autres contrôleurs de domaine qui sont également des serveurs DNS dans le domaine. Les enregistrements DNS qui permettent des recherches entre les domaines sont stockés dans la zone de _msdcs.rootdomainname et sont répliqués sur les contrôleurs de domaine qui sont également des serveurs DNS dans l'ensemble de la forêt. Vous ne devez pas modifier cette configuration par défaut.
- Lorsque vous étendez votre domaine AD DS dans Azure, vous devez prendre quelques mesures supplémentaires. Le DNS intégré dans Azure ne prend pas en charge les domaines AD DS ; pour prendre en charge vos composants de domaine basés sur l'infonuage, vous devez faire ce qui suit :
 - Configurer un réseau virtuel Azure.
 - Configurer un site AD DS pour votre sous-réseau Azure.
 - Enregistrer votre DNS sur site avec le réseau virtuel Azure. Vous devez faire cela pour permettre à un ordinateur virtuel Azure de communiquer avec votre AD DS sur site.
 - Après avoir promu avec succès un ordinateur virtuel Azure à un contrôleur de domaine/serveur DNS AD DS, enregistrez l'adresse IP de cet ordinateur virtuel en tant serveur DNS de votre réseau virtuel Azure. Cela permet une communication AD DS locale et la résolution de noms pour les autres ordinateurs virtuels dans votre sous-réseau Azure.

Éléments UPN à prendre en compte

Dans un environnement multidomaine ou multiforêts, se connecter devient plus compliqué, car les utilisateurs doivent connaître le domaine qui contient leur compte d'utilisateur. Les utilisateurs peuvent se connecter en utilisant le nom NetBIOS du domaine et de leur compte SAM ou l'attribut UPN plus convivial, qui est formaté comme une adresse courriel. L'UPN par défaut est *utilisateur@ DNS-domaine-prénom*. Un UPN est généralement plus facile à retenir et dans de nombreuses organisations, il peut correspondre à l'adresse de messagerie principale de l'utilisateur. Si vous décidez d'utiliser l'attribut UPN pour vous connecter, il y a plusieurs choses dont vous devez tenir compte :

- Les suffixes DNS. Par défaut, le suffixe UPN correspond au FQDN DNS du domaine où le compte d'utilisateur existe. Dans des environnements AD DS complexes où il y a plusieurs domaines dans une arborescence de domaine, le suffixe UPN peut devenir très long et il est difficile de s'en souvenir. Par exemple, dans un environnement AD DS organisé par région et service, un UPN échantillon par défaut peut ressembler à user@hr.northamerica.contoso.com. Dans cette situation, vous pouvez décider d'utiliser un suffixe commun UPN pour tous les utilisateurs dans le domaine. Le suffixe UPN n'a pas à être un domaine DNS valide, mais, dans de nombreux cas, les organisations choisissent d'utiliser leur nom de domaine de messagerie pour simplifier le processus de connexion pour les utilisateurs. La console **Domaines et approbations Active Directory** vous permet de spécifier des suffixes UPN substituts pour un domaine. Vous précisez le suffixe UPN pour un compte d'utilisateur lors de la création du compte et vous pouvez le modifier à tout moment par la suite.
- Catalogue global. Pour autoriser la connexion avec un UPN, la disponibilité d'un serveur de catalogue global peut être nécessaire. Si un suffixe UPN substitut est utilisé et que le compte d'ordinateur n'est pas dans le même domaine que le compte d'utilisateur, un serveur de catalogue global est nécessaire pour résoudre l'UPN qui est spécifié lors de la connexion.
- Scénarios d'authentification fédérée. Si votre organisation met à profit AD FS pour effectuer une authentification fédérée avec un service basé sur l'infonuage informatique comme Office 365, le suffixe UPN utilisé doit être un domaine DNS externe valide appartenant à votre organisation. Cela est nécessaire, car une approbation de fédération ne peut pas être créée avec un domaine DNS qui n'existe seulement que dans votre infrastructure AD DS interne.

Testez vos connaissances

| Question | |
|--|------------------------|
| Quel est le niveau fonctionnel minimum de domaine dans lequel vous devez déployer un contrôleur de domaine AD DS Windows Server 2016 ? | |
| Sélectionnez la réponse correcte. | |
| | Windows Server 2003 |
| | Windows Server 2008 |
| | Windows Server 2008 R2 |
| | Windows Server 2012 R2 |
| | Windows Server 2016 |

Testez vos connaissances

| Question | |
|--|-------------------------------------|
| Parmi les éléments suivants, lequel pouvez-vous utiliser pour optimiser la résolution de noms dans les espaces de noms DNS ? | |
| Sélectionnez la réponse correcte. | |
| | Redirecteurs conditionnels |
| | Sites AD DS |
| | Ordre de recherche des suffixes DNS |
| | Zones stub DNS |
| | Serveurs de catalogue global |

Leçon 3

Configuration d'approbations AD DS

Les approbations AD DS permettent l'accès aux ressources dans un environnement AD DS complexe. Lorsque vous déployez un seul domaine, vous pouvez facilement accorder l'accès aux ressources dans le domaine pour les utilisateurs et les groupes du domaine. Lorsque vous implémentez plusieurs domaines ou forêts, vous devez vous assurer que les approbations appropriées sont en place pour permettre le même accès aux ressources. Cette leçon décrit comment les approbations travaillent dans un environnement AD DS, et comment vous pouvez configurer les approbations pour répondre à vos besoins d'affaires.

Objectifs de la leçon

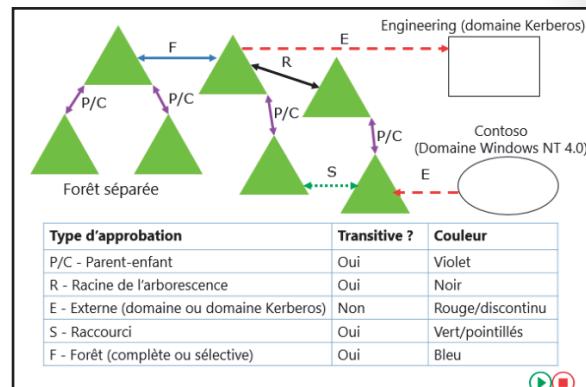
À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- Décrire les types d'approbations que vous pouvez configurer dans un environnement Windows Server 2016 ;
- Expliquer comment les approbations fonctionnent dans une forêt AD DS ;
- Expliquer comment les approbations fonctionnent entre les forêts AD DS ;
- Décrire comment configurer les paramètres d'approbation avancés ;
- Configurer une approbation de forêt.

Aperçu des différents types d'approbations AD DS

Dans une forêt AD DS multidomaine, les relations d'approbation à deux sens sont générées automatiquement entre les domaines AD DS, afin qu'il y ait un chemin d'approbation entre tous les domaines AD DS. Les approbations qui sont créées automatiquement dans la forêt sont toutes des approbations transitives. Cela signifie que si le domaine A approuve le domaine B, et que le domaine B approuve le domaine C, alors le domaine A approuve le domaine C.

Il existe d'autres types d'approbations que vous pouvez déployer. Les principaux types d'approbation sont décrits dans le tableau suivant :

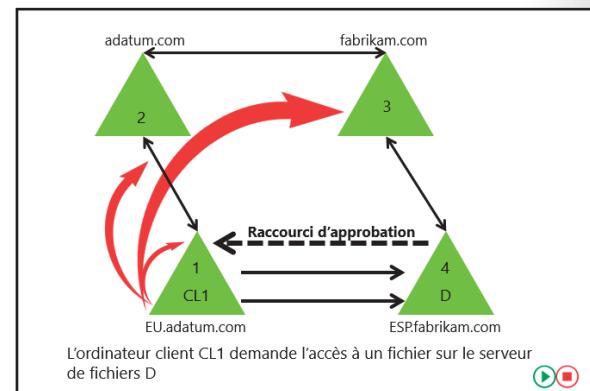


| Type d'approbation | Transitivité | Direction | Description |
|-----------------------|--------------|------------------|---|
| Parent et enfant | Transitivité | Bidirectionnelle | Lorsque vous ajoutez un nouveau domaine AD DS à une arborescence AD DS existante, des approbations entre le nouveau parent et l'enfant sont créées. |
| Racine d'arborescence | Transitivité | Bidirectionnelle | Quand une nouvelle arborescence AD DS est créée dans une forêt AD DS existante, une nouvelle approbation racine d'arborescence est créée. |

| Type d'approbation | Transitivité | Direction | Description |
|-------------------------------|----------------------------|-------------------------------------|--|
| Externe | Non transitive | À sens unique ou dans les deux sens | Les approbations externes permettent l'accès aux ressources qu'il faut accorder avec un domaine Windows NT 4.0 ou un domaine AD DS dans une autre forêt. Celles-ci peuvent également être mises en place pour fournir un cadre pour une migration. |
| Domaine | Transitif ou non transitif | À sens unique ou dans les deux sens | Les approbations de domaine établissent un chemin d'accès à l'authentification entre un domaine Windows Server AD DS et un royaume Kerberos v5 implémenté en utilisant un service de répertoire autre que AD DS. |
| Forêt (complète ou sélective) | Transitivité | À sens unique ou dans les deux sens | Les approbations entre forêts AD DS permettent à deux forêts de partager des ressources. |
| Raccourci | Non transitive | À sens unique ou dans les deux sens | Vous pouvez configurer les raccourcis d'approbation pour améliorer les temps d'authentification entre les domaines AD DS qui sont dans différentes parties d'une forêt AD DS. Il n'y a pas de raccourcis d'approbation par défaut; ils doivent être créés par un administrateur. |

Comment les approbations fonctionnent-elles dans une forêt

Lorsque vous configurez des approbations entre domaines soit au sein de la même forêt, dans l'ensemble des forêts, ou avec un domaine externe, des informations au sujet de ces approbations, comme la transitivité et le type, sont stockées dans AD DS. Un objet de domaine approuvé stocke ces informations. Cet objet de domaine est créé et stocké dans le conteneur système dans AD DS lorsque vous configurez une approbation.



Comment les approbations permettent aux utilisateurs d'accéder à des ressources dans une forêt

Lorsque l'utilisateur dans le domaine tente d'accéder à une ressource partagée dans un autre domaine de la forêt, l'ordinateur de l'utilisateur contacte d'abord un contrôleur de domaine dans son domaine pour demander un ticket de session à la ressource. Parce que la ressource n'est pas dans le domaine de l'utilisateur, le contrôleur de domaine doit déterminer si une approbation existe avec le domaine cible.

Le contrôleur de domaine peut utiliser l'approbation de l'objet de domaine pour vérifier que l'approbation existe. Toutefois, pour accéder à la ressource, l'ordinateur client doit communiquer avec un contrôleur de domaine dans chaque domaine le long du chemin d'approbation. Le contrôleur de domaine dans le domaine de l'ordinateur du client renvoie l'ordinateur client à un contrôleur de domaine dans le domaine suivant sur le chemin d'approbation. Si ce n'est pas le domaine dans lequel se trouve la ressource, ce contrôleur de domaine renvoie l'ordinateur client vers un contrôleur de domaine dans le domaine suivant. Finalement, l'ordinateur client est renvoyé à un contrôleur de domaine dans le domaine où se trouve la ressource, et le client reçoit un ticket de session pour accéder à la ressource.

Le chemin d'accès à l'approbation est le chemin le plus court dans la hiérarchie d'approbations. Dans une forêt dans laquelle seules les approbations de défaut sont configurées, le chemin d'accès à l'approbation monte de l'arborescence de domaine au domaine racine de la forêt, puis descend dans l'arborescence de domaine vers le domaine cible. Si les raccourcis d'approbation sont configurés, le chemin d'accès à l'approbation peut consister en un seul bond à partir du domaine de l'ordinateur client au domaine contenant la ressource.

Comment les approbations fonctionnent-elles entre les forêts

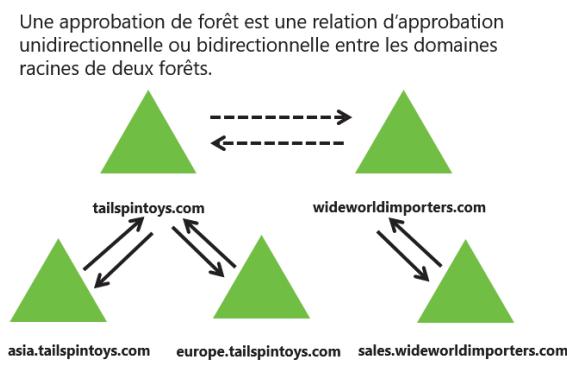
Si l'environnement AD DS contient plus d'une forêt, il est possible de mettre en place des relations d'approbations entre les domaines racines de forêt AD DS. Ces approbations de forêt peuvent être soit des approbations à l'échelle de la forêt, soit des approbations sélectives. Les approbations de forêt peuvent être à sens unique ou dans les deux sens. Les approbations de forêt sont aussi transitives pour les domaines dans chaque forêt.

Une relation d'approbation de forêt permet aux utilisateurs authentifiés par un domaine d'une forêt d'accéder aux ressources situées dans un domaine dans une autre forêt, à la condition qu'on leur ait accordé les droits d'accès. Si l'approbation de forêt est à sens unique, les contrôleurs de domaine dans la forêt de confiance peuvent fournir des tickets de session aux utilisateurs dans un domaine de la forêt approuvée. Les approbations de forêt sont nettement plus faciles à établir, maintenir et administrer que les relations d'approbation distinctes entre les différents domaines des différentes forêts.

Les approbations de forêt sont particulièrement utiles dans les scénarios qui impliquent une collaboration entre plusieurs organisations, ou des fusions et acquisitions, ou au sein d'une même organisation comportant plusieurs forêts dans lesquelles les données et les services AD DS doivent être isolés. Les approbations de forêt sont également utiles pour les fournisseurs de services d'application, pour les extranets commerciaux collaborateurs, et pour les entreprises qui recherchent une solution d'autonomie administrative.

Les approbations de forêt présentent les avantages suivants :

- Gestion simplifiée des ressources parmi les forêts Windows Server 2008 (ou versions plus récentes) grâce à la réduction du nombre d'approbations externes nécessaires pour le partage des ressources;
- Relations d'approbation à deux sens complètes avec chaque domaine de chaque forêt;
- Utilisation de l'authentification du nom de l'utilisateur principal (UPN) entre deux forêts ;
- Utilisation des protocoles d'authentification Kerberos version 5 (v5) pour améliorer la fiabilité des données d'autorisation transférées entre les forêts ;



- Flexibilité de l'administration. Les tâches administratives peuvent être propres à chaque forêt.

Vous pouvez créer une approbation de forêt seulement entre deux forêts AD DS ; vous ne pouvez pas étendre l'approbation implicitement à une troisième forêt. Cela signifie que si vous créez une approbation de forêt entre la forêt 1 et la forêt 2, puis que vous créez une approbation de forêt entre la forêt 2 et la forêt 3, la forêt 1 n'a pas d'approbation implicite avec la forêt 3. Les approbations de forêt ne sont pas transitives entre plusieurs forêts.

Vous devez répondre à plusieurs exigences avant de pouvoir implémenter une approbation de forêt, notamment vous assurer que le niveau fonctionnel de la forêt est Windows Server 2003 ou une version plus récente, et que vous disposez d'une résolution de noms DNS entre les forêts.

Configurer des paramètres avancés de confiance AD DS

Dans certains cas, les approbations peuvent entraîner des problèmes de sécurité. En outre, si une approbation est mal configurée, les utilisateurs appartenant à un autre domaine peuvent accéder de façon non désirée à certaines ressources. Il existe plusieurs technologies qui peuvent vous aider à contrôler et à gérer la sécurité dans une approbation.

Filtrage SID

Par défaut, quand vous établissez une approbation de forêt ou de domaine, vous déclenchez une quarantaine dans le domaine, également appelée filtrage des SID. Lorsqu'un utilisateur s'authentifie dans un domaine approuvé, l'utilisateur présente des données d'autorisation qui comprennent les SID de tous les groupes auxquels l'utilisateur appartient. De plus, les données d'autorisation de l'utilisateur comprennent l'historique SID de l'utilisateur et des groupes de l'utilisateur. Le filtrage SID empêche l'utilisation abusive de l'attribut SID-History en permettant la lecture des SID seulement à partir de l'attribut objectSID et non à partir de l'attribut SID-History.

Dans un scénario de domaine approuvé, un administrateur peut utiliser les informations d'identification administratives dans le domaine approuvé pour charger les SID qui sont les mêmes que les SID des comptes privilégiés dans votre domaine dans l'attribut SID-History d'un utilisateur. Cet utilisateur aurait alors des niveaux inappropriés d'accès aux ressources dans votre domaine. Le filtrage SID empêche cela en permettant au domaine d'approbation de filtrer les SID du domaine approuvé qui ne sont pas les SID primaires des entités de sécurité. Chaque SID comprend le SID du domaine d'origine, de sorte que lorsqu'un utilisateur d'un domaine approuvé présente la liste des SID de l'utilisateur et les SID des groupes de l'utilisateur, le filtrage SID charge le domaine de confiance d'annuler tous les SID sans le domaine SID du domaine approuvé. Le filtrage des SID est activé par défaut pour toutes les approbations sortantes vers des domaines et des forêts externes.

Authentification sélective

Quand vous créez une approbation externe ou une approbation de forêt, vous pouvez contrôler l'étendue de l'authentification des principaux de sécurité approuvés. Il existe deux modes d'authentification pour une approbation externe ou de forêt :

- Authentification pour l'ensemble du domaine (dans le cas d'une approbation externe) ou authentification pour l'ensemble de la forêt (dans le cas d'une approbation de forêt)
- Authentification sélective

Les considérations de sécurité dans les approbations de forêt comprennent :

- Filtrage SID
- Authentification sélective
- Routage de suffixes de noms

Une approbation mal configurée peut permettre un accès non autorisé aux ressources.

En choisissant l'authentification pour l'ensemble du domaine ou de la forêt, vous permettez à tous les utilisateurs approuvés de s'authentifier pour accéder à des services sur tous les ordinateurs du domaine approuvé. Par conséquent, les utilisateurs approuvés peuvent être autorisés à accéder à toutes les ressources du domaine autorisé. Si vous utilisez cette authentification, tous les utilisateurs d'un domaine ou d'une forêt approuvés sont considérés comme des utilisateurs authentifiés dans le domaine d'approbation. Aussi, si vous choisissez l'authentification pour l'ensemble du domaine ou de la forêt, toute ressource bénéficiant des autorisations accordées aux utilisateurs authentifiés est accessible immédiatement aux utilisateurs approuvés du domaine.

Si toutefois vous choisissez l'authentification selective, tous les utilisateurs du domaine approuvé sont des identités approuvées. Cependant, ils ne sont autorisés à s'authentifier que pour les services sur les ordinateurs que vous spécifiez. Quand ils utilisent l'authentification selective, les utilisateurs ne deviendront des utilisateurs authentifiés dans le domaine cible, mais vous pouvez explicitement leur accorder la permission **autorisation d'authentifier** sur des ordinateurs particuliers.

Par exemple, imaginez que vous avez une approbation externe avec le domaine d'une organisation partenaire. Vous voulez vous assurer que seuls les utilisateurs du groupe de marketing de l'organisation partenaire peuvent accéder aux dossiers partagés sur un seul de vos nombreux serveurs de fichiers. Vous pouvez configurer l'authentification selective pour la relation d'approbation, puis octroyer aux utilisateurs approuvés le droit de s'authentifier pour ce serveur de fichiers uniquement.

Routage de suffixes de noms

Le routage de suffixes de noms est un mécanisme de gestion du routage des requêtes d'authentification dans l'ensemble des forêts exécutant Windows Server 2003 ou une nouvelle forêt, qui sont liées entre elles par des approbations de forêt. Pour simplifier l'administration des requêtes d'authentification, quand vous créez une approbation de forêt, AD DS redirige par défaut tous les suffixes de noms uniques. Un *suffixe de nom unique* est un suffixe de nom dans une forêt (tel qu'un suffixe UPN), un suffixe de nom de principal de service (SPN), une forêt DNS ou le nom d'une arborescence de domaine qui n'est subordonné à aucun autre suffixe de nom. Par exemple, le nom de forêt DNS contoso.com est un suffixe de nom unique dans la forêt contoso.com.

AD DS dirige tous les noms subordonnés aux suffixes de nom unique implicitement. Par exemple, si la forêt utilise contoso.com comme suffixe de nom unique, les demandes d'authentification pour tous les domaines enfants de contoso.com (childdomain.contoso.com) sont routées, car les domaines enfants font partie du suffixe de nom de contoso.com. Les noms enfants apparaissent dans le composant logiciel enregistrable **Domaines et approbations Active Directory**. Si vous souhaitez exclure des membres d'un domaine enfant de l'authentification dans la forêt spécifiée, vous pouvez désactiver le routage de suffixe de nom pour ce nom. Vous pouvez également désactiver le routage pour le nom de forêt lui-même.



Lectures supplémentaires :

- Pour plus d'informations sur la configuration de la mise en quarantaine du filtre SID sur des approbations externes, reportez-vous à : <http://aka.ms/Sveqfn>
- Pour plus d'informations sur l'activation de l'authentification selective sur une approbation de forêt, reportez-vous à : <http://aka.ms/Blp826>
- Pour plus d'informations sur le routage de suffixe de noms, reportez-vous à : <http://aka.ms/Egc6g7>

Démonstration : configurer une approbation de forêt

Dans cette démonstration, vous allez apprendre à :

- Configurer la résolution de noms DNS en utilisant un redirecteur conditionnel
- Configurer une approbation de forêt selective à deux sens

Procédure de démonstration

Configurer la résolution de noms DNS en utilisant un redirecteur conditionnel

- Configurez la résolution de nom DNS entre adatum.com et treyresearch.net en créant un redirecteur conditionnel de sorte que **LON-DC1** est doté d'un renvoi vers **TREY-DC1** comme le serveur DNS pour le domaine DNS **treyresearch.net**.
- Configurez un redirecteur conditionnel sur **TREY-DC1** de sorte qu'il ait un renvoi vers **LON-DC1** pour le domaine DNS **adatum.com**.

Configurer une approbation de forêt sélective à deux sens

- Sur **LON-DC1**, dans **Domaines et approbations Active Directory**, créez une approbation de forêt à deux sens sélective entre **adatum.com** et **treyresearch.net** en fournissant les informations d'identification du domaine **treyresearch.net** compte **Administrateur**.

Testez vos connaissances

| Question | |
|--|---|
| Parmi les éléments suivants, lequel doit être en place avant de pouvoir créer une approbation de forêt ? | |
| Sélectionnez la réponse correcte. | |
| | Résolution de noms entre les domaines racines dans chaque forêt |
| | Niveau fonctionnel de la forêt de Windows Server 2003 ou de la version ultérieure |
| | Niveau fonctionnel de la forêt de Windows Server 2008 ou de la version ultérieure |
| | Niveau fonctionnel de la forêt de Windows Server 2012 ou de la version ultérieure |
| | Les contrôleurs de domaine doivent être activés pour l'authentification sélective |

Testez vos connaissances

| Question | |
|---|--------------------------------------|
| Quel paramètre de confiance AD DS vous permet de contrôler l'étendue de l'authentification des entités de sécurité de confiance ? | |
| Sélectionnez la réponse correcte. | |
| | Routage de suffixes de noms |
| | Délégation Kerberos contrainte (KCD) |
| | Authentification sélective |
| | Filtrage SID |
| | SID-History |

Atelier pratique : Domaine et gestion des approbations dans AD DS

Scénario

A. Datum Corporation a déployé un domaine unique AD DS avec tous les contrôleurs de domaine situés dans son centre de données de Londres. Comme l'entreprise s'est agrandie et qu'elle a ajouté des filiales ayant un grand nombre d'utilisateurs, il devient de plus en plus évident que l'environnement AD DS actuel ne répond pas aux exigences de l'entreprise. L'équipe du réseau est préoccupée par la quantité de trafic réseau lié à AD DS qui traverse les liaisons WAN, qui deviennent très utilisées.

La société est également de plus en plus intégrée avec les organisations partenaires, dont certaines ont besoin d'accéder aux ressources et applications partagées qui sont situées sur le réseau interne A. Datum. Le département de la sécurité à A. Datum veut faire en sorte que l'accès à ces utilisateurs externes soit aussi sécurisé que possible.

En tant que l'un des administrateurs de réseau supérieurs à A. Datum, vous êtes responsable de l'implémentation d'une infrastructure AD DS qui répond aux besoins de l'entreprise. Vous êtes responsable de la planification d'un domaine AD DS et du déploiement d'une forêt qui fournit des services optimaux pour les utilisateurs internes et externes, tout en répondant aux exigences de sécurité à A. Datum.

Objectifs

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

- Implémenter des approbations de forêts
- Implémenter des domaines enfants dans AD DS

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels : **22742A-LON-DC1**, **22742A-LON-DC2**, **22742A-TOR-DC1**, **22742A-LON-SVR2** et **22742A-TREY-DC1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-LON-DC1**, et dans le volet **actions**, cliquez sur **démarrer**.
3. Dans le volet d'**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 : **Pa55w.rd**.
5. Répétez les étapes 2 et 4 pour **22742A-LON-DC2**, **22742A-LON-SVR2**, et **22742A-TOR-DC1**.
6. Démarrer **22742A-TREY-DC1** et connectez-vous en tant qu'**TreyResearch\Administrateur** avec le mot de passe **Pa55w.rd**.

Exercice 1 : Implémentation d'approbations de forêts

Scénario

A. Datum travaille sur plusieurs projets prioritaires de concert avec une organisation partenaire nommée Trey Research. Pour simplifier le processus d'autorisation d'accès aux ressources situées dans les deux organisations, un WAN a été déployé entre Londres et Munich, où Trey Research se trouve. Vous devez alors mettre en œuvre et valider un lien de confiance entre les deux forêts et configurer l'approbation pour permettre l'accès à des serveurs sélectionnés uniquement à Londres.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les zones de stub pour la résolution de noms DNS
2. Configurer une approbation de forêt avec l'authentification sélective
3. Configurer un serveur pour l'authentification sélective

► Tâche 1 : Configurer les zones de stub pour la résolution de noms DNS

1. Sur **LON-DC1**, en utilisant la console **gestion des DNS**, configurer une zone de stub DNS pour **treyresearch.net** :
 - o Utiliser **172.16.10.10** comme serveur **DNS maître**.
2. Sur **TREY-DC1**, en utilisant la console **gestion des DNS**, configurer une zone de stub DNS pour **adatum.com** :
 - o Utiliser **172.16.0.10** comme serveur **DNS maître**.

► Tâche 2 : Configurer une approbation de forêt avec l'authentification sélective

1. Sur **LON-DC1**, créez une approbation sortante à sens unique entre la forêt AD DS **treyresearch.net** et la forêt **adatum.com**. Configurez l'approbation pour utiliser l'authentification sélective.
2. Confirmez et validez l'approbation de **treyresearch.net**.

► Tâche 3 : Configurer un serveur pour l'authentification sélective

1. Sur l'ordinateur **LON-DC1**, à partir du **Gestionnaire de serveurs**, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Configurez les autorisations d'objet d'ordinateur **LON-SVR2** afin que les membres du groupe **Treyresearch\IT** aient la permission **Autorisation de s'authentifier**. Si vous êtes invité à fournir des informations d'identification, saisissez **Treyresearch\Administrateur** avec le mot de passe **Pa55w.rd**.
3. Sur **LON-SVR2**, créer un dossier partagé nommé **IT-Données**, et accorder l'accès **Lire-écrire** aux membres du groupe **Treyresearch\IT**. Si vous êtes invité à fournir des informations d'identification, saisissez **Treyresearch\Administrateur** avec le mot de passe **Pa55w.rd**.
4. Ajouter le nom d'utilisateur **Alice** au groupe **Admins du domaine** dans le domaine **treyresearch**.
5. Déconnectez-vous de **TREY-DC1**.
6. Connectez-vous à **TREY-DC1** en tant que **Treyresearch\Alice** avec le mot de passe **Pa55w.rd**, et vérifiez que vous pouvez accéder au dossier partagé sur **LON-SVR2**.

Résultats : à la fin de cet exercice, vous devrez avoir implémenté les approbations de forêts.

Exercice 2 : Mise en œuvre des domaines enfants dans AD DS

Scénario

A. Datum a décidé de déployer un nouveau domaine enfant dans la forêt adatum.com pour la région de l'Amérique du Nord. Le premier contrôleur de domaine sera déployé à Toronto et le nom de domaine sera na.adatum.com. Vous devez configurer et installer le nouveau contrôleur de domaine.

Les tâches principales de cet exercice sont les suivantes :

1. Installer un contrôleur de domaine dans un domaine enfant.
2. Vérifier la configuration de la confiance par défaut.
3. Préparer le module suivant.

► Tâche 1 : Installer un contrôleur de domaine dans un domaine enfant

1. Sur **TOR-DC1**, démarrez **Gestionnaire de serveur** puis installez les AD DS binaires.
2. Lorsque les AD DS binaires sont installés, utilisez l'**Assistant Configuration des services de domaine Active Directory** pour installer et configurer **TOR-DC1** en tant que contrôleur de domaine AD DS pour un nouveau domaine enfant nommé **na.adatum.com**.
3. Lorsque vous êtes invité, utilisez **Pa55w.rd** comme mot de passe pour le **Mode restauration des services d'annuaire (DSRM)**. Une fois la configuration terminée, le serveur redémarre automatiquement.

► Tâche 2 : Vérifier la configuration de la confiance par défaut

1. Connectez-vous à **TOR-DC1** as **NA\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Assurez-vous que le pare-feu Windows est désactivé pour tous les profils.
3. À partir du **Gestionnaire de serveur**, lancez la console **Domaines et approbations Active Directory**, et vérifiez les approbations parent enfant.



Remarque : Si vous recevez un message que l'approbation ne peut pas être validée ou que la vérification de canal sécurisé a échoué, assurez-vous que vous avez terminé l'étape 2, puis attendez au moins de 10 à 15 minutes avant d'essayer à nouveau.

Résultats : à la fin de cet exercice, vous devez avoir implémenté des domaines enfants dans AD DS.

► Tâche 3 : Préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-DC2**, **22742A-TOR-DC1**, **22742A-TREY-DC1**, **22742A-LON-SVR2**, et **22741A-NA-RTR**.

Question : Lors de la création de l'approbation entre Adatum.com et TreyResearch.net, des zones de stub DNS ont été créées pour permettre la résolution de nom entre les deux forêts. Quelle autre solution auriez-vous pu utiliser à la place d'une zone de stub DNS ?

Question : Lorsque vous créez une approbation de forêt, pourquoi voudriez-vous créer une approbation sélective au lieu d'une approbation totale ?

Révision du module et éléments à retenir

Question de contrôle des acquis

Question : Vous êtes l'administrateur AD DS pour A. Datum Corporation. Actuellement, votre environnement AD DS est configuré dans un modèle de domaine unique, forêt unique en utilisant l'espace de noms adatum.com. A. Datum a récemment annoncé qu'ils sont en expansion de l'Europe vers de nouveaux continents grâce à l'acquisition d'une société nommée Trey Research. Trey Research opère actuellement en Amérique du Nord et en Asie. L'environnement AD DS de Trey Research se compose d'une seule forêt nommée treyresearch.net ayant un domaine racine de la forêt vide, et des domaines affiliés qui s'alignent sur chaque continent qu'ils opèrent dans (na.treyresearch.net et asia.treyresearch.net). Les objectifs à long terme pour A. Datum sont d'intégrer pleinement Trey Research dans les opérations quotidiennes de A. Datum. L'équipe de direction d'A. Datum souhaite également adopter le modèle régional des opérations utilisé par Trey Research. En tant qu'administrateur AD DS pour A. Datum, comment voulez-vous combiner la forêt de adatum.com avec la forêt de treyresearch.net ? Discuter des objectifs à court terme et à long terme de l'intégration AD DS et comment les différentes exigences pourraient changer votre approche.

Problèmes courants et conseils de dépannage

| Problème courant | Conseil pour la résolution du problème |
|--|--|
| Vous recevez des messages d'erreur tels que : <ul style="list-style-type: none"> ○ Échec de la recherche DNS ○ Serveur indisponible ○ Le domaine n'existe pas ○ Le contrôleur de domaine est introuvable | |
| L'utilisateur ne peut être authentifié pour accéder aux ressources sur un autre domaine AD DS ou Kerberos. | |

Module 4

Implémentation et administration des sites AD DS et réPLICATION

Sommaire :

| | |
|--|------|
| Vue d'ensemble du module | 4-1 |
| Leçon 1 : Vue d'ensemble de la réPLICATION AD DS | 4-2 |
| Leçon 2 : Configuration des sites AD DS | 4-11 |
| Leçon 3 : Configuration et surveillance de la réPLICATION AD DS | 4-20 |
| Atelier pratique : Implémentation des sites AD DS et réPLICATION | 4-27 |
| Contrôle des acquis et éléments à retenir | 4-33 |

Vue d'ensemble du module

Lorsque vous déployez les services de domaine Active Directory (AD DS), il est important de fournir une infrastructure de connexion efficace et un service d'annuaire hautement disponible. L'implémentation de plusieurs contrôleurs de domaine dans toute l'infrastructure vous aide à atteindre ces deux objectifs. Cependant, vous devez vous assurer que AD DS réplique les informations Active Directory entre chaque contrôleur de domaine dans la forêt.

Dans ce module, vous apprendrez comment AD DS réplique les informations entre les contrôleurs de domaine dans un site unique et à travers plusieurs sites. Vous apprendrez également comment créer des sites multiples et comment surveiller la réPLICATION pour optimiser la réPLICATION AD DS et le trafic d'authentification.

Objectifs

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

- Décrire comment la réPLICATION AD DS fonctionne.
- Configurer les sites AD DS pour aider à optimiser l'authentification et le trafic de réPLICATION.
- Configurer et surveiller la réPLICATION AD DS.

Leçon 1

Vue d'ensemble de la réPLICATION AD DS

Au sein d'une infrastructure AD DS, les contrôleurs de domaine standards répliquent les informations Active Directory en utilisant un modèle de réPLICATION maître multiple. Cela signifie que si un changement se produit sur un contrôleur de domaine, ce changement se réplique ensuite vers tous les autres contrôleurs de domaine dans le domaine et potentiellement vers tous les contrôleurs de domaine à travers l'ensemble de la forêt. Cette leçon donne un aperçu de la façon dont AD DS réplique l'information entre les contrôleurs de domaine standard et également les contrôleurs de domaine en lecture seule (RODC).

Objectifs de la leçon

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

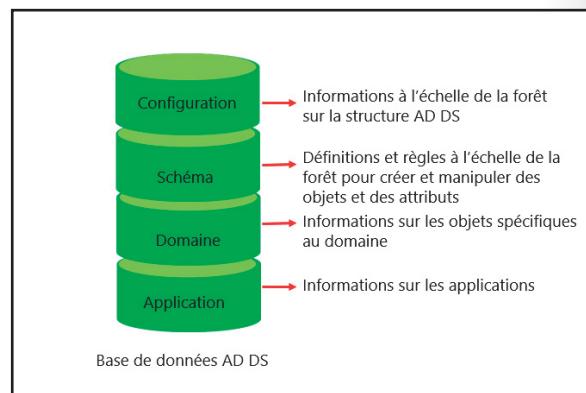
- Décrire des partitions AD DS.
- Décrire les caractéristiques de la réPLICATION AD DS.
- Expliquer comment fonctionne la réPLICATION AD DS dans un site.
- Expliquer comment résoudre les conflits de réPLICATION.
- Expliquer comment la topologie de réPLICATION est générée.
- Expliquer comment fonctionne la réPLICATION SYSVOL.

Quelles sont les partitions AD DS ?

Le magasin de données Active Directory contient des informations que AD DS distribue à tous les contrôleurs de domaine à travers l'infrastructure de la forêt. Une grande partie des informations contenues dans la banque de données sont distribuées dans un seul domaine. Toutefois, certaines informations peuvent être liées et reproduites dans la forêt entière, quelles que soient les limites du domaine.

Pour aider à offrir une efficacité et une évolutivité de réPLICATION entre les contrôleurs de domaine, les données Active Directory sont séparées

logiquement en plusieurs partitions. Chaque partition est une unité de réPLICATION et chaque partition a sa propre topologie de réPLICATION. Les partitions par défaut incluent les éléments suivants :



- Partition de configuration. La partition de configuration est créée automatiquement lorsque vous créez le premier contrôleur de domaine dans une forêt. La partition de configuration contient des informations sur la structure AD DS à l'échelle de la forêt, y compris quels domaines et sites existent et quels contrôleurs de domaine existent dans chaque domaine. La partition de configuration stocke également des informations sur les services à l'échelle de la forêt tels que DHCP (Dynamic Host Configuration Protocol) et des modèles de certificats d'autorisation. Cette partition est répliquée sur tous les contrôleurs de domaine de la forêt. Elle est plus petite que les autres partitions et ses objets ne changent pas souvent ; par conséquent, la réPLICATION est également peu fréquente.
- Partition de schéma. La partition de schéma contient les définitions de tous les objets et les attributs que vous pouvez créer dans le magasin de données, ainsi que les règles de création et de manipulation. Les informations de schéma sont répliquées sur tous les contrôleurs de domaine de la

forêt. Par conséquent, tous les objets doivent être conformes à toutes les règles de définition des objets et attributs de schéma. AD DS contient un ensemble de classes par défaut et des attributs que vous ne pouvez pas modifier. Toutefois, si vous avez des informations d'identification Schema Admins, vous pouvez étendre le schéma en ajoutant de nouveaux attributs et classes pour représenter les classes propres à l'application. De nombreuses applications telles que Microsoft Exchange Server et Microsoft System Center Configuration Manager peuvent étendre le schéma pour offrir des améliorations de configuration propres à l'application. Ces changements visent le contrôleur de domaine qui contient le rôle de maître de schéma de la forêt. Seul le maître de schéma est autorisé à faire des ajouts à des classes et des attributs. Semblable à la partition de configuration, la partition de schéma est petite et a besoin de se répliquer uniquement lorsque données qui y sont stockées subissent des changements, ce qui ne se produit pas souvent, sauf si le schéma est étendu.

- Partition de domaine. Lorsque vous créez un nouveau domaine, AD DS crée automatiquement et reproduit une instance de la partition de domaine vers tous les contrôleurs de domaine du domaine. La partition de domaine contient des informations sur tous les objets spécifiques à un domaine, y compris les utilisateurs, les groupes, les ordinateurs, les unités d'organisation (OU) et les paramètres du système relatifs aux domaines. Cela est généralement la plus grande des partitions AD DS car elle stocke tous les objets contenus dans le domaine. Les modifications apportées à cette partition sont assez constantes car chaque fois qu'un objet est créé, supprimé ou modifié en changeant la valeur d'un attribut, ces changements doivent ensuite être répliqués. Tous les objets dans chaque partition de domaine dans une forêt sont stockés dans le catalogue global avec seulement un sous-ensemble de leurs valeurs d'attribut.
- Partition d'application. Les magasins de partition d'application stockent informations relatives aux applications n'appartenant pas à un domaine qui peuvent tendre à être mises à jour fréquemment ou qui ont une durée de vie déterminée, comme une partition Domain Name System (DNS) lorsque le DNS intégré à Active Directory est activé. Une application est généralement programmée pour déterminer comment il stocke, catégorise et utilise des informations spécifiques à l'application qui sont stockées dans la base de données Active Directory. Pour empêcher la réPLICATION inutile d'une partition d'application, vous pouvez désigner quels contrôleurs de domaine dans une forêt accueilleront la partition de l'application spécifique. Contrairement à une partition de domaine, une partition d'application ne stocke pas des objets principaux de sécurité, tels que les comptes d'utilisateurs. De plus, le catalogue global ne stocke pas les données qui sont contenues dans les partitions d'application. La taille et la réPLICATION de la fréquence de la partition d'application peuvent varier considérablement selon l'utilisation. L'utilisation d'un DNS avec un Active Directory intégré avec un grand et robuste DNS de nombreux contrôleurs de domaine, serveurs et ordinateurs clients se traduit par la réPLICATION fréquente de la partition.



Remarque : Vous pouvez utiliser l'Active Directory Service Interfaces Editor (ADSI Edit) pour vous connecter aux partitions et les voir.

Caractéristiques de la réPLICATION AD DS

Une conception efficace de réPLICATION AD DS assure que chaque partition sur un contrôleur de domaine est compatible avec les répliques de cette partition qui sont hébergées sur d'autres contrôleurs de domaine. En règle générale, tous les contrôleurs de domaine ont exactement les mêmes informations dans leurs répliques à un moment donné, car des changements se produisent en permanence dans la partition. Cependant, la réPLICATION AD DS garantit que toutes les modifications apportées à une partition sont transférées à toutes les répliques de la partition. La réPLICATION AD DS (appelée *intégrité*) équilibre la précision et la consistance (appelée *convergence*) avec les performances, maintenant ainsi le trafic de réPLICATION à un niveau raisonnable.

- La réPLICATION à maître multiple assure :
 - Précision (intégrité)
 - Cohérence (convergence)
 - Performance (en maintenant le trafic de réPLICATION à un niveau raisonnable)
- Les principales caractéristiques de la réPLICATION AD DS comprennent :
 - RéPLICATION à maître multiple
 - RéPLICATION par extraction
 - RéPLICATION stockage et transfert
 - Cloisons
 - Génération automatique d'une topologie de réPLICATION efficace et robuste
 - RéPLICATION multivaleur et au niveau de l'attribut
 - Contrôle distinct de la réPLICATION intersite
 - Détection et gestion de collision

Les principales caractéristiques de la réPLICATION AD DS incluent :

- RéPLICATION maître multiple. Tout contrôleur de domaine, sauf un RODC, peut initier et engager un changement dans AD DS. Ceci fournit la tolérance aux pannes et élimine la dépendance par rapport à un seul contrôleur de domaine pour assurer les opérations du magasin d'annuaire.
- RéPLICATION par réception. Un contrôleur de domaine demande ou *tire*, les changements des autres contrôleurs de domaine. Même si un contrôleur de domaine peut notifier ses partenaires de réPLICATION de changements dans le répertoire, ou interroger ses partenaires pour voir s'ils ont des changements dans le répertoire, finalement, les contrôleurs de domaine demandent et tirent les changements eux-mêmes.
- RéPLICATION différée. Un contrôleur de domaine peut tirer les changements d'un partenaire de réPLICATION, puis mettre ces changements à la disposition d'un autre partenaire de réPLICATION. Par exemple, contrôleur de domaine B peut tirer changements initiés par le contrôleur de domaine A. Ensuite, le contrôleur de domaine C peut tirer les changements du contrôleur de domaine B. Cela permet d'équilibrer la charge de réPLICATION pour les domaines qui contiennent plusieurs contrôleurs de domaine.
- Partitionnement magasin de données. Les contrôleurs de domaine d'un domaine hébergent le contexte de nommage de domaine pour leurs domaines, ce qui contribue à réduire au minimum la réPLICATION, en particulier dans les forêts multidomaines. Les contrôleurs de domaine accueillent également des copies des partitions de schéma et configuration qui sont répliquées à l'échelle de la forêt. Cependant, les changements de partitions de configuration et de schéma sont beaucoup moins fréquents que dans la partition de domaine. Par défaut, d'autres données, y compris les partitions d'annuaire d'applications et l'ensemble d'attributs partiels (le catalogue global), ne se répliquent pas vers chaque contrôleur de domaine dans la forêt. Vous pouvez activer la réPLICATION pour qu'elle soit universelle en configurant tous les contrôleurs de domaine dans une forêt en tant que serveurs de catalogue global.
- Génération automatique d'une topologie de réPLICATION efficace et robuste. Par défaut, AD DS configure une topologie de réPLICATION multidirectionnelle et efficace de sorte que la perte d'un contrôleur de domaine ne fait pas obstacle à la réPLICATION. AD DS met automatiquement à jour cette topologie tandis que des contrôleurs de domaine sont ajoutés, supprimés ou déplacés entre les sites.

- RéPLICATION au niveau des attributs. Lorsque l'attribut d'un objet change, seuls cet attribut et les métadonnées minimales décrivant cet attribut sont répliqués. L'objet entier ne se réplique pas, à l'exception de sa création initiale. Pour les attributs à valeurs multiples, tels que les noms de compte dans les attributs **Membre de** d'un compte de groupe, seuls des changements dans des noms réels se répliquent et non pas la liste complète des noms.
- Contrôle distinct de la réPLICATION intersite. Vous pouvez contrôler la réPLICATION entre les sites.
- DéTECTION et gestion des collisions. Bien que rare, à l'intérieur d'une fenêtre de réPLICATION unique, il est possible de modifier un attribut sur deux contrôleurS de domaine différents, créant ainsi un conflit. Si cela se produit, vous devez concilier les deux changements. AD DS a des algorithmes de résOLUTION qui satisfont presque tous les scénarios.

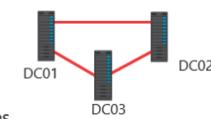
Comment la réPLICATION AD DS fonctionne-t-elle dans un site ?

La réPLICATION AD DS dans un seul site, qui a lieu automatiquement, est appelée *réPLICATION intrasite*. Cependant, vous pouvez également la configurer pour qu'elle se produise manuellement si des applications dans votre environnement exigent une planification de réPLICATION plus spécifique. Les concepts suivants se rapportent à la réPLICATION intrasite :

- Objets de connexion
- Vérificateur de cohérence des données
- Notification
- Sondage

La réPLICATION intrasite utilise :

- Objets de connexion pour la réPLICATION entrante dans un contrôleur de domaine
- Le vérificateur de cohérence des données crée automatiquement une topologie qui est efficace (trois tronçons au maximum) et robuste (bidirectionnelle)
- Notifications dans lesquelles le contrôleur de domaine informe ses partenaires en aval qu'un changement est disponible
- Interrogation, dans laquelle le contrôleur de domaine recherche des modifications avec ses partenaires en amont :
 - L'agent de réPLICATION du répertoire du contrôleur de domaine en aval réplique les modifications
 - Les modifications apportées à toutes les partitions détenues par les deux contrôleurS de domaine sont répliquées



Objets de connexion

Un contrôleur de domaine qui réplique les modifications d'un autre contrôleur de domaine est appelé *partenaire de réPLICATION*. Les objets de connexion relient les partenaires de réPLICATION. Un objet de connexion représente le chemin de réPLICATION d'un contrôleur de domaine à un autre. Les objets de connexion sont unidirectionnels, ce qui représente une réPLICATION par réCEPTION entrante uniquement.

Pour afficher et configurer des objets de connexion, ouvrez **Sites et services Active Directory**, puis sélectionnez le conteneur **Paramètres NTDS** de l'objet de serveur d'un contrôleur de domaine. Vous pouvez forcer la réPLICATION entre deux contrôleurS de domaine par un clic droit sur l'objet de connexion, puis en sélectionnant **Répliquer maintenant**. Notez que la réPLICATION est entrante seulement, donc si vous voulez répliquer les deux contrôleurS de domaine, vous devez répliquer l'objet de connexion entrant de chaque contrôleur de domaine.

Vérificateur de cohérence des données

Les chemins de réPLICATION que les objets de connexion construisent entre les contrôleurS de domaine créent la réPLICATION de la topologie de la forêt. Vous ne devez pas créer la topologie de réPLICATION manuellement. Par défaut, AD DS crée une topologie qui assure une réPLICATION efficace. La topologie est bidirectionnelle, ce qui signifie que si un contrôleur de domaine échoue, la réPLICATION se poursuit sans interruption. La topologie garantit également que pas plus de trois sauts de réseau se produisent entre deux contrôleurS de domaine.

Sur chaque contrôleur de domaine, un composant de AD DS appelé vérificateur de cohérence permet de générer et d'optimiser la réPLICATION automatiquement entre les contrôleurs de domaine dans un site. Le vérificateur de cohérence évalue les contrôleurs de domaine dans un site, puis crée des objets de connexion pour construire la topologie dans les deux sens et à trois sauts qui a été décrite plus haut. Si vous ajoutez ou supprimez un contrôleur de domaine, ou si un contrôleur de domaine ne répond pas, le vérificateur de cohérence réarrange la topologie dynamique, l'ajout et la suppression d'objets de connexion pour reconstruire une topologie de réPLICATION efficace. Le vérificateur de cohérence fonctionne à intervalles spécifiés (toutes les 15 minutes par défaut) et désigne les itinéraires de réPLICATION entre les contrôleurs de domaine qui sont les connexions les plus favorables disponibles à ce moment.

Vous pouvez créer manuellement des objets de connexion pour spécifier les chemins de réPLICATION qui devraient persister. Généralement, la création manuelle d'un objet de connexion n'est pas nécessaire ni recommandée, car le vérificateur de cohérence des données ne vérifie pas et n'utilise pas l'objet de connexion manuelle pour le basculement. Le vérificateur de cohérence des données ne supprime pas non plus les objets de connexion manuelle, ce qui signifie que vous ne devez pas oublier de supprimer les objets de connexion que vous créez manuellement.

Notification

Quand un changement se produit sur une partition Active Directory sur un contrôleur de domaine, le contrôleur de domaine met en attente le changement de réPLICATION de ses partenaires. Par défaut, le serveur source attend 15 secondes pour avertir son premier partenaire de réPLICATION du changement. La *Notification* est le processus par lequel un partenaire en amont informe ses partenaires en aval qu'un changement est disponible. Par défaut, le contrôleur de domaine source attend ensuite trois secondes entre les notifications à d'autres partenaires. Ces retards, appelés *délai de notification initiale* et le *retard ultérieur de notification*, sont conçus pour décaler le trafic réseau que la réPLICATION intrasite peut causer.

Après avoir reçu la notification, le partenaire en aval demande les modifications au contrôleur de domaine source et l'agent de réPLICATION d'annuaire tire les modifications du contrôleur de domaine source. Par exemple, supposez que le contrôleur de domaine **DC01** initialise un changement dans AD DS. Quand **DC02** reçoit le changement de **DC01**, il procède au changement dans son répertoire. **DC02** met le changement pour la réPLICATION en attente chez ses propres partenaires en aval.

Ensuite, supposons **DC03** soit un partenaire de réPLICATION en aval de **DC02**. Après 15 secondes, **DC02** notifie **DC03** qu'il a un changement. **DC03** effectue le changement répliqué dans son répertoire et il informe ensuite ses partenaires en aval. Le changement a fait deux sauts, de **DC01** à **DC02**, puis de **DC02** à **DC03**. La topologie de réPLICATION garantit que pas plus de trois sauts se produisent avant que tous les contrôleurs de domaine sur le site ne reçoivent le changement. Avec environ 15 secondes par saut, le changement est totalement répliqué sur le site en moins d'une minute.

Sondage

Parfois, un contrôleur de domaine peut ne pas apporter des modifications à ses répliques pendant une période prolongée, en particulier pendant les heures creuses. Supposons que cela est le cas avec **DC01**. Ceci veut dire que **DC02**, son partenaire de réPLICATION en aval, ne reçoit pas de notifications de **DC01**. **DC01** aussi peut-être en ligne, ce qui l'empêcherait d'envoyer des notifications à **DC02**.

Il est important que **DC02** sache que son partenaire en amont est en ligne et n'a tout simplement pas de modifications. Cela se produit par un processus appelé *interrogation*. Pendant l'interrogation, le partenaire de réPLICATION en aval en contacte le partenaire de réPLICATION en amont avec les requêtes pour savoir si des changements sont mis en attente pour la réPLICATION. Par défaut, l'intervalle d'interrogation pour la réPLICATION intrasite est une fois par heure. Vous pouvez configurer la fréquence d'interrogation à partir des propriétés d'un objet de connexion en cliquant sur **Modifier la planification**, bien que nous ne le recommandions pas.

Si un partenaire en amont ne parvient pas à répondre aux demandes répétées d'interrogation, le partenaire en aval lance le vérificateur de cohérence pour vérifier la topologie de réPLICATION. Si le serveur en amont est en effet hors ligne, le vérificateur de cohérence réarrange la réPLICATION de la topologie du site pour tenir compte du changement.

Question : Décrivez les circonstances qui se produisent lorsque vous créez manuellement un objet de connexion entre les contrôleurs de domaine dans un site.

Résolution des conflits de réPLICATION

Parce qu'AD DS prend en charge un modèle de réPLICATION maître multiple, des conflits de réPLICATION peuvent se produire. En règle générale, trois types de conflits de réPLICATION peuvent se produire dans AD DS :

- La modification simultanée de la même valeur d'attribut du même objet sur deux contrôleurs de domaine.
- L'ajout ou modification du même objet sur un contrôleur de domaine en même temps que l'objet conteneur pour l'objet est supprimé sur un autre contrôleur de domaine.
- L'ajout d'objets avec le même nom unique relatif dans le même conteneur sur différents contrôleurs de domaine en même temps.

• Dans les modèles de réPLICATION à maître multiple, les conflits de réPLICATION surviennent quand :

- Le même attribut est modifié sur deux contrôleurs de domaine simultanément
- Un objet est déplacé ou ajouté à un conteneur supprimé sur un autre contrôleur de domaine
- Deux objets avec le même nom unique relatif sont ajoutés au même conteneur sur deux contrôleurs de domaine différents

• Pour résoudre les conflits de réPLICATION, AD DS utilise :

- Numéro de version
- Horodatage
- GUID du serveur

Pour aider à minimiser les conflits, tous les contrôleurs de domaine de la forêt enregistrent et reproduisent des changements d'objet au niveau de l'attribut ou de la valeur plutôt qu'au niveau de l'objet. Par conséquent, la modification de deux attributs d'objets différents, tels que le mot de passe de l'utilisateur et le code postal, ne provoque pas un conflit, même si vous les modifiez en même temps à différents endroits.

Lorsqu'une mise à jour d'origine est appliquée à un contrôleur de domaine, un timbre est créé, qui se déplace avec la mise à jour tandis qu'il se réplique vers d'autres contrôleurs de domaine. Le timbre contient les composants suivants :

- Numéro de version. Le numéro de version commence à un pour chaque attribut d'objet et augmente de un pour chaque mise à jour. Lors de l'exécution d'une mise à jour d'origine, la version mise à jour de l'attribut est un nombre supérieur à la version de l'attribut qui est écrasée.
- Horodatage. L'horodatage est le temps et la date d'origine de la mise à jour dans le fuseau horaire universel, selon l'horloge système du contrôleur de domaine où le changement se produit.
- Identificateur unique au niveau mondial de serveur (GUID - Globally Unique Identifier). Le GUID du serveur identifie le contrôleur de domaine qui a effectué la mise à jour d'origine.

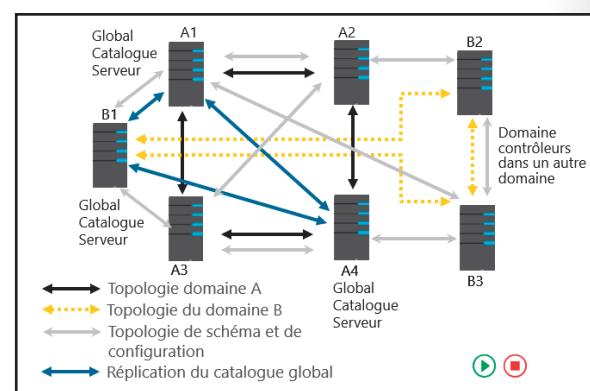
Conflits de réPLICATION habituels

Le tableau suivant présente plusieurs conflits et il décrit comment AD DS résout ces problèmes.

| Conflit | Résolution |
|--|---|
| Valeur d'attribut | Si la valeur du numéro de version est la même, mais que la valeur d'attribut est différente, alors l'horodateur est évalué. L'opération de mise à jour qui a la valeur la plus élevée du tampon remplace la valeur d'attribut de l'opération de mise à jour avec la valeur d'horodatage inférieure. Certains attributs à plusieurs valeurs peuvent être mis à jour, par exemple une valeur dans un attribut Membre de et seront traités comme des événements distincts réplifiables. |
| Ajouter ou déplacer sous un objet conteneur supprimé, ou la suppression d'un objet conteneur | Une fois la résolution effectuée sur toutes les répliques, AD DS supprime l'objet conteneur et l'objet de la feuille est faite d'un enfant du conteneur LostAndFound . Les tampons ne sont pas impliqués dans la présente résolution. |
| Ajout d'objets avec le même nom distinctif relatif | L'objet avec le tampon le plus ancien conserve le nom distinctif relatif. AD DS attribue à l'objet fraternel un nom distinctif relatif unique par le contrôleur de domaine. L'assignation de nom est le nom distinctif relatif + CNF : Un caractère réservé (l'astérisque, *) + GUID de l'objet. Cette assignation de nom garantit que le nom généré n'est pas en conflit avec le nom de tout autre objet. |

Comment la topologie de réPLICATION est-elle générée ?

La *topologie de réPLICATION* est la voie par laquelle les données de réPLICATION se déplacent à travers un réseau. Pour créer une topologie de réPLICATION, AD DS doit déterminer quels contrôleurs de domaine répliquent les données avec d'autres contrôleurs de domaine. AD DS crée une topologie de réPLICATION sur la base des informations que AD DS contient. Parce que chaque partition AD DS peut être répliquée vers différents contrôleurs de domaine d'un site, la topologie de réPLICATION peut différer pour les partitions de schéma, de configuration, de domaine et application.



Parce que tous les contrôleurs de domaine au sein d'une forêt partagent les partitions de schéma et de configuration, AD DS réplique les partitions de schéma et de configuration vers à tous les contrôleurs de domaine. Les contrôleurs de domaine dans le même domaine répliquent également la partition de domaine. En outre, les contrôleurs de domaine qui hébergent une partition d'application répliquent également la partition d'application. Pour optimiser le trafic de réPLICATION, un contrôleur de domaine peut avoir plusieurs partenaires de réPLICATION pour des partitions différentes. Dans un site unique, la topologie de réPLICATION est résistante -aux défaillances et redondante. Cela signifie que si le site contient plus de deux contrôleurs de domaine, chaque contrôleur de domaine a au moins deux partenaires de réPLICATION pour chaque partition AD DS.

Comment sont répliquées les partitions de schémas et de configuration ?

La réPLICATION de la partition de schéma et de configuration suit le même processus que toutes les autres partitions d'annuaire. Cependant, parce que ces partitions sont à l'échelle de la forêt plutôt que de l'ensemble du domaine, des objets de connexion pour ces partitions peuvent exister entre les deux contrôleurs de domaine, indépendamment du domaine du contrôleur de domaine. En outre, la topologie de réPLICATION pour ces partitions inclut tous les contrôleurs de domaine dans la forêt.

Comment le catalogue global affecte-t-il la réPLICATION ?

La partition de configuration contient des informations sur la topologie du site et d'autres données globales pour tous les domaines qui sont membres de la forêt. AD DS réPLIQUE la partition de configuration à tous les contrôleurs de domaine par le biais de la réPLICATION normale à l'échelle de la forêt. Chaque serveur de catalogue global obtient des informations de domaine en communiquant avec un contrôleur de domaine pour ce domaine et en obtenant les informations de réPLIQUE partielle. Chaque serveur de catalogue global a un accès complet à la partition de domaine de son propre domaine et par conséquent, n'a pas à demander un ensemble de réPLICATION partielle de ces informations. La partition de configuration fournit également des contrôleurs de domaine avec une liste de serveurs de catalogue global de la forêt.

Les serveurs de catalogue global enregistrent les enregistrements de service DNS dans la zone DNS qui correspond au domaine racine de la forêt. Ces documents, qui sont enregistrés uniquement dans la zone DNS racine de la forêt, aident les clients et les serveurs à localiser les serveurs de catalogue global dans la forêt pour offrir des services de connexion client.

Comment la réPLICATION SYSVOL fonctionne-t-elle ?

SYSVOL est une collection de fichiers et dossiers sur chaque contrôleur de domaine qui sont liés à l'emplacement %SystemRoot%\SYSVOL. SYSVOL contient des scripts de connexion et les objets qui se rapportent à la stratégie de groupe, tels que les modèles de stratégie de groupe. Le contenu du dossier SYSVOL est réPLIQUÉ sur chaque contrôleur de domaine dans le domaine en utilisant la topologie d'objet de connexion et le calendrier que le vérificateur de cohérence crée.

Selon la version du contrôleur de domaine du système d'exploitation, le niveau fonctionnel du domaine et l'état de la migration de SYSVOL, le service de réPLICATION de fichiers (FRS) ou la réPLICATION du système de fichiers distribués (DFS) réPLIQUE les changements SYSVOL entre contrôleurs de domaine. FRS a été utilisé principalement dans Windows Server 2003 R2 et les structures de domaine plus anciennes. FRS a des limites à la fois en termes de capacité et de performance, ce qui a conduit à l'adoption de la réPLICATION DFS. FRS n'est plus disponible sur les contrôleurs de domaine qui exécutent Windows Server 2012 R2 et versions antérieures lorsque le domaine est au niveau de domaine fonctionnel Windows Server 2012 R2 ou version supérieure. Si le niveau fonctionnel de la forêt est Windows Server 2008 R2 ou version ultérieure, la réPLICATION DFS est utilisée.

- SYSVOL contient des scripts d'ouverture de session, des modèles de stratégie de groupe et des GPO avec leur contenu
- La réPLICATION SYSVOL peut se faire en utilisant :
 - Le service de réPLICATION de fichiers (FRS), qui est principalement utilisé dans Windows Server 2003 et les structures de domaine antérieures
 - La réPLICATION DFS, qui est utilisée dans Windows Server 2008 et domaines ultérieurs
- Pour transférer la réPLICATION SYSVOL de FRS à la réPLICATION DFS :
 - Le niveau fonctionnel du domaine doit être au moins Windows Server 2008
 - Utilisez l'outil **Dfsrmig.exe** pour effectuer la migration

Dans Windows Server 2008 et les domaines ultérieurs, vous pouvez utiliser la réPLICATION DFS pour réPLiquer le contenu de SYSVOL. La réPLICATION DFS prend en charge la planification de la réPLICATION et la limitation de bande passante et elle utilise un algorithme de compression appelé compression différentielle à distance (RDC, Remote Differential Compression). En utilisant RDC, la réPLICATION DFS réPLique uniquement les différences ou les changements dans les fichiers entre les deux serveurs, entraînant une diminution de l'utilisation de la bande passante lors de la réPLICATION. Si un fichier qui est stocké dans SYSVOL change, la réPLICATION DFS va réPLiquer automatiquement les modifications de fichiers dans les dossiers SYSVOL sur les autres contrôleurS de domaine dans le domaine.



Remarque : Vous pouvez utiliser l'outil **Dfsrmig.exe** pour migrer la réPLICATION SYSVOL de FRS vers la réPLICATION DFS. Pour que la migration réussisse, le niveau fonctionnel du domaine doit être au moins Windows Server 2008.

Question : Pourquoi la réPLICATION est-elle importante dans le catalogue global ?

Leçon 2

Configuration des sites AD DS

Dans un site unique, la réPLICATION AD DS se produit automatiquement sans tenir compte de l'utilisation du réseau. Cependant, certaines entreprises ont de multiples emplacements reliés par des réseaux étendus (WAN, Wide Area Networks). Si tel est le cas, vous devez vous assurer que la réPLICATION AD DS n'a pas d'incidence négative sur l'utilisation du réseau entre les sites. Vous pourriez aussi avoir besoin de localiser des services de réseau à un emplacement spécifique. Par exemple, vous voudrez peut-être que les utilisateurs dans une succursale s'authentifient sur un contrôleur de domaine dans leur bureau local plutôt que sur la connexion WAN sur un contrôleur de domaine dans le bureau principal. Vous pouvez implémenter des sites AD DS pour aider à gérer la bande passante sur les connexions réseau lentes ou peu fiables et aider à la localisation de service pour l'authentification et de nombreux autres services conscients du site sur le réseau.

Objectifs de la leçon

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

- Décrire les sites AD DS.
- Expliquer pourquoi les entreprises peuvent implémenter des sites supplémentaires.
- Configurer des sites AD DS supplémentaires.
- Décrire comment fonctionne la réPLICATION entre les sites.
- Décrire le générateur de topologie intersite (ISTG).
- Décrire les enregistrements de ressources de service (SRV).
- Décrire comment les ordinateurs clients localisent les contrôleurs de domaine au sein des sites.
- Expliquer comment déplacer les contrôleurs de domaine entre les sites.

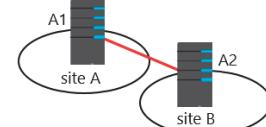
Quels sont les sites AD DS ?

Pour la plupart des administrateurs, un site est un lieu physique comme un bureau ou une ville qui est généralement séparé par une connexion WAN. Ces sites se connectent physiquement par des liens de réseau qui peuvent varier dans la bande passante disponible. Ensemble, des emplacements physiques et des liens constituent l'infrastructure de réseau physique.

AD DS représente l'infrastructure de réseau physique avec des objets appelés **sites**. Les objets du site AD DS sont stockés dans le conteneur de **Configuration** (CN = Sites, CN = Configuration, DC = *domaine racine de la forêt*) et sont utilisés pour réaliser trois tâches de gestion des services primaires :

- Gérer le trafic de réPLICATION Un site Active Directory représente une partie très connectée de votre entreprise. Lorsque vous définissez un site, les contrôleurs de domaine sur le site reproduisent les changements presque instantanément. Cependant, vous pouvez gérer et planifier la réPLICATION entre les sites selon les besoins. En règle générale, il existe deux types de connexions réseau au sein d'un environnement d'entreprise : hautement connectée et moins fortement connectée. De manière

- Les sites identifient les emplacements réseau avec des connexions réseau rapides et fiables
- Les sites sont associés à des objets de sous-réseau
- Les sites sont utilisés pour gérer :
 - La réPLICATION lorsque les contrôleurs de domaine sont séparés par des liaisons lentes et coûteuses
 - Localisation du service :
 - Authentification du contrôleur de domaine
 - Services ou applications prenant en charge AD DS (prise en charge de site)



conceptuelle, un changement apporté à AD DS devrait se répliquer immédiatement vers d'autres contrôleurs de domaine dans le réseau hautement connecté dans lequel le changement est survenu. Cependant, vous ne souhaitez peut-être pas que le changement se réplique vers un autre site immédiatement si vous avez un lien plus lent, plus cher, ou moins fiable. Au lieu de cela, vous pouvez optimiser les performances, réduire les coûts et gérer la bande passante en gérant la réPLICATION sur moins de segments hautement connectés de votre entreprise.

- Offrir un service de localisation. Les sites Active Directory vous aident à localiser les services, y compris ceux que les contrôleurs de domaine fournissent. Lors de la connexion, les clients Windows sont dirigés automatiquement vers les contrôleurs de domaine dans leurs sites. Si les contrôleurs de domaine ne sont pas disponibles dans leurs sites, ils sont dirigés vers les contrôleurs de domaine sur le site le plus proche qui peut authentifier le client efficacement. De nombreux autres services tels que les ressources DFS répliquées sont également conscients du site, afin d'assurer que les utilisateurs soient dirigés vers une copie locale de la ressource.
- Les objets de stratégie de groupe (GPO) peuvent être liés à un site. Dans ce cas, le site représente le sommet de la hiérarchie GPO AD DS et les paramètres GPO AD DS sont d'abord appliqués ici.

Que sont les objets de sous-réseau ?

Les *objets de sous-réseau* identifient les adresses de réseau qui correspondent à des ordinateurs de sites AD DS. Un *sous-réseau* est un segment d'un réseau TCP/IP auquel un ensemble d'adresses IP logiques sont affectées. Car les objets de sous-réseau mappent au réseau physique, tout comme les sites. Un site peut être constitué d'un ou plusieurs sous-réseaux. Par exemple, si votre réseau possède trois sous-réseaux à New York et deux à Londres, vous pouvez créer un site à New York et un à Londres, respectivement, puis ajouter les sous-réseaux aux sites respectifs.



Remarque : Lorsque vous concevez votre configuration de site AD DS, il est essentiel de mapper correctement les sous-réseaux IP aux sites. De même, si la configuration du réseau sous-jacent change, vous devez vous assurer que ces changements sont mis à jour pour refléter le sous-réseau IP actuel au mapping du site. Les contrôleurs de domaine utilisent les informations de sous-réseau IP dans AD DS pour mapper les ordinateurs clients et serveurs au site AD DS correct. Si ce mappage n'est pas précis, des opérations AD DS telles que l'authentification du trafic et l'application des stratégies de groupe sont susceptibles de se produire sur les liaisons WAN et peuvent se perturber.

Premier site par défaut

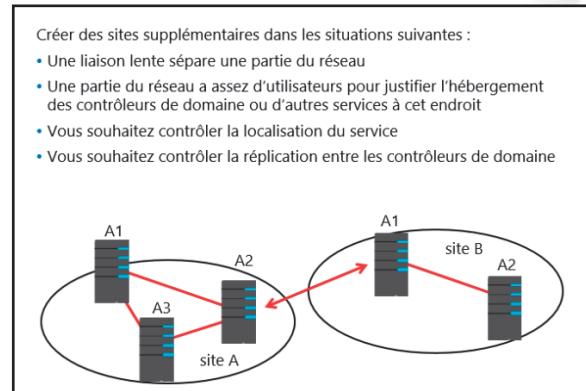
AD DS crée un site par défaut lorsque vous installez premier contrôleur de domaine de forêt. Par défaut, ce site est nommé **Default-First-Site-Name**. Vous pouvez donner un nom plus descriptif à ce site.

Lorsque vous installez le premier contrôleur de domaine de la forêt, AD DS le place automatiquement sur le site par défaut. Si vous avez un seul site, il est pas nécessaire de configurer des sous-réseaux ou des sites supplémentaires, parce que toutes les machines seront couvertes par le site **Default-First-Site-Name** par défaut. Cependant, plusieurs sites devraient avoir des sous-réseaux qui leur sont associés au besoin.

Pourquoi implémenter des sites supplémentaires ?

Chaque forêt Active Directory comprend au moins un site. Vous devez créer des sites supplémentaires lorsque :

- Une liaison lente sépare une partie du réseau. Comme mentionné précédemment, un site est caractérisé par un emplacement ayant une connectivité rapide, fiable et peu coûteuse. Si deux sites sont reliés par une liaison lente, vous devez configurer chaque emplacement comme site AD DS distinct. Un lien lent est généralement celui qui a une connexion inférieure à 512 kilobits par seconde (Kbps).
- Une partie du réseau a assez d'utilisateurs pour justifier l'hébergement des contrôleurs de domaine ou d'autres services à cet endroit. Les concentrations d'utilisateurs peuvent également influer sur la conception de votre site. Si un emplacement de réseau dispose d'un nombre suffisant d'utilisateurs pour lesquels l'incapacité de s'authentifier serait problématique, placez un contrôleur de domaine dans l'emplacement pour prendre en charge l'authentification au sein de l'emplacement. Après avoir placé un contrôleur de domaine ou un autre service distribué à un emplacement qui prend en charge les utilisateurs, vous pouvez gérer la réplication AD DS vers l'emplacement ou localiser l'utilisation des services en configurant un site Active Directory pour représenter l'emplacement.
- Vous voulez contrôler le service de localisation. En établissant des sites AD DS, vous pouvez vous assurer que les clients utilisent les contrôleurs de domaine qui sont les plus proches d'eux pour l'authentification, ce qui réduit la latence et l'authentification du trafic sur les connexions WAN. Dans la plupart des scénarios, chaque site contient un contrôleur de domaine. Cependant, vous pouvez configurer des sites pour localiser les services autres que l'authentification, tels que DFS, Windows BranchCache et les services Exchange Server. Dans ce cas, certains sites peuvent être configurés sans un contrôleur de domaine.
- Vous souhaitez contrôler la réplication entre les contrôleurs de domaine. Il peut exister des scénarios dans lesquels deux contrôleurs de domaine bien connectés sont autorisés à communiquer seulement à certains moments de la journée. La création de sites vous permet de contrôler quand et comment a lieu la réplication entre les contrôleurs de domaine.



Démonstration : Configuration des sites AD DS

Dans cette démonstration, vous allez apprendre à configurer des sites AD DS.

Procédure de démonstration

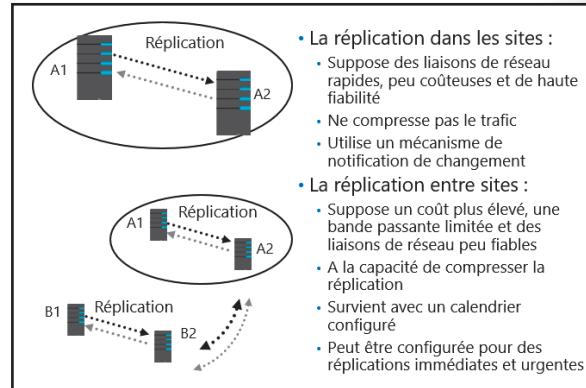
1. Sur l'ordinateur **LON-DC1**, à partir du **Gestionnaire de serveurs**, ouvrez **Sites et services Active Directory**.
2. Renommez le site **Default-First-Site-Name LondonHQ**.
3. Cliquez avec le bouton droit sur le nœud **Sites**, puis cliquez sur **Nouveau site**. Indiquez le nom **Toronto**, puis associez le nouveau site au lien du site par défaut.
4. Créer des sites supplémentaires au besoin.
5. Dans le volet de navigation, cliquez avec le bouton droit sur **Sous-réseaux**, puis cliquez sur **Nouveau sous-réseau**.

6. Fournir le préfixe **172.16.0.0/24**, puis associez le préfixe IP à un objet de site disponible.
7. Si nécessaire, déplacez un contrôleur de domaine vers le nouveau site.

Comment la réPLICATION entre les sites fonctionne-t-elle ?

Les principales caractéristiques de la réPLICATION au sein d'un site sont les suivantes :

- Les connexions réseau au sein d'un site sont fiables et ont une bande passante disponible suffisante.
- Le trafic de réPLICATION dans un site n'est pas comprimé, car un site suppose des connexions réseau très rapides et fiables. Ne pas compresser le trafic de réPLICATION permet de réduire la charge de traitement sur les contrôleurs de domaine. Cependant, le trafic non compressé peut augmenter la bande passante du réseau.



Les principales caractéristiques de la réPLICATION entre les sites sont les suivantes :

- Les liens de réseau entre les sites ont limité la bande passante disponible peuvent avoir un coût plus élevé et peuvent ne pas être fiables.
- Le trafic de réPLICATION entre les sites peut être conçu pour optimiser la bande passante en comprimant l'ensemble du trafic de réPLICATION. Le trafic de réPLICATION est comprimé à 10 pour cent à 15 pour cent de sa taille d'origine avant qu'il ne transmette. Bien que la compression optimise la bande passante du réseau, elle impose une charge de traitement supplémentaire sur les contrôleurs de domaine quand elle compresse et décomprime les données de réPLICATION.
- La réPLICATION entre les sites se produit automatiquement après avoir défini les valeurs configurables comme un calendrier ou un intervalle de réPLICATION. Vous pouvez planifier la réPLICATION pendant des heures bon marché ou hors pointe. Par défaut, les modifications sont répliquées entre les sites selon un calendrier que vous définissez et non selon le moment où les changements se produisent. L'intervalle spécifie la fréquence à laquelle les contrôleurs de domaine vérifient les changements au cours de la période où la réPLICATION peut se produire.

Modifier les notifications entre sites AD DS

De par leur nature, les changements dans les sites AD DS sont répliqués entre les contrôleurs de domaine dans différents sites selon un calendrier de réPLICATION défini et non selon le moment auquel les changements se produisent, comme avec la réPLICATION intrasite. De ce fait, le temps de latence de réPLICATION dans la forêt peut être égal à la somme des plus grandes latences de réPLICATION le long du trajet le plus long de réPLICATION d'une partition d'annuaire. Dans certains cas, cela peut être inefficace.

Pour éviter la latence de réPLICATION, vous pouvez configurer les notifications de changement sur les connexions entre les sites. En modifiant l'objet lien de site, vous pouvez activer la notification de changement entre les sites pour toutes les connexions qui se produisent sur ce lien. Parce que le partenaire de réPLICATION à travers le site reçoit la notification des changements, l'intervalle de réPLICATION intersite est effectivement ignoré. Le contrôleur de domaine d'origine informe le contrôleur de domaine dans l'autre site qu'il présente un changement, comme il le fait dans un site unique.

Pour des changements tels que le verrouillage de compte ou des changements liés à la sécurité similaires, la réPLICATION IMMÉDIATE est cruciale. Dans ces situations, la réPLICATION D'URGENCE est utilisée. La *réPLICATION D'URGENCE* contourne le délai de notification et les processus changent les notifications immédiatement. Ceci ne concerne que les notifications de changement. Si vous ne disposez pas de notifications de changement activées entre les sites, la réPLICATION HONORE encore l'intervalle de réPLICATION sur le lien du site.

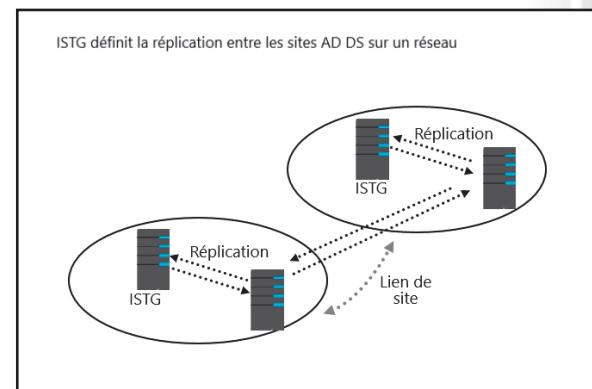


Remarque : Lorsque le mot de passe d'un utilisateur change, la réPLICATION IMMÉDIATE est initiée au domaine principal des opérations de l'émulateur du contrôleur maître. Cela diffère de la réPLICATION D'URGENCE, car elle se produit immédiatement, sans tenir compte de l'intervalle de réPLICATION intersite.

Qu'est-ce que le générateur de topologie intersite (ISTG, Inter-Site Topology Generator) ?

Lorsque vous configurez plusieurs sites, le vérificateur de cohérence sur un contrôleur de domaine dans chaque site est désigné comme ISTG du site. Il n'y a qu'un seul ISTG par site, quel que soit le nombre de domaines ou d'autres partitions d'annuaire le site comprend. ISTG est responsable du calcul idéal topologie de réPLICATION du site à travers les liens du site.

Lorsque vous ajoutez un nouveau site à la forêt, chaque ISTG de site détermine quelles partitions d'annuaire sont présentées dans le nouveau site. Le ISTG calcule ensuite le nombre de nouveaux objets de connexion nécessaires pour répliquer les informations requises par le nouveau site.



Serveurs têtes de pont

Dans certains réseaux, vous pouvez spécifier que seuls certains contrôleurs de domaine sont responsables de la réPLICATION INTERSITE. Vous pouvez le faire en spécifiant les serveurs de tête de pont. Les serveurs de tête de pont sont responsables de toute réPLICATION dans et hors du site. ISTG crée l'accord de connexion requis dans son répertoire et cette information est ensuite répliquée sur le serveur tête de pont. Le serveur tête de pont crée alors une connexion de réPLICATION avec le serveur tête de pont sur le site distant et la réPLICATION commence. Si un partenaire de réPLICATION devient indisponible, le ISTG sélectionne, si possible, un autre contrôleur de domaine automatiquement. Si les serveurs têtes de pont ont été attribués manuellement et s'ils ne sont plus disponibles, ISTG ne sélectionne pas automatiquement d'autres serveurs.

Sélection de serveurs têtes de pont

Le ISTG sélectionne automatiquement les serveurs de tête de pont et crée la topologie de réPLICATION intersite pour assurer que les changements se répliquent efficacement entre les serveurs têtes de pont qui partagent un lien de site. Les serveurs tête de pont sont sélectionnés par partition, il est donc possible qu'un contrôleur de domaine dans un site puisse être le serveur tête de pont pour le schéma, tandis qu'un autre l'est pour la configuration. Cependant, vous trouverez généralement qu'un contrôleur de domaine est le serveur tête de pont pour toutes les partitions dans un site à moins qu'il n'y ait des contrôleurs de domaine d'autres domaines ou partitions d'annuaire d'applications. Dans ce scénario, les serveurs têtes de pont seront choisis pour ces partitions. Les serveurs têtes de pont désignés sont également utiles lorsque vous avez des pare-feu entre les sites qui permettent uniquement la réPLICATION entre des contrôleurs de domaine spécifiques.

Vue d'ensemble des enregistrements SRV

Lorsque vous ajoutez un contrôleur de domaine à un domaine, le contrôleur de domaine annonce ses services en créant l'enregistrement de ressources de service (SRV) (également connu sous le nom *enregistrements de localisation*) dans le DNS. Contrairement aux enregistrements de ressources de l'hôte (A), convertissant les noms d'hôte en adresses IP, les services de conversion des enregistrements SRV en noms d'hôtes. Par exemple, pour publier sa capacité à fournir un accès d'authentification et de répertoire, un contrôleur de domaine enregistre protocole Kerberos version 5 et les enregistrements SRV LDAP (Lightweight Directory Access Protocol). Ces enregistrements SRV sont ajoutés à plusieurs dossiers dans les zones DNS de la forêt.

| <ul style="list-style-type: none"> Les contrôleurs de domaine enregistrent les enregistrements SRV comme suivit : _tcp.adatum.com : Tous les contrôleurs de domaine dans le domaine _tcp.nom du site._sites.adatum.com : Tous les services dans un site spécifique | | | | | | | | | | | | | | | | |
|--|------------------------------|------------------------------|------------------------------|---------|------|------------------------------|-----------------|---------------------|-----------|------------------------------|--------------|---------------------|-------|------------------------------|---------------|---------------------|
| <table border="1"> <thead> <tr> <th>Nom</th> <th>Type</th> <th>Emplacement du service (SRV)</th> <th>Données</th> </tr> </thead> <tbody> <tr> <td>_tcp</td> <td>Emplacement du service (SRV)</td> <td>[0][0][0][3268]</td> <td>lon-dc1.adatum.com.</td> </tr> <tr> <td>_kerberos</td> <td>Emplacement du service (SRV)</td> <td>[0][100][88]</td> <td>lon-dc1.adatum.com.</td> </tr> <tr> <td>_ldap</td> <td>Emplacement du service (SRV)</td> <td>[0][100][389]</td> <td>lon-dc1.adatum.com.</td> </tr> </tbody> </table> | Nom | Type | Emplacement du service (SRV) | Données | _tcp | Emplacement du service (SRV) | [0][0][0][3268] | lon-dc1.adatum.com. | _kerberos | Emplacement du service (SRV) | [0][100][88] | lon-dc1.adatum.com. | _ldap | Emplacement du service (SRV) | [0][100][389] | lon-dc1.adatum.com. |
| Nom | Type | Emplacement du service (SRV) | Données | | | | | | | | | | | | | |
| _tcp | Emplacement du service (SRV) | [0][0][0][3268] | lon-dc1.adatum.com. | | | | | | | | | | | | | |
| _kerberos | Emplacement du service (SRV) | [0][100][88] | lon-dc1.adatum.com. | | | | | | | | | | | | | |
| _ldap | Emplacement du service (SRV) | [0][100][389] | lon-dc1.adatum.com. | | | | | | | | | | | | | |

Dans la zone de domaine, un dossier nommé **_tcp** contient les enregistrements SRV pour tous les contrôleurs de domaine dans le domaine. De plus, dans la zone de domaine se trouve un dossier nommé **_sites**, qui contient des sous-dossiers pour chaque site configuré dans le domaine. Chaque dossier spécifique du site contient des enregistrements SRV qui représentent les services qui sont disponibles sur le site. Par exemple, si un contrôleur de domaine est situé dans un site, un enregistrement SRV est situé au niveau du chemin **-sites\nom du site\ _tcp**, où **nom du site** est le nom du site.

Un enregistrement SRV typique contient les informations suivantes :

- Le nom du service et le port. Cette portion de l'enregistrement SRV indique un service avec un port fixe. Il n'a pas besoin d'être un port connu. Les enregistrements SRV comprennent LDAP (port 389), Kerberos (port 88), le protocole d'authentification Kerberos V5 (kpasswd, le port 464) et les services de catalogue global (port 3268).
- Protocole. Le Transmission Control Protocol (TCP) ou User Datagram Protocol (UDP) est indiqué en tant que protocole de transport pour le service. Le même service peut utiliser les deux protocoles dans les enregistrements SRV séparés. Les enregistrements Kerberos, par exemple, sont enregistrés pour les protocoles TCP et UDP. Les clients de Microsoft utilisent uniquement TCP, mais les clients d'UNIX peuvent utiliser à la fois UDP et TCP.
- Nom d'hôte. Le nom d'hôte correspond à l'enregistrement d'hôte (A) des ressources pour le serveur qui héberge le service. Lorsqu'un client demande un service, le serveur DNS renvoie l'enregistrement SRV et les enregistrements de ressources d'hôte associé (A) de sorte que le client n'a pas besoin de présenter une requête distincte pour résoudre l'adresse IP du service.

Le nom du service dans un enregistrement SRV suit la hiérarchie DNS standard avec des composants séparés par des points. Par exemple, le service Kerberos d'un contrôleur de domaine est enregistré comme : **kerberos._tcp.nom du site._sites.nom de domaine**, où :

- Kerberos est un centre de distribution de clés Kerberos qui utilise TCP comme protocole de transport.
- _tcp** est n'importe lequel des services basés sur TCP sur le site.
- nom du site** est le site du contrôleur de domaine qui enregistre le service.
- _sites** est l'ensemble des sites qui sont enregistrés avec DNS.
- nom de domaine** est le nom de domaine ou d'une zone, par exemple, **contoso.com**.

Comment les ordinateurs clients localisent-ils les contrôleurs de domaine au sein des sites ?

Lorsque vous joignez un système d'exploitation client Windows à un domaine, puis redémarrez, le client termine un processus d'emplacement et d'inscription de contrôleur de domaine. Le but de ce processus d'inscription est de localiser le contrôleur de domaine avec l'emplacement le plus efficace et le plus proche de l'emplacement du client selon les informations de sous-réseau.

Le procédé de localisation d'un contrôleur de domaine est le suivant :

1. Le nouveau client cherche tous les contrôleurs de domaine dans le domaine. Tandis que le nouveau client de domaine redémarre, il reçoit une adresse IP d'un serveur DHCP et est prêt à s'authentifier sur le domaine. Toutefois, le client ne sait pas où trouver un contrôleur de domaine. Par conséquent, le client interroge un contrôleur de domaine en interrogeant le dossier **_tcp**, qui contient les enregistrements SRV pour tous les contrôleurs de domaine dans le domaine.
2. Le client tente un ping LDAP sur tous les contrôleurs de domaine dans une séquence. DNS renvoie une liste de tous les contrôleurs de domaine correspondants et le client tente de tous les contacter au premier démarrage.
3. Le premier contrôleur de domaine répond. Le premier contrôleur de domaine qui répond au client examine l'adresse IP du client, croise cette adresse avec des objets sous-réseau et informe le client du site auquel appartient le client. Le client stocke le nom du site dans son registre, puis interroge pour les contrôleurs de domaine dans le dossier propre au site **_tcp**.
4. Le client cherche tous les contrôleurs de domaine sur le site. Le DNS renvoie une liste de tous les contrôleurs de domaine sur le site.
5. Le client tente une séquence de ping LDAP sur tous les contrôleurs de domaine sur le site. Le contrôleur de domaine qui répond le premier authentifie le client.
6. Le client crée un lien. Le client crée un lien avec le contrôleur de domaine qui a répondu en premier, puis tente de s'authentifier avec le même contrôleur de domaine à l'avenir. Si le contrôleur de domaine est indisponible, le client interroge le dossier du site **_tcp** à nouveau et tente à nouveau de se lier au premier contrôleur de domaine qui répond sur le site.

Si le client se déplace vers un autre site, ce qui peut être le cas avec un ordinateur portable, le client tente de s'authentifier à son contrôleur de domaine préféré. Le contrôleur de domaine remarque que l'adresse IP du client est associée à un site différent et il renvoie alors le client vers le nouveau site. Le client interroge tous les contrôleurs de domaine sur le site local.

Couverture du site automatique

Vous pouvez configurer des sites pour diriger les utilisateurs vers des copies locales des ressources dupliquées, telles que les dossiers partagés répliqués au sein d'un espace de noms DFS. Il peut y avoir des scénarios dans lesquels vous n'aurez besoin que de la localisation des services sans avoir besoin d'un contrôleur de domaine situé sur le site. Dans ce cas, un contrôleur de domaine à proximité enregistre ses enregistrements SRV sur le site en utilisant un processus appelé *la couverture du site*.

Le procédé de localisation d'un contrôleur de domaine est le suivant :

1. Le nouveau client cherche tous les contrôleurs de domaine dans le domaine
2. Le client tente une séquence de ping LDAP pour trouver tous les contrôleurs de domaine
3. Le premier contrôleur de domaine répond
4. Le client cherche tous les contrôleurs de domaine dans le site
5. Le client tente une séquence de ping LDAP pour trouver tous les contrôleurs de domaine dans le site
6. Le client forme une affinité

Un site sans un contrôleur de domaine est généralement couvert par un contrôleur de domaine dans un site avec le plus bas coût de lien de site sur le site qui nécessite une couverture. Vous pouvez également configurer la couverture du site et la priorité d'enregistrement SRV manuellement si vous souhaitez contrôler l'authentification dans les sites sans contrôleur de domaine.

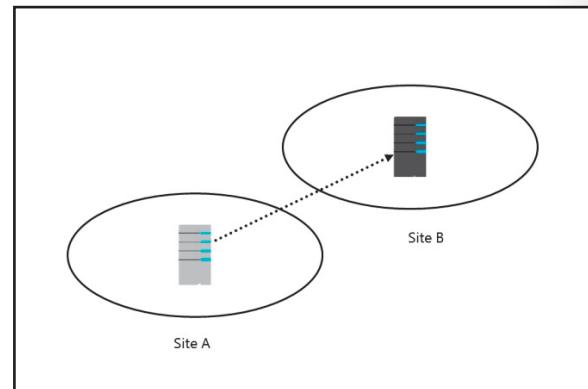


Lectures supplémentaires : Pour plus d'informations, consultez : « Trouver un contrôleur de domaine sur le site le plus proche » sur : <http://aka.ms/Cjpzdd>

Déplacement des contrôleurs de domaine entre les sites

Vous pouvez déplacer les contrôleurs de domaine entre les sites si nécessaire. Pour déplacer un contrôleur de domaine, procédez comme suit en utilisant un compte avec des priviléges d'administrateur de domaine :

1. Déplacer le contrôleur de domaine vers le nouveau site.
2. Sur un autre contrôleur de domaine dans le même domaine, ouvrir **Sites et services Active Directory**.
3. Développer le site qui contient le contrôleur de domaine que vous souhaitez déplacer.
4. Cliquez avec le bouton droit sur le contrôleur de domaine que vous souhaitez déplacer, puis cliquez sur **Déplacer**.
5. Choisir le nouveau site de la liste.



Dans certaines situations, une entreprise peut avoir des ordinateurs dans un endroit qui n'a pas les contrôleurs de domaine ou là où les contrôleurs de domaine sont indésirables. Vous pouvez créer des sites sans contrôleurs de domaine. Cependant, comme indiqué ci-dessus, le site n'aurait alors pas de liste de contrôleur de domaine correspondante dans le chemin `_sites\sitename\tcp`. Dans ce cas, plusieurs solutions possibles existent :

- Déployer RODC. Si l'entretien du contrôleur de domaine et la sécurité de la base de données AD DS qu'il contient sont les principales préoccupations, vous pouvez déployer des RODC.
- Utiliser la couverture de site automatique. Dans le cas d'un site vide, un contrôleur de domaine du prochain site le plus proche décide automatiquement de prendre soin de ce site et enregistre également ses enregistrements pour ce site. Vous pouvez ajuster ou forcer cela en utilisant la stratégie de groupe.
- Ajouter le sous-réseau à un site existant. Si le site est bien relié avec seulement quelques ordinateurs, vous voudrez peut-être éviter le coût du maintien d'un serveur là-bas. Dans ce cas, vous pouvez ajouter le sous-réseau local du site à un emplacement central ou à un emplacement de site de centre de données avec plusieurs contrôleurs de domaine.

Dans l'exemple de la section de l'enregistrement SRV dans le sujet « Vue d'ensemble des enregistrements SRV », les ordinateurs clients à l'emplacement distant sans contrôleur de domaine seraient identifiés comme appartenant au site central. Ce serait un problème uniquement si les contrôleurs de domaine du site central n'étaient pas disponibles. Dans ce cas, les clients peuvent utiliser les informations d'identification mises en cache pour s'authentifier localement. Parce que le pont de lien de site automatique, qui sera traité dans la prochaine leçon, est activé par défaut, l'authentification de domaine peut encore avoir lieu sur le pont de lien de sites où plusieurs sites existent.

Testez vos connaissances

| Question | |
|---|---|
| Lequel des éléments suivants n'est pas à considérer pour l'implémentation des sites AD DS ? | |
| Sélectionnez la réponse correcte. | |
| | Réduction de l'utilisation de la bande passante entre les sites du réseau. |
| | Appliquer les paramètres de stratégie de groupe dans un emplacement unique de votre entreprise. |
| | Déterminer le contrôleur de domaine utilisé par les ordinateurs client pour l'authentification. |
| | Créer un site de sauvegarde pour la reprise après sinistre. |
| | Contrôler l'accès aux applications et services pour un certain segment de votre réseau. |

Leçon 3

Configuration et surveillance de la réPLICATION AD DS

Après avoir configuré les sites qui représentent votre infrastructure de réseau, l'étape suivante consiste à déterminer si des liens de site supplémentaires sont nécessaires pour aider à gérer la réPLICATION AD DS. AD DS offre plusieurs options que vous pouvez configurer pour contrôler la façon dont la réPLICATION se produit sur les liens du site. Vous devez aussi comprendre les outils que vous pouvez utiliser pour surveiller et gérer la réPLICATION dans un environnement de réseau AD DS.

Objectifs de la leçon

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

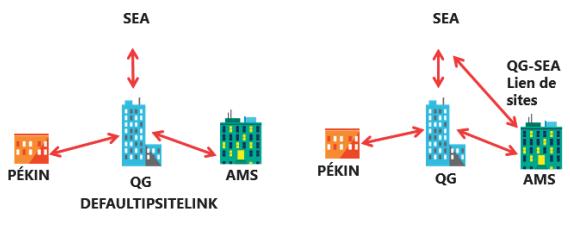
- Décrire les liens de site AD DS.
- Expliquer le concept de pont de liaison de site.
- Décrire la mise en cache d'appartenance au groupe universel.
- Décrire comment gérer la réPLICATION intersite.
- Configurer la réPLICATION intersite AD DS.
- Décrire les outils pour le suivi et la gestion de la réPLICATION.

Quels sont les liens de site AD DS ?

Pour que deux sites échangent des données de réPLICATION, un lien de site doit les relier. Un *lien de site* est un chemin logique que le vérificateur de cohérence de données et ISTG utilisent pour établir la réPLICATION entre sites. Lorsque vous créez des sites supplémentaires, vous devez sélectionner au moins un lien de site qui relie le nouveau site à un site existant. Sauf si un lien de site est en place, le vérificateur de cohérence de données ne peut pas établir des connexions entre des ordinateurs sur des sites différents et la réPLICATION ne se produit pas entre les sites.

Les liens de site contiennent des sites

- Dans un lien de site, un objet de connexion peut être créé entre deux contrôleurs de domaine
- Le lien de site par défaut, DEFAULTSITELINK, ne convient pas toujours à votre topologie de réseau



Contrôle de chemins de réPLICATION avec des liens de site

Il est important de se rappeler qu'un lien de site représente un chemin disponible pour la réPLICATION. Un lien de site unique ne contrôle pas les routes du réseau qui sont utilisées. Lorsque vous créez un lien de site et y ajoutez des sites, vous dites à AD DS qu'il peut se répliquer entre l'un des sites associés avec le lien de site. Le ISTG crée des objets de connexion et ces objets déterminent le chemin de réPLICATION réel. Bien que la topologie de réPLICATION que l'ISTG construit réponde AD DS efficacement, elle peut ne pas être efficace avec la topologie de votre réseau.

Pour mieux comprendre ce concept, prenons l'exemple suivant. Lorsque vous créez une forêt, un seul site objet lien est créé : **DEFAULTSITELINK**. Par défaut, chaque nouveau site que vous ajoutez est associé à **DEFAULTSITELINK**. **DEFAULTSITELINK** et tous les autres liens de sites existants ont un coût par défaut de 100 et une période de réPLICATION par défaut de 180 minutes.

Prenons l'exemple d'une entreprise avec trois bureaux et un centre de données au siège. Les trois bureaux chacun se connectent au centre de données avec un lien dédié. Vous créez des sites pour chaque succursale : Seattle (**SEA**), Amsterdam (**AMS**) et **Beijing (Pékin)**. Chacun des sites, y compris le siège, est associé à l'objet de lien du site **DEFAULTTIPSITELINK**.

Parce que tous les quatre sites sont sur le même lien de site, vous indiquez à AD DS que les quatre sites peuvent se répliquer les uns avec les autres. Cela signifie que Seattle peut répliquer les modifications d'Amsterdam ; Amsterdam peut répliquer les modifications de Beijing (Pékin) ; et Beijing (Pékin) peut répliquer les modifications du siège, qui à son tour réplique les modifications de Seattle. Dans plusieurs de ces chemins de réPLICATION, le trafic de réPLICATION sur le réseau circule à travers le siège en allant d'une branche à l'autre. Avec un lien de site unique, vous ne créez pas une topologie de réPLICATION hub-and-spoke, même si la topologie de votre réseau est hub-and-spoke.

Pour aligner votre topologie de réseau sur la réPLICATION AD DS, vous devez créer des liens spécifiques du site. Autrement dit, vous pouvez créer manuellement des liens de sites qui reflètent votre topologie de réPLICATION prévue. En reprenant l'exemple précédent, vous devez créer trois liens de site comme suit :

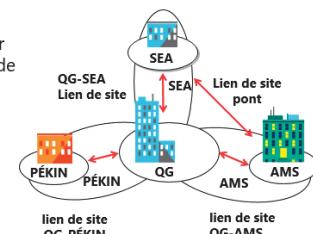
- **QG-AMS** inclut le siège et les sites d'Amsterdam.
- **QG-SEA** inclut le siège et les sites de Seattle.
- **QG-Beijing (Pékin)** inclut le siège et les sites de Beijing (Pékin).

Après avoir créé des liens de site, l'ISTG utilise la topologie pour construire une topologie de réPLICATION intersite qui relie chaque site, puis créé des objets de connexion automatiquement pour configurer les chemins de réPLICATION. En tant que meilleure pratique, vous devez configurer votre topologie de site correctement et éviter de créer des objets de connexion manuellement.

Qu'est-ce qu'un pontage de lien de site ?

Après avoir créé des liens de site et que l'ISTG génère des objets de connexion pour répliquer les partitions entre les contrôleurs de domaine qui partagent un lien de site, votre travail peut se terminer. Dans de nombreux environnements, en particulier ceux avec des topologies de réseau simples, des liens de site peuvent être suffisants pour gérer la réPLICATION intersite. Dans les réseaux plus complexes, cependant, vous pouvez configurer des composants supplémentaires et des propriétés de réPLICATION.

- Par défaut, le pontage automatique de lien de site :
 - Permet à l'ISTG de créer des objets de connexion entre les liens de site
 - Permet de désactiver la transitivité dans les propriétés du transport IP
- Les ponts de liens de site :
 - Vous permettent de créer manuellement des liens de site transittifs
 - Sont utiles uniquement lorsque transitivité est désactivée



Pontage de lien de site automatique

Par défaut, tous les liens de site sont pontés. Par exemple, si les sites d'Amsterdam et du siège sont liés et si les sites de l'administration centrale et Seattle sont liés, alors Amsterdam et Seattle sont liés avec un coût combiné. En théorie, cela signifie que l'ISTG peut créer un objet de connexion directement entre un contrôleur de domaine à Seattle et un contrôleur de domaine à Amsterdam, si un contrôleur de domaine n'était pas disponible au siège de la réPLICATION. Cela se produit en travaillant autour de la topologie de réseau hub-and-spoke.

Vous pouvez désactiver le pontage de lien de site automatique en ouvrant les propriétés du transport IP dans le conteneur **Intersite Transports**, puis effacez la case à cocher **Relier tous les liens de sites**.

Ponts de lien de site

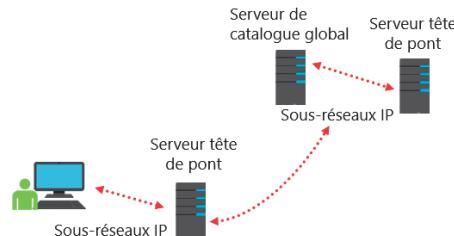
Un pont de liens de sites relie deux ou plusieurs liens de site d'une manière qui crée un lien transitif. Les ponts de liens de site ne sont nécessaires que lorsque vous avez effacé le contenu de la case à cocher **Relier tous les liens de sites** pour le protocole de transport. Rappelez-vous que le pontage de lien de site automatique est activé par défaut, ce qui signifie que les ponts de lien de sites ne sont pas nécessaires. Cependant, vous pouvez maintenir le pontage de lien de site activé pour la majorité des sites, mais aussi configurer un pont de lien de site à coût intermédiaire. Par exemple, supposons que vous ayez de nombreux sites, mais les branches A et B sont toutes deux connectées directement au siège de l'entreprise avec un coût par défaut de 100. Le siège social dispose d'un centre de données de sauvegarde, **HQ-HA**, qui est également liée à un coût de 100 entre le siège social et le site A et le site B. Dans le cas où tous les contrôleurs de domaine seraient disponibles dans **HQ-HA**, vous voulez vous assurer que le site A peut aller sur le site B. Cela vous permet de garder le pontage de liens de site mais aussi de configurer un pont de liens de sites avec un coût de 150 pour le site A au site B. Cela est supérieur au coût de 100 soit pour site **HQ-HA**, mais moins que le coût sans le pont de liens de sites. Ce coût serait de 200—100 du site A à HQ-HA, plus le coût de 100 à HQ-HA au site B. Cela fait du coût du pont de lien de site de 150 un coût intermédiaire.

Le schéma sur la diapositive montre comment vous pouvez utiliser un pont de liens de sites dans une forêt dans laquelle le pontage de lien de site automatique est désactivé. En créant les ponts de lien de sites **AMS-HQ-SEA** qui incluent les liens de site **HQ-AMS** et **HQ-SEA**, ces deux liens de site deviennent *transitifs*, ou pontés. Par conséquent, une connexion de réPLICATION peut être faite entre un contrôleur de domaine à Amsterdam et un contrôleur de domaine à Seattle.

Qu'est-ce que la mise en cache d'appartenance au groupe universel ?

Une question à laquelle vous pourriez avoir besoin de faire face lorsque vous configurez AD réPLICATION DS est de savoir s'il faut déployer des serveurs de catalogue global dans chaque site. Parce que les serveurs de catalogue global sont nécessaires lorsque les utilisateurs se connectent au domaine, le déploiement d'un serveur de catalogue global dans chaque site optimise l'expérience utilisateur. Toutefois, si vous déployez un serveur de catalogue global dans un site, il peut y avoir du trafic de réPLICATION supplémentaire. Cela peut être un problème si la connexion réseau entre les sites AD DS a limité la bande passante et qu'il y a d'autres domaines avec un grand nombre d'objets dans la forêt. Dans ces scénarios, vous pouvez déployer des contrôleurs de domaine sous Windows Server 2008 ou versions ultérieures, puis activer la mise en cache d'appartenance au groupe universel pour le site.

La mise en cache d'appartenance à un groupe universel permet aux contrôleurs de domaine, dans un site sans serveur de catalogue global, de mettre en cache l'appartenance à un groupe universel



Comment la mise en cache l'appartenance au groupe universel fonctionne-t-elle ?

Un contrôleur de domaine dans un site qui a activé la mise en cache à l'appartenance au groupe universelle stocke les informations de groupe universelles localement après qu'un utilisateur ait tenté de se connecter pour la première fois. Le contrôleur de domaine obtient des informations d'appartenance au groupe de l'utilisateur à partir d'un serveur de catalogue global dans un autre site. Il met alors les informations indéfiniment et actualise périodiquement. La prochaine fois que l'utilisateur tentera de se connecter, le contrôleur de domaine obtient les informations d'appartenance au groupe universel de son cache local sans contacter un serveur de catalogue global.

Par défaut, les informations d'appartenance au groupe universel dans le cache de chaque contrôleur de domaine sont actualisées toutes les huit heures. Pour actualiser le cache, les contrôleurs de domaine envoient une demande de confirmation de l'appartenance à un groupe universel à un serveur de catalogue global désigné.

Vous pouvez configurer la mise en cache de l'appartenance au groupe universel des paramètres du nœud **Paramètres de site NTDS**.

Gestion de la réPLICATION intersite

Lorsque vous créez un lien de site, vous pouvez utiliser plusieurs options de configuration pour aider à gérer la réPLICATION intersite. Ces options sont les suivantes :

- Coûts du lien de site. Les coûts de lien du site gèrent le flux de trafic de réPLICATION lorsqu'il existe plus d'une voie pour le trafic de réPLICATION. Vous pouvez configurer les coûts de lien de sites pour indiquer qu'un lien particulier remplit une ou plusieurs exigences ou conditions. Par exemple, il peut être plus rapide et plus fiable, ou bien il peut être préféré. Les liens lents ont des coûts plus élevés et les liens rapides ont des coûts inférieurs. Ad ds se réplique en utilisant la connexion au coût le plus bas. Par défaut, tous les liens de site sont configurés à un coût de 100.
- Fréquence de réPLICATION. La réPLICATION intersite est basée uniquement sur l'interrogation. Par défaut, toutes les trois heures un partenaire de réPLICATION sonde ses partenaires de réPLICATION en amont afin de déterminer si des changements sont disponibles. Cet intervalle de réPLICATION peut être trop long pour les entreprises qui veulent que les changements de réPERTOIRE se répliquent plus rapidement. Vous pouvez modifier l'intervalle d'interrogation en accédant aux propriétés de l'objet de lien de site. L'intervalle d'interrogation minimum est fixé toutes les 15 minutes.
- Planifications de réPLICATION. Par défaut, la réPLICATION se produit 24 heures par jour. Cependant, vous pouvez limiter la réPLICATION intersite à des moments précis en changeant les attributs de planification d'un lien de site.

- Coûts de lien de site :
 - La réPLICATION utilise les connexions au coût le plus bas
- RéPLICATION :
 - Lors de l'interrogation, la tête de pont en aval interroge ses partenaires en amont
 - La valeur par défaut est de 3 heures
 - Le minimum est de 15 minutes
 - La valeur recommandée est de 15 minutes
 - Calendriers de réPLICATION :
 - 24 heures par jour
 - Peut être programmée



Démonstration : Configuration de la réPLICATION intersite AD DS

Au cours de cette démonstration, vous allez apprendre à configurer des réPLICATIONS intersite AD DS.

Procédure de démonstration

1. Dans le **Gestionnaire de serveur**, ouvrez **Sites et services Active Directory**.
2. Renommez le **DEFAULTIPSITELINK** en **LON-TOR**.
3. Cliquez avec le bouton droit sur le lien du site, puis cliquez sur **Propriétés**.
4. Modifiez le coût, l'intervalle de réPLICATION et le calendrier selon les besoins.
5. Si nécessaire, ouvrez les propriétés du nœud **IP**, puis modifiez l'option **Relier tous les liens de sites**.

Outils pour le suivi et la gestion de la réPLICATION

Après avoir implémenté votre configuration de réPLICATION, vous devez être en mesure de contrôler la réPLICATION pour une prise en charge, optimisation et dépannage continu. Deux outils sont particulièrement utiles pour la création de rapports et l'analyse de réPLICATION : l'outil de diagnostic de réPLICATION (**Repadmin.exe**) et le Domain Controller Diagnostics Tool (**Dcdiag.exe**).

Repadmin.exe est un outil de ligne de commande qui vous permet de signaler l'état de la réPLICATION sur chaque contrôleur de domaine. Les informations que **Repadmin.exe** produit

peuvent vous aider à repérer un problème de réPLICATION potentiel dans la forêt. Vous pouvez afficher des niveaux de détail jusqu'aux métadonnées de réPLICATION pour les objets et les attributs spécifiques, ce qui permet d'identifier où et quand un changement problématique a été fait dans AD DS. Vous pouvez même utiliser **Repadmin.exe** pour créer la topologie de réPLICATION et forcer la réPLICATION entre les contrôleurs de domaine.

Repadmin.exe prend en charge un certain nombre de commandes qui effectuent des tâches spécifiques. Vous pouvez en apprendre davantage sur chaque commande en saisissant **repadmin/ ?:command** lors d'une invite de commandes. La plupart des commandes nécessitent des arguments. De nombreuses commandes prennent un paramètre **DC_LIST**, qui est simplement une étiquette de réseau (DNS, le nom NetBIOS ou l'adresse IP) d'un contrôleur de domaine. Voici quelques-unes des tâches que vous pouvez accomplir à l'aide de **Repadmin.exe** :

- Afficher des partenaires de réPLICATION pour un contrôleur de domaine. Pour afficher les connexions de réPLICATION d'un contrôleur de domaine, saisissez **repadmin/showrepl DC_LIST**. Par défaut, **repadmin.exe** ne montre que les connexions intersite. Ajoutez l'argument **/repsto** pour aussi voir les connexions intersite.
- Afficher des objets de connexion pour un contrôleur de domaine. Saisissez **repadmin/showconn DC_LIST** pour afficher les objets de connexion pour un contrôleur de domaine.
- Afficher des métadonnées sur un objet, ses attributs et réPLICATION. Vous pouvez en apprendre beaucoup sur la réPLICATION en examinant un objet sur deux contrôleurs de domaine différents pour savoir quels attributs ont été répliqués ou non. Saisissez **repadmin/showobjmeta DC_LIST object**, où **DC_LIST** indique que le contrôleur de domaine ou les contrôleurs à interroger. Vous pouvez utiliser un astérisque pour indiquer tous les contrôleurs de domaine. **Object** est un identifiant unique pour l'objet (son nom unique ou le GUID, par exemple).

Vous pouvez également apporter des modifications à votre infrastructure de réPLICATION en utilisant l'outil **Repadmin.exe**. Voici quelques-unes des tâches de gestion que vous pouvez accomplir :

- Lancer le vérificateur de cohérence des données. Saisissez **repadmin/kcc** pour forcer le vérificateur de cohérence des données à recalculer la topologie de réPLICATION entrante pour le serveur.
- Forcer la réPLICATION entre les deux partenaires. Vous pouvez utiliser **Repadmin.exe** pour forcer la réPLICATION d'une partition entre une source et un contrôleur de domaine cible. Saisissez **repadmin/replicate Destination_DC_LIST Source_DC_Name naming_context**.
- Synchroniser un contrôleur de domaine avec tous les partenaires de réPLICATION. Saisissez **repadmin/syncall DC/A /e** pour synchroniser un contrôleur de domaine avec tous ses partenaires, y compris dans d'autres sites.

- Exemples **Repadmin.exe** :
 - **repadmin /showrepl Lon-dc1.adatum.com**
 - **repadmin /showconn Lon-dc1 adatum.com**
 - **repadmin /showobjmeta Lon-dc1 "cn=Linda Miller,ou=..."**
 - **repadmin /kcc**
- **Dcdiag.exe /test:testName:**
 - FrsEvent ou DFSREvent
 - Intersite
 - KccEvent
 - RéPLICATIONS
 - Topologie
- Contrôler la réPLICATION avec le gestionnaire d'opérations
- Windows PowerShell

Dcdiag.exe effectue un certain nombre de tests et de rapports sur la santé globale de la réPLICATION et la sécurité d'AD DS. Exécuté par lui-même, **Dcdiag.exe** effectue des tests sommaires et rapporte les résultats. À l'autre extrême, **Dcdiag.exe/c** effectue presque chaque test. Les résultats des tests peuvent être redirigés vers des fichiers de différents types, y compris XML. Saisissez **dcdiag /?** pour obtenir des informations complètes d'utilisation.

Vous pouvez également spécifier un ou plusieurs tests à effectuer en utilisant le paramètre **/test:Nom du test**. Les tests qui sont directement liés à la réPLICATION incluent :

- **FrsEvent**. Cela signale des erreurs de fonctionnement dans FRS.
- **DFSREvent**. Cela signale des erreurs de fonctionnement dans le système de réPLICATION DFS.
- **intersite**. Cela contrôle les échecs qui empêchent ou retardent la réPLICATION intersite.
- **KccEvent**. Cela permet d'identifier les erreurs dans le vérificateur de cohérence.
- **RéPLICATIONs**. Cela contrôle la réPLICATION en temps opportun entre les contrôleurS de domaine.
- **Topologie**. Celui-ci vérifie que la topologie de réPLICATION est connectée entièrement pour tous les contrôleurS de domaine.
- **VerifyReplicas**. Cela permet de vérifier que toutes les partitions d'annuaire d'applications sont instanciées pleinement sur tous les contrôleurS de domaine qui hébergent des répliques.

Surveillance de la réPLICATION avec Microsoft System Center Operations Manager

Vous pouvez installer le Pack d'administration Active Directory Domain Services pour Operations Manager sur le contrôleur de domaine. Ce pack d'administration contient de nombreuses alertes, des vues, des tâches et des rapports pour une variété de fonctions AD DS, y compris la réPLICATION.

La section **Surveillance de la réPLICATION** recueille des données de performance de réPLICATION pour inclure les alertes de réPLICATION, la réPLICATION intersite, la latence de réPLICATION et les deux octets de trafic entrants et sortants de réPLICATION par seconde. Le pack d'administration contient également plusieurs diagrammes de topologie de réPLICATION qui couvrent des liens de site, des objets de connexion et des objets de connexion brisés. Il contient également des rapports sur les objets de connexion de réPLICATION, les liens de site de réPLICATION, la bande passante de la réPLICATION et la latence de réPLICATION.

Le directeur des opérations surveille quatre zones de réPLICATION primaires dans le cadre du pack d'administration :

- Contrôle de cohérence du maître des opérations. Cette partie essentielle de la réPLICATION permet aux partenaires de réPLICATION de se mettre d'accord sur quels contrôleurS de domaine sont dans un rôle de maître d'opérations.
- Surveillance de la réPLICATION de latence. Cela garantit que les changements AD DS se répliquent en temps opportun et cela peut envoyer périodiquement ses propres événements de réPLICATION pour garantir que tous les partenaires de réPLICATION fonctionnent correctement.
- Nombre de partenaires de réPLICATION. Cela garde la trace du nombre de partenaires de réPLICATION que possède un contrôleur de domaine. Si le nombre est inférieur ou supérieur à un certain seuil, il déclenche une alerte.
- Fournisseur de réPLICATION. Cela contrôle et rend compte sur tous les liens de réPLICATION pour chaque contrôleur de domaine. Vous utilisez Windows Management Instrumentation pour trouver le statut de lien.

Nouveaux applets de commande Windows PowerShell pour la réPLICATION AD DS

Windows Server 2016 prend en charge plusieurs applets de commande Windows PowerShell pour créer, configurer et surveiller la réPLICATION AD DS. Le tableau suivant décrit certains de ces applets.

| Applet de commande | Données renvoyées |
|---|--|
| Get-ADReplicationConnection | Une connexion de réPLICATION AD DS spécifique ou un ensemble d'objets de connexion de réPLICATION AD DS basées sur un filtre spécifique. |
| Get-ADReplicationFailure | Une description d'un échec de la réPLICATION AD DS. |
| Get-ADReplicationPartnerMetadata | Métadonnées de réPLICATION pour un ensemble d'un ou plusieurs partenaires de réPLICATION. |
| Get-ADReplicationSite | Un site de réPLICATION AD DS spécifique ou un ensemble d'objets de site de réPLICATION des objets basés sur un filtre spécifique. |
| Get-ADReplicationSiteLink | Un lien spécifique du site Active Directory ou un ensemble de liens de site basé sur un filtre spécifique. |
| Get-ADReplicationSiteLinkBridge | Un pont de liaison de site Active Directory spécifique ou un ensemble d'objets de pont de liaison de sites basés sur un filtre spécifique. |
| Get-ADReplicationSubnet | Un sous-réseau Active Directory spécifique ou un ensemble de sous-réseaux Active Directory basé sur un filtre spécifique. |



Lectures supplémentaires : Pour plus d'informations, consultez : « Administration d'applets de commande AD DS dans Windows PowerShell » à l'adresse : <http://aka.ms/lkjgof>

Vérifiez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|--|---------|
| La durée la plus courte de réPLICATION que vous pouvez configurer avec la planification de la réPLICATION de site est de 15 minutes. | |

Atelier pratique : Implémentation des sites AD DS et réPLICATION

Scénario

La corporation A. Datum a déployé un seul domaine AD DS, avec tous les contrôleurs de domaine situés dans le centre de données de Londres. Étant donné que l'entreprise a grandi et qu'elle dispose de plus de bureaux avec un grand nombre d'utilisateurs, il est devenu évident que l'environnement AD DS actuel ne répond pas aux exigences de l'entreprise. Les utilisateurs de certains bureaux signalent que la connexion à leur ordinateur peut prendre un certain temps. L'accès aux ressources du réseau comme les serveurs de l'entreprise, sous Microsoft Exchange Server 2016 et Microsoft SharePoint Server 2016, peut être lent et il arrive sporadiquement que les serveurs échouent.

En tant que l'un des administrateurs de réseau de haut niveau, vous êtes responsable de la planification et de l'implémentation d'une infrastructure AD DS qui vous aidera à répondre aux impératifs professionnels de l'entreprise. Vous êtes responsable de la configuration des sites AD DS et de la réPLICATION pour optimiser l'expérience de l'utilisateur et l'utilisation du réseau au sein de l'entreprise.

Objectifs

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

- Modifier le site par défaut qui a été créé dans AD DS.
- Créer des sites et des sous-réseaux supplémentaires.
- Configurer la réPLICATION AD DS.
- Surveiller et réparer la réPLICATION AD DS.

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels : **22742A-LON-DC1**, **22742A-LON-DC2** et **22742A-TOR-DC1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd.**

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

1. Sur l'ordinateur hôte, cliquez sur **Démarrer**, puis sur **Outils d'administration** et enfin sur **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-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 : **Pa55w.rd.**
5. Répétez les étapes 2 à 4 pour **22742A-LON-DC2** et **22742A-TOR-DC1**.

Exercice 1 : Modification du site par défaut

Scénario

A. Datum a décidé de mettre en œuvre des sites AD DS supplémentaires pour optimiser l'utilisation du réseau pour le trafic réseau AD DS. Votre première étape dans l'implémentation du nouvel environnement consiste à installer un nouveau contrôleur de domaine pour le site de Toronto. Vous devez ensuite reconfigurer le site par défaut et attribuer des sous-réseaux d'adresses IP appropriées pour le site.

Enfin, votre tâche est de changer le nom du site par défaut **LondonHQ** et de l'associer au sous-réseau IP **172.16.0.0/24**, qui est la gamme de sous-réseau du siège social de Londres.

Les tâches principales de cet exercice sont les suivantes :

1. Installer le contrôleur de domaine Toronto.
2. Renommer le site par défaut.
3. Configurer des sous-réseaux IP associés au site par défaut.

► Tâche 1 : Installer le contrôleur de domaine Toronto

1. Sur **TOR-DC1**, démarrez le **Gestionnaire de serveur** et installez **Services de domaine Active Directory**.
2. Lorsque les AD DS binaires ont été installés, utilisez l'**Assistant Configuration Active Directory Domain Services** pour installer et configurer **TOR-DC1** en tant que contrôleur de domaine supplémentaire pour **Adatum.com**. En dessous de **Saisissez le mot de passe du Mode restauration des services d'annuaire (DSRM)**, saisissez **Pa55w.rd** dans les zones **Mot de passe** et **Confirmer le mot de passe**. Laissez le serveur redémarrer comme indiqué.
3. Quand l'ordinateur redémarre, connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.

► Tâche 2 : Renommer le site par défaut

1. Si nécessaire, sur **LON-DC1**, ouvrez la console **Gestionnaire de serveur**.
2. Ouvrez **Sites et services Active Directory**, puis renommez le site **Default-First-Site-Name LondonHQ**.
3. Vérifiez que **LON-DC1** et **TOR-DC1** sont membres du site **LondonHQ**.

► Tâche 3 : Configurer des sous-réseaux IP associés au site par défaut

1. Si nécessaire, sur **LON-DC1**, ouvrez la console **Gestionnaire de serveur**, puis ouvrez **Sites et services Active Directory**.
2. Créez un sous-réseau présentant la configuration suivante :
 - o Préfixe : **172.16.0.0/24**
 - o Objet du site: **LondonHQ**

Résultats : Une fois cette opération terminée, vous devez avoir reconfiguré avec succès le site par défaut et affecté les sous-réseaux d'adresses IP sur le site.

Exercice 2 : Création de sites et sous-réseaux supplémentaires

Scénario

La prochaine étape que vous prenez pour mettre en œuvre la conception de site AD DS est de configurer le nouveau AD DS site. Le premier site que vous avez besoin de mettre en œuvre est le site de Toronto pour le centre de données en Amérique du Nord. L'équipe du réseau à Toronto souhaite également dédier un site nommé **Test** dans le centre de données de Toronto. Vous avez été informé que l'adresse de sous-réseau IP Toronto est **172.16.1.0/24** et l'adresse de sous-réseau IP de réseau de test est **172.16.100.0/24**.

Les tâches principales de cet exercice sont les suivantes :

1. Créer les sites AD DS pour Toronto.
2. Créer des sous-réseaux IP qui sont associés avec les sites de Toronto.

► Tâche 1 : Créer les sites AD DS pour Toronto

1. Si nécessaire, sur **LON-DC1**, ouvrez la console **Gestionnaire de serveur**, puis ouvrez **Sites et services Active Directory**.
2. Créez un sous-réseau présentant la configuration suivante :
 - o Nom : **Toronto**
 - o Objet lien de site : **DEFAULTIPSITELINK**
3. Créez un sous-réseau présentant la configuration suivante :
 - o Nom : **Test**
 - o Objet lien de site : **DEFAULTIPSITELINK**

► Tâche 2 : Créer des sous-réseaux IP qui sont associés avec les sites de Toronto

1. Si nécessaire, sur **LON-DC1**, ouvrez **Sites et services Active Directory**.
2. Créez un sous-réseau présentant la configuration suivante :
 - o Préfixe : **172.16.1.0/24**
 - o Objet du site **Toronto**
3. Créez un sous-réseau présentant la configuration suivante :
 - o Préfixe : **172.16.100.0/24**
 - o Objet du site **Test**
4. Dans le volet de navigation, cliquez sur le dossier **Sous-réseaux**. Vérifiez dans le volet d'informations que les deux sous-réseaux sont créés et associés à leur site approprié.

Résultats : Une fois cette opération terminée, vous devez avoir créé avec succès deux sites supplémentaires représentant les adresses de sous-réseau IP à Toronto.

Exercice 3 : Configuration de la réPLICATION AD DS

Scénario

Maintenant que les sites AD DS ont été configurés pour Toronto, votre prochaine étape consiste à configurer les liens de sites pour gérer la réPLICATION entre les sites, puis de déplacer le **TOR-DC1** contrôleur de domaine sur le site de **Toronto**. Actuellement, tous les sites appartiennent à **DEFAULTIPSITELINK**.

Vous devez modifier le site de liaison de telle sorte que **LondonHQ** et **Toronto** appartiennent à un lien de site commun appelé **LON-TOR**. Vous devez configurer ce lien de façon à ce qu'il se réplique toutes les heures. En outre, vous devez lier le site **Test** uniquement au site **Toronto** en utilisant un lien de site nommé **TOR-TEST**. La réPLICATION ne doit pas être disponible du site **Toronto** au site **Test** pendant les heures de travail entre 9 h et 15 h. Vous devez ensuite utiliser des outils pour surveiller la réPLICATION entre les sites.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les liens du site entre les sites AD DS.
2. Déplacer TOR-DC1 sur le site Toronto.
3. Surveiller la réPLICATION de site AD DS.

► Tâche 1 : Configurer les liens du site entre les sites AD DS

1. Si nécessaire, sur **LON-DC1**, ouvrez **Sites et services Active Directory**.
2. Créez un sous-réseau présentant la configuration suivante :
 - Nom : **TOR-TEST**
 - Sites : **Toronto, Test**
 - Modifiez le calendrier pour permettre la réPLICATION du **lundi 9 h au vendredi 15 h**.
3. Renommez **DEFAULTIPSITELINK**, puis configurez-le avec les paramètres suivants :
 - Nom : **LON-TOR**
 - Sites : **LondonHQ, Toronto**
 - RéPLICATION : Toutes les **60** minutes

► Tâche 2 : Déplacer TOR-DC1 sur le site Toronto

1. Si nécessaire, sur **LON-DC1**, ouvrez **Sites et services Active Directory**.
2. Déplacez **TOR-DC1** du site **LondonHQ** au site **Toronto**.
3. Vérifiez que **TOR-DC1** est situé sous le nœud **Serveurs** sur le site **Toronto**.

► Tâche 3 : Surveiller la réPLICATION de site AD DS

1. Sur **LON-DC1**, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
2. Utilisez les commandes suivantes pour contrôler la réPLICATION de site :

```
Repadmin /kcc
```

Cette commande recalcule la topologie de réPLICATION entrante pour le serveur.

```
Repadmin /showrep1
```

Vérifiez que la dernière réPLICATION avec **TOR-DC1** a réussi.

```
Repaadmin /bridgeheads
```

Cette commande affiche les serveurs tête de pont pour la topologie de site.

```
Repaadmin /rep1summary
```

Cette commande affiche un résumé des tâches de réPLICATION. Vérifiez qu'aucune erreur n'apparaît.

```
DCDiag /test:replications
```

Vérifiez que tous les tests de connectivité et de réPLICATION ont bien réussi.

3. Basculez vers **TOR-DC1**, puis répétez les commandes pour afficher les informations à partir de la perspective **TOR-DC1**.

Résultats : Après avoir terminé cet exercice, vous aurez configuré les liens du site et contrôlé la réPLICATION.

Exercice 4 : Surveillance et dépannage de la réPLICATION AD DS

Scénario

Une fois les sites et la réPLICATION AD DS établis, A. Datum éprouve des problèmes de réPLICATION. Vous devez utiliser les outils de surveillance et de dépannage pour diagnostiquer le problème et le résoudre.

Les tâches principales de cet exercice sont les suivantes :

1. Produire une erreur.
2. Surveiller la réPLICATION de site ad ds.
3. Réparer la réPLICATION ad ds.
4. Préparez le module suivant.

► Tâche 1 : Produire une erreur

1. Si nécessaire, sur **LON-DC1**, ouvrez la console **Gestionnaire de serveur**, puis ouvrez **Sites et services Active Directory**.
2. Dans **Sites et services Active Directory**, répliquez **TOR-DC1** avec **LON-DC1** depuis le site **LondonHQ**.
3. Dans Windows PowerShell, exécutez :

```
Get-ADReplicationUpToDateNessVectorTable -Target "adatum.com"
```

4. Observez les résultats, puis notez la date et l'heure de l'événement de réPLICATION la plus récente.
5. Aller à **TOR-DC1**, Ouvert **Windows PowerShell**, puis exécutez les commandes Windows PowerShell suivantes :

```
CD \Labfiles\Mod04.\Mod04Ex4.ps1
```

► Tâche 2 : Surveiller la réPLICATION de site AD DS

1. Sur **TOR-DC1**, dans **Sites et services Active Directory**, réPLIQUEZ **LON-DC1** avec **TOR-DC1** du site **Toronto**.
2. Sur **TOR-DC1**, dans Windows PowerShell, exécutez les applets de commande suivants, puis observez les résultats.

```
Get-ADReplicationUpToDateNessVectorTable -Target "adatum.com"  
Get-AdReplicationSubnet -filter *  
Get-AdReplicationSiteLink-filtre *
```

► Tâche 3 : Dépanner la réPLICATION AD DS

1. Sur **TOR-DC1**, dans Windows PowerShell, déterminez les paramètres de l'adresse IP de l'ordinateur, puis exécutez l'applet de commande suivante:

```
Get-DNSClient | Set-DnsClientServerAddress -ServerAddresses ( "172.16.0.10",  
"172.16.0.25")
```

Assurez-vous que les paramètres de l'adresse IP sont corrects.

2. Allez à **Sites et services Active Directory**, puis réPLIQUEZ **LON-DC1** avec **TOR-DC1** depuis le site **Toronto**. Examinez les objets afin de déterminer s'il en manque.
3. Sur **TOR-DC1**, ouvrez l'**Explorateur de fichiers**. Recherchez **C:\Labfiles\Mod04**.
4. Cliquez avec le bouton droit sur le dossier **Mod04EX4Fix.ps1**, puis sélectionnez **ExéCuter avec PowerShell**.
5. Dans **Sites et services Active Directory**, examinez tous les objets que vous avez créés précédemment. Assurez-vous que le lien du site a été créé dans le nœud **Intersite Transports** et que des sous-réseaux ont été créés dans le nœud **Sous-réseaux**.
6. Sur **LON-DC1** et **TOR-DC1**, fermez toutes les fenêtres ouvertes, puis déconnectez-vous des deux ordinateurs virtuels.

Résultats : À la fin de cet exercice, vous devrez avoir diagnostiqué et résolu les problèmes liés à la réPLICATION.

► Tâche 4 : Préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-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 **22742A-LON-DC2** et **22742A-TOR-DC1**.

Question : Vous décidez d'ajouter un nouveau contrôleur de domaine nommé **LON-DC2** au site **LondonHQ**. Comment pouvez-vous assurer que **LON-DC2** passe tout le trafic de réPLICATION au site **Toronto** ?

Question : Vous avez ajouté un nouveau contrôleur de domaine nommé **LON-DC2** au site **LondonHQ**. Quelles partitions AD DS sont modifiées en conséquence ?

Question : Dans l'atelier pratique, vous avez créé un lien de site distinct pour les sites **Toronto** et **Test**. Que pouvez-vous aussi avoir à faire pour vous assurer que **LondonHQ** ne crée pas automatiquement un objet de connexion directement avec le site **Test** ?

Contrôle des acquis et éléments à retenir

Bonnes Pratiques

Mettre en œuvre les meilleures pratiques suivantes lorsque vous gérez des sites Active Directory et la réPLICATION dans votre environnement :

- Toujours fournir au moins un ou plusieurs serveurs de catalogue globaux par site.
- S'assurer que tous les sites possèdent des sous-réseaux appropriés associés.
- Lorsque vous configurez les planifications de réPLICATION pour la réPLICATION intersite, ne configurez pas de longs intervalles sans réPLICATION.
- Évitez d'utiliser le protocole SMTP (Simple Mail Transfer Protocol) comme protocole de réPLICATION.

Problèmes courants et conseils de dépannage

| Problème courant | Conseil pour la résolution du problème |
|---|--|
| Un client n'arrive pas à localiser un contrôleur de domaine dans son site. | |
| La réPLICATION entre les sites ne fonctionne pas. | |
| La réPLICATION entre deux contrôleurs de domaine dans le même site ne fonctionne pas. | |

Questions de contrôle des acquis

Question : Dans une entreprise multi-site, pourquoi est-il important que tous les sous-réseaux soient identifiés et associés à un site ?

Question : Quels sont les avantages et les inconvénients de la réDUCTION de l'intervalle de réPLICATION intersite ?

Question : Quelle est l'utilité d'un serveur tête de pont ?

Outils

Le tableau suivant répertorie les outils référencés par ce module.

| Outil | Utilisation | Emplacement |
|---|---|---------------------------------------|
| Console Sites et services Active Directory | Créer des sites, des sous-réseaux, des liens de site, des pontages de lien de site, une réPLICATION forcée et relancer le vérificateur de cohérence de données. | Outils Gestionnaire de serveur |

| Outil | Utilisation | Emplacement |
|---|---|--------------------|
| Repadmin.exe | Indique l'état de la réPLICATION sur chaque contrôleur de domaine, crée la topologie de réPLICATION ainsi que la réPLICATION forcée et affiche les niveaux de détail au bas des métadonnées de réPLICATION. | Ligne de commande |
| Dcdiag.exe | Effectue un certain nombre de tests et de rapports sur la santé globale de la réPLICATION et la sécurité d'AD DS. | Ligne de commande |
| Get-ADReplicationConnection | Une connexion de réPLICATION AD DS spécifique ou un ensemble d'objets de connexion de réPLICATION AD DS basés sur un filtre spécifique. | Windows PowerShell |
| Get-ADReplicationFailure | Une description d'un échec de la réPLICATION AD DS. | Windows PowerShell |
| Get-ADReplicationPartnerMetadata | Métadonnées de réPLICATION pour un ensemble d'un ou plusieurs partenaires de réPLICATION. | Windows PowerShell |
| Get-ADReplicationSite | Un site de réPLICATION AD DS spécifique ou un ensemble d'objets de site de réPLICATION des objets basés sur un filtre spécifique. | Windows PowerShell |
| Get-ADReplicationSiteLink | Un lien spécifique du site Active Directory ou un ensemble de liens de site basé sur un filtre spécifique. | Windows PowerShell |
| Get-ADReplicationSiteLinkBridge | Un pont de liaison de site Active Directory spécifique ou un ensemble d'objets de pont de liaison de sites basés sur un filtre spécifique. | Windows PowerShell |
| Get-ADReplicationSubnet | Un sous-réseau Active Directory spécifique ou un ensemble de sous-réseaux Active Directory basé sur un filtre spécifique. | Windows PowerShell |

Module 5

Mise en place d'une stratégie de groupe

Sommaire :

| | |
|---|------|
| Vue d'ensemble du module | 5-1 |
| Leçon 1 : Introduction d'une stratégie de groupe | 5-2 |
| Leçon 2 : Mise en œuvre et administration des GPO | 5-14 |
| Leçon 3 : Cadre et traitement de la stratégie de groupe | 5-22 |
| Atelier pratique A : Implémentation d'une infrastructure de stratégie de groupe | 5-38 |
| Leçon 4 : Résolution de problèmes de l'application des GPO | 5-42 |
| Atelier pratique B : Dépannage de l'infrastructure de stratégie de groupe | 5-50 |
| Révision du module et Takeaways | 5-56 |

Vue d'ensemble du module

Depuis la sortie de Microsoft Windows 2000, la fonctionnalité de stratégie de groupe des systèmes d'exploitation Windows a fourni une infrastructure dans laquelle les administrateurs peuvent définir des paramètres de manière centralisée en vue de les installer sur les ordinateurs de leur entreprise. Dans un environnement géré par une infrastructure de stratégie de groupe bien établie, un administrateur configure très peu directement l'ordinateur d'un utilisateur. Vous pouvez définir, appliquer et mettre à jour l'ensemble des configurations à l'aide des paramètres des « Objets de stratégie de groupe (GPO) ». En utilisant les paramètres des GPO, vous pouvez affecter un site entier ou un domaine au sein d'une entreprise, ou vous pouvez vous concentrer sur une seule unité organisationnelle (UO). Le filtrage basé sur l'appartenance à un groupe de sécurité et d'autres attributs vous permettent de redéfinir la cible pour vos paramètres des GPO. Ce module vous expliquera en quoi consiste la stratégie de groupe ainsi que son fonctionnement et décrira la meilleure façon de la mettre en place au sein de votre entreprise.

Objectifs

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

- Expliquer ce qu'est la stratégie de groupe ;
- Mettre en œuvre et administrer les GPO ;
- Décrire le cadre et le traitement de la stratégie de groupe ;
- Dépanner l'application GPO.

Leçon 1

Introduction d'une stratégie de groupe

La stratégie de groupe compte plusieurs composants en interaction. Pour mettre en œuvre et assurer le bon fonctionnement de la stratégie de groupe, vous devez savoir ce que chaque composant fait et comment ils travaillent ensemble. En outre, vous devez savoir comment assembler ces composants dans des configurations différentes. Ce cours donne un aperçu complet des composants, procédures et fonctions de la stratégie de groupe.

Objectifs des leçons

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

- Décrire la gestion de la configuration ;
- Décrire la stratégie de groupe ;
- Expliquer les avantages d'utiliser la stratégie de groupe ;
- Décrire les GPO ;
- Expliquer la portée des GPO ;
- Expliquer l'héritage des GPO ;
- Décrire les services à la clientèle et les extensions côté clients de la stratégie de groupe ;
- Décrire les nouvelles fonctionnalités de la stratégie de groupe dans Windows Server 2016.

Qu'est-ce que la gestion de la configuration ?

Si, par exemple, vous ne possédez qu'un seul ordinateur à la maison et que vous souhaitez modifier le fond d'écran, vous pouvez le faire de plusieurs façons différentes. La plupart du temps, les gens vont dans **Personnalisation** depuis les **Paramètres** dans Windows 10, puis effectuent la modification en utilisant l'interface du système d'exploitation Windows. Bien que cela fonctionne bien pour un seul ordinateur, cela peut être fastidieux si vous souhaitez faire le changement sur plusieurs ordinateurs. La mise en œuvre de toute modification et le maintien d'un environnement cohérent est plus difficile avec plusieurs ordinateurs.

- La *Gestion de la configuration* est une approche centralisée pour appliquer une ou plusieurs modifications à au moins deux utilisateurs ou ordinateurs
- Les éléments clés de la gestion de la configuration sont les suivants :
 - Paramètre
 - Portée
 - Application

La *Gestion de la configuration* est une approche centralisée afin d'effectuer une ou plusieurs modifications à plus d'un utilisateur ou d'un ordinateur. Les éléments clés de la gestion de configuration sont les suivants :

- Paramètre. Un paramètre est également connu sous la définition centralisée d'un changement. Le paramètre permet à un utilisateur ou à un ordinateur d'obtenir un état de configuration souhaitée.
- Portée. La portée d'un changement correspond au nombre d'ordinateurs ou d'utilisateurs que le paramètre vise.
- Application. L'application est un mécanisme ou un processus qui permet au paramètre de s'appliquer aux utilisateurs et ordinateurs au sein du cadre.

La stratégie de groupe est un cadre dans les systèmes d'exploitation Windows qui comprend des composants se trouvant dans les services de domaine de répertoire actif (AD DS), des contrôleurs de domaine, ainsi que sur chaque serveur Windows et client. Avec ces composants, vous pouvez gérer la configuration dans un domaine AD DS.

Vue d'ensemble des outils et des consoles de stratégie de groupe

L'élément le plus fondamental de la stratégie de groupe est chaque paramètre de stratégie.

Chaque paramètre de stratégie s'appelle également une stratégie. La stratégie définit un changement de configuration spécifique que vous pouvez appliquer, tel qu'un paramètre de stratégie qui empêche un utilisateur d'accéder à des outils d'édition de registre. Si vous définissez ce paramètre de stratégie, puis l'appliquer à l'utilisateur, l'utilisateur est incapable d'utiliser des outils tels que REGEDIT (regedit.exe).

Sachez que certains paramètres sont destinés à l'utilisateur : ces paramètres s'appellent *les paramètres de configuration de l'utilisateur* (ou *politiques de l'utilisateur*). Et certains paramètres sont destinés à l'ordinateur : ces paramètres s'appellent *les paramètres de configuration de l'ordinateur* (ou *politiques informatiques*).

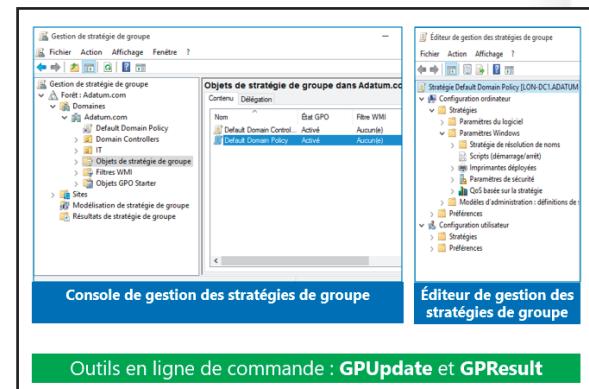
La stratégie de groupe gère différents paramètres de stratégie et le cadre de la stratégie de groupe est extensible. En fin de compte, vous pouvez gérer à peu près l'ensemble des paramètres qui peuvent se configurer grâce à la stratégie de groupe.

Dans la fenêtre **Éditeur de gestion des stratégies de groupe**, vous pouvez définir un paramètre de stratégie en cliquant deux fois dessus. Le paramètre de politique boîte de dialogue **Propriétés** apparaît. Les paramètres de stratégie dans la zone appelée **Modèles d'administration** peut avoir trois états : **Non configuré**, **Activé** et **Désactivé**.

Dans un nouveau GPO, chaque politique est réglé par défaut sur **Non configuré**. Par conséquent, le GPO ne modifie pas la configuration existante de ce paramètre en question pour l'utilisateur ou l'ordinateur. Si vous activez ou désactivez un paramètre de stratégie, la configuration des utilisateurs et des ordinateurs sur laquelle le GPO s'applique est modifiée. Lorsque vous reconfigurez le paramètre **Modèle d'administration** dans sa valeur **Pas configuré**, vous le reconfigurez dans sa valeur par défaut. Certains paramètres restent configurés sur l'ordinateur même si vous supprimez le paramètre des GPO.

L'effet de la modification varie selon le paramètre de stratégie. Par exemple, si vous activez le paramètre de stratégie **Empêcher l'accès aux outils d'édition de registre**, les utilisateurs ne peuvent pas ouvrir l'éditeur de registre, regedit.exe. Si vous désactivez ce paramètre de stratégie, vous permettez aux utilisateurs d'ouvrir l'éditeur de registre. Notez qu'avec la double négation dans cet exemple de paramètre de stratégie, vous désactivez une stratégie qui empêche une action, permettant ainsi l'action. Certains paramètres de stratégie regroupent plusieurs configurations en une seule politique et ceux-ci pourraient nécessiter des paramètres supplémentaires.

Remarque : De nombreux paramètres de stratégie sont complexes et le fait de les activer ou de les désactiver pourraient ne pas être évident. En outre, certains paramètres de stratégie ne concernent que certaines versions du système d'exploitation Windows. Assurez-vous d'examiner un texte explicatif sur un paramètre de stratégie dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe** ou dans l'onglet **Expliquer** dans le paramètre de stratégie de la boîte de



dialogue **Propriétés**. En outre, toujours tester les effets d'un paramètre de stratégie et de ses interactions avec d'autres paramètres de stratégie avant de déployer un changement dans votre environnement de production.

Configuration de l'ordinateur et Configuration utilisateur

Il existe deux grandes divisions de paramètres de stratégie : les paramètres de l'ordinateur, qui se trouvent dans l'ordinateur **Nœud Configuration** et les paramètres de l'utilisateur, qui se situent dans le nœud **Configuration utilisateur** :

- Le nœud **Configuration de l'ordinateur** contient les paramètres qui s'appliquent aux ordinateurs, quelle que soit la personne qui s'y connecte. Les paramètres de l'ordinateur s'appliquent lorsque le système d'exploitation démarre, au cours de l'actualisation du fond, puis, par la suite, toutes les 1h30 à 2h00.
- Le nœud **Configuration utilisateur** contient les paramètres applicables lorsqu'un particulier se connecte à l'ordinateur, au cours de l'actualisation du fond, puis, par la suite, toutes les 1h30 à 2h00.

Au sein des nœuds **Configuration de l'ordinateur** et **Configuration utilisateur** figurent les nœuds **Politiques** et **Préférences**. Vous en apprendrez plus sur la configuration des paramètres dans les nœuds Politiques et Préférences, dans le module 6 « Gestion des paramètres utilisateur avec les GPO ».

Au sein de la **Politiques** les nœuds, sous la **Configuration de l'ordinateur** le nœud et **Configuration utilisateur** nœud, sont une hiérarchie de dossiers qui contiennent les paramètres de stratégie. Parce qu'il existe des milliers de paramètres, ce cours n'a pas pour but d'examiner chaque paramètre. Cependant, les grandes catégories de paramètres dans les dossiers méritent d'être définies.

Le nœud Paramètres du logiciel

Le nœud Paramètres du logiciel est le premier nœud. Il ne contient que l'extension de l'installation du logiciel, ce qui vous permet d'indiquer comment votre entreprise installe et gère ses applications.

Le nœud Paramètres Windows

Dans les deux nœuds **Configuration de l'ordinateur** et **Configuration utilisateur**, le nœud **Politiques** contient le nœud **Paramètres Windows**, qui comprend les nœuds **Scripts**, **Paramètres de sécurité** et **Qualité de service (QoS) basée sur la stratégie**. Il contient également le dossier **Stratégie de résolution de noms** qui comprend les paramètres de configuration de DirectAccess.

Le nœud Scripts

Avec l'extension des scripts, vous pouvez indiquer deux types de scripts : scripts de démarrage et d'arrêt dans les nœuds **Configuration de l'ordinateur** et scripts de connexion et de déconnexion dans le nœud **Configuration utilisateur**. Les scripts de démarrage et d'arrêt sont exécutés au démarrage ou à l'arrêt de l'ordinateur. Les scripts de connexion et de déconnexion sont exécutés lorsqu'un utilisateur se connecte ou se déconnecte. Lorsque vous attribuez plusieurs scripts de connexion et de déconnexion ou de démarrage et d'arrêt à un utilisateur ou un ordinateur, l'extension côté client du script (CSE) exécute les scripts à partir du haut vers le bas de la liste. Vous pouvez déterminer l'ordre d'exécution pour plusieurs scripts dans la boîte de dialogue **Propriétés**. Lorsqu'un ordinateur est éteint, la CST traite d'abord les scripts de déconnexion, suivis par les scripts d'arrêt. Par défaut, la valeur délai d'attente pour les scripts de traitement est de 10 minutes. Si les scripts de déconnexion et d'arrêt nécessitent plus de 10 minutes pour traiter, vous devez ajuster la valeur de délai d'attente par le biais d'un paramètre de stratégie. Vous pouvez utiliser un langage de script ActiveX pour écrire des scripts. Certaines possibilités incluent Microsoft Visual Basic Scripting Edition (VBScript) ; JScript ; Perl et des fichiers de commandes de type MS-DOS (.bat et .cmd). Les scripts de connexion sur un répertoire de réseau partagé dans une autre forêt sont pris en charge pour la connexion de réseau à travers les forêts. Windows 7, Windows 8 et Windows 10, ainsi que tous les supports de scripts d'interface en ligne de commande Windows PowerShell. Les CSE seront expliquées en détail plus loin dans ce cours.

Le nœud Paramètres de sécurité

En utilisant le nœud **Paramètres de sécurité**, un administrateur de sécurité peut configurer la sécurité avec les GPO. Vous pouvez le faire après, ou au lieu de, en utilisant un modèle de sécurité pour configurer la sécurité du système.

Le nœud Qualité de service (QoS) basée sur la stratégie

Ce nœud Qualité de service (QoS), connu sous le nœud **Qualité de qualité (QoS) basée sur la stratégie**, définit les stratégies qui gèrent le trafic du réseau. Par exemple, vous voudrez peut-être vous assurer que les utilisateurs du service des finances aient la priorité pour lancer une application critique du réseau pendant la période des rapports financiers de clôture d'année. Vous pouvez le faire en utilisant le nœud **Qualité de qualité (QoS) basée sur la stratégie**.

Uniquement dans le nœud **Configuration utilisateur**, le dossier **Paramètres Windows** contient le nœud additionnel **Redirection de dossiers**. Avec la redirection de dossiers, vous pouvez rediriger les données utilisateur et les paramètres des dossiers tels que les **Données d'application**, le **bureau**, les **Documents**, les **Photos**, la **Musique** et les **Favoris** de leur emplacement de profil d'utilisateur par défaut à un autre emplacement sur le réseau, où vous pouvez les gérer de manière centralisée.

Le nœud Modèles d'administration

Dans les nœuds **Configuration de l'ordinateur** et **Configuration utilisateur**, le nœud **Modèles d'administration** contient les paramètres de stratégie de groupe basés sur le registre. Des milliers de ces paramètres peuvent configurer l'environnement de l'utilisateur et de l'ordinateur. En tant qu'administrateur, vous pouvez passer beaucoup de temps à modifier ces paramètres. Pour vous aider avec ces paramètres, une description de chaque paramètre de stratégie est disponible à deux endroits :

- Sur l'onglet **Expliquer**, dans la boîte de dialogue pour le paramètre **Propriétés**. En outre, l'onglet **Paramètres** dans la boîte de dialogue pour chaque paramètre **Propriétés** indique également le logiciel ou le système d'exploitation requis pour le paramètre.
- Sur l'onglet **Étendu** de la fenêtre de l'**Éditeur de gestion des stratégies de groupe** fenêtre. L'onglet **Étendu**, qui apparaît sur la partie inférieure droite du volet d'informations, fournit une description de chaque paramètre sélectionné dans une colonne entre l'arborescence de la console et le volet des paramètres. En outre, il indique le logiciel ou système d'exploitation requis pour chaque paramètre.

Vous pouvez utiliser la commande **gpupdate** pour lancer une actualisation de la stratégie de groupe. Vous en apprendrez davantage sur la commande **gpupdate** plus loin dans ce module.

Pour savoir quels sont les GPO et les paramètres qui s'appliquent à un ordinateur et un utilisateur, vous pouvez utiliser la commande **gpresult**. La commande **gpresult** peut afficher plus ou moins de détails selon les options que vous sélectionnez.

Démonstration : Exploration des outils et consoles de stratégie de groupe

Dans cette démonstration, vous allez apprendre à :

- Ouvrir la Console de gestion des stratégies de groupe (GPMC) ;
- Créer un GPO ;
- Configurer un paramètre ;
- Effectuer une actualisation de la stratégie de groupe ;
- Examiner quels sont les GPO qui s'appliquent à l'ordinateur et à l'utilisateur.

Procédures de démonstration

- Ouvrez l'**Éditeur de gestion des stratégies de groupe**.
- Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, dans le volet de navigation, accédez à **Objets de stratégie de groupe**.
- Créez un GPO nommé **Désactiver le panneau de configuration**, puis modifiez-le.
- Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, dans le volet de navigation, sous **Configuration utilisateur**, créez des **Stratégies** et des **Modèles d'administration**, puis cliquez sur **Panneau de configuration**.
- Dans le volet d'informations, cliquez deux fois sur **Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC**.
- Activez le paramètre, taper un commentaire, puis fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.
- Affichez les onglets **Étendue**, **Détails** et **Paramètres**.
- Associez le GPO **Désactiver le panneau de configuration** au domaine.
- Affichez les onglets **Objets de stratégie de groupe associés** et **Héritage de stratégie de groupe**.
- Ouvrez une fenêtre **Windows PowerShell** en tant qu'administrateur.
- Dans l'**Administrateur : fenêtre Windows PowerShell**, saisissez la commande suivante, puis appuyez sur Entrée :

```
gpupdate
```

- Vérifiez que les paramètres de l'ordinateur et de l'utilisateur ont été mis à jour avec succès.

- Entrez la commande suivante, puis appuyez sur Entrée :

```
gpresult /r
```

- Vérifiez que la sortie de la commande dans la section **Paramètres utilisateur**, dans la liste **GPO concernés**, le GPO **Désactiver le panneau de configuration** est répertoriée.
- Fermez la fenêtre **Windows PowerShell**.

Avantages de l'utilisation de la stratégie de groupe

La stratégie de groupe est un outil administratif performant. Vous pouvez utiliser des GPO pour entrer plusieurs paramètres dans un grand nombre d'ordinateurs et pour de nombreux utilisateurs. Parce que vous pouvez les appliquer à différents niveaux, depuis un ordinateur local vers un domaine, vous pouvez également concentrer ces paramètres avec précision.

Vous utilisez principalement la stratégie de groupe pour configurer les paramètres que vous ne voulez pas que les utilisateurs configurent. En outre, vous pouvez utiliser la stratégie de groupe pour normaliser les environnements de bureau sur tous les ordinateurs au sein d'une ou de toutes les unités organisationnelles. Vous pouvez également utiliser la stratégie de groupe pour plus de sécurité, pour configurer certains paramètres de système avancés et à d'autres fins que les sections ci-dessous détaillent.

- La stratégie de groupe est un outil administratif très puissant
- Vous pouvez l'utiliser pour appliquer différents types de paramètres à un grand nombre d'utilisateurs et d'ordinateurs
- En règle générale, vous utilisez les GPO pour :
 - Appliquer les paramètres de sécurité
 - Gérer les paramètres d'application de bureau
 - Déployer des logiciels d'application
 - Gérer la redirection de dossiers
 - Définir les paramètres réseau

Application des paramètres de sécurité

Dans le système d'exploitation Windows Server 2016, les GPO comprennent un grand nombre de paramètres liés à la sécurité qui concernent les utilisateurs et les ordinateurs. Par exemple, vous pouvez appliquer les paramètres du pare-feu Windows et vous pouvez configurer l'audit ainsi que d'autres paramètres de sécurité. Vous pouvez également configurer des ensembles complets d'attribution des droits utilisateur.

Gestion des paramètres de bureau et des applications

Vous pouvez utiliser la stratégie de groupe pour fournir un bureau et un environnement d'application cohérents à tous les utilisateurs de votre entreprise. En utilisant les GPO, vous pouvez configurer chaque paramètre qui touche à l'aspect et à la convivialité de l'environnement de l'utilisateur. Vous pouvez également configurer les paramètres pour certaines applications qui prennent en charge les GPO.

Déploiement de logiciels

Avec la stratégie de groupe, vous pouvez déployer des logiciels pour les utilisateurs et les ordinateurs. Vous pouvez utiliser la stratégie de groupe pour déployer tous les logiciels qui est disponible dans le format .msi. En outre, vous pouvez lancer l'installation automatique du logiciel, ou vous pouvez laisser vos utilisateurs décider s'ils souhaitent que le logiciel soit déployé sur leur ordinateur.



Remarque : Le déploiement des progiciels volumineux avec les GPO pourrait ne pas être le moyen le plus efficace pour installer une application sur les ordinateurs de votre entreprise. Dans de nombreux cas, il pourrait être plus utile d'installer des applications dans le cadre de l'image d'ordinateur de bureau.

Gestion de la redirection de dossiers

Grâce à l'option de redirection de dossiers, il est plus facile de sauvegarder les fichiers de données des utilisateurs. En redirigeant les dossiers, vous permettez également aux utilisateurs d'avoir accès à leurs données indépendamment de l'ordinateur sur lequel ils se connectent. En outre, vous pouvez centraliser toutes les données des utilisateurs à un même endroit, sur un serveur de réseau, tout en offrant une expérience utilisateur qui s'assimile au stockage de ces dossiers sur leur ordinateur. Vous pouvez, par exemple, configurer la redirection de dossiers pour rediriger les dossiers des utilisateurs **Documents** vers un dossier partagé sur un serveur réseau.

Définition des paramètres réseau

En utilisant la stratégie de groupe, vous pouvez configurer divers paramètres réseau sur l'ordinateur des clients. Vous pouvez, par exemple, appliquer des paramètres pour les réseaux sans fil afin de permettre aux utilisateurs de se connecter uniquement aux ensembles de services identifiants spécifiques et grâce aux paramètres d'authentification et de cryptage prédéfinis. Vous pouvez également créer des stratégies applicables aux paramètres de réseau câblé et quelques fonctions de Windows Server 2016 utilisent la stratégie de groupe pour configurer le côté client de services, tels que DirectAccess.

Objets de stratégie de groupe

Vous définissez les paramètres de stratégie dans un GPO. Un GPO est un objet qui contient un ou plusieurs paramètres de stratégie applicables à un ou plusieurs paramètres de configuration pour les utilisateurs ou ordinateurs.

 **Remarque :** Vous gérez les GPO en utilisant la console GPMC.

Le GPMC affiche les GPO dans un conteneur nommé **Objets de stratégie de groupe**. Pour créer un GPO dans un domaine, cliquez avec le bouton droit sur le conteneur **Objets de stratégie de groupe**, cliquez sur **Nouveau**, puis indiquez un nom pour le GPO. Pour modifier les paramètres de configuration dans un GPO, cliquez avec le bouton droit sur le GPO, puis cliquez sur **Modifier**. Cela ouvre la fenêtre de l'**Éditeur de gestion des stratégies de groupe**. Pour créer un GPO dans Windows PowerShell, veuillez exécuter l'applet de commande suivante :

```
New-GPO -Name "Sales GPO" -comment "This is the sales GPO"
```

Il est également possible de créer un GPO et de l'associer au domaine ou à une UO lors de sa création, en cliquant avec le bouton droit sur le conteneur, puis en cliquant sur **Créer un GPO dans le domaine et le lier ici**.

 **Remarque :** Pour que les paramètres dans l'objet prennent effet, vous devez appliquer ou associer le GPO à un site, un domaine ou une UO dans la hiérarchie AD DS.

Vue d'ensemble de la portée des GPO

Vous définissez les modifications de configuration en configurant les paramètres de stratégie dans les GPO. Cependant, les changements de configuration dans un GPO ne concernent pas les ordinateurs ou les utilisateurs de votre entreprise jusqu'à ce que vous indiquez les ordinateurs ou utilisateurs auxquels le GPO s'applique. Il s'agit de la *portée* d'un GPO. La portée d'un GPO est l'ensemble des utilisateurs et des ordinateurs qui appliquent les paramètres du GPO.

Vous pouvez utiliser plusieurs méthodes pour gérer la portée des GPO. La première est le lien

GPO. Vous pouvez associer des GPO à des sites, des domaines ou des UO dans AD DS. Le site, le domaine ou l'unité organisationnelle devient alors la portée maximale du GPO. Tous les ordinateurs et les utilisateurs du site, du domaine ou de l'unité organisationnelle, y compris ceux les UO enfants, sont concernés par les configurations indiquées par les paramètres de stratégie dans le GPO.

Un GPO est :

- Un conteneur pour un ou plusieurs paramètres de stratégie
- Géré avec la GPMC
- Stocké dans un conteneur de GPO
- Modifié avec l'Éditeur de gestion des stratégies de groupe
- Appliqué à un niveau spécifique dans la hiérarchie AD DS

• La portée d'un GPO rassemble les utilisateurs et les ordinateurs qui appliqueront les paramètres dans le GPO

• Vous pouvez utiliser plusieurs méthodes pour définir la portée d'un GPO :

- Associer le GPO à un conteneur, comme une unité d'organisation
- Effectuer un filtrage à l'aide des paramètres de sécurité
- Effectuer un filtrage à l'aide des filtres WMI

• Pour les préférences de stratégie de groupe :

- Vous pouvez filtrer ou cibler les paramètres que vous configurez par préférences de stratégie de groupe au sein d'un GPO en fonction de plusieurs critères



Remarque : Vous pouvez associer un GPO à plus d'un site, d'un domaine ou d'une unité organisationnelle. Vous devez être prudent lorsque vous associez les GPO à plusieurs sites, car ils peuvent entraîner des problèmes de performance lorsque la stratégie est appliquée. En effet, dans un réseau multisite, les GPO sont stockés dans les contrôleurs de domaine du domaine où la stratégie a été créée. Par conséquent, les ordinateurs dans d'autres domaines pourraient devoir emprunter une liaison lente de réseau étendu (WAN) pour obtenir les GPO.

Vous pouvez affiner la portée du GPO avec l'un des deux types de filtres. Grâce aux filtres de sécurité, vous pouvez utiliser des autorisations pour indiquer à quels utilisateurs, ordinateurs ou membres des groupes de sécurité le GPO s'applique ou pas. Les filtres Windows Management Instrumentation (WMI) indiquent un champ en utilisant les caractéristiques d'un système, comme la version du système d'exploitation ou l'espace libre sur le disque. Utilisez les filtres de sécurité et les filtres WMI pour affiner ou préciser la portée dans le cadre initial créé par le lien d'un GPO.



Remarque : Windows Server 2008 a introduit une nouvelle composante de la stratégie de groupe appelée les préférences de stratégie de groupe. Vous pouvez filtrer ou cibler les paramètres que vous configurez par les préférences de stratégie de groupe au sein d'un GPO basé sur plusieurs critères. Grâce aux préférences ciblées, vous pouvez affiner davantage la portée des préférences dans un seul GPO.

Vue d'ensemble de l'héritage des GPO

Vous pouvez créer et associer des GPO à un site, un domaine ou une unité organisationnelle.

Lorsque vous appliquez plusieurs GPO au même conteneur, cela a un effet sur les paramètres des GPO. Pour la plupart des paramètres de stratégie, le GPO avec la plus haute priorité et qui contient le paramètre spécifique détermine la valeur finale du paramètre. Pour quelques paramètres, la valeur finale est, en fait, la combinaison de valeurs entre les GPO.

Les GPO sont traités sur un ordinateur client dans l'ordre suivant :

1. Objets de stratégie de groupe local ;
2. GPO au niveau du site ;
3. GPO au niveau du domaine ;
4. GPO des UO, y compris toute UO imbriquée, en commençant par l'UO la plus éloignée de l'objet utilisateur ou ordinateur.

Les GPO sont traités sur un ordinateur client dans l'ordre suivant :

1. GPO locaux
2. GPO au niveau du site
3. GPO de domaine
4. GPO de l'unité d'organisation, y compris les unités d'organisation imbriquées



Remarque : Dans les points suivants, le terme *conteneur* décrit un site, un domaine et une unité organisationnelle. Dans ce contexte, il ne décrit pas les conteneurs AD DS, parce que vous ne pouvez pas associer les GPO aux conteneurs AD DS.

Les GPO qui s'appliquent aux conteneurs de niveau supérieur passent à travers tous les sous-conteneurs de cette partie de l'arborescence AD DS. Par exemple, un paramètre de stratégie appliqué à une unité organisationnelle s'applique également à toutes les unités organisationnelles enfants en dessous. Le GPO local est traité en premier et l'unité organisationnelle à laquelle l'ordinateur ou l'utilisateur appartient est traitée en dernier. Le dernier GPO traité est le paramètre efficace.

Plusieurs options de stratégie de groupe peuvent modifier ce comportement d'héritage par défaut.

Ces options sont les suivantes :

- **Ordre de liaison.** Utilisez cette option pour définir l'ordre de priorité pour les GPO liés à un conteneur donné. Le lien GPO avec l'un des ordres de liaison a la priorité la plus élevée sur ce conteneur. Si vous modifiez l'ordre de liaison, cela n'aura pas d'effet, à moins que les GPO qui sont associés au même emplacement aient des paramètres contradictoires.
- **Imposé.** Avec cette option, vous pouvez indiquer qu'un GPO a la priorité sur tous les GPO qui sont associés aux conteneurs enfants. En outre, un GPO que le système d'exploitation Windows impose au niveau du domaine remplace un GPO qu'il impose au niveau d'une UO. En général, vous imposez un GPO pour vous assurer que les ordinateurs utilisent les paramètres au niveau de l'entreprise et que les administrateurs de service ne remplacent pas ces paramètres en créant d'autres GPO.
- **Bloquer l'héritage.** Avec cette option, vous pouvez empêcher une unité organisationnelle ou un domaine d'hériter des GPO de tout conteneur parent. Les liens GPO appliqués seront toujours hérités. En règle générale, vous bloquez l'héritage pour permettre à un service de gérer les paramètres de stratégie de groupe séparément du reste de l'entreprise.
- **Lien activé.** La possibilité d'indiquer si un système d'exploitation Windows traite un lien GPO spécifique pour le conteneur auquel il est associé. Lorsque vous n'activez pas de lien, le système d'exploitation Windows ne traite pas le GPO. En règle générale, cela se fait pendant le dépannage lorsque vous souhaitez désactiver le traitement d'un GPO pour le supprimer en tant que source d'erreurs de configuration.



Remarque : Rappelez-vous que l'héritage des GPO est sur une base par paramètre plutôt qu'une base par GPO.

Le service à la clientèle et les extensions côté client de la stratégie de groupe

Application de la stratégie de groupe

Il est important de comprendre comment les stratégies de groupe s'appliquent sur les ordinateurs des clients. Les étapes suivantes expliquent le processus :

1. Quand l'actualisation d'une stratégie de groupe commence, un service qui est en cours d'exécution sur tous les ordinateurs basés sur Windows, connu sous le nom de service client de stratégie de groupe dans Windows Vista et les versions ultérieures, ainsi que dans Windows 2008 et les versions ultérieures détermine quels GPO s'appliquent à l'ordinateur ou l'utilisateur.
2. Le service client de stratégie de groupe télécharge les GPO qui ne sont pas encore mis en cache.

Processus d'application de la stratégie de groupe :

1. Le client de stratégie de groupe récupère les GPO
2. Le client télécharge et met en cache les GPO
3. Les extensions côté client traitent les paramètres

• Les paramètres de stratégie dans le noeud **Configuration de l'ordinateur** s'appliquent au démarrage du système puis toutes les 90-120 minutes

• Les paramètres de stratégie dans le noeud **Configuration utilisateur** s'appliquent lors la connexion puis toutes les 90-120 minutes

3. Les extensions côté client de stratégie de groupe interprètent les paramètres d'un GPO et effectuent les changements appropriés sur l'ordinateur local ou sur l'utilisateur actuellement connecté. Il existe des extensions côté client pour chaque grande catégorie de paramètre de stratégie. Par exemple, il existe une extension de sécurité côté client qui applique les modifications de sécurité, une extension côté client qui lance le démarrage et les scripts de connexion, une CST qui installe le logiciel et une extension côté client qui modifie les clés de registre et les valeurs. Chaque version du système d'exploitation Windows a ajouté des extensions côté client pour étendre la portée fonctionnelle de la stratégie de groupe. Par ailleurs, il existe une douzaine d'extensions côté client dans les systèmes d'exploitation Windows.

L'une des idées les plus importantes à retenir sur la stratégie de groupe est qu'elle est axée sur le client. Le service client de stratégie de groupe retire les GPO du domaine, ce qui fait que les extensions côté client appliquent les paramètres de manière locale. La stratégie de groupe n'est pas une technologie « push ».

Vous pouvez voir les extensions côté client installées sur un ordinateur en plaçant la clé dans le Registre **HKLM\Logiciel\Microsoft\Windows NT\Version actuelle\Winlogon\Extensions GP**. Vous pouvez configurer le comportement des extensions côté client en utilisant la stratégie de groupe. La plupart des extensions côté client appliquent des paramètres d'un GPO uniquement si ce GPO a changé. Ce comportement améliore le traitement global de la stratégie par la suppression des applications redondantes des mêmes paramètres. La plupart des stratégies s'appliquent de telle manière que les utilisateurs standard ne peuvent pas changer le paramètre sur leur ordinateur. Ils seront toujours soumis à la configuration imposée par la stratégie de groupe. Cependant, les utilisateurs standard peuvent modifier certains paramètres et un utilisateur peut changer de nombreux paramètres si cet utilisateur est un administrateur sur le système. Si les utilisateurs de votre environnement sont des administrateurs sur leur ordinateur, vous devez tenir compte de la configuration des extensions côté client pour appliquer à nouveau les paramètres de stratégie même si le GPO n'a pas changé. Ainsi, si un utilisateur administratif modifie une configuration de sorte qu'elle n'est plus conforme à la stratégie, la configuration sera remise à son état conforme lors de la prochaine actualisation de la stratégie de groupe.

 **Remarque :** Vous pouvez configurer les extensions côté client pour appliquer à nouveau les paramètres de stratégie lors de la prochaine actualisation, même si le GPO n'a pas changé. Vous pouvez le faire en configurant un GPO qui s'applique aux ordinateurs, puis en définissant les paramètres dans le nœud **Configuration ordinateur\Stratégies\Modèles d'administration\System\Stratégie de groupe**. Pour chaque CST que vous souhaitez configurer, ouvrez leur paramètre de traitement de stratégie, tel que **Traitement de la stratégie de registre pour le registre CST**. Cliquez sur **Activé**, puis activez la case **Traiter même si les objets de stratégie de groupe n'ont pas changé**.

L'extension de la sécurité côté client gère une exception importante aux paramètres de stratégie de traitement par défaut. L'extension de la sécurité côté client applique à nouveau les paramètres de sécurité toutes les 16 heures, même si un GPO n'a pas changé.

 **Remarque :** Activez le paramètre de stratégie **Attendre toujours le réseau au démarrage et à l'ouverture de session** pour tous les clients basés sur Windows. Sans ce paramètre, par défaut, les clients de Windows XP et des versions ultérieures actualisent de manière asynchrone. L'utilisateur se connecte pour utiliser les informations d'identification mises en cache. L'avantage est que le bureau s'affiche plus rapidement et que l'utilisateur peut commencer à travailler sans attendre l'application de la stratégie de groupe. Cela signifie que lorsque l'ordinateur du client démarre et que l'utilisateur se connecte, il ne reçoit pas les dernières stratégies du domaine. La stratégie de groupe actualisera le fond une fois l'utilisateur connecté. Vous trouverez le paramètre dans **Configuration ordinateur\Stratégies\Modèles d'administration\System\Connexion**. Assurez-vous de lire le texte explicatif du paramètre de stratégie. Le paramètre passe le traitement de la stratégie de groupe en mode synchrone, ce qui peut rendre le traitement plus lent, mais il assure un environnement plus cohérent.

Actualisation de la stratégie de groupe

Les paramètres de stratégie dans le nœud **Configuration de l'ordinateur** s'appliquent au démarrage du système, puis, par la suite, toutes les 1h30 à 2h00. Les paramètres de stratégie dans le nœud **Configuration utilisateur** s'applique lors de la connexion, puis, par la suite, toutes les 1h30 à 2h00. L'application des politiques s'appelle *Actualisation de la stratégie de groupe*.

L'actualisation lors du démarrage du système et de la connexion de l'utilisateur est également référencée comme une actualisation de premier plan. L'actualisation périodique qui a lieu toutes les 1h30 à 2h00 et les actualisations manuelles s'appellent toutes deux des actualisations de fond. Certaines extensions côté client s'appliquent uniquement à des paramètres au cours du traitement de premier plan.



Remarque : Vous pouvez également forcer une actualisation de stratégie en utilisant la commande **gpupdate**.

Nouvelles fonctionnalités de la stratégie de groupe dans Windows Server 2016

Windows Server 2016 présente quelques modifications et améliorations concernant les GPO, qui sont les suivantes :

- Prise en charge limitée pour Nano Server ; Bien que Nano Server ne prend pas directement en charge la stratégie de groupe, les applets de commande PowerShell vous permettent d'importer les paramètres du GPO après les avoir exportés à l'aide de Windows PowerShell. Vous pouvez importer les types de paramètres suivants sur un serveur Nano :
 - Paramètres d'enregistrement ; Vous exportez les paramètres d'enregistrement dans un fichier .POL avant de les importer sur un serveur Nano.
 - Paramètres de sécurité ; Vous exportez les paramètres de sécurité d'un fichier .INF avant de les importer sur un serveur Nano.
 - Paramètres de vérification. Vous exportez les paramètres de vérification dans un fichier .CSV avant de les importer sur un serveur Nano.
- Les modèles d'administration Windows 10 sont inclus. Les fichiers nécessaires pour configurer les paramètres spécifiques Windows 10 sont inclus dans Windows Server 2016.

Windows Server 2016 introduit quelques modifications et améliorations à la stratégie de groupe, notamment :

- Importation des types de paramètres de stratégie suivants sur Nano Server :
 - Les paramètres d'enregistrement
 - Les paramètres de sécurité
 - Les paramètres de vérification
- Intégration des modèles d'administration Windows 10

Classer l'activité

Classer chaque élément dans la catégorie appropriée. Indiquez votre réponse en écrivant le numéro de catégorie à droite de chaque élément.

| Éléments | |
|----------|-------------------------|
| 1 | Domaine |
| 2 | Utilisateur |
| 3 | Unité organisationnelle |
| 4 | Ordinateur |
| 5 | Site |
| 6 | Groupe |
| 7 | Conteneur utilisateurs |
| 8 | Conteneur ordinateurs |

| Catégorie 1 | Catégorie 2 |
|-----------------------|------------------------------|
| Peut relier les GPO à | Ne peut pas relier les GPO à |

Leçon 2

Mise en œuvre et administration des GPO

Avant de déployer une solution de stratégie de groupe, vous devez être familiarisé avec les procédures pour travailler avec les GPO, y compris comment créer, associer, modifier et gérer les GPO avec Windows PowerShell et dans la console GPMC. Vous devez également savoir où les GPO sont stockés dans les contrôleurs de domaine. Au sein d'une entreprise, certains utilisateurs peuvent demander à avoir certaines responsabilités administratives concernant les GPO, de sorte que vous devez aussi savoir déléguer des autorisations pour créer des GPO. Cette leçon enseigne sur toutes ces choses. Les GPO Starter, qui peuvent contenir des paramètres préconfigurés, font également partie de ce cours.

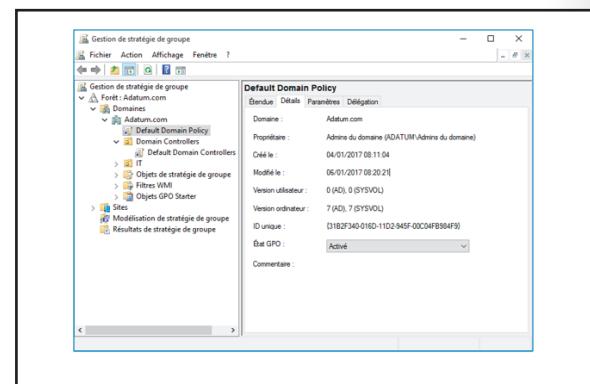
Objectifs des leçons

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

- Expliquer ce que sont les GPO basés sur un domaine ;
- Décrire le stockage des GPO ;
- Décrire les GPO Starter ;
- Décrire les tâches courantes de gestion des GPO ;
- Expliquer comment déléguer l'administration des stratégies de groupe.

Qu'est-ce que des GPO basés sur un domaine ?

Les GPO basés sur un domaine sont des GPO créés dans AD DS et stockés sur les contrôleurs de domaine. Vous pouvez les utiliser pour gérer la configuration centralisée des utilisateurs de domaine et des ordinateurs. Lorsque vous installez AD DS et créer un domaine, deux GPO sont créés automatiquement : **Stratégie de domaine par défaut** et **Stratégie des contrôleurs de domaine par défaut**.



Stratégie de domaine par défaut

Ce GPO est lié au domaine et n'a pas de groupe de sécurité ou de filtres WMI. Par conséquent, il concerne tous les utilisateurs et les ordinateurs dans le domaine, y compris les ordinateurs qui sont des contrôleurs de domaine, mais il n'y a que les paramètres dans la section **Configuration de l'ordinateur**. Ce GPO contient les paramètres de stratégie qui indiquent le mot de passe, le verrouillage des comptes et les stratégies de protocole Kerberos Version 5. Vous ne devez pas ajouter des paramètres de stratégie qui n'ont pas de rapport avec ce GPO. Si vous devez configurer d'autres paramètres généraux dans votre domaine, créez des GPO supplémentaires qui sont associés au domaine.

Stratégie des contrôleurs de domaine par défaut

Ce GPO est lié à l'unité organisationnelle des contrôleurs de domaine. Les comptes d'ordinateur pour les contrôleurs de domaine étant conservés exclusivement dans l'UO **Contrôleurs de domaine** et d'autres comptes d'ordinateur devant être conservés dans d'autres UO, ce GPO concerne uniquement les contrôleurs de domaine. Vous ne devez modifier que le GPO **Contrôleurs de domaine par défaut** pour mettre en œuvre vos stratégies de vérification et attribuer les droits d'utilisateur requis sur les contrôleurs de domaine.



Remarque : De nombreux administrateurs préfèrent ne pas modifier l'un des GPO par défaut et comptent plutôt sur le processus de création de GPO supplémentaires, ainsi que leur association aux mêmes objets conteneurs. Si un incident se produit et que vous devez restaurer les GPO par défaut à leurs paramètres d'origine, tous vos changements seront perdus, si vous avez modifié les deux GPO par défaut.

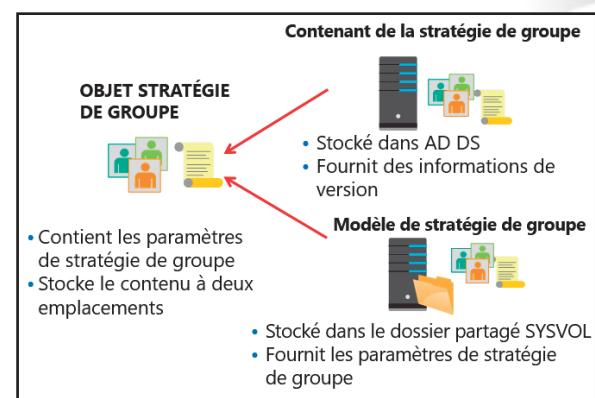


Remarque : Les ordinateurs fonctionnant sous les systèmes d'exploitation Windows disposent également de GPO locaux, qui sont généralement remplacés par des GPO basés sur un domaine à la priorité plus élevée. Cependant, lorsque les ordinateurs ne sont pas connectés à un domaine, ce sont uniquement les GPO locaux qui s'appliquent. Windows Vista et les versions ultérieures, ainsi que Windows 2008 et les versions ultérieures acceptent le concept de plusieurs GPO locaux. Le GPO sur un **ordinateur local** est le même que dans les versions précédentes des systèmes d'exploitation Windows. Dans le nœud **Configuration de l'ordinateur**, vous pouvez configurer tous les paramètres liés à l'informatique. Dans le nœud **Configuration utilisateur**, vous pouvez configurer les paramètres que vous souhaitez appliquer à tous les utilisateurs sur l'ordinateur. Vous pouvez modifier les paramètres de l'utilisateur dans le GPO **Ordinateur local** à l'aide des paramètres utilisateur dans les deux nouveaux GPO locaux suivants : les **Administrateurs** et les **Non-administrateurs**. Ces deux GPO appliquent les paramètres utilisateur aux utilisateurs connectés s'ils sont membres du groupe local des administrateurs, auquel cas ils utiliseront le GPO **Administrateurs**, ou s'ils ne font pas partie du groupe des administrateurs, ils utiliseront donc le GPO **Non-administrateurs**. Vous pouvez redéfinir les paramètres de l'utilisateur plus loin avec un GPO local qui s'applique à un compte d'utilisateur spécifique. Les GPO locaux spécifiques à l'utilisateur sont associés à des comptes d'utilisateur locaux et pas à des domaines.

Il est important de savoir que les paramètres des GPO de domaine se combinent avec ceux qui sont appliqués à l'aide des GPO locaux. Cependant, les GPO de domaine s'appliquant en dernier, ils ont la priorité sur les paramètres des GPO locaux. Vous pouvez désactiver les GPO locaux en configurant le paramètre **Désactiver le traitement des objets de stratégie de groupe locaux** dans un GPO de domaine. Sachez que le GPO local contient de nombreux paramètres importants, y compris les paramètres de sécurité que vous devez configurer dans un GPO de domaine.

Stockage des GPO

Les paramètres de stratégie de groupe sont présentés comme des GPO dans les outils de l'interface utilisateur AD DS (UI), mais un GPO est constitué en fait de deux composantes : un conteneur de stratégie de groupe et un modèle de stratégie de groupe. Le conteneur de stratégie de groupe est un objet AD DS qui est stocké dans le conteneur **Objets de stratégie de groupe** dans le cadre de nommage de domaine du répertoire. Comme tous les objets AD DS, chaque conteneur de stratégie de groupe comprend un attribut identificateur global unique (GUID) qui identifie



l'objet dans AD DS. Le conteneur de stratégie de groupe définit les attributs de base du GPO. Les paramètres se trouvent dans le modèle de stratégie de groupe, qui est un ensemble de fichiers stockés dans le SYSVOL de chaque contrôleur de domaine dans le chemin d'accès

%SystemRoot%\SYSVOL\Domaine\Stratégies\GPOGUID, où GPOGUID est le GUID du conteneur de

stratégie de groupe. Lorsque vous changez les paramètres d'un GPO, les modifications sont enregistrées dans le modèle de stratégie de groupe du contrôleur de domaine à partir duquel le GPO a été ouvert, qui par défaut est le contrôleur de domaine qui détient le rôle premier des opérations d'émulateur de contrôleur de domaine principal (PDC). Par défaut, en cas d'actualisation de stratégie de groupe, les extensions côté client appliquent des paramètres d'un GPO uniquement si le GPO a été mis à jour.

Le service client de stratégie de groupe peut identifier un GPO mis à jour par son numéro de version. Chaque GPO possède un numéro de version qui augmente chaque fois qu'une modification est apportée. Le numéro de version est stocké comme un attribut de conteneur de stratégie de groupe et dans un fichier texte, **Gpt.ini**, dans le dossier **Modèle de stratégie de groupe**. Le client de stratégie de groupe connaît le numéro de version de chaque GPO qu'il a précédemment appliqué. Si, au cours de l'actualisation de stratégie de groupe, le client de stratégie de groupe découvre que le numéro de version du conteneur de stratégie de groupe a été modifié, les extensions côté client sauront que le GPO est mis à jour.

RéPLICATION DES GPO

Les conteneurs de stratégie de groupe et les modèles de stratégie de groupe sont répliqués entre tous les contrôleurs de domaine dans un seul domaine, dans AD DS. Cependant, différents mécanismes de duplication sont utilisés pour ces deux éléments. Le conteneur de stratégie de groupe dans AD DS réplique en utilisant un agent de réPLICATION d'annuaire. Un agent de réPLICATION d'annuaire utilise une topologie générée par Knowledge Consistency Checker, que vous pouvez définir ou affiner manuellement. Il en résulte que le conteneur de stratégie de groupe est répliqué en quelques secondes à tous les contrôleurs de domaine d'un site et il est également copié entre les sites basés sur la configuration de la réPLICATION intersite.

Le modèle de stratégie de groupe dans le SYSVOL se réplique à l'aide de l'une des deux technologies suivantes. Le service de réPLICATION de fichiers (FRS) réplique SYSVOL dans des domaines qui exécutent Windows Server 2008, Windows Server 2008 R2, Windows Server 2003 et Microsoft Windows 2000 Server. Si tous les contrôleurs de domaine exécutent Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 ou Windows Server 2016, vous devez configurer la réPLICATION SYSVOL en utilisant la réPLICATION de système de fichiers réparti (DFS-R), qui est un mécanisme plus efficace et plus fiable. Nous vous recommandons d'utiliser la DFS-R, parce que le FRS est désormais obsolète.

Le conteneur de stratégie de groupe et le modèle de stratégie de groupe répliquant de manière séparée, il est possible qu'ils se désynchronisent pendant un court laps de temps. En règle générale, lorsque cela se produit, le conteneur de stratégie de groupe se réplique en premier sur un contrôleur de domaine. Les systèmes qui ont obtenu leur liste de GPO ordonnés à partir de ce contrôleur de domaine identifient le nouveau conteneur de stratégie de groupe, tentent de télécharger le modèle de stratégie de groupe et notent que les numéros de version ne sont pas les mêmes. Une erreur de traitement de la stratégie est alors enregistré dans le journal des événements. Si l'inverse se produit et que le modèle de stratégie de groupe se réplique à un contrôleur de domaine avant le conteneur de stratégie de groupe, les clients ayant alors obtenu leur liste de GPO ordonnés de ce contrôleur de domaine ne seront pas informés du nouveau GPO jusqu'à ce que le conteneur de stratégie de groupe se réplique.

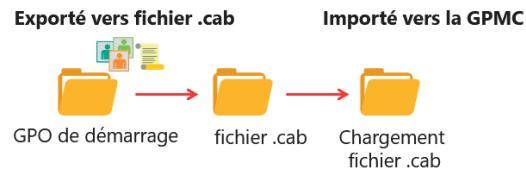
Quels sont les GPO de démarrage ?

Vous utilisez un GPO Starter comme modèle à partir duquel vous pouvez créer d'autres GPO au sein de la GPMC. Les GPO Starter peuvent uniquement contenir des paramètres de modèle d'administration. Vous pouvez utiliser un GPO Starter pour indiquer un point de départ aux nouveaux GPO créés dans votre domaine. Le GPO Starter peut déjà contenir des paramètres spécifiques qui sont les meilleures pratiques recommandées par Microsoft pour votre environnement. Vous pouvez exporter les GPO Starter ou les importer depuis les fichiers CAB (.cab) pour les répartir de manière simple et efficace vers d'autres environnements. La console GPMC stocke les GPO Starter dans le dossier nommé **GPO Starter**, qui se trouve dans SYSVOL.

Lorsque vous cliquez sur le bouton **Créer un dossier pour les GPO Starter**, situé dans le nœud **GPO Starter** de la console GPMC, 10 GPO Starter sont alors créés par défaut.

Un GPO de démarrage :

- Enregistre les paramètres des modèles d'administration sur lesquels les nouveaux objets GPO seront basés
- Peut être exporté vers des fichiers .cab
- Peut être importé dans d'autres domaines d'une organisation



Tâches courantes de gestion des GPO

Comme pour les données importantes et les ressources liées à AD DS, vous devez sauvegarder les GPO pour protéger l'intégrité des AD DS et GPO. Non seulement la console GPMC fournit une sauvegarde basique et restaure les options, mais elle contrôle également davantage les GPO à des fins administratives. Pour gérer les GPO, vous disposez des options suivantes :

- Sauvegarde des GPO. Vous pouvez sauvegarder les GPO de manière séparée ou dans leur ensemble avec la GPMC. Vous devez uniquement fournir un emplacement de sauvegarde, qui peut être un dossier local ou partagé valide. Vous devez avoir l'autorisation de lecture sur le GPO pour le sauvegarder. Chaque fois que vous effectuez une sauvegarde, une nouvelle version de sauvegarde du GPO est créée, qui fournit l'historique des sauvegardes. Si vous souhaitez effectuer une sauvegarde automatique de tous les GPO, vous pouvez exécuter l'applet de commande Windows PowerShell suivante :

```
Backup-GPO -all -path E:\GPOBackup -comment "Powershell backup of GPOs"
```

Vous pouvez gérer les GPO en utilisant GPMC ou Windows PowerShell. Voici quelques options pour gérer l'état des GPO :



- Restauration des GPO sauvegardés. Vous pouvez restaurer une version d'un GPO. Si un GPO est corrompu ou que vous le supprimez, vous pouvez restaurer l'une des versions historiques de ce GPO. L'interface de restauration vous permet d'afficher les paramètres stockés dans la version sauvegardée avant de le restaurer. La restauration d'un GPO ne restaure pas les liens des GPO. Vous devez le faire manuellement par la suite.
- Importation des paramètres des GPO à partir d'un GPO sauvegardé. Vous pouvez importer des paramètres de stratégie d'un GPO dans un autre. En important un GPO, vous pouvez transférer les paramètres d'un GPO sauvegardé vers un GPO existant. L'importation d'un GPO transfère uniquement les paramètres des GPO. Le processus d'importation n'importe pas les liens des GPO. Les

entités de sécurité définies dans la source peuvent avoir besoin de migrer vers la cible à l'aide des tables de migration.

- Copie des GPO Vous pouvez copier des GPO en utilisant la GPMC dans le même domaine et à travers les domaines. Une copie duplique un GPO direct et existant vers le domaine de destination souhaité. Un nouveau GPO est toujours créé au cours de ce processus. Le nouveau GPO est nommé **Copie de Nom de l'ancien GPO**. Par exemple, si vous avez copié un GPO nommé **Bureau**, la nouvelle version s'appelle alors **Copie de bureau**. Une fois que vous copiez et collez le fichier dans le conteneur **Objets de stratégie de groupe**, vous pouvez renommer la stratégie. Le domaine de destination peut être tout domaine approuvé dans lequel vous avez le droit de créer de nouveaux GPO. Lors de la copie entre les domaines, les entités de sécurité définies dans la source peuvent avoir besoin de migrer vers la cible.
- Tables de migration. Lors de l'importation des GPO ou en les copiant entre les domaines, vous pouvez utiliser des tables de migration pour modifier les références du GPO qui doivent être ajustées pour le nouvel emplacement. Par exemple, vous devrez peut-être remplacer le chemin d'accès Convention de dénomination universelle (UNC) par celui de Redirection de dossier à l'aide d'un chemin UNC qui est approprié au nouveau groupe d'utilisateurs auquel le GPO sera appliqué. Vous pouvez créer des tables de migration avant ce processus, ou vous pouvez les créer lors de l'importation ou de la copie par domaine. Les tables de migration sont également utiles si vous souhaitez déplacer les GPO à partir d'un environnement de test dans votre domaine de production.

Si quelque chose arrive aux deux GPO par défaut, **Stratégie de domaine par défaut** et **Stratégie des contrôleurs de domaine par défaut**, vous pouvez restaurer un GPO ou les deux à l'aide de l'utilitaire de ligne de commande **DCGPOFix**. Si vous exécutez **DCGPOFix** sans aucun paramètre, vous restaurez les GPO par défaut. Pour restaurer uniquement le GPO **Stratégie de domaine par défaut**, il vous suffit d'ajouter le paramètre **/Cible : domaine**. De même, vous pouvez restaurer le GPO **Stratégie des contrôleurs de domaine par défaut** en ajoutant le paramètre **/Cible : DC**.

En plus d'utiliser la console GPMC et l'Éditeur des stratégies de groupe, vous pouvez également effectuer des tâches administratives courantes relatives aux GPO à l'aide de Windows PowerShell. Vous pouvez utiliser **obtenir-commande -module stratégie de groupe** pour obtenir une liste de toutes les commandes de stratégie de groupe. Le tableau suivant présente quelques tâches administratives les plus courantes avec Windows PowerShell :

| Nom du l'applet de commande | Description |
|----------------------------------|---|
| Nouveau-GPO | Créer un GPO |
| Nouvelle-GPLink | Créer un lien GPO pour le GPO indiqué |
| Sauvegarder-GPO | Sauvegarde les GPO indiqués |
| Restaurer-GPO | Restaure les GPO indiqués |
| Copier-GPO | Copie un GPO |
| Obtenir-GPO | Obtient les GPO indiqués |
| Importer-GPO | Importe les paramètres sauvegardés dans un GPO indiqué |
| Programmer-GPIInheritance | Accorde des autorisations spécifiques à un groupe d'utilisateurs ou de sécurité pour les GPO indiqués |

Délégation de l'administration de la stratégie de groupe

En déléguant des tâches liées aux GPO, vous pouvez répartir la charge de travail administrative dans toute l'entreprise. Vous pouvez confier à un groupe la création et la modification des GPO, tandis qu'un autre groupe peut effectuer des rapports et des analyses. Un troisième groupe pourra être en charge de la création de filtres WMI.

Vous pouvez déléguer les tâches de stratégie de groupe suivantes :

- Création de GPO ;
- Modification de GPO ;
- Gestion des liens de la stratégie de groupe pour un site, un domaine ou une UO ;
- Modélisation de la stratégie de groupe des analyses sur un domaine ou une UO donnés ;
- Lecture des données des résultats de la stratégie de groupe pour les objets dans un domaine ou une UO donnés ;
- Création de filtres WMI dans un domaine.

- La délégation de tâches liées aux GPO permet de répartir la charge de travail administratif dans toute l'entreprise
- Vous pouvez déléguer indépendamment les tâches de stratégie de groupe suivantes :
 - Création de GPO
 - Modification des GPO
 - Gestion des liens de stratégie de groupe pour un site, un domaine ou UO
 - Exécution de l'analyse de modélisation de la stratégie de groupe dans un domaine ou UO
 - Lecture des données des résultats de stratégie de groupe dans un domaine ou UO
 - Création de filtres WMI dans un domaine

Le groupe des propriétaires et créateurs de la stratégie de groupe permet aux membres qui créent des GPO de les modifier ou de les supprimer.

Autorisations par défaut de la stratégie de groupe

Par défaut, l'utilisateur et les groupes suivants contrôlent de A à Z la gestion des GPO :

- Administrateurs du domaine ;
- Administrateurs de l'entreprise ;
- Propriétaires et créateurs de la stratégie de groupe ;
- Système local.

Le groupe d'utilisateurs authentifiés est autorisé à lire et à appliquer la stratégie de groupe à tous les GPO.

Création de GPO

Par défaut, seuls les administrateurs du domaine, les administrateurs de l'entreprise, ainsi que les propriétaires et créateurs de la stratégie de groupe peuvent créer de nouveaux GPO. Vous pouvez utiliser deux méthodes pour octroyer ce droit à un groupe ou à un utilisateur :

- Ajoutez l'utilisateur ou un groupe au groupe des propriétaires et créateurs de la stratégie de groupe ;
- Accordez de manière explicite l'autorisation à un groupe ou à un utilisateur à créer des GPO à l'aide de la GPMC.

Modification de GPO

Pour modifier un GPO, l'utilisateur doit disposer de l'accès vers le GPO « Lire et écrire ». Vous pouvez accorder cette autorisation à l'aide de la console GPMC.

Gestion des liens GPO

La possibilité d'associer les GPO à un conteneur est une autorisation qui est propre à ce conteneur. Dans la GPMC, vous pouvez gérer cette autorisation via l'onglet **Délégation** sur le conteneur. Vous pouvez également la déléguer en utilisant **Délégation de l'assistant de contrôle** dans Utilisateurs et ordinateurs Active Directory.

Modélisation et résultats de la stratégie de groupe

Vous pouvez déléguer la possibilité d'utiliser les outils de reporting de la même manière : par le biais de la GPMC ou de la **Délégation de l'assistant de contrôle** dans Utilisateurs et ordinateurs Active Directory.

Création de filtres WMI

Vous pouvez déléguer la possibilité de créer et de gérer des filtres WMI de la même manière : par le biais de la GPMC ou de la **Délégation de l'assistant de contrôle** dans Utilisateurs et ordinateurs Active Directory.

Démonstration : Délégation de l'administration de la stratégie de groupe

Dans cette démonstration, vous allez apprendre à :

- Déléguer des autorisations pour créer des GPO ;
- Déléguer des autorisations pour lier les GPO ;
- Déléguer des autorisations pour afficher les résultats de la stratégie de groupe.

Procédure de démonstration

Faire d'Aurore un administrateur local sur LON-SVR1

1. Basculez vers **LON-DC1**.
2. Exécutez le script Windows PowerShell situé dans **E:\Labfiles\Mod05\Set-LocalAdmin.ps1** pour faire de **Beth** un administrateur local sur **LON-SVR1**.

Vérifiez les permissions des utilisateurs avant délégation

1. Basculez vers **LON-SVR1**.
2. Connectez-vous en tant qu'**Adatum\Aurore** avec le mot de passe **Pa55w.rd**.
3. Dans le **Gestionnaire de serveur**, ajoutez la fonctionnalité **Gestion de la stratégie de groupe**.
4. Fermez la **Gestion de la stratégie de groupe**.
5. Essayez de créer un GPO. L'élément de menu **Nouveau** est grisé car Beth n'a pas obtenu les autorisations pour créer des GPO.
6. Essayez de lier un GPO au domaine **Adatum.com**. L'élément de menu **Lier un GPO existant** est grisée car Beth ne dispose pas des autorisations pour lier les GPO au domaine.
7. Essayez de lier un GPO à l'UO **IT**. L'élément de menu **Lier un GPO existant** est grisé car Beth ne dispose pas également des autorisations pour lier les GPO à l'UO IT.
8. Ouvrez une invite de commandes Windows PowerShell, puis exécutez la commande suivante :

```
GPResult /r
```

9. Dans la sortie de la commande, notez que seul les paramètres de l'**Utilisateur** sont affichés car Beth n'est pas autorisée à afficher les résultats de stratégie de groupe pour les paramètres de l'ordinateur.

Déléguer des autorisations

- Sur **LON-DC1**, basculez vers la fenêtre **Gestion des stratégies de groupe**.
- Dans l'onglet **Délégation** pour le conteneur des **Objets de la stratégie de groupe**, ajoutez **Beth** à la liste.
- Dans l'onglet **Délégation** sur l'UO **IT**, ajoutez **Beth** avec l'autorisation **Lier les GPO**.
- Dans l'onglet **Délégation** sur le domaine **Adatum.com**, ajoutez **Beth** avec l'autorisation **Lire les données des résultats de la stratégie de groupe**.

Vérifiez les autorisations après la délégation

- Basculez vers **LON-SVR1**.
- Dans la fenêtre **Gestion de la stratégie de groupe**, cliquez sur puis cliquez avec le bouton droit sur le domaine **Adatum.com**, puis cliquez sur **Actualiser**.
- Créez un nouveau GPO nommé **GPO de Beth**.
- Essayez de lier un GPO au domaine **Adatum.com**. **Lier un GPO existant** est toujours grisé car Beth ne peut pas lier les GPO à l'UO **IT**.
- Liez le **GPO de Beth** au OU **IL**.
- Basculez vers la fenêtre **Windows PowerShell**.
- Dans la fenêtre **Windows PowerShell**, saisissez la commande suivante, puis appuyez sur Entrée :

```
GPResult /r
```

- Dans la sortie de la commande, notez que les deux paramètres **Ordinateur** et **l'Utilisateur** sont affichés.

Testez vos connaissances

| Question | |
|--|---|
| Quels sont les groupes AD DS dont les membres peuvent des GPO par défaut ? (Sélectionnez trois réponses) | |
| Sélectionnez la réponse correcte. | |
| | Administrateurs du domaine |
| | Opérateurs de compte |
| | Administrateurs de l'entreprise |
| | Administrateurs GPO |
| | Propriétaires créateurs de la stratégie de groupe |

Leçon 3

Cadre et traitement de la stratégie de groupe

Un GPO est, par lui-même, une collection d'instructions de configuration qui sera traitée par les extensions côté client des ordinateurs. Jusqu'à ce que le GPO ait une portée, il ne s'applique à aucun utilisateur ni ordinateur. La portée du GPO détermine les extensions côté client des ordinateurs qui vont recevoir et traiter les GPO et seuls les ordinateurs ou les utilisateurs dans le cadre d'un GPO appliqueront les paramètres dans ce GPO. Par conséquent, vous devez adapter la portée des GPO à votre environnement. Dans cette leçon, vous allez en apprendre davantage sur chacun des mécanismes avec lesquels vous pouvez limiter la portée d'un GPO et, dans le processus, vous en apprendrez davantage sur les concepts de la demande, de l'héritage et de la priorité de la stratégie de groupe.

Objectifs des leçons

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

- Décrire les liens GPO ;
- Expliquer comment lier les GPO ;
- Décrire le traitement de la stratégie de groupe ;
- Expliquer comment configurer l'héritage et la priorité du GPO ;
- Expliquer comment utiliser le filtrage de sécurité pour modifier la portée de la stratégie de groupe ;
- Décrire les filtres WMI ;
- Expliquer comment filtrer l'application de stratégie de groupe ;
- Expliquer comment activer ou désactiver les GPO et les nœuds GPO ;
- Décrire le traitement de la stratégie de bouclage ;
- Décrire les considérations pour des liaisons lentes et des systèmes déconnectés ;
- Expliquer comment identifier lorsque les paramètres entrent en vigueur.

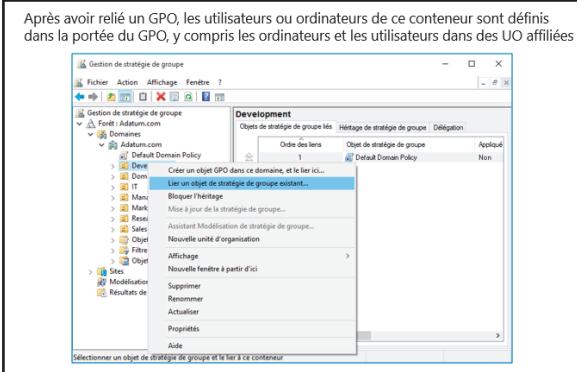
Que sont les liens GPO ?

Vous pouvez lier un GPO à un ou plusieurs des sites AD DS, domaines ou UO. Après avoir lié un GPO, les utilisateurs ou ordinateurs dans ce conteneur se trouvent dans le cadre du GPO, y compris les ordinateurs et les utilisateurs dans des UO enfants.

Lier un GPO

Pour lier un GPO, il faut :

1. Cliquer avec le bouton droit sur le domaine ou l'unité organisationnelle dans l'arborescence de la console GPMC, puis cliquer sur **Lier comme GPO existant**.
2. Si vous n'avez pas encore créé de GPO, cliquez sur **Créer un GPO dans ce {Domaine | UO} Et lier le ici**.



Vous pouvez choisir les mêmes commandes pour lier un GPO à un site, mais par défaut, vos sites AD DS ne sont pas visibles dans la console GPMC. Pour afficher les sites de la console GPMC, cliquez avec le bouton droit sur **Sites** dans l'arborescence de la console GPMC, puis cliquez sur **Afficher les sites**. Il est impossible de créer et de lier un GPO à un site en une seule opération.

 **Remarque :** Un GPO qui est lié à un site affecte tous les ordinateurs du site, sans tenir compte du domaine auquel appartiennent les ordinateurs, tant que tous les ordinateurs appartiennent à la même forêt Active Directory. Par conséquent, lorsque vous liez un GPO à un site, ce GPO peut appliquer à plusieurs domaines dans une forêt. Les GPO liés au site sont stockés sur les contrôleurs de domaine dans le domaine dans lequel vous créez le GPO. Par conséquent, les contrôleurs de domaine pour ce domaine doivent être accessibles pour les GPO liés aux sites à appliquer correctement. Si vous implémentez des stratégies liées aux sites, vous devez considérer l'application de la stratégie lors de la planification de votre infrastructure réseau. Vous pouvez placer un contrôleur de domaine à partir du domaine du GPO dans le site auquel la stratégie est liée ou pour assurer que la connectivité WAN offre un accès à un contrôleur de domaine dans le domaine du GPO.

Lorsque vous liez un GPO à un conteneur, vous définissez la portée initiale du GPO. Sélectionnez un GPO, puis cliquez sur l'onglet **Portée** pour identifier les conteneurs auxquels le GPO est lié. Dans le volet des détails de la console GPMC, les liens GPO sont affichés dans la première section de l'onglet **Portée**.

L'impact des liens du GPO est que le service Group Policy Client télécharge le GPO si les objets de l'ordinateur ou de l'utilisateur entrent dans le cadre de la liaison. Le GPO est téléchargé seulement s'il est nouveau ou mis à jour. Le service Group Policy Client met en cache le GPO pour que l'actualisation de la stratégie soit plus efficace.

Lier un GPO à plusieurs UO

Vous pouvez lier un GPO à plus d'un site ou unité organisationnelle. Il est fréquent, par exemple, d'appliquer une configuration aux ordinateurs dans plusieurs UO. Vous pouvez définir la configuration dans un seul GPO, puis relier ce GPO à chaque unité organisationnelle. Si vous modifiez ultérieurement les paramètres du GPO, vos modifications seront applicables à toutes les UO auxquelles le GPO est lié.

Supprimer ou désactiver un lien GPO

Une fois que vous avez lié un GPO, le lien GPO apparaît dans la console GPMC sous le site, domaine ou unité organisationnelle. L'icône du lien GPO a un petit raccourci en forme de flèche. Lorsque vous cliquez avec le bouton droit sur le lien GPO, un menu contextuel apparaît. Pour supprimer un lien GPO, cliquez avec le bouton droit sur le lien GPO dans l'arborescence de la console GPMC, puis cliquez sur **Supprimer**.

La suppression d'un lien GPO ne supprime pas le GPO lui-même, qui reste dans le conteneur **Objets de la stratégie de groupe**. Cependant, la suppression du lien ne modifie pas le champ d'application du GPO, de sorte qu'il ne s'applique plus aux ordinateurs et aux utilisateurs au sein de l'objet du conteneur précédemment lié.

Vous pouvez également modifier un lien GPO en le désactivant. Pour désactiver un lien GPO, cliquez avec le bouton droit sur le lien GPO dans l'arborescence de la console GPMC, puis désactivez l'option **Lien activé**. Lorsque vous désactivez le lien, vous modifiez le champ d'application du GPO de sorte qu'il ne concerne plus les ordinateurs et les utilisateurs de ce conteneur. Cependant, le lien reste afin que vous puissiez plus facilement le réactiver. Vous pouvez reconnaître un lien non disponible parce qu'il apparaît en estompé.

Démonstration : Lier des GPO

Dans cette démonstration, vous apprendrez à :

- Créer et éditer deux GPO ;
- Lier les GPO à des emplacements différents ;
- Désactiver un lien GPO ;
- Supprimer un lien GPO.

Procédures de démonstration

Créer et éditer deux GPO

1. Ouvrez **Gestion des stratégies de groupe**.
2. Créez deux nouveaux GPO nommés **Supprimer la commande Exécuter** et **Ne pas supprimer la commande Exécuter**.
3. Modifier les paramètres des deux GPO.

Lier les GPO à des emplacements différents

1. Liez le GPO **Supprimer la commande Exécuter** au domaine. Le GPO **Supprimer la commande Exécuter** est désormais attaché au domaine **Adatum.com**.
2. Liez le GPO **Ne pas supprimer la commande Exécuter** à l'UO **Informatique**. Le GPO **Ne pas supprimer la commande Exécuter** est désormais attaché à l'UO **Informatique**.
3. Affichez l'héritage du GPO sur l'UO **Informatique**. L'onglet **Héritage de stratégie de groupe** montre l'ordre de priorité pour les GPO.

Désactiver un lien GPO

1. Désactivez le GPO **Supprimer la commande Exécuter** sur le domaine **Adatum.com**.
2. Actualisez l'onglet **Héritage de stratégie de groupe** pour l'UO **Informatique**, puis remarquez les résultats dans le volet d'informations. Le GPO **Supprimer la commande Exécuter** n'est plus répertorié.

Supprimer un lien GPO

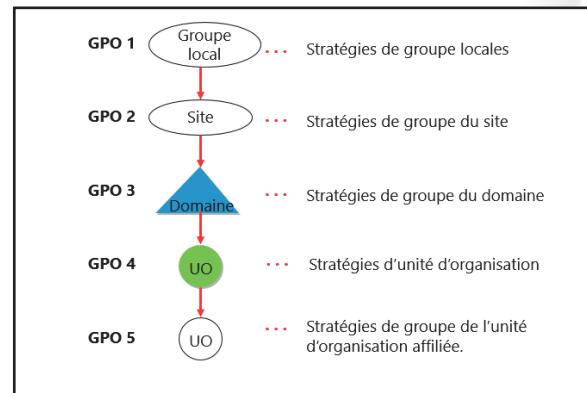
1. Sélectionnez l'UO **Informatique**, puis supprimez le lien GPO **Ne pas supprimer la commande Exécuter**. Vérifiez la suppression du GPO **Ne pas supprimer la commande Exécuter** et l'absence du GPO **Retirer la commande Exécuter**.
2. Activez le GPO **Supprimer la commande Exécuter** sur le domaine **Adatum.com**. Actualisez la fenêtre **Héritage de stratégie de groupe** pour l'UO **Informatique**, puis remarquez les résultats dans le volet d'informations.

Ordre de traitement d'une stratégie de groupe

Les GPO qui s'appliquent à un utilisateur, un ordinateur, ou les deux ne s'appliquent pas tous à la fois. La stratégie de groupe s'applique aux GPO dans un ordre particulier. Cet ordre signifie que les paramètres traités en premier pourraient être remplacés par des paramètres contradictoires qui sont traités ultérieurement.

La stratégie de groupe suit l'ordre de traitement hiérarchique suivant :

1. Objets de stratégie de groupe locaux. Chaque ordinateur qui exécute Microsoft Windows 2000 ou plus récent possède au moins un objet de stratégie de groupe local. L'objet de stratégie de groupe local s'applique en premier.
2. Objets de stratégie de groupe du site. Les objets de stratégie de groupe liés aux sites s'appliquent en deuxième. S'il y a plusieurs GPO de site, ils appliquent de façon synchrone dans l'ordre indiqué.
3. Objets de stratégie de groupe du domaine. Les objets de stratégie de groupe liés au domaine s'appliquent en troisième. S'il y a plusieurs GPO de domaine, ils appliquent de façon synchrone dans l'ordre indiqué.
4. Objets de stratégie de groupe de l'unité d'organisation. Les objets de stratégie de groupe liés aux UO de niveau supérieur s'appliquent en quatrième. S'il y a plusieurs GPO d'UO de niveau supérieur, ils appliquent de façon synchrone dans l'ordre indiqué.
5. Objets de stratégie de groupe d'UO enfant. Les objets de stratégie de groupe liés aux UO enfant s'appliquent en cinquième. S'il y a plusieurs GPO d'UO enfant, ils appliquent de façon synchrone dans l'ordre indiqué. Quand il y a plusieurs niveaux d'UO enfant, les objets de stratégie de groupe liés aux UO de niveau supérieur s'appliquent en premier, puis les objets de stratégie de groupe pour les UO de niveau inférieur s'appliquent ensuite.



En application de stratégie de groupe, la règle générale veut que la dernière stratégie appliquée gagne. Par exemple, une stratégie qui limite l'accès au **Panneau de contrôle** appliquée au niveau du domaine pourrait être inversée par une stratégie appliquée au niveau de l'UO pour les objets contenus dans cette UO particulière.

Si vous liez plusieurs GPO à une UO, leur traitement se produit dans l'ordre que l'administrateur spécifie sur l'onglet **Objets de stratégie de groupe liés** de l'UO dans la GPMC. Par défaut, le traitement est activé pour tous les liens GPO. Vous pouvez désactiver le lien GPO d'un conteneur pour bloquer entièrement l'application d'un GPO pour un site, un domaine ou une UO en particulier. Notez que si le même GPO est lié à d'autres conteneurs ailleurs dans la hiérarchie AD DS, le GPO continuera de traiter dans ces conteneurs si les liens sont activés.

Vous pouvez également désactiver l'utilisateur ou la section de configuration ordinateur d'un GPO particulier indépendamment de l'utilisateur ou de l'ordinateur. Si l'on sait qu'une section d'une stratégie est vide, la désactivation de l'autre côté accélérera légèrement le traitement de la stratégie. Par exemple, si vous avez une stratégie qui fournit uniquement la configuration du bureau utilisateur, vous pourriez désactiver le côté ordinateur de la stratégie.

Configuration l'héritage et la préséance GPO

Vous pouvez configurer le même paramètre de stratégie dans plusieurs GPO, ce qui peut entraîner des conflits de GPO. Par exemple, vous pouvez activer un paramètre de stratégie dans un GPO, le désactivez dans un autre puis ne pas le configurer dans un troisième. Dans ce cas, la précédence du GPO détermine le paramètre de stratégie appliquée par le client. Un GPO avec une précédence plus élevée l'emporte sur un GPO avec précédence inférieure. La précédence est représentée sous forme de numéro dans la GPMC. Plus le nombre s'approche de 1, plus la précédence est importante. Par conséquent, un GPO qui a une précédence de 1 prévaudra sur les autres GPO. Sélectionnez le conteneur AD DS correspondant, puis cliquez sur l'onglet **Héritage de stratégie de groupe** pour afficher la précédence de chaque GPO.

- L'application des GPO liés à chacun des résultats de conteneurs entraîne un effet cumulatif appelé *l'héritage de stratégie* :
 - Priorité par défaut : Locale → Site → Domaine → Unité d'organisation → Unité d'organisation affiliée... (LSDUO)
 - Visible sur l'onglet **Héritage de stratégie de groupe**
- Ordre des liens (attribut du lien vers l'objet de stratégie de groupe) :
 - Réduction du nombre → En haut de la liste → Priorité
- Bloquer l'héritage (attribut de l'UO) :
 - Bloque le traitement des GPO à partir d'un niveau plus élevé
- Appliqué (attribut du lien vers l'objet de stratégie de groupe) :
 - Les GPOs appliqués sont prioritaires sur Bloquer l'héritage
 - Les paramètres GPO appliqués prévalent sur les paramètres incompatibles dans les GPO inférieurs

Lorsque vous activez ou désactivez un paramètre de stratégie dans un GPO de précédence supérieure, le paramètre configuré prend effet. Cependant, rappelez-vous que les paramètres de stratégie sont définis sur **Non configuré**, par défaut. Si un paramètre de stratégie n'est pas configuré dans un GPO de précédence supérieure, le paramètre de stratégie activé ou désactivé dans un GPO de précédence inférieure prendra effet.

Vous pouvez lier plus d'un GPO à un objet conteneur AD DS. L'ordre de liaison des GPO détermine la priorité des GPO dans un tel scénario. Les GPO avec un ordre de liaison supérieur ont préséance sur les GPO avec un ordre de liaison inférieur. Lorsque vous sélectionnez une UO dans la GPMC, l'onglet **Objets de stratégie de groupe liés** affiche l'ordre de liaison des GPO liés à cette UO.

Le comportement par défaut de la stratégie de groupe est tel que les GPO liés à un conteneur de niveau supérieur sont hérités par des conteneurs de niveau inférieur. Lorsqu'un ordinateur démarre ou qu'un utilisateur se connecte, le client de stratégie de groupe examine l'emplacement de l'ordinateur ou l'objet USER dans AD DS et évalue les GPO avec des étendues qui comprennent l'ordinateur ou l'utilisateur. Ensuite, les extensions côté client appliquent les paramètres de stratégie de ces GPO. Les stratégies s'appliquent séquentiellement, en commençant par les stratégies liées au site, suivies par celles liées au domaine, puis par celles liées aux UO ; des UO de niveau supérieur jusqu'à l'UO dans laquelle l'utilisateur ou l'objet USER existe. Il s'agit d'une application en couches de paramètres, donc un GPO qui est appliqué plus tard dans le processus, car il a une précédence plus élevée, l'emporte sur les paramètres appliqués plus tôt dans le processus.

L'application séquentielle des GPO crée un effet appelé *l'héritage de la stratégie*. Les stratégies sont héritées, donc l'ensemble de stratégie qui en résulte pour un utilisateur ou un ordinateur sera l'effet cumulatif des stratégies de site, de domaine et de l'UO.

Par défaut, les GPO hérités ont une précédence inférieure aux GPO liés directement au conteneur. Par exemple, vous pouvez configurer un paramètre de stratégie pour désactiver l'utilisation d'outils de modification du registre pour tous les utilisateurs dans le domaine en configurant le paramètre de stratégie dans un GPO lié au domaine. Ce GPO et son paramètre de stratégie sont hérités par tous les utilisateurs du domaine. Cependant, vous voulez probablement que les administrateurs puissent utiliser les outils de modification du registre, de manière à pouvoir lier un GPO à l'UO qui contient les comptes des administrateurs, puis configurer le paramètre de stratégie pour permettre l'utilisation des outils de modification du registre. Parce que le GPO lié à l'UO des administrateurs a une précédence supérieure au GPO hérité, les administrateurs seront en mesure d'utiliser les outils de modification du registre.

Précédence de GPO liés multiples

Si plusieurs GPO sont liés à un objet conteneur AD DS, l'ordre de liaison de l'objet détermine leur précédence.

Pour modifier la précédence d'un lien GPO :

1. Sélectionnez l'objet conteneur AD DS dans l'arborescence de la console GPMC.
2. Cliquez sur l'onglet **Objets de stratégie de groupe liés** dans le volet d'informations.
3. Sélectionnez le GPO.
4. Utilisez les flèches **Vers le haut**, **Vers le bas**, **Déplacer vers le haut** et **Déplacer vers le bas** pour modifier l'ordre de liaison du GPO sélectionné.

Bloquer l'héritage

Vous pouvez configurer un domaine ou une UO pour empêcher l'héritage des paramètres de stratégie. Il s'agit de *l'héritage de blocage*. Pour bloquer l'héritage, cliquez avec le bouton droit sur le domaine ou l'UO dans l'arborescence de la console GPMC, puis sélectionnez **Bloquer l'héritage**.

L'option **Bloquer l'héritage** est une propriété d'un domaine ou d'une UO, de sorte qu'il bloque tous les paramètres de stratégie de groupe de GPO liés aux parents dans la hiérarchie de stratégie de groupe. Par exemple, lorsque vous bloquez l'héritage sur une UO, l'application GPO commence par des GPO liés directement à cette UO. Par conséquent, les GPO liés à des UO de niveau supérieur, au domaine, ou au site ne s'appliqueront pas.

Utilisez l'option **Bloquer l'héritage** avec parcimonie car le blocage d'héritage complique l'évaluation de la précédence et de l'héritage de stratégie de groupe. Avec le filtrage de groupe de sécurité, vous pouvez définir la portée d'un GPO avec soin afin qu'il s'applique uniquement aux utilisateurs et ordinateurs appropriés en premier lieu, ce qui rend superflue l'utilisation de l'option **Bloquer l'héritage**.

Mettre en application un lien GPO

En outre, vous pouvez définir un lien GPO pour qu'il soit **Appliqué**. Pour appliquer un lien GPO, cliquez avec le bouton droit sur le lien GPO dans l'arborescence de la console, puis cliquez sur **Appliqué** dans le menu contextuel. Lorsque vous définissez un lien GPO sur **Appliqué**, le GPO prend le niveau de précédence le plus élevé ; Les paramètres de stratégie dans ce GPO prévaudront sur les paramètres de stratégie contradictoires dans d'autres GPO. En outre, lorsqu'un lien est appliqué, il le sera aux conteneurs enfant, même lorsque ces conteneurs sont définis sur **Bloquer l'héritage**. L'option **Appliqué** entraîne l'application de la stratégie à tous les objets dans son étendue. L'option **Appliqué** entraîne la substitution des stratégies contradictoires et s'applique indépendamment du fait que l'option **Bloquer l'héritage** soit utilisée.

L'application est utile lorsque vous devez configurer un GPO qui définit une configuration mandatée par vos stratégies de sécurité informatique et d'utilisation internes. Par conséquent, vous devez vous assurer que d'autres GPO ne remplacent pas ces paramètres. Vous pouvez le faire en appliquant le lien du GPO.

Évaluer la précédence

Pour faciliter l'évaluation de la précédence du GPO, vous pouvez simplement sélectionner une UO ou un domaine, puis cliquez sur l'onglet **Héritage de stratégie de groupe**. Cet onglet affiche la précédence résultante des GPO, représentant le lien GPO, l'ordre du lien, blocage de l'héritage et l'application du lien. Cet onglet ne tient pas compte ni des stratégies qui sont liées à un site, ni de la sécurité du GPO ou du filtrage WMI.

Utilisation du filtrage de sécurité pour modifier la portée de la stratégie de groupe

Bien qu'il soit possible d'utiliser les options **Mise en application** et **Bloquer l'héritage** pour contrôler l'application des GPO à des objets conteneurs, vous pourriez avoir besoin d'appliquer les GPO uniquement à certains groupes d'utilisateurs ou d'ordinateurs plutôt qu'à l'ensemble des utilisateurs ou des ordinateurs dans l'étendue du GPO. Vous ne pouvez pas lier directement un GPO à un groupe de sécurité, mais il existe un moyen d'appliquer les GPO à des groupes de sécurité spécifiques. Les paramètres d'un GPO s'appliquent uniquement aux utilisateurs qui possèdent les autorisations

Autoriser la lecture et Autoriser l'application de la stratégie de groupe au GPO.

Chaque GPO dispose d'une liste de contrôle d'accès (ACL) qui définit les autorisations sur ce GPO. Deux autorisations, Autoriser la lecture et Autoriser l'application de la stratégie de groupe, sont nécessaires pour qu'un GPO s'applique à un utilisateur ou à un ordinateur. Par exemple, si un GPO est étendu à un ordinateur par son lien vers l'UO de l'ordinateur, mais que l'ordinateur ne dispose pas des autorisations Autoriser la lecture et Autoriser l'application de stratégie de groupe, il ne téléchargera pas et n'appliquera pas le GPO. Par conséquent, en définissant les autorisations appropriées pour les groupes de sécurité, vous pouvez filtrer un GPO pour que ses paramètres ne s'appliquent qu'aux ordinateurs et aux utilisateurs que vous spécifiez.

Par défaut, les membres du groupe Utilisateurs authentifiés reçoivent l'autorisation Autoriser l'application de la stratégie de groupe sur chaque nouveau GPO. Cela signifie que, par défaut, tous les utilisateurs et ordinateurs sont affectés par les GPO définis pour leur domaine, site ou UO, quels que soient les autres groupes dans lesquels ils pourraient être membres. Par conséquent, il existe deux façons de filtrer l'étendue du GPO :

- Supprimez l'autorisation Appliquer la stratégie de groupe, définie par défaut sur Autoriser, pour le groupe Utilisateurs authentifiés, mais ne définissez pas cette autorisation sur Refuser. Ensuite, déterminez les groupes auxquels le GPO devraient être appliqués et définissez les autorisations Autoriser la lecture et Autoriser l'application de la stratégie de groupe pour ces groupes sur Autoriser.
- Identifier les groupes auxquels le GPO ne devraient pas être appliqués, puis définissez l'autorisation Appliquer la stratégie de groupe pour ces groupes sur Refuser. Si vous refusez l'autorisation Appliquer la stratégie de groupe à un GPO, l'utilisateur ou l'ordinateur ne sera pas en mesure d'appliquer les paramètres dans le GPO, même si l'utilisateur ou de l'ordinateur est membre d'un autre groupe qui possède l'autorisation Appliquer la stratégie de groupe. Ces groupes sont également appelés *groupes d'exemption*.

Vous pouvez utiliser le filtrage de groupe de sécurité pour gérer l'étendue d'un GPO au cours des essais. Au lieu de créer une unité d'organisation affiliée pour gérer la portée du GPO pour les tests, lier le GPO à l'emplacement auquel il appartient dans la production. Cependant, au lieu de permettre au GPO de s'appliquer aux Utilisateurs authentifiés, ou au groupe de sécurité de la production, configurez un groupe de sécurité spécialement conçu pour limiter l'étendue du GPO aux utilisateurs et aux ordinateurs appropriés. L'avantage de cette pratique est qu'elle donne une image beaucoup plus réaliste de la façon dont le GPO fonctionnera dans la production parce que vous ne limitez pas artificiellement la portée ou la priorité en l'associant à une unité d'organisation de test séparé. En d'autres termes, vous obtenez une meilleure image de la façon dont le GPO interagit avec d'autres GPO qui sont déjà en production. Et pourtant, vous maintenez toujours le plein contrôle sur les utilisateurs et les ordinateurs spécifiques qui relèvent du champ d'application du test. Vous devez définir le filtrage de sécurité sur le GPO avant de le lier à l'UO ou au domaine.

• Autorisation Appliquer la stratégie de groupe :

- Le GPO possède une ACL (onglet **Délégation** → **Avancée**)
- Les membres du groupe Utilisateurs authentifiés possèdent les autorisations par défaut d'Appliquer la stratégie de groupe

• Pour définir uniquement la portée aux utilisateurs des groupes globaux sélectionnés :

- Supprimez le groupe Utilisateurs authentifiés
- Ajoutez des groupes globaux appropriés : Doivent être des groupes globaux (les GPO ne sont pas définis dans la portée au domaine local)

• Pour définir la portée aux utilisateurs, à l'exception de ceux des groupes sélectionnés :

- Dans l'onglet **Délégation**, cliquez sur **Avancé**
- Ajoutez des groupes globaux appropriés
- Refusez l'autorisation Appliquer la stratégie de groupe

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

Filtrage d'un GPO à appliquer à des groupes spécifiques

Pour appliquer un GPO à un groupe de sécurité spécifique :

1. Sélectionnez le GPO dans le conteneur **Objet de stratégie de groupe** dans l'arborescence de la console.
2. Sur l'onglet **Étendue**, dans la section **Filtrage de sécurité**, sélectionnez le groupe **Utilisateurs authentifiés**, puis cliquez sur **Supprimer**.
3. Cliquez sur **OK** pour confirmer les modifications.
4. Cliquez sur **Ajouter**.
5. Sélectionnez le groupe auquel vous souhaitez appliquer la stratégie, puis cliquez sur **OK**.

Filtrage d'un GPO pour exclure des groupes spécifiques

L'onglet **Étendue** d'un GPO ne vous permet pas d'exclure des groupes spécifiques. Pour exclure un groupe, c'est-à-dire refuser l'autorisation Appliquer la stratégie de groupe, vous devez utiliser l'onglet **Délégation**.

Pour refuser à un groupe l'autorisation Appliquer la stratégie de groupe :

1. Sélectionnez le GPO dans le conteneur **Objet de stratégie de groupe** dans l'arborescence de la console.
2. Cliquez sur l'onglet **Délégation**, puis sur **Avancé**.
3. Dans la boîte de dialogue **Paramètres de sécurité**, cliquez sur **Ajouter**.
4. Sélectionnez le groupe que vous voulez exclure du GPO.
5. Cliquez sur **OK**. Le groupe que vous avez sélectionné reçoit l'autorisation Autoriser la lecture par défaut.
6. Désactivez la case à cocher d'autorisation **Autoriser la lecture**.
7. Activez la case à cocher **Refuser l'application de la stratégie de groupe**.
8. Cliquez sur **OK**. Vous recevez un avertissement spécifiant que les autorisations Refuser remplacent d'autres autorisations. Étant donné que les autorisations Refuser remplacent les autorisations Autoriser, nous vous recommandons de les utiliser avec parcimonie. Le message d'avertissement vous rappelle de cette meilleure pratique. Le processus visant à exclure des groupes avec l'autorisation Refuser l'application de la stratégie de groupe est beaucoup plus fastidieuse que le processus qui permet d'inclure des groupes dans la section Filtrage de sécurité de l'onglet **Étendue**.
9. Cliquez **Oui** pour confirmer que vous souhaitez continuer.



Remarque : Les autorisations Refuser ne sont pas disponibles sur l'onglet **Étendue**.

Malheureusement, lorsque vous excluez un groupe, l'exclusion ne figure pas dans la section **filtrage de sécurité** de l'onglet **Étendue**. Voici une raison de plus d'utiliser les autorisations Refuser avec parcimonie.



Remarque : Si vous supprimez le groupe Utilisateurs authentifiés, puis définissez l'étendue d'un GPO à un groupe spécifique, les utilisateurs ne seront pas en mesure de lire la stratégie pour effectuer les tâches de gestion de stratégie de groupe. Assurez-vous d'assigner au personnel approprié l'autorisation d'accès en lecture au GPO, mais ne leur assignez pas l'autorisation Appliquer une stratégie.

À quoi servent les filtres WMI ?

Les administrateurs peuvent utiliser la technologie de l'infrastructure de gestion Windows Management Instrumentation (WMI) pour surveiller et contrôler les objets gérés dans un réseau. Une requête WMI est capable de filtrer les systèmes en fonction des caractéristiques, y compris la mémoire vive (RAM), la vitesse du processeur, la capacité du disque, l'adresse IP, la version du système d'exploitation, le niveau de service pack, les applications installées et les propriétés de l'imprimante. Comme WMI expose presque chaque propriété de chaque objet à l'intérieur d'un ordinateur, la liste des attributs que vous pouvez utiliser dans une requête WMI est pratiquement illimitée. Les requêtes WMI sont écrites à l'aide de Langage de requêtes WMI (WQL).

- Les requêtes WMI peuvent filtrer les GPO en fonction des caractéristiques du système, y compris :
 - RAM
 - Vitesse du processeur
 - Capacité du disque
 - Adresse IP
 - Version du système d'exploitation
- Les requêtes WMI sont écrites en utilisant le WQL, par exemple Sélectionner * dans Win32_OperatingSystem où l'on trouve des versions comme « 10.% »
- Les filtres WMI peuvent être coûteux en termes de performances de traitement de stratégie de groupe



Vous pouvez utiliser une requête WMI pour créer un filtre WMI, que vous pouvez utiliser pour filtrer un GPO. La stratégie de groupe vous permet de déployer des applications logicielles et des services packs. Vous pouvez créer un GPO pour déployer une application, puis utiliser un filtre WMI pour préciser que la stratégie devrait s'appliquer uniquement aux ordinateurs dotés d'un système d'exploitation et d'un service pack particuliers. La requête WMI pour identifier de tels systèmes est :

```
select * from Win32_OperatingSystem where Version like "10.%"
```

La requête ci-dessus retourne vrai pour les ordinateurs qui exécutent Windows 10 et Windows Server 2016.

Lorsque le service Client de stratégie de groupe évalue les GPO qu'il a téléchargés pour déterminer ceux qui devraient être remis aux extensions côté client pour le traitement, il exécute la requête sur le système local. Si le système répond aux critères de la requête, le résultat de la requête est Vrai logique, et les extensions côté client traitent le GPO.

WMI expose des espaces de noms, au sein desquels il existe des classes qui peuvent être interrogées. De nombreuses classes utiles, notamment **Win32_OperatingSystem**, se trouvent dans un espace de noms appelé **root\CIMv2**.

Pour créer un filtre WMI :

1. Cliquez avec le bouton droit sur le noeud **Filtres WMI** dans l'arborescence de la console GPMC, puis cliquez sur **Nouveau**. Tapez un nom et une description pour le filtre, puis cliquez sur **Ajouter**.
2. Dans la zone de texte **Espace de noms**, tapez l'espace de noms de votre requête ou cliquez sur **Parcourir** pour sélectionner les espaces de noms disponibles.
3. Dans la zone de texte **Requête**, tapez la requête, puis cliquez sur **OK**.

Pour filtrer un GPO avec un filtre WMI :

1. Sélectionnez le GPO ou le lien GPO dans l'arborescence de la console GPMC.
2. Cliquez sur l'onglet **Étendue**.
3. Dans la liste déroulante **WMI**, sélectionnez le **Filtre WMI**.

Vous pouvez filtrer un GPO avec un seul filtre WMI, mais vous pouvez créer un filtre WMI avec une requête complexe qui utilise plusieurs critères. Vous pouvez lier un seul filtre WMI à un ou plusieurs GPO. L'onglet **Général** d'un filtre WMI affiche les GPO qui utilisent le filtre WMI. Il existe deux mises en garde importantes concernant les filtres WMI :

- Tout d'abord, la syntaxe WQL des requêtes WMI peut être difficile à maîtriser. Vous pouvez souvent trouver des exemples sur Internet lorsque vous effectuez une Research en utilisant les mots-clés **filtre WMI** et **requête WMI** avec une description de la requête que vous souhaitez créer.
- Deuxièmement, les filtres WMI peuvent avoir un impact négatif sur les performances de traitement de stratégie de groupe. Étant donné que le service client de stratégie de groupe doit effectuer la requête WMI à chaque intervalle de traitement de la stratégie, il y a un léger impact sur les performances du système toutes les 90 à 120 minutes. Avec les performances des ordinateurs actuels, l'impact peut ne pas être perceptible. Cependant, vous devez tester les effets d'un filtre WMI avant de le déployer largement dans votre environnement de production. En outre, certaines requêtes WMI sont plus coûteuses en termes de performances de traitement ; une demande portant sur l'espace disque disponible peut prendre plus de temps qu'une demande portant sur la version du système d'exploitation.

 **Remarque :** Une requête WMI est traitée une seule fois, même si vous l'utilisez pour filtrer l'étendue de plusieurs GPO.

Démonstration : Filtrage de l'application de la stratégie de groupe

Dans cette démonstration, vous apprendrez à :

- Créer un GPO et le lier à l'UO **Informatique** ;
- Filtrer l'application de stratégie de groupe en utilisant le filtrage de groupe de sécurité ;
- Filtrer l'application de stratégie de groupe en utilisant le filtrage WMI.

Procédures de démonstration

Créer un GPO et le lier à l'unité d'organisation Service informatique

1. Ouvrez **Console de gestion des stratégies de groupe** sur **LON-DC1**.
2. Créez un GPO nommé **Supprimer le menu Aide** puis liez-le à l'UO **Informatique**.
3. Modifiez les paramètres du GPO pour supprimer l'entrée **Aide** du menu **Démarrer**.

Filtrer l'application de stratégie de groupe en utilisant le filtrage de groupe de sécurité

1. Supprimez l'entrée **Utilisateurs authentifiés** de la liste **Filtrage de sécurité** pour le GPO **Supprimer le menu Aide** dans l'UO **Informatique**.
2. Ajoutez l'utilisateur **Beth Burke** à la liste de filtrage de sécurité. Maintenant, seule Beth Burke possède l'autorisation Appliquer la stratégie.

Filtrer l'application de stratégie de groupe en utilisant le filtrage WMI

1. Créez un filtre WMI nommé **Filtre Version du système**.
2. Ajoutez la demande suivante au filtre :

```
select * from Win32_OperatingSystem where Version like "6.%"
```
3. Enregistrez la requête en tant que **Filtre Version du système**.
4. Créez un GPO nommé **Mises à jour de logiciel** et liez-le à l'UO **Informatique**.
5. Modifiez les propriétés de la stratégie de manière à utiliser le filtre Version du système.
6. Fermez la console de Gestion de stratégie de groupe.

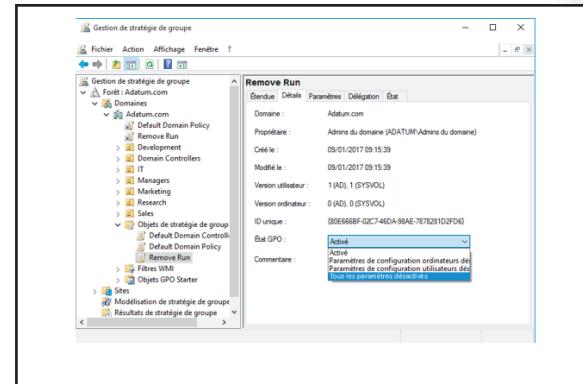
Comment activer ou désactiver les GPO et les nœuds GPO

Vous pouvez empêcher les paramètres dans le nœud **Configuration de l'ordinateur** ou les nœuds **Configuration utilisateur** d'effectuer des traitements lors de l'actualisation de la stratégie en modifiant l'option **État GPO**. Ceci est utile si vous souhaitez optimiser le traitement des GPO ou si vous souhaitez désactiver une partie spécifique d'un GPO pour un dépannage.

Pour activer ou désactiver les nœuds d'un GPO, sélectionnez le GPO ou le lien GPO dans l'arborescence de la console, cliquez sur l'onglet **Informations** (montré dans l'image de la diapositive), puis sélectionnez l'une des options suivantes à partir de la liste déroulante **État GPO** :

- Activé.** Les paramètres de configuration de l'ordinateur et les paramètres de configuration de l'utilisateur seront traités par les extensions côté client lors de l'actualisation de la stratégie.
- Tous les paramètres désactivés.** Les extensions côté client ne traiteront pas le GPO lors l'actualisation de la stratégie.
- Paramètres de configuration ordinateurs désactivés.** Au cours de l'actualisation de la stratégie d'ordinateur, les paramètres de configuration de l'ordinateur dans le GPO ne seront pas appliqués.
- Paramètres de configuration utilisateurs désactivés.** Au cours de l'actualisation de la stratégie d'utilisateur, les paramètres de configuration de l'utilisateur dans le GPO ne seront pas appliqués.

Vous pouvez configurer l'état GPO pour optimiser le traitement de la stratégie. Par exemple, si un GPO contient uniquement des paramètres utilisateur, alors définir l'option **État GPO** de manière à désactiver les paramètres de l'ordinateur empêche le service Client de stratégie de groupe d'essayer de traiter le GPO pendant l'actualisation de la stratégie d'ordinateur. Étant donné que le GPO ne contient aucun paramètre de l'ordinateur, il n'est pas nécessaire de traiter le GPO et vous pouvez économiser quelques cycles de processeur.



Remarque : Vous pouvez définir une configuration qui devrait s'activer en cas d'urgence, d'incident de sécurité, ou autres catastrophes dans un GPO, puis lier le GPO de sorte qu'il est inclus dans l'étendue aux utilisateurs et ordinateurs appropriés. Ensuite, désactivez le GPO. Si vous avez besoin de déployer la configuration, activez le GPO. Vous devriez ensuite utiliser la GPMC pour forcer une actualisation de la stratégie sur tous les ordinateurs.

Traitement d'une stratégie de bouclage

Par défaut, les paramètres d'un utilisateur proviennent de GPO qui sont étendus à l'objet USER dans AD DS. Peu importe l'ordinateur auquel l'utilisateur se connecte, le jeu de stratégies résultant qui détermine l'environnement de l'utilisateur est le même. Cependant, il existe des situations dans lesquelles vous voudrez peut-être configurer certains paramètres de stratégie de groupe qui affectent un utilisateur, en fonction de l'ordinateur qu'il ou elle utilise. Par exemple, vous voudrez peut-être standardiser et verrouiller le Bureau d'utilisateurs lorsqu'ils se connectent à des ordinateurs dans des environnements étroitement gérés, tels que des salles de conférence, des zones d'accueil, des laboratoires, des salles de classe et des kiosques. Ceci est également important pour les scénarios d'infrastructure de bureau virtuel, notamment les machines virtuelles à distance et les Services Bureau à distance.

- Offre la possibilité d'appliquer des paramètres de stratégie de groupe aux utilisateurs en fonction de l'ordinateur auquel l'utilisateur se connecte
- Mode Remplacement :
 - Seule la liste des GPO basés sur l'objet informatique est utilisée
- Mode Fusion :
 - La liste des GPO basés sur l'ordinateur est prioritaire sur la liste des GPO basés sur l'utilisateur
- Utile dans les environnements étroitement gérés et les ordinateurs à usage spécial, tels que :
 - Les serveurs terminaux, les ordinateurs à accès public et les salles de classe



Imaginez un scénario dans lequel vous souhaitez appliquer une apparence d'entreprise standard à l'ensemble des ordinateurs de bureau Windows présents dans les salles de conférence et autres lieux publics de votre bureau. Comment allez-vous gérer cette configuration centralisée à l'aide de la stratégie de groupe ? Les paramètres de stratégie qui permettent de configurer l'apparence du bureau sont situés dans le nœud **Configuration utilisateur** d'un GPO. Par conséquent, par défaut, les paramètres s'appliquent aux utilisateurs, quel que soit l'ordinateur auquel ils se connectent. Le traitement de la stratégie par défaut ne vous permet pas de définir l'étendue des paramètres utilisateur afin de les appliquer aux ordinateurs, quel que soit l'utilisateur qui se connecte. C'est ainsi que le traitement de la stratégie de bouclage peut être utile.

Le traitement de la stratégie de bouclage modifie l'algorithme par défaut utilisé par le service Client de stratégie de groupe utilise pour obtenir la liste ordonnée des GPO qui devraient être appliquées à la configuration d'un utilisateur. Normalement, le nœud **Configuration utilisateur** des GPO étendus à l'objet USER détermine la configuration de l'utilisateur. Lorsque vous activez le traitement de la stratégie de bouclage, le nœud **Configuration utilisateur** des GPO étendus à l'objet Ordinateur détermine la configuration de l'utilisateur.

Comme tous les paramètres de stratégie dans la section **Modèles d'administration** d'un GPO, le paramètre de stratégie **Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur** qui se trouve dans le dossier **Configuration ordinateur\Stratégies\Modèles d'administration\Système\Stratégie de groupe** dans la fenêtre **Éditeur de gestion des stratégies de groupe** peut être défini sur **Non configuré**, **Activé**, ou **Désactivé**.

Lorsqu'elle est activée, la stratégie peut spécifier le mode Remplacer ou Fusionner :

- Remplacer. Ce mode remplace entièrement la liste des GPO pour l'utilisateur par la liste des GPO déjà obtenue pour l'ordinateur au démarrage de celui-ci. Les paramètres dans le nœud **Configuration utilisateur** des GPO de l'ordinateur s'appliquent à l'utilisateur. Le mode Remplacer est utile dans la situation d'une salle de classe, où les utilisateurs doivent recevoir une configuration standard, plutôt que la configuration appliquée aux utilisateurs dans un environnement moins géré.
- Fusionner. Ce mode ajoute la liste des GPO obtenue pour l'ordinateur à au démarrage de celui-ci à la liste des GPO obtenue pour l'utilisateur lors de la connexion. Étant donné que la liste des GPO obtenue pour l'ordinateur s'applique plus tard, les paramètres des GPO dans la liste de l'ordinateur sont prioritaires s'ils entrent en conflit avec les paramètres de la liste de l'utilisateur. Ce mode est utile pour appliquer des paramètres supplémentaires aux configurations typiques des utilisateurs. Par

exemple, vous pouvez permettre à un utilisateur de recevoir sa configuration typique lors de sa connexion à un ordinateur dans une salle de conférence ou une zone d'accueil, mais en remplaçant le fond d'écran avec une image standard et en désactivant l'utilisation de certaines applications ou de certains périphériques.



Remarque : Lorsque vous combinez le traitement de bouclage avec le filtrage de groupe de sécurité, l'application des paramètres utilisateur lors de l'actualisation de la stratégie utilise les informations d'identification de l'ordinateur pour déterminer quels GPO appliquer dans le cadre du traitement de bouclage. Toutefois, l'utilisateur connecté doit également posséder l'autorisation Appliquer la stratégie de groupe pour que le GPO puisse être appliqué correctement. En outre, l'indicateur de traitement de bouclage est configuré sur une base par session, plutôt que par GPO.

Considérations pour des liaisons lentes et systèmes déconnectés

Par défaut, seuls quelques-uns des paramètres que vous pouvez configurer avec la stratégie de groupe s'appliqueront si la vitesse de liaison est trop lente entre l'ordinateur de l'utilisateur et votre réseau avec domaine. Par exemple, le déploiement de logiciels par l'intermédiaire de GPO serait inapproprié sur des liaisons lentes. En outre, il est important de considérer l'effet de la stratégie de groupe sur les ordinateurs qui sont déconnectés du réseau avec domaine.

Liaisons lentes

Le service Client de stratégie de groupe règle la question des liaisons lentes en détectant la vitesse de connexion au domaine et en déterminant si la connexion doit être considérée comme une liaison lente. Chaque extension côté client détermine l'application des paramètres. L'extension du logiciel, par exemple, est configurée pour renoncer au traitement de la stratégie afin que le logiciel ne soit pas installé si une liaison lente est détectée.



Remarque : Par défaut, une liaison est considérée lente si elle est inférieure à 500 kilobits par seconde (Kbits/s). Vous pouvez toutefois attribuer un nombre inférieur à cette valeur.

Si la stratégie de groupe détecte une liaison lente, elle définit un indicateur pour signaler que la liaison avec les extensions côté client est lente. Les extensions côté client peuvent alors détecter si les paramètres de stratégie de groupe applicables doivent être traités. Le tableau suivant décrit le comportement par défaut des extensions côté client.

| Extension côté client | Traitement de liaison lente | Peut-il être modifié ? |
|--|-----------------------------|------------------------|
| Traitement de la stratégie du Registre | Activé | Non |
| Maintenance d e Internet Explorer | Désactivé | Oui |
| Stratégie d'installation de logiciel | Désactivé | Oui |

| Extension côté client | Traitement de liaison lente | Peut-il être modifié ? |
|--|-----------------------------|------------------------|
| Stratégie de redirection de dossier | Désactivé | Oui |
| Stratégie de scripts | Désactivé | Oui |
| Stratégies de sécurité | Activé | Non |
| Stratégie de sécurité du protocole Internet (IPsec) | Désactivé | Oui |
| Stratégie sans fil | Désactivé | Oui |
| Stratégie de récupération du système de fichiers EFS | Activé | Oui |
| Stratégie de quota de disque | Désactivé | Oui |

Ordinateurs déconnectés

Si un utilisateur travaille s'en être déconnecté au réseau, les paramètres appliqués précédemment par la stratégie de groupe restent actifs. De cette façon, l'expérience d'un utilisateur est identique, indépendamment du fait qu'il ou elle soit sur le réseau ou non. Il existe des exceptions à cette règle, notamment les scripts de démarrage, d'arrêt, d'ouverture et de fermeture de session ne seront pas exécutés si l'utilisateur est déconnecté.

Si un utilisateur distant se connecte au réseau, le Client de stratégie de groupe se réveille puis détermine ensuite si l'actualisation de stratégie de groupe a été manquée. Si oui, il exécute une actualisation de la stratégie de groupe pour obtenir les derniers GPO du domaine. Encore une fois, les extensions côté client déterminent si les paramètres de ces GPO ont été appliqués, en fonction de leurs paramètres de traitement de stratégie.

 **Remarque :** Ce processus ne s'applique pas à Windows XP ou Windows Server 2003 ni aux systèmes d'exploitation antérieurs. Il ne s'applique qu'à Windows Vista et supérieur et à Windows 2008 et supérieur.

Identifier le moment où les paramètres entrent en vigueur

Vous devez terminer plusieurs processus avant que les paramètres de stratégie de groupe ne soient appliqués à un utilisateur ou à un ordinateur. Cette rubrique traite ces processus.

La RéPLICATION GPO DOIT SE PRODUIRE

Avant qu'un GPO ne puisse être appliqué, le conteneur de stratégie de groupe dans l'AD DS doit répliquer au contrôleur de domaine à partir duquel le service Client de stratégie de groupe obtient sa liste ordonnée de GPO. En outre, le modèle de stratégie de groupe dans SYSVOL doit répliquer vers le même contrôleur de domaine.

- La RéPLICATION GPO doit se produire
- Les changements de groupe doivent se reproduire
- L'actualisation de la stratégie de groupe doit se produire
- L'utilisateur doit se déconnecter et se connecter ou l'ordinateur doit redémarrer
- Vous devez effectuer une actualisation manuelle
- La plupart des CSE n'appliquent pas de nouveau les paramètres GPO inchangés

Les changements de groupe doivent se reproduire

Si vous avez ajouté un nouveau groupe ou modifié l'appartenance à un groupe utilisé pour filtrer le GPO, cette modification devra également être répliquée. De plus, la modification doit être dans le jeton de sécurité de l'ordinateur et l'utilisateur, ce qui demande un redémarrage de l'ordinateur pour actualiser son appartenance à un groupe ou une connexion et une déconnexion de l'utilisateur afin d'actualiser l'appartenance à un groupe.

L'actualisation de la stratégie de groupe de l'utilisateur ou de l'ordinateur doit se produire

Par défaut, l'actualisation de la stratégie de groupe se produit au démarrage pour les paramètres de l'ordinateur, lors de la connexion pour les paramètres utilisateur et, par la suite, toutes les 90-120 minutes par la suite.



Remarque : Rappelez-vous que l'impact pratique de l'intervalle d'actualisation de la stratégie de groupe a lieu, en moyenne, à la moitié de ce temps ou 45-60 minutes avant que la modification ne soit appliquée à votre environnement.

Par défaut, les clients avec Windows XP, Windows Vista, Windows 7, Windows 8, de Windows 8.1 et Windows 10 ne font que des actualisations d'arrière-plan au démarrage et lors de la connexion, ce qui signifie qu'un client peut démarrer et un utilisateur peut se connecter sans recevoir les dernières stratégies du domaine. Il est fortement recommandé de modifier ce comportement par défaut de sorte à mettre en œuvre les modifications apportées à la stratégie de façon prévisible et contrôlée. Activez le paramètre de la stratégie **Toujours attendre le réseau au démarrage et à l'ouverture de session pour tous les clients Windows**. Le paramètre se trouve sous **Configuration ordinateur\Stratégies\Modèles d'administration\Système\Ouverture de session**. Assurez-vous de lire le texte explicatif du paramètre de stratégie. Cela n'a aucune incidence sur le démarrage ou le temps de connexion pour les ordinateurs qui ne sont pas connectés à un réseau. Si l'ordinateur détecte qu'il est déconnecté, il n'attend un réseau.

L'utilisateur doit se déconnecter puis se connecter ou redémarrer l'ordinateur

Bien que la plupart des paramètres sont appliqués lors d'une actualisation de la stratégie d'arrière-plan, quelques extensions côté client n'appliquent pas le paramètre jusqu'au prochain démarrage ou prochain événement d'ouverture de session. Par exemple, les stratégies de démarrage et script d'ouverture de session récemment ajoutées ne sont pas exécutées jusqu'au prochain démarrage de l'ordinateur ou prochaine ouverture de session. Le logiciel sera installé lors du prochain démarrage s'il est affectés aux paramètres de l'ordinateur. Les modifications apportées aux stratégies Redirection de dossiers ne prendront effet qu'à la prochaine ouverture de session.

Vous devez actualiser manuellement la stratégie de groupe

Lorsque vous essayez de traiter la stratégie de groupe, vous devez lancer une actualisation manuelle de la stratégie de groupe pour ne pas devoir attendre la prochaine actualisation d'arrière-plan. Vous pouvez utiliser la commande **gpupdate** pour lancer une actualisation de la stratégie de groupe. Utilisée seule, cette commande déclenche un traitement identique à une actualisation de stratégie de groupe d'arrière-plan. Aussi bien la stratégie de l'ordinateur comme de l'utilisateur sont actualisées. Utilisez le paramètre **/cible:ordinateur** ou **/cible:utilisateur** pour limiter l'actualisation aux paramètres de l'ordinateur ou de l'utilisateur, respectivement. Par défaut, lors de l'actualisation d'arrière-plan, les paramètres ne sont appliqués que si le GPO a été actualisé. Le commutateur **/forcer** entraîne le système à réappliquer tous les paramètres à tous les GPO appliqués à l'utilisateur ou à l'ordinateur. Certains paramètres de stratégie requièrent une déconnexion ou un redémarrage avant d'être appliqués. Le commutateur **/se déconnecter** et **/démarrer** de **gpupdate** entraîne une déconnexion ou un redémarrage, respectivement. Vous pouvez utiliser ces commutateurs lorsque vous appliquez des paramètres qui requièrent une déconnexion ou un redémarrage.

Par exemple, la commande qui entraînera une actualisation complète de l'application et, au besoin, le redémarrage et la connexion pour appliquer les paramètres de stratégie actualisés est :

```
gpupdate /force /logoff /boot
```

La plupart des extensions côté client ne réappliquent pas les paramètres si le GPO n'a pas été modifié

Rappelez-vous que la plupart des extensions côté client n'appliquent les paramètres d'un GPO que si la version de GPO a été modifiée. Ainsi, si un utilisateur peut modifier un paramètre de stratégie de groupe spécifié au départ, le paramètre ne sera plus en conformité avec les paramètres que le GPO spécifie jusqu'à ce que le GPO soit modifié. Heureusement, la plupart des paramètres de stratégie ne peuvent être modifiés par un utilisateur non administratif. Toutefois, si un utilisateur est un administrateur de son ordinateur, ou si le paramètre de stratégie affecte une partie du registre ou du système dont l'utilisateur est autorisé à modifier, cela pourrait s'avérer être problématique.

Vous avez la possibilité d'instruire chaque extension côté client à réappliquer les paramètres de GPO, même si les GPO n'ont pas été modifiés. Vous pouvez configurer le comportement de traitement de chaque extension côté client dans les paramètres de stratégie sous **Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe**.

Question : Vérifiez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|--|---------|
| Il est possible de relier plus d'un filtre WMI à un GPO. | |

Testez vos connaissances

| Question |
|--|
| Laquelle des options suivantes pouvez-vous configurer dans le GPMC pour changer l'ordre de traitement par défaut de la stratégie de groupe ? (Choisissez toutes les réponses applicables.) |
| Sélectionnez la réponse correcte. |
| Filtres WMI |
| Filtrage de la sécurité |
| Bloquer l'héritage |
| Police |
| Traitement de bouclage |

Atelier pratique A : Implémentation d'une infrastructure de stratégie de groupe

Scénario

Votre gestionnaire vous a demandé d'utiliser la stratégie de groupe pour mettre en œuvre les paramètres de sécurité normalisés afin de verrouiller les écrans d'ordinateur lorsque les utilisateurs laissent des ordinateurs sans surveillance pendant 10 minutes ou plus. Vous devez également configurer un paramètre de stratégie qui permettra d'éviter l'accès à certains programmes sur les ordinateurs locaux.

Vous avez configuré la stratégie de groupe de façon à verrouiller les écrans d'ordinateur lorsque les utilisateurs laissent des ordinateurs sans surveillance pendant 10 minutes ou plus. Cependant, après un certain temps, un ingénieur vous informe qu'une application critique utilisée par l'équipe d'ingénierie de Research avorte lorsque l'écran de veille démarre. Un ingénieur vous a demandé d'empêcher le paramètre de GPO de s'appliquer à tout membre du groupe de sécurité de Research. Il vous a également demandé de configurer les ordinateurs de la salle de conférence de manière à ce qu'ils soient exemptés de la stratégie d'entreprise. Cependant, vous devez vous assurer que les ordinateurs de la salle de conférence utilisent un temps de repos de 2 heures.

Créez les stratégies dont vous avez besoin pour évaluer les RSoP pour les utilisateurs de votre environnement. Assurez-vous d'optimiser l'infrastructure de stratégie de groupe et de vérifier que toutes les stratégies sont appliquées comme prévu.

Objectifs

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

- Créer et configurer des GPO ;
- Gérer l'étendue de GPO.

Configuration de l'atelier pratique

Durée approximative : **40 minutes**

Ordinateurs virtuels. **22742A-LON-DC1**, **22742A-LON-DC2**, **22742A-LON-CL1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**.

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-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 : **Administrateur**
 - Mot de passe : **Pa55w.rd**.
 - Domaine : **Adatum**
5. Répétez les étapes 2 et 4 pour **22742A-LON-DC2**.
6. Répétez les étapes 2 et 3 pour **22742A-LON-CL1**. Ne vous connectez pas à **LON-CL1** tant qu'il ne vous a pas été demandé de le faire.

Exercice 1 : Création et configuration des GPO

Scénario

Votre gestionnaire vous a demandé d'utiliser la stratégie de groupe pour mettre en œuvre les paramètres de sécurité normalisés afin de verrouiller les écrans d'ordinateur lorsque les utilisateurs laissent des ordinateurs sans surveillance pendant 10 minutes ou plus. Elle vous a également demandé de configurer un paramètre de stratégie qui permettra d'éviter l'accès à des outils d'édition de registre sur les ordinateurs locaux.

Les tâches principales de cet exercice sont les suivantes :

1. Créer et modifier un GPO ;
2. Lier le GPO ;
3. Voir les effets des paramètres du GPO.

► Tâche 1 : Créer et modifier un GPO

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, ouvrez la **console de Gestion des stratégies de groupe**.
2. Créez un GPO nommé **Normes ADATUM** dans le conteneur **Objets de Stratégie de groupe**.
3. Modifiez la stratégie **Normes ADATUM**, puis accédez à **Configuration utilisateur\Stratégie\Modèles d'administration\Système**.
4. Empêchez les utilisateurs d'accéder au registre en activant le paramètre de la stratégie **Empêcher l'accès au registre des outils d'édition**.
5. Accédez au dossier **Configuration utilisateur\Stratégies\Modèles d'administration\Panneau de configuration\Personnalisation**, puis configurez la stratégie **Temporisation de l'écran de veille** sur **600 secondes**.
6. Activez le paramètre de la politique **Écran de veille protégé par mot de passe**, puis fermez la fenêtre **Éditeur de gestion de stratégie de groupe**.

► Tâche 2 : Lier le GPO

- Liez le GPO **Normes ADATUM** au domaine **Adatum.com**.

► Tâche 3 : Voir les effets des paramètres du GPO

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Ouvrez le Panneau de configuration. Dans **Pare-feu Windows**, autorisez la **Gestion à distance du journal d'événements** et le trafic **Infrastructure de gestion Windows (WMI)**.
3. Déconnectez-vous, puis connectez-vous en tant que **Adatum\Connie** avec le mot de passe **Pa55w.rd**.
4. Essayez de modifier le temps d'attente de l'écran de veille et reprendre les paramètres. La stratégie de groupe vous empêche de le faire.
5. Essayez d'exécuter **Éditeur du Registre**. La stratégie de groupe vous empêche de le faire.

Résultats : Après avoir terminé cet exercice, vous devriez avoir créé, édité et partagé le GPO requis.

Exercice 2 : Gestion de l'étendue GPO

Scénario

Vous avez utilisé la stratégie de groupe pour mettre en œuvre les paramètres de sécurité normalisés afin de verrouiller les écrans d'ordinateur lorsque les utilisateurs laissent des ordinateurs sans surveillance pendant 10 minutes ou plus. Cependant, après un certain temps, un ingénieur vous informe qu'une application critique utilisée par l'équipe d'ingénierie de Research avorte lorsque l'écran de veille démarre. Il vous a demandé d'empêcher le paramètre GPO de s'appliquer à tout membre du groupe de sécurité de Research. Il vous a également demandé de configurer les ordinateurs de la salle de conférence de manière à ce qu'ils soient exemptés de la stratégie d'entreprise. Cependant, vous devez vous assurer que les ordinateurs des salles de conférence utilisent toujours un temps de repos de 2 heures.

Les tâches principales de cet exercice sont les suivantes :

1. Créer et lier les GPO requis ;
2. Vérifier l'ordre de priorité ;
3. Configurer l'étendue d'un GPO avec filtrage de sécurité ;
4. Configurer le traitement de bouclage ;
5. Pour préparer l'atelier suivant.

► Tâche 1 : Créer et lier les GPO requis

1. Sur **LON-DC1**, dans la **console Gestion de stratégie de groupe**, créez un nouveau GPO nommé **Modification de l'application de Research** lié à l'unité d'organisation **Research**.
2. Configurez le paramètre de stratégie **temporisation de l'écran de veille** sur désactivé, puis fermez la fenêtre **Éditeur de gestion de stratégie de groupe**.

► Tâche 2 : Vérifier l'ordre de priorité

- Dans l'arborescence **Console de gestion de stratégie de groupe**, sélectionnez l'unité d'organisation **Research**, puis cliquez sur l'onglet **Héritage de stratégie de groupe**. Notez que le GPO **Modification de l'application de Research** est prioritaire sur le GPO **NORMES ADATUM**. Le paramètre de stratégie temporisation de l'écran de veille que vous venez de configurer dans le GPO **Modification de l'application de Research** sera appliqué après avoir paramétré le GPO **Normes ADATUM**. Par conséquent, le nouveau réglage remplacera le paramètre de normes et prévaudra. La mise en veille automatique de l'écran ne sera pas disponible pour les utilisateurs dans le cadre du GPO **Modification de l'application de Research**.

► Tâche 3 : Configurer le cadre d'un GPO avec filtrage de sécurité

1. Sur **LON-DC1**, dans la Console de gestion de stratégie de groupe, sélectionnez le GPO **Modification de l'application de Research**. Notez que dans la section **Filtrage de sécurité**, le GPO est appliqué par défaut à tous les utilisateurs authentifiés.
2. Dans la section **Filtrage de sécurité**, retirez **Utilisateurs authentifiés** et ajoutez le groupe **Research**.

► Tâche 4 : Configurer le traitement de bouclage

1. Sur **LON-DC1**, dans la **Console de gestion de stratégie de groupe**, Créez une nouvelle unité d'organisation nommée **Kiosques** sous le domaine.
2. Sous **Kiosques**, créez une unité d'organisation liée nommée **Salles de conférence**.
3. Créez un nouveau GPO nommé **Paramètres de la Salle de conférence**, puis associez-le à l'unité d'organisation **Salles de conférence**.

4. Modifiez le GPO **Paramètres de la Salle de conférence**, puis modifiez la stratégie **Temporisation de l'écran de veille** pour lancer l'écran de veille au bout de 120 minutes.
5. Dans la section **Configuration de l'ordinateur** du GPO, modifiez le paramètre de stratégie **Mode de configuration de traitement de bouclage de la stratégie de groupe utilisateur** de sorte à utiliser le **mode Fusionner**.

Résultats : À la fin de cet exercice, vous devrez avoir configuré les paramètres des objets de stratégie de groupe (GPO).

► **Tâche 5 : Se préparer l'atelier suivant**

- Après avoir terminé cet atelier pratique, laissez tous les ordinateurs virtuels s'exécuter pour l'atelier pratique suivant.

Question : De nombreuses organisations comptent beaucoup sur le filtrage du groupe de sécurité pour étendre les GPO, plutôt que de lier des GPO aux unités d'organisation spécifiques. Dans ces organisations, les GPO sont généralement liés très en amont dans la structure logique Active Directory au domaine lui-même ou à une unité d'organisation de premier niveau. De quels avantages bénéficiiez-vous en utilisant le filtrage de groupe de sécurité plutôt que les liens GPO pour gérer l'étendue d'un GPO ?

Question : Pourquoi peut-il être utile de créer un groupe d'exemption - un groupe qui se voit refuser la permission d'application de la stratégie de groupe - pour chaque GPO créé.

Question : Utilisez-vous le traitement de la stratégie de bouclage dans votre organisation ? Dans quels scénarios et pour quels paramètres de stratégie la stratégie de bouclage peut-elle apporter une valeur ajoutée ?

Leçon 4

Résolution de problèmes de l'application des GPO

Avec l'interaction de plusieurs paramètres dans plusieurs GPO appliqués en utilisant différentes méthodes, l'application de stratégie de groupe peut être complexe à analyser et à comprendre. Par conséquent, vous devez vous équiper afin d'évaluer et résoudre vous-même efficacement la mise en œuvre de stratégie de groupe. Vous devez être en mesure d'identifier les problèmes potentiels avant qu'ils ne surviennent et résoudre des défis imprévus. Les systèmes d'exploitation Windows Server fournissent des outils indispensables pour soutenir la stratégie de groupe. Dans cette leçon, vous allez explorer l'utilisation de ces outils dans les scénarios de résolution proactive et réactive des problèmes et de l'assistance.

Objectifs des leçons

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

- Expliquer comment Appliquer les GPOs ;
- Décrire le Groupe de stratégies résultant (RSOP) ;
- Expliquer comment générer des rapports RSOP ;
- Exécuter une analyse avec l'Assistant Modélisation de stratégie de groupe ;
- Expliquer comment analyser les journaux d'événements de stratégie de groupe ;
- Détecter des problèmes quant à l'intégrité des GPO.

Actualisation des GPO

Les paramètres de configuration de l'ordinateur sont appliqués au démarrage et sont actualisés à intervalles réguliers. Tout script de démarrage est exécuté au démarrage de l'ordinateur. L'intervalle par défaut est de 90 minutes, plus un temps aléatoire entre 0 et 30 minutes, mais cette durée est paramétrable. L'exception à l'intervalle défini se rapporte aux contrôleurs de domaine, dont les paramètres sont actualisés toutes les cinq minutes.

Les paramètres utilisateur sont appliqués lors de la connexion et sont actualisés à intervalles réguliers paramétrables - la valeur par défaut est également de 90 minutes, plus un temps aléatoire entre 0 et 30 minutes. Tout script d'ouverture de session est exécuté lors de la connexion.

- Lorsque vous appliquez des GPO, rappelez-vous que :
 - Les paramètres de l'ordinateur s'appliquent au démarrage
 - Les paramètres utilisateur s'appliquent lors de la connexion
 - Les stratégies sont actualisées à des intervalles réguliers configurables
 - Les paramètres de sécurité sont actualisés au moins toutes les 16 heures
 - Les stratégies sont actualisées manuellement en utilisant :
 - L'utilitaire en ligne de commande **gpupdate**
 - La cmdlet Windows PowerShell **Invoke-gpupdate**
 - Grâce à la fonctionnalité Actualiser la stratégie de groupe à distance, vous pouvez actualiser les stratégies à distance



Remarque : Un certain nombre de paramètres utilisateur requièrent deux connexions avant que l'utilisateur ne voit l'effet sur le GPO. Cela est dû au fait que les utilisateurs qui se connectent sur le même ordinateur utilisent des identifiants en cache pour accélérer les connexions. Cela signifie que même si les paramètres de stratégie sont transmis à l'ordinateur, l'utilisateur est déjà connecté et les paramètres ne seront donc pas appliqués avant la prochaine connexion. Le paramètre **Redirection de dossiers** en est un exemple.

Vous pouvez modifier l'intervalle d'actualisation en configurant un paramètre de stratégie de groupe. Pour les paramètres de l'ordinateur, vous pouvez trouver le paramètre de l'intervalle d'actualisation dans le nœud **Configuration ordinateur\Stratégies\Modèles d'administration\Système\Stratégie de groupe**. Pour les paramètres de l'utilisateur, vous pouvez trouver l'intervalle d'actualisation dans les paramètres correspondants sous **Configuration utilisateur**. Une exception à l'intervalle d'actualisation sont les paramètres de sécurité. La section paramètres de sécurité de stratégie de groupe est actualisée au moins tous les 16 heures, quel que soit l'intervalle défini pour l'actualisation. Ceci ne peut être configuré via la Stratégie de groupe.

Vous pouvez également actualiser la stratégie de groupe manuellement. L'utilitaire de ligne de commande **gpupdate** actualise et fournit de nouvelles configurations de stratégie de groupe et supprime les paramètres qui ne sont plus valables. La commande **gpupdate/force** actualise tous les paramètres de stratégie de groupe. Une nouvelle cmdlet **Invoquer-gpupdate** de Windows PowerShell effectue également la même fonction, mais requiert l'installation du module Active Directory. L'avantage de la cmdlet est que vous pouvez l'utiliser pour actualiser la stratégie de groupe sur d'autres ordinateurs que celui auquel vous êtes connecté en utilisant le paramètre **-Ordinateur**.

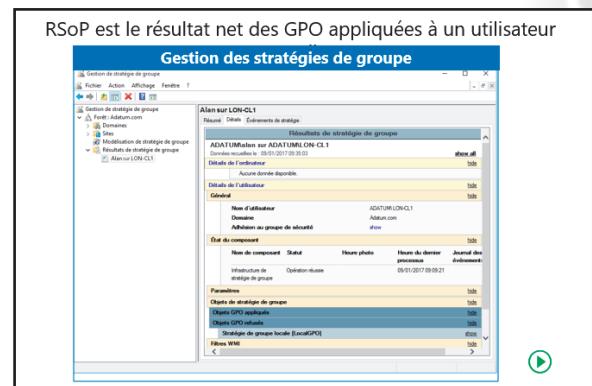
Vous ne pouvez pas pousser les paramètres de stratégie de groupe à un client. Le client tire toujours les paramètres du contrôleur de domaine. Une fonctionnalité introduite dans Windows Server 2012 permet de démarrer à distance une actualisation de stratégie de groupe. Cette fonctionnalité permet aux administrateurs d'utiliser la console GPMC pour cibler une unité d'organisation et forcer l'actualisation d'une stratégie de groupe sur tous ses ordinateurs et utilisateurs actuellement connectés. Pour ce faire, cliquez -avec le bouton droit sur une unité d'organisation, puis cliquez sur **Mise à jour de la stratégie de groupe**. La mise à jour est effectuée en 10 minutes. Une fenêtre de ligne de commande s'ouvrira lorsque le client exécutera l'actualisation.

 **Remarque :** Parfois, l'échec d'un GPO à appliquer est le résultat de problèmes avec la technologie sous-jacente responsable de la réplication AD DS et SYSVOL. Dans Windows Server 2016, vous pouvez afficher l'état de réplication à l'aide de la console GPMC, en sélectionnant le nœud **Domaine**, en cliquant sur l'onglet **Etat**, puis en cliquant sur **Déetecter maintenant**.

Qu'est-ce que le RSOP ?

L'héritage de la stratégie de groupe, les filtres et les exceptions sont complexes et il est souvent difficile de déterminer les paramètres de stratégie qui seront appliqués. Le *Groupe résultant de stratégie* (RSOP) est l'effet net des GPO appliqués à un utilisateur ou à un ordinateur, en tenant compte des liens de GPO, des exceptions telles que Héritage forcé et bloqué, l'application de la sécurité et des filtres WMI, des liens lents et le traitement de bouclage.

Le RSOP est également une collection d'outils qui vous aident à évaluer, à modéliser et à résoudre les problèmes de l'application des paramètres de stratégie de groupe. RSOP peut interroger un ordinateur local ou distant et rapporter les paramètres exacts appliqués à l'ordinateur et à tout utilisateur qui a ouvert une session sur l'ordinateur. RSOP peut également modéliser les paramètres de stratégie dont l'application est prévue pour un utilisateur ou un ordinateur sous plusieurs scénarios, y compris le déplacement de l'objet entre les unités d'organisation ou des sites, ou modifier l'appartenance de l'objet au groupe. Grâce à ces fonctionnalités, RSOP peut vous aider à gérer et à résoudre des problèmes relatifs à des stratégies contradictoires.



Windows Server 2016 fournit les outils suivants pour effectuer une analyse RSoP :

- **Assistant Résultats de stratégie de groupe**
- **Assistant Modélisation de stratégie de groupe**
- **GPResult.exe**

Génération de rapports RSoP

Pour vous aider à analyser l'effet cumulatif des GPO et les paramètres de stratégie sur un utilisateur ou un ordinateur de votre organisation, la GPMC intègre l'**Assistant Résultats de stratégie de groupe**. Si vous voulez comprendre exactement quels paramètres de stratégie s'appliquent à un utilisateur ou à un ordinateur et pourquoi ils ont été appliqués, alors l'**Assistant Résultats de stratégie de groupe** est l'outil à utiliser.

Génération de rapports RSoP avec l'Assistant Résultats de stratégie de groupe

L'**Assistant Résultats de stratégie de groupe** peut atteindre le fournisseur WMI d'un ordinateur local ou distant sous Windows Vista ou systèmes d'exploitation plus récents. Le fournisseur WMI peut signaler tout ce qu'il y a à savoir sur la façon dont la stratégie de groupe a été appliquée au système. Il peut signaler la date du traitement, les GPO qui ont été appliqués, ceux qui ne l'on pas été et pourquoi, les erreurs rencontrées, ainsi que les paramètres exacts de stratégie et les GPO cibles qui prévalent.

Vous trouverez ci-dessous plusieurs exigences de fonctionnement de l'**Assistant Résultats de stratégie de groupe** :

- L'ordinateur cible doit être en ligne.
- Vous devez disposer d'identifiants d'administration sur l'ordinateur cible.
- L'ordinateur cible doit exécuter Windows XP ou un système d'exploitation plus récent.
- Vous devez être en mesure d'accéder à WMI sur l'ordinateur cible. Cela signifie que l'ordinateur doit être en ligne, connecté au réseau et accessible via les portes 135 et 445.



Remarque : Effectuer une analyse RSoP en utilisant l'**Assistant Résultats de stratégie de groupe** est juste un exemple de l'administration à distance. Pour effectuer l'administration à distance, il se peut que vous deviez configurer des règles entrantes pour le pare-feu que vos clients et serveurs utilisent.

- Le service WMI doit être en exécution sur l'ordinateur cible.
- Si vous souhaitez analyser RSoP pour un utilisateur, ce dernier doit s'être connecté au moins une fois à l'ordinateur. Il n'est pas obligatoire que l'utilisateur ait ouvert une session lorsque vous exécutez l'Assistant Résultats de stratégie de groupe.

Une fois que toutes les exigences auront été remplies, vous pourrez exécuter une analyse RSoP. Exécuter un rapport RSoP :

1. Cliquez avec le bouton droit sur **Résultats de la stratégie de groupe** dans l'arborescence **Console de gestion de stratégie de groupe**, puis cliquez sur **Assistant Résultats de stratégie de groupe**.
2. L'**Assistant Résultats de stratégie de groupe** vous invite à sélectionner un ordinateur. Il se connecte alors au fournisseur WMI sur cet ordinateur et fournit une liste des utilisateurs qui y sont connectés. Vous pouvez ensuite sélectionner l'un des utilisateurs ou ignorer l'analyse RSOP pour les stratégies de configuration de l'utilisateur.
3. L'**Assistant Résultats de stratégie de groupe** produit un rapport RSOP détaillé au format HTML dynamique. Si la **Configuration de sécurité renforcée** de Microsoft Internet Explorer est configurée, vous serez invité à autoriser la console à afficher le contenu dynamique. Vous pouvez agrandir ou réduire chaque section du rapport en cliquant sur les liens **Afficher** ou **Masquer** ou en double-cliquant sur le titre de la section. Le rapport est affiché sur trois onglets :
 - o **Résumé**. L'onglet **Résumé** affiche l'état du traitement de la stratégie de groupe lors de la dernière actualisation. Vous pouvez identifier les informations recueillies sur le système, les GPO qui ont été appliqués et refusés, l'appartenance à un groupe de sécurité qui pourrait avoir affecté les GPO filtrés avec des groupes de sécurité, les filtres WMI analysés et le statut des extensions côté client.
 - o **Paramètres**. L'onglet **Paramètres** affiche les paramètres RSOP appliqués à l'ordinateur ou à l'utilisateur. Cet onglet vous montre exactement les paramètres appliqués à l'utilisateur et/ou à l'ordinateur via les effets de la mise en œuvre de votre stratégie de groupe. Vous pouvez accéder à une grande quantité d'informations à partir de l'onglet **Paramètres**, bien que certaines données ne sont pas rapportées, y compris l'IPsec, sans fil et les paramètres de stratégie de quota de disque.
 - o **Événements de stratégie**. L'onglet **Événements de stratégie** affiche les événements de stratégie de groupe à partir des journaux d'événements de l'ordinateur cible.
4. Une fois que vous aurez généré un rapport RSOP avec l'**Assistant Résultats de stratégie de groupe**, cliquez avec le bouton droit sur le rapport pour relancer la requête, imprimer le rapport, ou enregistrer le rapport sous forme de fichier XML ou HTML maintenant les sections dynamiques d'agrandissement et de réduction. Vous pouvez ouvrir les deux types de fichiers avec Internet Explorer, de sorte que le rapport RSOP puisse être porté en dehors de la GPMC.

Si vous cliquez avec le bouton droit sur le nœud du rapport lui-même, sous le nœud **Résultats de la stratégie de groupe** dans l'arborescence de la console, vous pouvez passer à **Vue avancée**. Dans **Vue avancée**, le RSOP s'affiche en utilisant le composant logiciel enfichable RSOP, qui montre tous les paramètres appliqués, y compris les stratégies IPsec, sans fil et de quota de disque.

Génération de rapports RSOP en utilisant GPResult.exe

La commande **GPResult.exe** est la version de la ligne de commande de l'**Assistant de résultats de la stratégie de groupe**. **GPResult** utilise le même fournisseur WMI que l'assistant et produit les mêmes informations. Vous pouvez même l'utiliser pour créer les mêmes rapports graphiques. **GPResult** fonctionne sur Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 et Windows Server 2016.

Lorsque vous exécutez la commande **GPResult**, vous êtes susceptible d'utiliser les options suivantes. Chaque option est suivie de sa description.

```
/s computername
```

Cette option spécifie le nom ou l'adresse IP d'un système distant. Si vous utilisez un point (.) pour le nom de l'ordinateur ou si vous n'incluez pas l'option **/s**, l'analyse RSOP est effectuée sur l'ordinateur local.

```
/scope [user | computer]
```

Cela affiche l'analyse RSOP pour les paramètres utilisateur ou ordinateur. Si vous omettez l'option **/étendue**, l'analyse RSOP inclut à la fois les paramètres utilisateur et ordinateur.

```
/user username
```

Ceci spécifie le nom de l'utilisateur pour lequel vous souhaitez afficher des données RSOP.

```
/r
```

Cette option affiche un résumé des données RSOP.

```
/v
```

Cette option affiche les données RSOP en clair, qui présente les informations les plus utiles.

```
/z
```

Ceci affiche des données en clair supplémentaires, y compris les détails de tous les paramètres de stratégie appliqués au système. Souvent, vous obtiendrez plus d'informations que nécessaire pour la résolution des problèmes typiques liés à la stratégie de groupe.

```
/u domain\user/p password
```

Ceci permet d'obtenir des informations d'identification qui sont dans le groupe Administrateurs d'un système distant. Sans ces identifiants, **GPResult** est exécuté en utilisant les informations d'identification que vous aurez utilisées pour vous connecter.

```
[/x | /h] filename
```

Cette option permet d'enregistrer les rapports au format XML ou HTML.

Résolution des problèmes de stratégie de groupe avec l'Assistant de résultats de la stratégie de groupe ou GPResult.exe

En tant qu'administrateur, vous rencontrerez probablement des scénarios qui demandent la résolution des problèmes de stratégie de groupe. Il se peut que vous deviez diagnostiquer et résoudre des problèmes, y compris :

- Les GPO ne sont pas du tout appliqués.
- Les RSOP pour un ordinateur ou un utilisateur ne sont ceux qui étaient attendus.

L'**Assistant de résultats de la stratégie de groupe** et **GPResult.exe** donneront souvent un aperçu utile du traitement et des problèmes d'application de la stratégie de groupe. Rappelez-vous que ces outils examinent le fournisseur WMI RSOP pour signaler exactement ce qui s'est produit sur un système. Examiner souvent le rapport RSOP vous indiquera les GPO dont l'étendue est incorrecte ou les erreurs de traitement de stratégie qui ont empêché l'application des paramètres de GPO.

Utilisation de Windows PowerShell pour gérer les rapports RSOP

Vous pouvez également utiliser Windows PowerShell pour gérer les RSOP. Utilisez la cmdlet

Get-GPResultantSetofPolicy pour générer des rapports RSOP. Par exemple, la commande suivante génère un rapport pour l'ordinateur spécifié (**Adatum.com\LON-CL1**) et l'utilisateur (Alan) au format HTML et l'enregistre dans le fichier spécifié :

```
Get-GPResultantSetOfPolicy -user Alan -computer Adatum\LON-CL1 -reporttype html -path c:\Report.html
```

Démonstration : Exécution d'une analyse par simulation avec l'Assistant Modélisation de stratégie de groupe

Si vous déplacez un ordinateur ou un utilisateur entre les sites, les domaines ou les OU, ou si vous modifiez leur appartenance à un groupe de sécurité, les GPO appliqués à cet utilisateur ou ordinateur seront alors souvent modifiés. Par conséquent, le RSoP de l'ordinateur ou de l'utilisateur sera différent. Le RSoP sera également modifié si un lien ou un traitement de bouclage lent se produit, ou en cas de modification d'une caractéristique du système ciblée par un filtre WMI.

Avant d'apporter l'une de ces modifications, vous devez évaluer leur impact potentiel sur le RSoP. Vous pouvez utiliser l'**Assistant de résultats de la stratégie de groupe** pour effectuer une analyse RSoP uniquement sur ce qui s'est réellement produit. Pour prédire l'avenir et effectuer des analyses de simulation, vous pouvez utiliser l'**Assistant Modélisation de stratégie de groupe**. Pour effectuer la modélisation de stratégie de groupe, cliquez avec le bouton droit sur le noeud **Modélisation de stratégie de groupe** dans l'arborescence **Console de gestion de stratégie de groupe**, cliquez sur **Assistant Modélisation de stratégie de groupe**, puis parcourez les pages de l'assistant pour modéliser l'analyse de simulation.

La modélisation est effectuée en procédant à une simulation sur un contrôleur de domaine ; ainsi, l'assistant vous demande d'abord de sélectionner un contrôleur de domaine. Vous n'avez pas besoin d'être connecté localement au contrôleur de domaine. Toutefois, la demande de modélisation sera effectuée sur le contrôleur de domaine. Ensuite, l'assistant vous demande de spécifier les paramètres pour la simulation. Vous devez :

- Sélectionner un utilisateur ou un objet ordinateur pour évaluer ou spécifier l'UO, le site ou le domaine à évaluer ;
- Choisir si un traitement lent de lien doit être simulé ;
- Indiquer si vous souhaitez simuler le traitement de bouclage et, si oui, choisissez le mode Remplacer ou Fusionner ;
- Sélectionner un site pour simuler ;
- Sélectionner les groupes de sécurité pour l'utilisateur et l'ordinateur ;
- Choisir le filtre WMI à appliquer dans la simulation du traitement de stratégie de l'utilisateur et de l'ordinateur.

Lorsque vous avez spécifié les paramètres de la simulation, l'assistant produit un rapport très similaire à celui de l'**Assistant de résultats de la stratégie de groupe** mentionné précédemment. L'onglet **Résumé** affiche un aperçu des GPO qui seront traités et l'onglet **Paramètres** détaille les paramètres de stratégie qui seront appliqués à l'utilisateur ou à l'ordinateur. Vous pouvez également enregistrer ce rapport en cliquant avec le bouton droit dessus, puis en cliquant sur **Enregistrer le rapport**.

Démonstration

Dans cette démonstration, vous apprendrez à :

- Utiliser **GPResult.exe** pour créer un rapport ;
- Utiliser l'**Assistant de rapports de stratégie de groupe** pour créer un rapport ;
- Utiliser l'**Assistant Modélisation de stratégie de groupe** pour créer un rapport.

Procédures de démonstration

Utiliser GPResult.exe pour créer un rapport

1. Sur **LON-DC1**, ouvrez une fenêtre **Invite de commandes**.
2. Exécutez les deux commandes suivantes :

```
Gpresult /r
Gpresult /h results.html
```

- Ouvrez le rapport **Results.html** dans Internet Explorer, puis examinez le rapport.

Utiliser l'Assistant de rapports de stratégie de groupe pour créer un rapport

- Fermez la **Invite de commandes**, puis ouvrez la **Console de gestion de stratégie de groupe**.
- À partir du nœud **Résultats de la stratégie de groupe**, ouvrez l'**Assistant de résultats de la stratégie de groupe**.
- Suivez toutes les instructions de l'Assistant en utilisant les paramètres par défaut.
- Examinez le rapport, puis enregistrez-le sur le bureau.

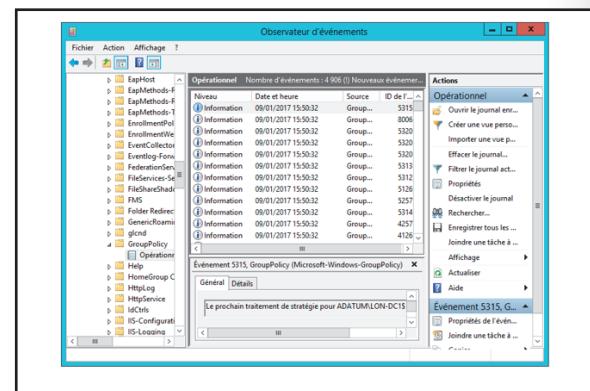
Utiliser l'Assistant Modélisation de stratégie de groupe pour créer un rapport

- À partir du nœud **Modélisation de stratégie de groupe**, ouvrez l'**Assistant Modélisation de stratégie de groupe**.
- Spécifiez l'utilisateur pour le rapport comme **Beth Burke** et le conteneur de l'ordinateur comme **IT OU**.
- Suivez toutes les instructions de l'Assistant en utilisant les paramètres par défaut, puis examinez le rapport.
- Fermez la console de Gestion de stratégie de groupe.

Examen des journaux d'événements de stratégie de groupe

Windows Vista et les versions ultérieures et Windows 2008 et supérieur améliorent votre capacité à résoudre les problèmes de stratégie de groupe, non seulement avec des outils RSoP, mais aussi grâce à une journalisation améliorée des événements de stratégie de groupe. Les journaux d'événements de stratégie de groupe comprennent :

- Journal système. Vous pouvez trouver des informations de haut niveau sur la stratégie de groupe, y compris les erreurs créées par le service Client de stratégie de groupe quand il ne peut pas se connecter à un contrôleur de domaine ou localiser les GPO.
- Journal des applications. Vous pouvez capturer les événements enregistrés par des extensions côté client.
- Journal des opérations de stratégie de groupe. Ce journal fournit des informations détaillées sur le traitement de stratégie de groupe.



Pour trouver les journaux de stratégie de groupe, ouvrez le composant logiciel enfichable **Observateur d'événements** ou la console. Les journaux des applications du Système sont dans le nœud **Journaux de Windows**. Le journal des opérations de stratégie de groupe se trouve dans

Journaux des applications et services\Microsoft\Windows\Stratégie de groupe\Opérations.

Vous pouvez télécharger l'outil de visualisation du journal de stratégie de groupe pour créer un fichier HTML contenant tous les événements relatifs à une actualisation de la stratégie de groupe.



Lectures supplémentaires : Pour télécharger le journal de stratégie de groupe, aller à : <http://aka.ms/E8oi7g>

Déetecter les problèmes d'intégrité de stratégie de groupe

L'infrastructure de stratégie de groupe doit fonctionner de manière optimale pour que vous puissiez appliquer correctement les paramètres de stratégie aux ordinateurs et aux utilisateurs. Dans les très grandes entreprises avec des milliers de GPO répartis sur plusieurs sites et fuseaux horaires, il pourrait y avoir un retard considérable de réPLICATION entre les contrôleurs de domaine.

Un décalage dans les numéros de version entre le conteneur de stratégie de groupe et le modèle de stratégie de groupe d'un GPO pourrait indiquer un problème avec la stratégie de groupe. Dans la Console de gestion de stratégie de groupe, vous pouvez créer un rapport affichant l'état d'intégrité global de l'infrastructure de stratégie de groupe pour un domaine. Vous pouvez également afficher l'état d'intégrité d'un seul GPO.

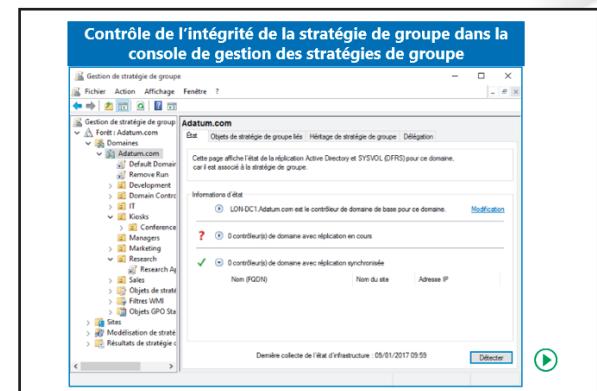
L'onglet Etat sur le domaine de la Console de gestion de stratégie de groupe peut afficher des informations indiquant l'état d'intégrité de l'infrastructure de stratégie de groupe. Les informations affichées sur l'onglet contiennent des informations sur les contrôleurs de domaine, la réPLICATION GPO et le suivi des versions GPO. L'état d'intégrité vous aide à trouver des irrégularités.

Vous pouvez effectuer une analyse de l'intégrité de l'ensemble du domaine ou d'un seul GPO. Effectuez la tâche depuis l'onglet Etat sur le domaine ou GPO sélectionné en cliquant sur **DéTECTER maintenant**. Choisissez le contrôleur de domaine que vous souhaitez sélectionner comme ligne de base. La console de gestion de stratégie de groupe compare ensuite le conteneur de stratégie de groupe et le modèle de stratégie de groupe de tous les contrôleurs de domaine dans le domaine sélectionné avec le contrôleur de domaine de la ligne de base.

L'analyse effectue les comparaisons suivantes :

- Autorisations pour chaque conteneur de stratégie de groupe ;
- Le numéro de version pour chaque modèle de stratégie de groupe ;
- Le nombre d'objets du conteneur de stratégie de groupe ;
- Les autorisations sur chaque modèle de stratégie de groupe ;
- Le numéro de version stocké pour chaque conteneur de stratégie de groupe ;
- Le nombre de dossiers et de fichiers de modèle de stratégie de groupe ;
- Les informations de hachage pour chaque fichier dans tous les modèles de stratégie de groupe.

Si la Console de gestion de stratégie de groupe ne peut pas communiquer avec un contrôleur de domaine lors de l'analyse, ou si un contrôleur de domaine n'est pas compatible avec le contrôleur de domaine utilisé comme ligne de base, la Console de gestion de stratégie de groupe ajoute alors le contrôleur de domaine analysé à la liste **Contrôleur(s) de domaine avec réPLICATION en cours**.



Atelier pratique B : Dépannage de l'infrastructure de stratégie de groupe

Scénario

Après avoir configuré les paramètres pour le département de la Research et de l'informatique dans les salles de conférence, vous voulez vous assurer que tous les paramètres s'appliquent comme prévu. Vous voulez faire cela en créant des rapports à la fois à partir de la console Group Policy Management et à partir d'un client. Vous n'avez pas accès à un ordinateur dans les salles de conférence ; vous devez donc simuler la façon dont les paramètres seront appliqués à l'aide d'analyses de modélisation de stratégie de groupe. Vous voulez enquêter sur les événements qui sont stockés dans l'Observateur d'événements concernant la stratégie de groupe. Vous avez entendu parler d'une fonctionnalité qui peut découvrir des erreurs dans l'infrastructure de stratégie de groupe et vous voulez vous assurer que les deux contrôleurs de domaine ont les mêmes informations concernant la stratégie de groupe.

Après un certain temps, vous recevez un billet Help desk ouvert par un utilisateur. Le problème est que les paramètres de l'économiseur d'écran qui ont été appliqués ne sont pas les bons paramètres pour l'utilisateur. Vous devez enquêter sur la question et vous assurer que les bons paramètres sont applicables à l'utilisateur.

Objectifs

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

- Vérifier l'application GPO ;
- Dépannage des GPO.

Configuration de l'atelier pratique

Durée approximative : **40 minutes**

Ordinateurs virtuels. **22742A-LON-DC1**, **22742A-LON-DC2**, **22742A-LON-CL1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd.**

Pour cet atelier pratique, vous utiliserez l'environnement d'ordinateur virtuel disponible. Avant de commencer l'atelier, vous devez remplir le Lab A. En outre, assurez-vous que les machines virtuelles suivantes sont en exécution. Pour créer un ordinateur virtuel, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-LON-DC1** et dans le volet **Actions**, cliquez sur **Démarrer**.
3. Dans le volet d'**Actions**, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
 - Nom d'utilisateur : **Administrateur**
 - Mot de passe : **Pa55w.rd.**
 - Domaine : **Adatum**
5. Répétez les étapes 2 et 4 pour **22742A-LON-DC2**.
6. Répétez les étapes 2 et 3 pour **22742A-LON-CL1**. Ne vous connectez pas à **LON-CL1** tant qu'il ne vous a pas été demandé de le faire.

Exercice 1 : Vérification de l'application GPO

Scénario

Après avoir configuré les paramètres pour le département de la Research et de l'informatique dans les salles de conférence, afin de vous assurer que tous les paramètres sont applicables comme prévu, vous devez créer des rapports RSOP à la fois à partir de la console Group Policy Management et d'un client. Vous n'avez pas accès à un ordinateur dans les salles de conférence ; vous devez donc simuler la façon dont les paramètres seront appliqués à l'aide d'analyses de modélisation de stratégie de groupe. Vous devez également enquêter sur les événements concernant la stratégie de groupe qui sont stockés dans l'Observateur d'événements.

Les tâches principales de cet exercice sont les suivantes :

1. Effectuer une analyse RSOP
2. Analyser RSOP avec GPResult
3. Évaluez les résultats GPO en utilisant l'Assistant Modélisation de stratégie de groupe
4. Examinez les événements de stratégie et déterminez l'état de l'infrastructure GPO

► Tâche 1 : Effectuer une analyse RSOP

1. Sur **LON-CL1**, vérifiez que vous êtes toujours connecté en tant qu'**Adatum\Connie**. Si nécessaire, utilisez le mot de passe **Pa55w.rd**.
2. Ouvrez une invite de commandes
3. Exécutez la commande **gpupdate/force**
4. Une fois la commande terminée, notez l'heure actuelle du système ; vous en aurez besoin pour une tâche ultérieure dans cet atelier :

Time

5. Redémarrez **LON-CL1**, puis attendez le redémarrage avant de procéder à la tâche suivante.
6. Sur **LON-DC1**, basculez vers **Console de gestion stratégie de groupe**.
7. Utilisez **Assistant des résultats de la stratégie de groupe** pour exécuter un rapport RSOP pour Connie sur **LON-CL1**.
8. Vérifiez les résultats. Pour configurer l'utilisateur et l'ordinateur, identifiez le moment de la dernière mise à jour de la stratégie et la liste des GPO autorisés et refusés. Identifier les composants utilisés pour traiter les paramètres de stratégie.
9. Cliquez sur l'onglet **Détails**. Vérifiez les paramètres qui ont été appliqués au cours de l'exécution de la stratégie de l'ordinateur et de l'utilisateur, puis identifiez le GPO à partir duquel les paramètres ont été obtenus.
10. Cliquez sur l'onglet **Événements de stratégie**, puis localisez l'événement qui enregistre l'actualisation de la stratégie que vous avez déclenché avec la commande **gpupdate**.
11. Cliquez sur l'onglet **Résumé**, cliquez avec le bouton droit sur la page, puis choisissez **Enregistrer le rapport**. Enregistrez le rapport RSOP en fichier HTML sur votre bureau. Ensuite, ouvrez le rapport RSOP dans Internet Explorer à partir du bureau.

► Tâche 2 : Analyser RSoP avec GPResult

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Miranda** avec le mot de passe **Pa55w.rd**.
2. À l'invite de commandes, exécutez la commande **gpresult /r**. Les résultats du résumé RSoP s'affichent. L'information est très similaire à l'onglet **Résumé** du rapport RSoP produit par l'**Assistant de résultats de la stratégie de groupe**.
3. À l'invite de commandes, saisissez **gpresult /v | more**, puis appuyez sur Entrée. Un rapport RSoP plus détaillé est produit. Notez que la plupart des paramètres de stratégie de groupe qui ont été appliqués par le client sont énumérés dans le présent rapport.
4. À l'invite de commandes, saisissez **gpresult /z | more**, puis appuyez sur Entrée. Le rapport RSoP le plus détaillé est produit.
5. À l'invite de commandes, saisissez **gpresult /h:"%userprofile%\Desktop\RSOP.html"**, puis appuyez sur Entrée. Un rapport RSoP est enregistré en fichier HTML sur votre bureau.
6. Ouvrez le rapport RSoP enregistré depuis votre bureau. Comparez le rapport, ses informations et sa mise en forme avec le rapport RSoP que vous avez enregistré dans la tâche précédente.
7. Déconnectez-vous de **LON-CL1**.

► Tâche 3 : Évaluer les résultats GPO en utilisant l'Assistant Modélisation de stratégie de groupe

1. Sur **LON-DC1**, dans **Console de gestion de stratégie de groupe**, ouvrez l'**Assistant Modélisation de stratégie de groupe**.
2. Sélectionnez **Adatum\Connie** comme l'utilisateur et **LON-CL1** comme ordinateur pour la modélisation.
3. À l'invite, activez la case **Traitements en boucle** puis cliquez sur **Fusionner**. Même si le GPO **Paramètres Salle de conférence** spécifie le traitement de bouclage, vous devez demander à l'**Assistant Modélisation de stratégie de groupe** d'inclure le traitement de bouclage dans sa simulation.
4. À l'invite, sur la page **Autres chemins de répertoires actifs**, sélectionnez l'emplacement **Salles de conférence**. Vous simulez l'effet de **LON-CL1** comme ordinateur de salle de conférence.
5. Accepter toutes les autres options comme valeurs par défaut.
6. Dans l'onglet **Résumé**, faites défiler jusqu'à et ci-besoin développez **Détails de l'utilisateur**, puis **Objets de stratégie de groupe**, puis **Objets de stratégie de groupe appliqués**.
7. Vérifiez si l'objet de stratégie de groupe des **Paramètres de salle de conférence** s'applique à Connie comme stratégie de l'utilisateur quand elle se connecte à **LON-CL1**, si **LON-CL1** se trouve dans l'UO **Salles de conférence**.
8. Faites défiler jusqu'à et ci-besoin développez **Détails\Stratégies\Modèles d'administration\Panneau de configuration\Personnalisation de l'utilisateur**.
9. Vérifiez que le délai d'attente de l'économiseur d'écran est de 7200 secondes (2 heures), le paramètre configuré par le GPO **Paramètres Salle de conférence** qui remplace la norme 10 minutes configurée par le GPO **Normes ADATUM**.

► **Tâche 4 : Examiner les événements de stratégie et déterminer l'état de l'infrastructure GPO**

1. Basculez vers **LON-CL1**. Connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Ouvrez l'Observateur d'événements.
3. Allez sur le journal **Système** sous **Journaux Windows** et triez les événements par la colonne **Source**.
4. Localisez l'événement **1500, 1501, 1502** ou **1503** avec la stratégie de groupe comme source et examinez les informations associées aux événements de stratégie de groupe.
5. Dans l'arborescence de la console, allez sur le journal **Opérationnel** sous **Journaux des applications et services\Microsoft\Windows\Stratégie de groupe**.
6. Localisez le premier événement lié à l'actualisation de la stratégie de groupe que vous avez lancée lors de la première opération avec la commande **gpupdate**. Examinez cet événement et les événements qui ont suivi.
7. Déconnectez-vous de **LON-CL1**.
8. Basculez vers **LON-DC1**.
9. Dans la fenêtre **Gestion de la stratégie de groupe**, vérifiez l'état de la stratégie de groupe pour le domaine.
10. Notez que **LON-DC1.Adatum.com** est répertorié comme contrôleur de domaine de référence et vérifiez si **LON-DC2.Adatum.com** l'est comme contrôleur de domaine avec réplication synchronisée. Certains stagiaires pourraient voir **LON-DC2.Adatum.com** répertorié comme contrôleur de domaine avec réplication en cours. Ceci est dû à l'environnement de laboratoire.

Résultats : Après avoir terminé cette opération, vous devriez avoir utilisé les outils RSOP avec succès pour vérifier l'application correcte de vos GPO, examiné les événements de stratégie de groupe et vérifié l'intégrité de l'infrastructure de stratégie de groupe.

Exercice 2 : Dépannage des GPO

Scénario

Un utilisateur a ouvert un ticket d'aide parce que les paramètres économiseur d'écran ne sont pas applicables comme prévu. Vous devez enquêter sur la question et vous assurer que les bons paramètres sont applicables à l'utilisateur.

Vous devez résoudre le problème d'application GPO rapporté que le personnel d'assistance de niveau 1 n'a pas pu résoudre.

| Enregistrement d'incident | |
|--|---------------|
| Numéro de référence de l'incident : 604531 | |
| Date de l'appel | 15 juillet |
| Durée de l'appel | 10:02 |
| Utilisateur | Connie Vaughn |
| Etat | OUVERT |

| Enregistrement d'incident |
|---|
| Détails de l'incident Un utilisateur signale que la configuration de la Research ne s'applique plus à lui. |
| Informations supplémentaires Un utilisateur rapporte que soudain, il a une durée fixe de 10 minutes avant que son économiseur d'écran est activé. En raison d'une demande que le Département de Research utilise, il est incapable de terminer son travail. |
| Plan d'action |
| Résolution |

Les tâches principales de cet exercice sont les suivantes :

1. Lire l'enregistrement d'incident du Help desk et simuler le problème ;
2. Mettre à jour le Plan d'action de l'enregistrement d'incident ;
3. Dépanner et résoudre le problème ;
4. Préparer le module suivant.

► **Tâche 1 : Lire l'enregistrement d'incident du Help desk et simuler le problème**

1. Lisez l'enregistrement d'incident du Help desk **604531** dans le scénario d'exercice.
2. Sur **LON-DC1**, exécutez le script Windows PowerShell **E:\Labfiles\Mod05\Mod05-1.ps1**.

► **Tâche 2 : Mettre à jour la section Plan d'action de l'enregistrement d'incident**

1. Lisez la section **Informations supplémentaires** de l'enregistrement d'incident ci-dessus.
2. Mettez à jour la section **Plan d'action** de l'enregistrement d'incident ci-dessus avec vos recommandations.

► **Tâche 3 : Dépanner et résoudre le problème**

1. Sur **LON-CL1**, connectez-vous en tant qu'**Adatum\Connie** avec le mot de passe **Pa55w.rd**.
2. Ouvrez le **Panneau de configuration**.
3. Dans le Panneau de configuration, cliquez sur **Changer l'économiseur d'écran**.
4. Vérifiez que **Attendre** est grisée et a une valeur de **10 minutes**.
5. Déconnectez-vous de **LON-CL1**.
6. Essayez de résoudre le problème à l'aide de vos connaissances des objets de stratégie de groupe Windows Server et des outils disponibles pour leur dépannage.
7. Mettre à jour la section Résolution de l'enregistrement d'incident.
8. Si vous ne pouvez pas résoudre le problème, demandez de l'aide à votre instructeur.



Remarque : Vous avez résolu le problème à partir du moment où l'économiseur d'écran de Connie Vaughn n'est pas verrouillé à 10 minutes.

Résultats : À la fin de cet exercice, vous aurez résolu le problème d'application GPO.

► Tâche 4 : Préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 à 3 pour **22742A-LON-CL1** et **22742A-LON-DC2**.

Question : Dans quelles situations avez-vous utilisé les rapports RSoP pour résoudre l'application de stratégie de groupe dans votre organisation ?

Question : Dans quelles situations avez-vous utilisé la modélisation de stratégie de groupe ? Si vous ne l'avez pas encore fait, dans quelles situations pouvez-vous envisager l'utilisation de la modélisation de stratégie de groupe ?

Révision du module et Takeaways

Questions de contrôle des acquis

Question : Vous avez affecté un script de connexion à une unité d'organisation via la stratégie de groupe. Le script se trouve dans un dossier réseau partagé nommé **Scripts**. Certains utilisateurs de l'unité reçoivent le script et d'autres non. Quelles sont les causes potentielles ?

Question : Quels sont les paramètres GPO appliqués à l'ensemble des liaisons lentes par défaut ?

Question : Vous devez vous assurer qu'une politique niveau domaine est appliquée, mais le groupe des gestionnaires doit être exemptés de la politique. Comment voulez-vous y parvenir ?

Problèmes courants et conseils de dépannage

| Problème courant | Conseil pour la résolution du problème |
|---|--|
| Les paramètres de stratégie de groupe ne sont pas appliquées à tous les utilisateurs ou les ordinateurs dans une unité d'organisation où un GPO est appliqué. | |
| Les paramètres de stratégie de groupe nécessitent parfois deux redémarrages pour s'appliquer. | |

Module 6

Gestion des paramètres de l'utilisateur avec la stratégie de groupe

Sommaire :

| | |
|---|------|
| Vue d'ensemble du module | 6-1 |
| Leçon 1 : Mise en œuvre des modèles d'administration | 6-2 |
| Leçon 2 : Configuration de la redirection de dossiers, de l'installation de logiciel et des scripts | 6-12 |
| Leçon 3 : Configuration des préférences de stratégie de groupe | 6-22 |
| Atelier pratique : Gestion des paramètres de l'utilisateur avec la stratégie de groupe | 6-29 |
| Révision du module et éléments à retenir | 6-38 |

Vue d'ensemble du module

En utilisant des objets de stratégie de groupe (GPO), vous pouvez mettre en place des environnements de bureau standard dans votre organisation avec des modèles d'administration, la redirection de dossiers, des préférences de stratégie de groupe et l'installation de logiciels. Il est important que vous sachiez comment utiliser ces fonctionnalités de stratégie de groupe pour pouvoir configurer correctement les ordinateurs de vos utilisateurs.

Dans ce module, vous apprendrez tout sur les modèles d'administration et la manière de les utiliser pour configurer les paramètres. Vous apprendrez également à configurer la fonctionnalité de redirection de dossiers ainsi qu'à utiliser les GPO pour gérer les logiciels et appliquer et configurer des scripts. Ce module couvre également les différentes préférences de stratégie de groupe et explique comment vous pouvez les utiliser pour gérer les paramètres.

Objectifs

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

- Mettre en œuvre des modèles d'administration
- Configurer la redirection de dossiers, l'installation de logiciels et les scripts
- Configurer les préférences de stratégie de groupe.

Leçon 1

Mise en œuvre des modèles d'administration

Les fichiers de modèle d'administration fournissent la majorité des paramètres GPO disponibles, qui modifient des clés spécifiques du registre. L'utilisation de modèles d'administration est appelée *stratégie basée sur le registre*, car tous les paramètres configurés dans les modèles d'administration entraînent des modifications dans le registre. Pour de nombreuses applications, l'utilisation d'une stratégie axée sur le registre est le moyen le plus simple et le plus efficace pour aider à la gestion centralisée des paramètres de stratégie. Dans cette leçon, vous apprendrez à configurer des modèles d'administration.

Objectifs de la leçon

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

- Mettre en œuvre des modèles d'administration
- Décrire les fichiers .adm et .admx
- Décrire le magasin central
- Décrire les utilisations pratiques des modèles d'administration
- Configurer les paramètres avec les modèles d'administration
- Expliquer comment importer des modèles de sécurité
- Expliquer comment gérer les modèles d'administration.

Que sont les modèles d'administration ?

Vous pouvez utiliser les modèles d'administration pour contrôler l'environnement d'un système d'exploitation et l'expérience utilisateur. Il existe deux séries de modèles d'administration :

- Les paramètres utilisateurs
- Les paramètres de l'ordinateur.

Lorsque vous configurez les paramètres dans le nœud **Modèles d'administration** du GPO, vous apportez des modifications au registre. Les modèles d'administration ont les caractéristiques suivantes :

- Ils sont organisés en sous-nœuds qui correspondent à des éléments spécifiques de l'environnement, tels que le réseau, les systèmes et les composants Windows.
- Les paramètres de la section « Ordinateur » du nœud **Modèles d'administration** modifient la ruche **HKEY_LOCAL_MACHINE** et les paramètres de la section « Utilisateur » du nœud **Modèles d'administration** modifient la ruche **HKEY_CURRENT_USER** dans le registre.
- Certains paramètres existent à la fois pour l'utilisateur et l'ordinateur. Le paramètre pour empêcher le lancement de Windows Live Messenger est ainsi présent dans les modèles relatifs à l'utilisateur et à l'ordinateur. En cas de paramétrage contradictoire, le paramètre de l'ordinateur prévaudra.

- Les modèles d'administration vous permettent de contrôler l'environnement du système d'exploitation et l'expérience utilisateur :
- Section de modèle d'administration pour ordinateurs :
 - Panneau de configuration
 - Réseau
 - Imprimantes
 - Système
 - Composants basés sur Windows
- Section des modèles administratifs pour les utilisateurs :
 - Panneau de configuration
 - Bureau
 - Réseau
 - Menu Démarrer et barre des tâches
 - Système
 - Composants basés sur Windows
- Chacune de ces sections principales contient plusieurs sous-dossiers pour vous aider à organiser d'autres paramètres

- Certains paramètres ne sont disponibles que pour certaines versions des systèmes d'exploitation Windows. Un certain nombre de nouveaux paramètres ne seront ainsi utilisables qu'avec Windows 10. Vous pouvez afficher les versions prises en charge pour un paramètre en double-cliquant sur celui-ci.

Le tableau suivant détaille l'organisation du nœud **Modèles d'administration**.

| Section Modèle d'administration | Paramètres |
|----------------------------------|--|
| Configuration ordinateur | <ul style="list-style-type: none"> • Panneau de configuration • Réseau • Imprimantes • Serveur • Menu Démarrer et Barre des tâches • Système • Composants Windows • Tous les paramètres |
| Configuration utilisateur | <ul style="list-style-type: none"> • Panneau de configuration • Bureau • Réseau • Dossiers partagés • Menu Démarrer et Barre des tâches • Système • Composants Windows • Tous les paramètres |

La plupart des nœuds contiennent plusieurs sous-dossiers qui vous permettent de raffiner l'organisation des paramètres en groupes logiques. Trouver le paramètre dont vous avez besoin peut s'avérer difficile, même avec cette organisation. Le nœud **Tous les paramètres** contient une liste triée par ordre alphabétique de tous les paramètres contenus dans tous les autres nœuds. Plus tard dans cette leçon, vous apprendrez comment filtrer les paramètres dans le nœud **Modèles d'administration** pour vous aider à localiser les paramètres.

À quoi servent les fichiers .adm et .admx ?

Tous les paramètres du nœud **Modèles d'administration** d'un GPO sont stockés dans des fichiers. Tous les systèmes d'exploitation actuellement pris en charge stockent les paramètres dans des fichiers .admx. Windows Server 2000 et Windows Server 2003 stockent les paramètres dans des fichiers .adm. Plus tard dans ce module, vous apprendrez à étendre les paramètres numériques que vous pouvez configurer avec les **Modèles d'administration** en ajoutant des fichiers supplémentaires contenant des paramètres.

- | |
|--|
| <ul style="list-style-type: none"> • Les fichiers .adm : <ul style="list-style-type: none"> • Sont copiés dans tous les GPO dans SYSVOL ; • Sont difficiles à personnaliser ; • Ne sont pas en langue neutre ; • Pourraient entraîner le ballonnement de SYSVOL s'il y a beaucoup de GPO. • Les fichiers .admx : <ul style="list-style-type: none"> • Sont en langue neutre ; • Les fichiers .adml fournissent la langue localisée ; • Ne sont pas stockés dans l'objet de stratégie de groupe ; • Sont extensibles grâce à XML. |
|--|

Fichiers .adm

Traditionnellement, les *fichiers .adm* définissent les paramètres qu'un administrateur peut configurer à travers la stratégie de groupe. Tous les systèmes d'exploitation et services packs Windows successifs ont inclus une version plus récente de ces fichiers. Les fichiers .adm utilisent leur propre langage de balisage. Par conséquent, il est difficile de les personnaliser.

Les fichiers .adm sont situés dans le dossier %SystemRoot%\Inf. Les fichiers .adm contiennent à la fois les paramètres et une description en langage clair. Par conséquent, l'écrasement d'un fichier .adm dans le SYSVOL pourrait modifier le texte que vous voyez lorsque vous modifiez un GPO.

Les fichiers .adm présentent un autre inconvénient potentiel : lorsque vous les créez, ils se copient dans tous les GPO et consomment environ 3 mégaoctets (Mo) d'espace, en fonction de la version du client. Même s'il s'agit d'un volume limité, ce phénomène peut entraîner une augmentation de la taille du dossier SYSVOL et du trafic de réPLICATION. Avec de nombreux GPO dans un domaine, cela pourrait conduire à ce qu'on appelle un *gonflement de SYSVOL* avec un SYSVOL occupant plusieurs gigaoctets (Go) d'espace.

Fichiers .admx

Les systèmes d'exploitation Windows Vista et Windows Server 2008 ont vu apparaître un nouveau format d'affichage des paramètres de stratégie basés sur le registre. Ces paramètres utilisent un format de fichier XML basé sur des normes connues sous le nom de *fichiers .admx*. Ces nouveaux fichiers remplacent les fichiers .adm. Cependant, vous pouvez toujours utiliser des fichiers .adm.

Dans tous les systèmes d'exploitation Windows depuis Windows Vista et Windows Server 2008, la stratégie de groupe continue de reconnaître les fichiers .adm personnalisés présents dans votre environnement existant, mais ignore tous les fichiers .adm remplacés par des fichiers .admx.

Contrairement aux fichiers .adm, les fichiers .admx ne sont pas stockés dans les GPO individuels. L'éditeur de stratégie de groupe local lit et affiche automatiquement les paramètres du magasin de fichiers .admx local. Par défaut, les fichiers .admx sont stockés dans le dossier Windows\PolicyDefinitions, mais ils peuvent être stockés sur un emplacement central, dont il sera question plus loin.

Les fichiers .admx sont de langue neutre. Les descriptions en langage clair des paramètres ne font pas partie des fichiers .admx. Celles-ci sont stockées dans des *fichiers .adml* spécifiques à une langue.

Cela signifie que les administrateurs peuvent regarder le même GPO et consulter les descriptions de la stratégie dans leur propre langue, disponibles dans leurs propres fichiers .adml.

Les fichiers .adml sont stockés dans les sous-dossiers du dossier PolicyDefinitions. À chaque langue correspond un dossier propre. Par exemple, le dossier **en-US** stocke les fichiers en anglais et le dossier **es-ES** stocke les fichiers en espagnol. Par défaut, seuls les fichiers .adml correspondant à la langue du système d'exploitation installé sont présents.

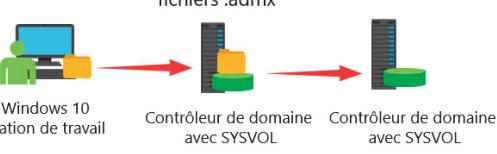
Vue d'ensemble du magasin central

Dans les entreprises avec une structure basée sur un domaine, vous pouvez créer un emplacement de stockage central pour les fichiers .admx, auquel toute personne ayant les autorisations nécessaires pour créer ou modifier des GPO peut accéder.

L'éditeur de gestion des stratégies de groupe lit et affiche automatiquement les paramètres de stratégie des modèles d'administration dans les fichiers .admx du magasin central, puis ignore les fichiers .admx stockés localement. Si le contrôleur de domaine ou le magasin central ne sont pas disponibles, le magasin local est utilisé.

Le magasin central :

- Est un référentiel central pour les fichiers .admx et .adml ;
- Est stocké dans SYSVOL ;
- Doit être créé manuellement ;
- Est détecté automatiquement par Windows Vista, Windows Server 2008 et les systèmes d'exploitation plus récents.



Les avantages de la création du magasin central sont :

- Vous vous assurez que les paramètres du nœud **Modèles d'administration** sont toujours les mêmes à chaque fois que quelqu'un édite un GPO.
- Lorsque Microsoft publie des fichiers .admx pour de nouveaux systèmes d'exploitation, la mise à jour avec les nouveaux fichiers s'effectue à un seul endroit.

Vous devez créer le magasin central manuellement, puis le mettre à jour manuellement sur un contrôleur de domaine.

L'utilisation de fichiers .admx dépend du système d'exploitation de l'ordinateur sur lequel vous créez ou modifiez le GPO. Selon le système d'exploitation et la configuration de votre serveur, les contrôleurs de domaine utilisent le service de réplication de fichiers ou la réplication de système de fichiers distribués (DFS) pour répliquer les données.

Pour créer un magasin central pour les fichiers .admx et .adml, créez un dossier et nommez-le **PolicyDefinitions** à l'emplacement suivant : ***FQDN\SYSVOL\iFQDN\Policies***, où <*FQDN*> est le nom de domaine pour vos services de domaine Active Directory (AD DS). Par exemple, pour créer un magasin central pour le domaine Test.Microsoft.com, créez un dossier **PolicyDefinitions** à l'emplacement suivant : **\Test.Microsoft.Com\SYSVOL\Test.Microsoft.Com\Policies**.

Un utilisateur doit copier tous les fichiers et sous-dossiers du dossier **PolicyDefinitions**, qui se trouve dans le dossier Windows sur un ordinateur sous Windows. Le dossier **PolicyDefinitions** stocke tous les fichiers .admx et les sous-dossiers stockent les fichiers .adml pour toutes les langues activées sur l'ordinateur client. Par exemple, sur un serveur sous Windows Server 2016 avec l'anglais activé, **C:\Windows\PolicyDefinitions** contiendra les fichiers .admx. Les fichiers .adml contenant les descriptions en anglais des paramètres définis dans les fichiers .admx se trouveront dans le sous-dossier **en-US**.



Remarque : Vous devez mettre à jour le dossier **PolicyDefinitions** pour chaque service pack et pour d'autres logiciels additionnels, tels que les fichiers .admx de Windows 10 version 1511 et de Microsoft Office 2016.

Discussion : Utilisations pratiques des modèles d'administration

Passez quelques minutes à examiner les modèles d'administration. Cherchez comment vous pourriez employer certains d'entre eux dans votre organisation.

Préparez-vous à partager des informations sur l'utilisation actuelle des GPO et des scripts d'ouverture de session dans votre organisation et à répondre par exemple aux questions suivantes :

- Comment assurez-vous la sécurité du poste de travail actuellement ?
- Quel est le degré actuel d'accès des utilisateurs à des fonctionnalités d'administration ?
- Quels paramètres de stratégie de groupe trouvez-vous utiles pour votre organisation ?

- Comment assurez-vous actuellement la sécurité du bureau ?
- De quel degré d'accès administratif à leurs systèmes les utilisateurs bénéficient-ils ?
- Quels paramètres de stratégie de groupe trouvez-vous utiles dans votre organisation ?



Question : Comment assurez-vous la sécurité du poste de travail actuellement ?

Question : Quel est le degré actuel d'accès des utilisateurs à des fonctionnalités d'administration ?

Question : Quels paramètres de stratégie de groupe trouvez-vous utiles pour votre organisation ?

Démonstration : Configuration des paramètres avec les modèles d'administration

Les outils de modification de stratégie de groupe dans Windows Server 2016 offrent plusieurs fonctionnalités qui facilitent la configuration et la gestion des GPO. Dans cette démonstration, vous pourrez passer en revue ces options.

Configurer un paramètre dans un modèle d'administration

Dans l'éditeur de gestion de stratégie de groupe, vous pouvez configurer un paramètre de stratégie en double-cliquant dessus. Le boîte de dialogue **Propriétés** du paramètre de stratégie apparaît.

Les paramètres de stratégie dans les modèles d'administration peuvent avoir trois états : **Non configuré**, **Activé** et **Désactivé**. Dans un nouveau GPO, chaque paramètre de stratégie est réglé par défaut sur **Non configuré**. Par conséquent, le GPO ne modifie pas la configuration existante de ce paramètre particulier pour l'utilisateur ou l'ordinateur.

L'effet de la modification varie selon le paramètre de stratégie. Par exemple, si vous activez le paramètre **Empêcher l'accès aux outils de modifications du Registre**, les utilisateurs ne sont pas en mesure de lancer l'Éditeur du Registre, Regedit.exe. Si vous désactivez ce paramètre de stratégie, vous permettez aux utilisateurs de lancer l'Éditeur du Registre. Notez qu'avec la double négation dans cet exemple de paramètre de stratégie, vous désactivez une stratégie qui empêche une action, permettant ainsi l'action.

Filtrer les paramètres de stratégie pour les modèles d'administration

L'absence d'aide à la recherche d'un paramètre de stratégie spécifique est l'un des inconvénients des versions précédentes des outils d'édition de stratégie de groupe. Avec des milliers de stratégies disponibles, il peut être difficile de trouver le paramètre que vous souhaitez configurer. L'Éditeur de gestion de stratégie de groupe dans Windows Server 2016 résout ce problème dans les **Modèles d'administration**. Vous pouvez maintenant créer des filtres pour localiser les paramètres de la stratégie.

Pour créer un filtre :

1. Cliquez avec le bouton droit sur **Modèles d'administration**, puis sur **Options de filtre**.
2. Pour localiser une stratégie spécifique, activez la case **Activer les filtres par mots clés**, saisissez les mots clés souhaités, puis sélectionnez les champs dans lesquels rechercher.

Vous pouvez également filtrer les paramètres de stratégie de groupe applicables à des versions spécifiques du système d'exploitation Windows, de Microsoft Internet Explorer et d'autres composants Windows. Toutefois, le filtre ne s'applique qu'aux paramètres du nœud **Modèles d'administration**.

Filtre sur les commentaires

Vous pouvez également poser des filtres et lancer des recherches sur les commentaires des paramètres de stratégie. Windows Server 2016 vous permet d'ajouter des commentaires aux paramètres de stratégie dans le nœud **Modèles d'administration**. Pour ce faire, double-cliquez sur un paramètre de stratégie, puis cliquez sur l'onglet **Commentaire**.

L'ajout de commentaires aux paramètres de stratégie configurés est recommandé. Il est recommandé de justifier un paramétrage et d'indiquer l'effet escompté. Il est également recommandé d'ajouter des commentaires au GPO lui-même. Windows Server 2016 vous permet de joindre des commentaires à un GPO :

- Dans l'Éditeur de gestion de stratégie de groupe, cliquez avec le bouton droit sur le nœud racine dans l'arborescence de la console, cliquez sur **Propriétés**, puis sur l'onglet **Commentaire**.

Comment copier les paramètres GPO

Les GPO de Starter ne peuvent contenir que des paramètres de stratégie de modèles d'administration. En plus d'utiliser les GPO de Starter, il existe deux autres façons de copier les paramètres d'un GPO dans un nouveau GPO :

1. Vous pouvez copier et coller des GPO entiers dans le conteneur des objets de stratégie de groupe de la console de gestion des stratégies de groupe (GPMC) afin d'obtenir un nouveau GPO avec tous les paramètres du GPO source.
2. Pour transférer des paramètres entre les GPO dans différents domaines ou forêts, cliquez-droit sur un GPO, puis sur **Sauvegarder**. Dans le domaine cible, créez un nouveau GPO, cliquez avec le bouton droit sur le GPO, puis cliquez sur **Importer les paramètres**. Vous serez en mesure d'importer les paramètres du GPO sauvegardé.

 **Lectures supplémentaires :** Pour plus d'informations, veuillez consulter : « Filtrer les paramètres de stratégie des modèles d'administration » à l'adresse : <http://aka.ms/Jcl669>

 **Remarque :** Le module 5, « Mise en œuvre d'une stratégie de groupe », explique les GPO de Starter en détail.

Dans cette démonstration, vous allez apprendre à :

- Configurer un paramètre dans **Modèles d'administration**
- Filtrer les paramètres de stratégie des modèles d'administration
- Ajouter des commentaires à un paramètre de stratégie
- Ajouter des commentaires à un GPO
- Créer un nouveau GPO en copiant un GPO existant
- Créer un nouveau GPO en important des paramètres préalablement exportés d'un autre GPO.

Procédure de démonstration

Configurer un paramètre de stratégie de modèles d'administration

1. Sur **LON-DC1**, ouvrez la **GPMC**.
2. Créez un nouveau GPO nommé **GPO1**, puis ouvrez-le.
3. Localisez le noeud **Configuration utilisateur\Stratégies\Modèles d'administration\Systèmes**.
4. Passez en revue les trois valeurs possibles pour le paramètre **Empêcher l'accès à l'invite de commandes**.

Filtrer les paramètres de stratégie des modèles d'administration

1. Filtrez les paramètres pour afficher uniquement ceux qui contiennent les mots-clés **économiseur d'écran** et visualisez les paramètres obtenus.
2. Filtrez les paramètres pour afficher uniquement les valeurs configurées et vérifiez l'affichage.

Ajouter des commentaires à un paramètre de stratégie

1. Ouvrez la fenêtre **Configuration utilisateur\Stratégies\Modèles d'administration\Panneau de configuration** et localisez **Personnalisation**.
2. Ajoutez un commentaire aux paramètres de stratégie **Un mot de passe protège l'écran de veille** et **Activer l'économiseur d'écran**.

Ajouter des commentaires à un GPO

- Ouvrez le nœud racine de la stratégie de GPO1, puis ajoutez un commentaire dans l'onglet **Commentaire**.

Créer un nouveau GPO en copiant un GPO existant

- Copiez **GPO1**, puis collez-le dans le dossier **Objets de stratégie de groupe**.

Créer un nouveau GPO par l'importation des paramètres qui ont été exportés d'un autre GPO

- Sauvegardez **GPO1**.
- Créez un nouveau GPO nommé **ADATUM Import**.
- Importez les paramètres à partir de la sauvegarde de **GPO1** dans le GPO **ADATUM Import**.

Importation des modèles de sécurité

Les administrateurs configurent souvent les paramètres de sécurité dans les GPO. La configuration des paramètres de sécurité dans un GPO peut être un travail fastidieux, surtout dans le cas des règles des pare-feu, en raison du nombre de règles et de paramètres à configurer.

Les *modèles de sécurité* sont des fichiers que vous utilisez pour gérer et configurer les paramètres de sécurité des ordinateurs sous Windows. Les modèles de sécurité sont constitués de paramètres divisés en sections logiques, en fonction des différentes catégories de paramètres de sécurité.

Lorsque vous configurez un modèle de sécurité, vous pouvez l'utiliser pour la configuration d'un seul ordinateur ou de plusieurs ordinateurs en réseau. Vous pouvez configurer et distribuer des modèles de sécurité de plusieurs façons :

- Outil en ligne de commande Secedit.exe. Vous pouvez utiliser Secedit.exe pour comparer la configuration actuelle d'un ordinateur qui exécute Windows Server 2016 avec des modèles de sécurité spécifiques.
- Composant logiciel enfichable Modèles de sécurité. Vous pouvez utiliser ce composant logiciel enfichable (snap-in) pour créer une stratégie de sécurité à l'aide de modèles de sécurité.
- Stratégie de groupe. Vous pouvez utiliser la stratégie de groupe pour analyser et configurer les paramètres de l'ordinateur et distribuer des paramètres de sécurité spécifiques.
- Security Compliance Manager. Vous pouvez utiliser Security Compliance Manager de Microsoft pour afficher les paramètres de sécurité, comparer les paramètres aux *baselines de sécurité* (groupes de paramètres fondés sur les guides de sécurité de Microsoft et les meilleures pratiques), personnaliser les paramètres, importer ou exporter des sauvegardes de GPO.

- Les modèles de sécurité contiennent les paramètres pour :
 - Stratégies de comptes
 - Stratégies locales
 - Journaux des événements
 - Groupes restreints
 - Services système
 - Registre
 - Système de fichiers
- Plus de paramètres de sécurité sont disponibles dans un GPO
- Les modèles de sécurité créés dans les modèles de sécurité enfichables peuvent être importés dans un GPO
- Le Compliance Manager Security peut exporter des lignes de base de sécurité dans un format de sauvegarde GPO

Composant logiciel enfichable Modèles de sécurité

Vous pouvez utiliser le snap-in Modèles de sécurité pour configurer les paramètres de sécurité dans les sections suivantes :

- Stratégies de comptes.** Cette section comprend un mot de passe, un verrouillage de compte et les stratégies de Kerberos version 5 (v5).

- **Stratégies locales.** Cette section comprend des stratégies d'audit, l'attribution des droits utilisateur et les options de sécurité.
- **Journal d'événements.** Cette section comprend les paramètres du journal des événements de l'application, du système et de la sécurité.
- **Groupes restreints.** Cette section définit les membres des groupes avec des autorisations et droits particuliers.
- **Services système.** Cette section comprend le démarrage et les autorisations pour les services système.
- **Registre.** Cette section comprend les autorisations relatives aux clés du Registre.
- **Système de fichiers.** Cette section comprend des autorisations sur les dossiers et les fichiers.

Vous pouvez utiliser le composant logiciel enfichable pour enregistrer le fichier .inf dans un emplacement connu ou pour indiquer l'emplacement standard des modèles de sécurité, à savoir le dossier **Documents\Sécurité\Modèles** dans le profil de l'utilisateur connecté.

Security Compliance Manager

Le nombre de paramètres de sécurité d'un ordinateur dépasse les capacités de configuration d'un modèle de sécurité. C'est pour cette raison que l'utilisation de Security Compliance Manager pour configurer la sécurité pourrait être une meilleure option. Microsoft met à jour Security Compliance Manager avec des baselines de sécurité que vous pouvez télécharger et utiliser dans votre propre environnement sans aucune modification. Vous pouvez également modifier les paramètres pour les adapter aux besoins de sécurité de votre organisation. Vous exportez les baselines que vous souhaitez utiliser sous forme de sauvegarde GPO. Vous importez ensuite la sauvegarde à l'aide de GPMC ou de Windows PowerShell.



Lectures complémentaires : Pour plus d'informations, veuillez consulter : « Security Compliance Manager (SCM) » à l'adresse : <http://aka.ms/Ypdcm>

Importer un modèle de sécurité dans un GPO

Une fois que vous avez créé votre modèle de sécurité, vous pouvez l'importer en procédant comme suit :

1. Dans la GPMC, créez un GPO.
2. Ouvrez le GPO en modification.
3. Dans l'**Éditeur de gestion de stratégie de groupe**, allez dans la section **Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité** du GPO.
4. Cliquez avec le bouton droit sur **Paramètres de sécurité** puis cliquez sur **Importer la stratégie**.
5. Dans la boîte de dialogue **Importer la stratégie à partir de**, sélectionnez le fichier de modèle de sécurité que vous souhaitez importer, puis cliquez sur **Ouvrir**.



Remarque : Le GPO va maintenant contenir les paramètres de sécurité configurés dans le modèle de sécurité.

Dans les versions précédentes de Windows Server, vous pouviez utiliser l'**Assistant de configuration de la sécurité** pour visualiser la configuration de Windows Server, puis créer une stratégie de sécurité basée sur cette configuration. Vous pouviez ensuite convertir la stratégie de sécurité en GPO en utilisant un outil en ligne de commande. L'**Assistant de configuration de la sécurité** n'est plus disponible dans Windows Server 2016.

Gestion des modèles d'administration

Comme indiqué précédemment, les modèles d'administration mettent à disposition des administrateurs des milliers de paramètres configurables que vous pouvez déployer vers des ordinateurs ou des utilisateurs. Vous pouvez également étendre l'ensemble configurable des paramètres de modèles d'administration pour inclure d'autres paramètres qui ne sont pas disponibles autrement. Pour étendre les modèles d'administration, suivez ces quatre étapes de haut niveau :

1. Téléchargez les modèles d'administration ou créez un nouveau modèle personnalisé à partir de zéro. De nombreux fournisseurs, y compris Microsoft et des développeurs tiers, proposent de télécharger gratuitement des modèles d'administration. Parmi les modèles d'administration, le modèle de Microsoft Office rencontre un grand succès. Ce modèle d'administration vous permet de personnaliser des paramètres spécifiques à Office, notamment des paramètres concernant chacune des applications incluses dans la suite Office.
2. Ajoutez les modèles d'administration au magasin central. Lorsque vous ajoutez les modèles d'administration pour une application dans le magasin central, un nouveau dossier ou un ensemble de dossiers contenant les nouveaux paramètres deviennent disponibles pour la personnalisation.
3. Personnalisez les paramètres du modèle d'administration. Vous pouvez personnaliser les paramètres du modèle d'administration de la même manière que vous personnalisez les paramètres GPO. L'utilisation de l'Éditeur de gestion de stratégie de groupe peut aider les administrateurs à personnaliser leurs applications.
4. Déployez le GPO avec les paramètres du modèle d'administration. Une fois que celui-ci est déployé, vous configurez les applications via les paramètres du modèle d'administration.

Vous devez télécharger les modèles d'administration au format .admx pour pouvoir mettre à jour le magasin central. Si les modèles d'administration pour une application donnée ne sont disponibles qu'au format .adm, vous pouvez utiliser le logiciel enfichable ADMX Migrator de Microsoft Management Console (MMC) pour convertir le fichier .adm en un ensemble de fichiers .admx et .adml.



Lectures supplémentaires : Pour plus d'informations, veuillez consulter : « ADMX Migrator » à l'adresse : <http://aka.ms/Ny5p5c>



Lectures supplémentaires : Pour plus d'informations, veuillez consulter : « Fichiers de modèles d'administration Office 2016 (ADMX/ADML) et outil de personnalisation Office » à l'adresse : <http://aka.ms/Nknzlx>

Vous pouvez également utiliser des fichiers .adm pour étendre l'ensemble des modèles d'administration, mais les paramètres seront uniquement accessibles dans le GPO dans lequel vous importez le fichier .adm. Pour étendre l'ensemble des modèles d'administration avec un fichier .adm, utilisez la procédure suivante :

1. Dans la GPMC, créez un nouveau GPO.
2. Ouvrez le GPO en modification.

3. Dans l'**Éditeur de gestion de stratégie de groupe**, cliquez avec le bouton droit sur le nœud **Modèles d'administration** du GPO, puis cliquez sur **Ajout/Suppression de modèles**.
4. Dans la boîte de dialogue **Ajout/suppression de modèles**, cliquez sur **Ajouter**.
5. Dans la boîte de dialogue **Modèles de stratégie**, accédez à l'emplacement du fichier .adm que vous souhaitez importer, sélectionnez le fichier, puis cliquez sur **Ouvrir**.



Remarque : Les paramètres supplémentaires doivent maintenant être disponibles dans **Modèles d'administration**.

Testez vos connaissances

| Question | |
|--|--------------------------|
| Quelles sont les sections disponibles dans le nœud Modèles d'administration sous le nœud Configuration utilisateur ? (Choisissez toutes les réponses applicables.) | |
| Sélectionnez la réponse correcte. | |
| | Bureau |
| | Composants Windows |
| | Serveur |
| | Système |
| | Panneau de configuration |

Confirmez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|---|---------|
| Vous pouvez créer le magasin central à travers la GPMC. | |

Leçon 2

Configuration de la redirection de dossiers, de l'installation de logiciel et des scripts

Vous pouvez utiliser des GPO pour déployer des scripts qui s'exécutent lors de la connexion ou la déconnexion des utilisateurs ou lors du démarrage ou de l'arrêt des ordinateurs. Vous pouvez également rediriger les dossiers inclus dans les profils des utilisateurs vers un serveur central. L'utilisation de la stratégie de groupe pour l'installation de logiciel vous permet de gérer l'installation de logiciels sur les ordinateurs clients. Ces fonctionnalités vous permettent de configurer les paramètres du bureau des utilisateurs plus facilement. Vous pouvez également si nécessaire créer un environnement de bureau standard qui répond aux besoins de votre organisation.

Objectifs de la leçon

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

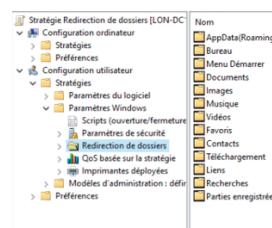
- Configurer la redirection de dossiers
- Expliquer les paramètres pour configurer la redirection de dossiers
- Décrire les paramètres de sécurité pour les dossiers redirigés
- Configurer la redirection de dossiers
- Gérer des logiciels avec la stratégie de groupe
- Décrire les paramètres de stratégie de groupe pour l'application des scripts
- Configurer des script avec des GPO.

Qu'est-ce que la redirection de dossiers ?

La *Redirection de dossiers* est une fonctionnalité qui permet de localiser les dossiers sur un serveur réseau et de les afficher comme s'ils étaient situés sur un disque local. Vous pouvez utiliser la redirection de dossiers pour gérer efficacement les données et éventuellement les sauvegarder. En redirigeant les dossiers, vous pouvez garantir à un utilisateur l'accès aux données, quel que soit l'ordinateur sur lequel il se connecte. La redirection de dossiers présente les caractéristiques suivantes :

- Lorsque vous redirigez les dossiers, vous ne stockez plus les dossiers sur le disque dur local d'un ordinateur mais dans un dossier partagé sur un serveur de fichiers réseau.
- Après redirection vers un serveur de fichiers, l'utilisateur voit toujours le dossier comme s'il était stocké sur le disque dur local.
- Vous pouvez utiliser la technologie Fichiers hors connexion avec la redirection pour synchroniser les données dans le dossier redirigé sur le disque dur local de l'utilisateur. Cela garantit que les utilisateurs ont accès à leurs données, même si une panne de réseau se produit ou si l'utilisateur travaille en mode hors connexion.

- La Redirection de dossiers permet aux dossiers d'être situés sur un serveur réseau, mais d'apparaître comme s'ils se trouvent sur un lecteur local
- Les dossiers pouvant être redirigés dans Windows Vista et les versions ultérieures sont :



Les ordinateurs sous Windows Vista et versions ultérieures peuvent rediriger les dossiers suivants :

- **AppData/Roaming**
- **Contacts**
- **Bureau**
- **Documents**
- **Téléchargements**
- **Favoris**
- **Liens**
- **Musique**
- **Images**
- **Parties enregistrées**
- **Recherches**
- **Menu Démarrer**
- **Vidéos**

Avantages de la redirection de dossiers

La redirection de dossier présente de nombreux avantages :

- Les utilisateurs qui se connectent à plusieurs ordinateurs peuvent accéder à leurs données à condition d'avoir accès au partage réseau.
- Les dossiers hors ligne permettent aux utilisateurs d'accéder à leurs données, même s'ils se déconnectent du réseau local (LAN).
- Vous pouvez facilement sauvegarder les données stockées sur des serveurs.
- La redirection des données du profil réduit considérablement la taille du profil d'itinérance.
- En cas de remplacement de la machine cliente, il y a moins de données à transférer.

Paramètres pour la configuration de la redirection de dossiers

Dans un GPO, les paramètres suivants sont disponibles pour la redirection de dossiers :

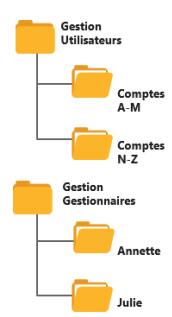
- **Aucune. Aucune** est le paramétrage par défaut. Avec ce réglage, la redirection de dossiers n'est pas activée.
- **De base.** Le paramètre **De base** est à utiliser pour :
 - Les utilisateurs qui redirigent leurs dossiers vers un espace commun.
 - Les utilisateurs ayant des besoins de confidentialité sur les données.
- **Avancée.** Vous pouvez utiliser le réglage **Avancée** pour spécifier différents emplacements réseau pour les différents groupes de sécurité de Active Directory.

• Configuration des options pour la Redirection de dossiers :

- Utilisez Redirection de dossiers de base lorsque tous les utilisateurs enregistrent leurs fichiers au même endroit ;
- Utilisez Redirection de dossiers avancée lorsque le serveur hébergeant l'emplacement du dossier est basé sur l'appartenance à un groupe ;
- Utilisez Suivi du dossier Documents pour forcer certains dossiers à devenir des sous-dossiers de Documents.

• Options d'emplacement du dossier cible :

- Créez un dossier pour chaque utilisateur sous le chemin racine ;
- Redirigez vers l'emplacement suivant ;
- Redirigez vers l'emplacement du profil utilisateur local ;
- Redirigez vers le répertoire de base de l'utilisateur (dossier Documents uniquement).



- **Suivre le dossier Documents.** **Suivre le dossier Documents** est disponible uniquement pour les dossiers **Images**, **Musique** et **Vidéos**. Ce paramètre fait du dossier concerné un sous-dossier du dossier **Documents**.

Emplacements du dossier cible pour les valeurs « De base » et « Avancée »

Si vous sélectionnez les valeurs **De base** ou **Avancée** pour le paramétrage, vous pouvez choisir parmi les options suivantes :

- **Créer un dossier pour chaque utilisateur sous le chemin racine.** Cette option crée un dossier sous la forme `\serveur\partage\nom du compte utilisateur\nom de dossier`. Si vous voulez stocker par exemple les paramètres de bureau des utilisateurs dans un dossier partagé appelé **Documents** sur un serveur nommé **LON-DC1**, le chemin de racine sera `\LON-DC1\Documents`. Chaque utilisateur dispose d'un chemin d'accès unique pour le dossier redirigé pour garantir la confidentialité des données. Par défaut, l'utilisateur bénéficie de droits exclusifs sur le dossier. Dans le cas du dossier **Documents**, le contenu actuel du dossier se déplace vers le nouvel emplacement.
- **Rediriger vers l'emplacement suivant.** Cette option utilise un chemin explicite pour l'emplacement de redirection. Dans ce cas, plusieurs utilisateurs partagent le même chemin pour le dossier redirigé. Par défaut, l'utilisateur bénéficie de droits exclusifs sur le dossier. Dans le cas du dossier **Documents**, le contenu actuel du dossier se déplace vers le nouvel emplacement.
- **Rediriger vers l'emplacement du profil utilisateur local.** Cette option permet de déplacer l'emplacement du dossier dans le profil d'utilisateur local sous le dossier **Utilisateurs**.
- **Rediriger vers le répertoire d'accueil de l'utilisateur.** Cette option est disponible uniquement pour le dossier **Documents**.

Suppression de la redirection de dossiers

Si vous décidez de supprimer la redirection de dossiers, vous devez également prendre une décision concernant les données contenues dans les dossiers redirigés. Par défaut, les données restent dans le dossier redirigé. Cela peut constituer un bon choix, mais vous devez alors trouver un moyen de mettre à nouveau les données à disposition des utilisateurs. La solution pourrait consister à créer un lecteur mappé pointant vers le dossier redirigé.



Remarque : Après avoir d'abord créé et appliqué un GPO qui fournit les paramètres de redirection des dossiers, les utilisateurs doivent fournir deux signatures avant que la redirection ne prenne effet. L'utilisation de la valeur **Avancée** pour la redirection de dossier pourrait exiger trois signatures. Cette contrainte vient du fait que les utilisateurs vont se connecter avec des informations d'identification mises en cache. Ceci s'applique seulement si l'option **Optimisation de connexion rapide** est activée, ce qui est le cas par défaut dans Windows 7 et les versions ultérieures. Pour que les paramètres de redirection de dossiers prennent effet avec une seule signature, le paramètre **Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session** doit être activé. Cependant, l'activation de ce paramètre de stratégie dégrade l'expérience utilisateur de la connexion dans son ensemble, car le temps de connexion s'allonge.

Question : Les utilisateurs d'un même département se connectent souvent sur différents ordinateurs. Ils doivent avoir accès à leur dossiers **Documents**. Il faut également que leurs données restent confidentielles. Quel paramètre de redirection de dossiers choisiriez-vous ?

Paramètres de sécurité pour les dossiers redirigés

Vous devez créer et configurer manuellement des autorisations sur un dossier réseau partagé pour stocker les dossiers redirigés en utilisant les autorisations répertoriées dans les tableaux de cette rubrique. Si les dossiers redirigés des utilisateurs n'existent pas, la redirection de dossiers peut les créer.

Les autorisations sur les dossiers sont gérées comme suit :

- Si vous laissez la redirection de dossiers créer des dossiers redirigés pour les utilisateurs, les autorisations correctes sur les sous-dossiers sont définies automatiquement.
- Si vous créez manuellement des dossiers, vous devez connaître les autorisations à appliquer.

Les tableaux ci-dessous illustrent ces autorisations.

| Permissions NTFS pour le dossier racine | |
|---|--|
| Créateur/Propriétaire | Contrôle total - sous-dossiers et fichiers uniquement |
| Administrateur | Aucun |
| Groupe de sécurité des utilisateurs qui enregistrent des données sur le partage | Liste des dossiers/Lecture de données, Création de dossiers/Ajouter des données - ce dossier seulement |
| Local System (Système local) | Contrôle total |

| Autorisations de partage pour dossier racine | |
|---|---|
| Créateur/Propriétaire | Contrôle total - sous dossiers et fichiers uniquement |
| Groupe de sécurité des utilisateurs qui enregistrent des données sur le partage | Contrôle total |

| Autorisations NTFS pour le dossier redirigé de chaque utilisateur | |
|---|---|
| Créateur/Propriétaire | Contrôle total - sous-dossiers et fichiers uniquement |
| %Nom d'utilisateur% | Contrôle total, propriétaire du dossier |
| Administrateurs | Contrôle total |
| Système | Contrôle total |

Permissions du système de fichiers NTFS pour le dossier racine

| | |
|---|---|
| Créateur/Propriétaire | Contrôle total - sous-dossiers et fichiers uniquement |
| Administrateur | Aucun |
| Groupe de sécurité des utilisateurs qui enregistrent des données sur le partage | Liste des dossiers/Lecture de données, Création de dossiers/Ajout de données - Ce dossier seulement |
| Système | Contrôle total |

Autorisations de partage pour dossier racine

| | |
|---|---|
| Créateur/Propriétaire | Contrôle total - sous-dossiers et fichiers uniquement |
| Groupe de sécurité des utilisateurs qui enregistrent des données sur le partage | Contrôle total |

Autorisations NTFS pour le dossier redirigé de chaque utilisateur

| | |
|-----------------------|---|
| Créateur/Propriétaire | Contrôle total - sous-dossiers et fichiers uniquement |
| %Nom d'utilisateur% | Contrôle total, propriétaire du dossier |
| Administrateurs | Contrôle total |
| Système | Contrôle total |

Démonstration : Configuration de la redirection de dossiers

Cette démonstration montre comment :

- Créer un dossier partagé dédié à la redirection de dossiers
- Créer un GPO pour rediriger le dossier Documents
- Tester la redirection de dossiers.

Procédure de démonstration

Créer un dossier partagé

1. Sur **LON-DC1**, créez un dossier nommé **C:\Redir**.
2. Partagez le dossier avec **Tout le monde**, avec une autorisation en **lecture/écriture**.

Créer un GPO pour rediriger le dossier Documents

1. Ouvrez la **GPMC**.
2. Créez un GPO nommé **Redirection de dossiers**, puis reliez-le au domaine **Adatum**.
3. Modifiez le GPO **Redirection de dossiers**.
4. Configurez les propriétés du dossier **Documents** de manière à utiliser le paramétrage **De base - Rediriger les dossiers de tout le monde vers le même emplacement**.
5. Veillez à ce que l'**emplacement du dossier cible** soit paramétré sur **Créer un dossier pour chaque utilisateur sous le chemin d'accès racine**.
6. Indiquez **\\\LON-DC1\Redir** comme chemin de la racine.
7. Fermez toutes les fenêtres actives sur **LON-DC1**.

Tester la redirection de dossiers

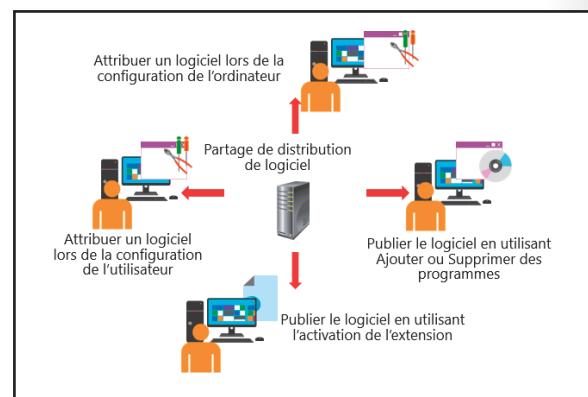
1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Modifiez les propriétés du dossier **Documents**. Le chemin doit maintenant être **\\\LON-DC1\Redir\Administrateur**.
3. Déconnectez-vous de **LON-CL1**.

Gestion des logiciels avec la stratégie de groupe

Windows Server 2016 inclut une fonctionnalité appelée **Installation et maintenance de logiciels**, qu'AD DS, la stratégie de groupe et le service Windows Installer utilisent pour installer, assurer la maintenance et supprimer des logiciels sur les ordinateurs de votre organisation.

Apport de l'installation de logiciel de la stratégie de groupe dans la gestion du cycle de vie des logiciels

Le cycle de vie d'un logiciel se compose de quatre phases : la préparation, le déploiement, la maintenance et la suppression. Vous pouvez utiliser la stratégie de groupe pour gérer toutes ces phases, sauf la préparation. Vous pouvez appliquer



des paramètres de stratégie de groupe à des utilisateurs ou des ordinateurs dans un site, un domaine ou une unité d'organisation (UO) pour installer, mettre à niveau ou supprimer des logiciels automatiquement.

En appliquant les paramètres de stratégie de groupe à un logiciel, vous pouvez gérer les phases de déploiement sans déployer le logiciel sur chaque ordinateur individuellement. L'utilisation de la stratégie de groupe pour gérer le cycle de vie des logiciels présente des avantages et des inconvénients, qu'il est important de prendre en compte.

Les avantages de l'utilisation de la stratégie de groupe pour gérer le cycle de vie d'un logiciel sont :

- L'installation de logiciel de la stratégie de groupe est disponible dans la stratégie de groupe et AD DS. Utiliser la stratégie de groupe ne représente donc pas un coût supplémentaire pour votre organisation. Vous pouvez toujours l'implémenter car elle est déjà installée et prête à l'emploi.
- L'installation de logiciel de la stratégie de groupe ne nécessite pas de logiciel client, de logiciel agent ou de logiciel de gestion supplémentaire. Les administrateurs informatiques peuvent utiliser des outils familiers tels que la GPMC et l'Éditeur de gestion de la stratégie de groupe pour gérer le cycle de vie du logiciel.
- L'installation de logiciel de la stratégie de groupe est rapide et facile à utiliser. Ceci permet à la fois de distribuer des logiciels plus rapidement et de réduire les coûts d'apprentissage informatique.

Les inconvénients de l'utilisation des stratégies de groupe pour gérer le cycle de vie d'un logiciel sont :

- L'installation de logiciel de la stratégie de groupe dispose de peu de fonctionnalités. Cette caractéristique limite la capacité à contrôler certains aspects de la distribution tels que le jour et l'heure de l'installation, l'ordre d'installation lors du déploiement de multiples applications et le processus de redémarrage, avec par exemple la suppression du redémarrage ou les fenêtres de redémarrage.
- L'installation de logiciel de la stratégie de groupe ne dispose pas de la fonctionnalité de création de rapports. Vous ne pouvez donc pas collecter facilement des informations telles que le nombre d'ordinateurs sur lesquels le logiciel a été installé, les ordinateurs sur lesquels l'installation a échoué ou les ordinateurs ne disposant pas du logiciel distribué. Cela peut conduire à un scénario de déploiement d'une mise à jour applicative qui aboutit à des tentatives d'installation sur des ordinateurs sur lesquels l'application à mettre à jour n'est plus présente.
- L'installation de logiciel de la stratégie de groupe est limitée au déploiement de packages Windows Installer. Avant d'être en mesure de déployer le logiciel en utilisant la stratégie de groupe, les administrateurs doivent convertir tous les programmes d'installation non .msi en packages .msi.



Remarque : Pour les grandes entreprises, en particulier celles avec plus de 500 ordinateurs et pour toute organisation avec des exigences spécifiques en matière de distribution de logiciels, le gestionnaire de configuration de Microsoft System Center fournit des fonctionnalités et un contrôle au niveau de l'entreprise. L'utilisation du gestionnaire de configuration de Microsoft System Center (Configuration Manager) sera plus intéressante que l'installation de logiciel de la stratégie de groupe pour la plupart des grandes entreprises, en raison des caractéristiques au niveau de l'entreprise et du contrôle fournis par Configuration Manager.

Deux méthodes de déploiement sont disponibles pour mettre des logiciels à disposition des clients. Les administrateurs peuvent installer des logiciels pour les utilisateurs ou les ordinateurs à l'avance par une affectation du logiciel, ou donner aux utilisateurs la possibilité d'installer le logiciel quand ils le souhaitent en publiant le logiciel dans AD DS. Les nœuds **Configuration utilisateur** et **Configuration de l'ordinateur** d'un GPO disposent tous les deux d'un nœud **Paramètres du logiciel**. Vous pouvez ajouter des logiciels à un GPO en ajoutant un nouveau package au nœud **Installation de logiciel**, puis spécifier si vous voulez l'attribuer ou le publier.

Vous pouvez également choisir d'appliquer le déploiement avancé pour un paquet. Utilisez cette option pour appliquer un fichier de personnalisation à un package pour un déploiement personnalisé - par exemple si vous utilisez l'outil de personnalisation Office pour créer un fichier de personnalisation de l'installation pour déployer Microsoft Office.

Attribution du logiciel

Lorsque vous attribuez un logiciel à un utilisateur, le menu **Démarrer** de l'utilisateur annonce la disponibilité du logiciel lorsque l'utilisateur se connecte. L'installation ne commence que si l'utilisateur double-clique sur l'icône de l'application ou sur un fichier associé à l'application.

L'affectation du logiciel présente les caractéristiques suivantes :

- Les utilisateurs ne partagent pas les applications attribuées. Lorsque vous attribuez un logiciel à un utilisateur, l'application que vous installez pour un utilisateur via la stratégie de groupe peut ne pas être disponible pour les autres utilisateurs. L'affectation du logiciel à un utilisateur est à privilégier lorsque le logiciel est utilisé par un sous-ensemble d'utilisateurs. C'est aussi le cas si le logiciel a des coûts de licence associés et que vous ne souhaitez pas acheter des licences inutiles.
- Lorsque vous attribuez une application à un ordinateur, l'application s'installe au prochain démarrage de l'ordinateur. L'application sera disponible pour tous les utilisateurs de l'ordinateur. Il est préférable d'affecter des logiciels à un ordinateur lorsque vous souhaitez installer le logiciel sur un ensemble spécifique d'ordinateurs ou sur tous les ordinateurs dans un environnement, quels que soient les utilisateurs de ces ordinateurs. Ceci se produit souvent lors de l'utilisation d'un logiciel agent, comme les agents de surveillance, les agents liés à la sécurité, ou les agents de gestion.

Publication du logiciel

Le raccourci **Programmes\Programmes et fonctionnalités** dans le Panneau de configuration annonce la publication d'une application pour l'utilisateur. Les utilisateurs peuvent installer l'application en utilisant le raccourci **Installer un programme à partir du réseau**. L'activation d'une extension peut également lancer l'installation de l'application. L'activation de l'extension lance l'installation du programme lorsqu'un utilisateur clique sur un type de fichier associé au programme.

La publication du logiciel présente les caractéristiques suivantes :

- Le Panneau de configuration n'annonce pas des applications aux utilisateurs qui ne possèdent pas la permission de les installer.
- Vous ne pouvez pas publier des applications pour des ordinateurs.

Déploiement des mises à jour logicielles

Les fournisseurs de logiciels proposent des mises à jour de logiciels pour apporter (généralement) des corrections mineures, telles que des mises à jour de performance ou des améliorations de fonctionnalités qui ne justifient pas une réinstallation complète de l'application. Microsoft publie des mises à jour logicielles sous la forme de fichiers .msp.

Les mises à jour plus importantes, qui offrent de nouvelles fonctionnalités, exigent des utilisateurs la mise à niveau du logiciel avec une version plus récente. Vous pouvez ouvrir le GPO qui déploie un logiciel, modifier les paramètres d'installation de logiciel, puis utiliser l'onglet **Mises à niveau** pour mettre à niveau un package. Lorsque vous effectuez des mises à jour en utilisant la stratégie de groupe, vous remarquerez les caractéristiques suivantes :

- Vous pouvez redéployer un package si le fichier d'origine Windows Installer a été modifié.
- Les mises à jour suppriment en général l'ancienne version d'une application et installent une version plus récente. Ces mises à niveau conservent généralement les paramètres de l'application.

- Vous pouvez supprimer des logiciels s'ils ont été livrés à l'origine en utilisant la stratégie de groupe. Ceci est utile si vous remplacez l'application d'une ligne métier (LOB) par une autre application. La suppression peut être obligatoire ou facultative.

Paramètres de stratégie de groupe pour l'application des scripts

Vous pouvez utiliser des scripts de stratégie de groupe pour effectuer un certain nombre de tâches. Certaines actions peuvent être à effectuer chaque fois qu'un ordinateur démarre ou s'arrête, ou lorsque les utilisateurs se connectent ou se déconnectent. Par exemple, vous pouvez utiliser des scripts pour :

- Nettoyer les postes de travail lorsque les utilisateurs se déconnectent et éteignent les ordinateurs
- Supprimer le contenu des répertoires temporaires
- Mapper des lecteurs ou des imprimantes
- Définir des variables d'environnement
- Attribuer des scripts à l'ordinateur pour fonctionner dans le contexte de sécurité du compte système local
- Attribuer des scripts à l'utilisateur qui se connecte pour un fonctionnement dans le contexte de sécurité de cet utilisateur.

- Vous pouvez utiliser les scripts pour effectuer de nombreuses tâches, telles que supprimer des fichiers de page, mapper des lecteurs et supprimer les dossiers temporaires pour les utilisateurs
- Les langages de scripts incluent VBScript, Jscript, Windows PowerShell et des fichiers de commandes
- Vous pouvez attribuer des paramètres de script de stratégie de groupe pour attribuer :
 - Pour les ordinateurs :
 - Des scripts de démarrage ;
 - Des scripts d'arrêt.
 - Pour les utilisateurs :
 - Des scripts d'ouverture de session ;
 - Des scripts de fermeture de session.

D'autres paramètres de la stratégie de groupe contrôlent certains aspects de l'exécution de scripts. Lors de l'attribution de plusieurs scripts par exemple, vous pouvez contrôler s'ils fonctionnent de manière synchrone ou asynchrone.

Vous pouvez écrire des scripts dans tout langage de script que le système d'exploitation du client sous Windows peut interpréter, comme Microsoft Visual Basic, Scripting Edition (VBScript) ; JScript ; de simples fichiers de commandes ou des fichiers batch.



Remarque : Dans tous les systèmes d'exploitation Windows depuis Windows Server 2008 R2 et Windows 7, l'interface utilisateur dans l'éditeur de stratégie de groupe local pour les scripts d'ouverture de session, de fermeture de session, de démarrage et d'arrêt fournit un onglet supplémentaire pour les scripts d'interface de ligne de commande Windows PowerShell. Vous pouvez déployer le script Windows PowerShell en l'ajoutant à cet onglet. Les systèmes d'exploitation peuvent exécuter des scripts Windows PowerShell via la stratégie de groupe.

Les scripts sont stockés dans des dossiers partagés sur le réseau. Vous devez vous assurer que le client a accès à cet emplacement réseau. Si les clients ne peuvent pas accéder à l'emplacement réseau, les scripts ne pourront pas s'exécuter. Les scripts peuvent être stockés sur tout emplacement réseau, mais il est recommandé d'utiliser le partage Netlogon car tous les utilisateurs et les ordinateurs reconnus par AD DS ont accès à cet emplacement.

Pour nombre de ces paramètres, l'utilisation des préférences de la stratégie de groupe est préférable à leur configuration dans les images Windows ou à l'utilisation de scripts d'ouverture de session. Les préférences de stratégie de groupe sont détaillées plus loin dans ce module.

Démonstration : Configuration des scripts avec des objets de stratégie de groupe

Cette démonstration montre comment :

- Créer un script d'ouverture de session pour afficher un message
- Créer et lier un GPO pour utiliser le script
- Se connecter à un ordinateur client et tester les résultats.

Procédure de démonstration

Créer un script d'ouverture de session pour afficher un message

1. Sur **LON-DC1**, démarrez le **Bloc-notes**, tapez la commande suivante, puis appuyez sur Entrée :
Msgbox "Ceci est le script"
2. Enregistrez le fichier sous **logon.vbs**.
3. Copiez le fichier dans le Presse-papiers.

Créer et lier un GPO pour utiliser le script

1. Utilisez la **Console de gestion des stratégies de groupe** pour créer un nouveau GPO nommé **Script d'ouverture de session utilisateur**, puis reliez-le au domaine **Adatum.com**.
2. Modifiez le GPO pour configurer un script d'ouverture de session.
3. Collez le fichier script **Logon.vbs**.
4. Ajoutez le script **Logon.vbs** aux scripts d'ouverture de session.

Se connecter à un ordinateur client et tester les résultats

1. Sur **LON-CL1**, connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Actualisez les paramètres de la stratégie de groupe sur l'ordinateur du client.
3. Connectez-vous en tant qu'**Adatum\Connie** avec le mot de passe **Pa55w.rd**.
4. Vérifiez que le message s'affiche dans une boîte de dialogue. Notez que l'affichage peut prendre jusqu'à dix minutes. Si le message n'apparaît pas, redémarrez **LON-CL1** et répétez les étapes un à trois.
5. Déconnectez-vous de **LON-CL1**.

Testez vos connaissances

| Question | |
|--|-------------------|
| Lequel des dossiers suivants pouvez-vous rediriger en utilisant la redirection de dossiers ? (Choisissez toutes les réponses applicables.) | |
| Sélectionnez la réponse correcte. | |
| | Documents |
| | Favoris |
| | AppData (Roaming) |
| | AppData (Local) |

| Question | |
|----------|--------------------|
| | Fichiers programme |

| Éléments | |
|----------|--------------------------------|
| 1 | Scripts d'ouverture de session |
| 2 | Scripts de démarrage |
| 3 | Attribuer logiciel |
| 4 | Scripts de déconnexion |
| 5 | Scripts d'arrêt |
| 6 | Redirection de dossiers |
| 7 | Publier logiciel |

| Catégorie 1 | Catégorie 2 | Catégorie 3 |
|---------------------------|--------------------------|--|
| Configuration utilisateur | Configuration ordinateur | Configuration utilisateur et Configuration de l'ordinateur |
| | | |

Leçon 3

Configuration des préférences de stratégie de groupe

Certaines organisations utilisent encore des scripts qui s'exécutent lorsque les utilisateurs se connectent. Ces scripts fournissent généralement des paramètres tels que les lecteurs mappés, les imprimantes et les changements de registre.

Windows Server 2008 et les systèmes d'exploitation plus récents disposent des préférences de stratégie de groupe. Vous pouvez configurer des paramètres, par exemple les lecteurs mappés, à diffuser à l'aide d'une stratégie de groupe. De plus, vous pouvez configurer les préférences en installant les outils d'administration de serveur distant (RSAT) sur un ordinateur client sous Windows 7 ou version ultérieure. Cela vous permet de fournir de nombreux paramètres communs à l'aide d'une stratégie de groupe.

Objectifs de la leçon

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

- Décrire les préférences de stratégie de groupe
- Comparer des préférences de stratégie de groupe et des paramètres de GPO
- Décrire les fonctionnalités des préférences de stratégie de groupe
- Configurer les préférences de stratégie de groupe.

Que sont les préférences de stratégie de groupe ?

Les préférences de stratégie de groupe contiennent plus de 20 extensions de stratégie de groupe qui étendent la plage des paramètres configurables dans un GPO. Vous pouvez maintenant utiliser les préférences de stratégie de groupe pour appliquer un certain nombre de paramètres qui s'appliquaient auparavant à des scripts, tels que les mappages de lecteurs et les imprimantes partagées.

Les systèmes d'exploitation Windows ultérieurs à Windows Server 2008 et Windows Vista Service Pack 2 (SP2) et les systèmes d'exploitation plus récents prennent en charge de manière native les préférences de stratégie de groupe.

Les extensions des préférences de stratégie de groupe développent la plage des paramètres configurables dans un objet de stratégie de groupe :

- Vous permettent de gérer les paramètres qui auparavant ne pouvaient être gérés grâce à la stratégie de groupe ;
- Sont pris en charge en mode natif sur Windows Server 2008 et les versions plus récentes et sur Windows Vista et les versions plus récentes ;
- Peuvent être créés, supprimés, remplacés ou mis à jour ;
- Les catégories comprennent les lecteurs mappés, les raccourcis, les changements de registre, les options d'alimentation, les tâches d'horaires et les paramètres d'Internet Explorer.

Exemples d'extensions de stratégie de groupe dans les préférences de stratégie de groupe (liste non exhaustive) :

- Options de dossier
- Mappages de lecteurs
- Registre
- Raccourcis
- Imprimantes
- Tâches planifiées
- Services
- Menu Démarrer

La configuration des préférences de stratégie de groupe ne nécessite aucun outil spécial ni aucune installation de logiciel. Les préférences de stratégie de groupe sont des éléments natifs de GPMC dans Windows Server 2008 et versions ultérieures. Elles s'appliquent de la même manière que les paramètres de stratégie de groupe par défaut. Les préférences ont deux sections distinctes : Paramètres Windows et Paramètres du Panneau de configuration.

Lorsque vous configurez une nouvelle préférence, vous pouvez effectuer les quatre actions de base suivantes pour l'utilisateur ou l'ordinateur :

- Créer. Créer un nouveau paramètre de préférence.
- Supprimer. Supprimer un paramètre de préférence existant.
- Remplacer. Supprimer et recréer un paramètre de préférence. Les préférences de stratégie de groupe remplacent alors tous les paramètres et les fichiers existants associés à l'élément de préférence.
- Mise à jour. Modifier un paramètre de préférence existant.

Comparaison des préférences de stratégie de groupe et des paramètres de stratégie de groupe

Les préférences de stratégie de groupe ont en commun avec les paramètres de stratégie de groupe d'appliquer des configurations à l'utilisateur ou de l'ordinateur. Cependant, il existe plusieurs différences dans la façon dont vous pouvez les configurer et les appliquer. L'une de ces différences est que les préférences ne sont pas appliquées, mais vous pouvez les configurer pour les réappliquer automatiquement.

Voici les principales différences entre les paramètres de stratégie de groupe et les préférences de stratégie de groupe :

- Les préférences ne sont pas appliquées.
- Les préférences de stratégie de groupe désactivent l'interface utilisateur pour les paramètres que vous configurez. Les préférences ne le font pas.
- Les paramètres de stratégie de groupe peuvent s'appliquer à intervalles réguliers. Cependant, vous pouvez configurer les préférences à appliquer une seule fois, ou suivant les mêmes intervalles que les paramètres de stratégie de groupe.
- Les utilisateurs finaux peuvent modifier tous les paramètres de préférences qui s'appliquent à travers la stratégie de groupe, mais les paramètres de stratégie de groupe empêchent les utilisateurs de les modifier.
- Dans certains cas, vous pouvez configurer les mêmes paramètres via un paramètre de stratégie et un élément de préférence. Si des paramètres de préférence et de stratégie de groupe contradictoires configurent et s'appliquent au même objet, c'est toujours la valeur du paramètre de stratégie qui s'applique.

| Paramètres de stratégie de groupe | Préférences de stratégie de groupe |
|--|---|
| Appliquer strictement les paramètres de stratégie en écrivant les paramètres dans les zones du registre que les utilisateurs standards ne peuvent modifier | Sont écrites dans les emplacements normaux dans le registre que l'application ou la fonctionnalité du système d'exploitation utilise pour stocker le réglage |
| En général, désactiver l'interface utilisateur pour les paramètres gérés par la stratégie de groupe | Ne pas faire en sorte que la fonctionnalité de l'application ou du système d'exploitation désactive l'interface utilisateur pour les réglages qu'ils configurent |
| Actualiser les paramètres de stratégie à un intervalle régulier | Actualiser les préférences en utilisant le même intervalle que les paramètres de stratégie de groupe par défaut, mais peut être configuré pour s'appliquer une seule fois |



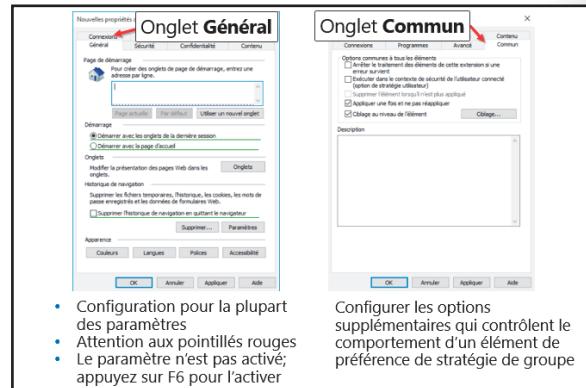
Remarque : Alors que la définition de la stratégie de groupe désactive l'interface utilisateur pour un réglage donné, l'utilisateur peut modifier le réglage s'il a la possibilité de modifier le registre.

Fonctionnalités des Préférences de stratégie de groupe

Après avoir créé une préférence de stratégie de groupe, vous devez en configurer les propriétés. Des préférences différentes nécessiteront des informations d'entrée différentes. Par exemple, les préférences de raccourcis nécessitent des chemins cibles, alors que les variables d'environnement nécessitent des types et des valeurs variables. Les préférences fournissent également un certain nombre de caractéristiques dans les propriétés communes pour faciliter le déploiement.

Onglet Général

Vous configurez généralement les paramètres de base d'une préférence dans l'onglet **Général**. Ici, la première étape consiste à spécifier l'action pour la préférence : **Créer**, **Effacer**, **Remplacer**, ou **Mettre à jour**. Différents paramètres sont disponibles en fonction de l'action initiale sélectionnée. Par exemple, lors de la création d'un mappage de lecteur, vous devez fournir un chemin Universal Naming Convention (UNC) et une option pour la lettre que vous souhaitez affecter au lecteur.



- Configuration pour la plupart des paramètres
- Attention aux pointillés rouges
- Le paramètre n'est pas activé; appuyez sur F6 pour l'activer

Configurer les options supplémentaires qui contrôlent le comportement d'un élément de préférence de stratégie de groupe

Onglet Commun

Les options communes sont compatibles avec toutes les préférences. Vous pouvez utiliser l'onglet **Commun** pour contrôler le comportement de la préférence de la manière suivante :

- **Arrêter le traitement des éléments de cette extension si une erreur survient.** Si une erreur se produit lors du traitement d'une préférence, aucune autre préférence dans cet objet de stratégie de groupe ne sera traitée.
- **Exécuter dans le contexte de sécurité de l'utilisateur connecté.** Les préférences peuvent s'exécuter en tant que compte système ou qu'utilisateur connecté. Ce paramètre force des éléments de préférence à s'exécuter dans le contexte de l'utilisateur connecté à la place du compte système. Il est utile lorsque vous configurez les lecteurs mappés et les imprimantes, lorsque vous voulez que les informations d'identification de l'utilisateur permettent de se connecter à la ressource partagée.
- **Supprimer cet élément quand il est n'est plus appliqué.** Contrairement à des paramètres de stratégie, les préférences ne sont pas supprimées lorsque le GPO qui les a livrées est retiré. Ce paramètre va changer ce comportement. Si vous sélectionnez cette option, l'action passe à **Remplacer**. Soyez cependant prudent lorsque vous utilisez cette option, car les préférences de stratégie de groupe modifient le registre à l'emplacement normal. Des problèmes imprévus pourraient donc se produire en cas d'utilisation de cette option.
- **Appliquer une fois et ne pas réappliquer.** En fonctionnement normal, les préférences sont actualisées sur la base du même intervalle que les paramètres de stratégie de groupe. Ce paramètre modifie ce comportement pour appliquer le réglage une seule fois pour un utilisateur ou un ordinateur.
- **Utiliser le ciblage au niveau élément.** L'une des caractéristiques les plus puissantes des préférences est le ciblage au niveau élément des préférences. Vous pouvez utiliser cette fonction pour définir des critères qui permettront de déterminer exactement quels utilisateurs ou ordinateurs recevront une préférence. Ces critères sont notamment (liste non exhaustive) :
 - Nom de l'ordinateur
 - Plage d'adresses IP
 - Système d'exploitation

- Groupe de sécurité
- Utilisateur
- Requêtes Windows Management Instrumentation (WMI)

Activation et désactivation des réglages dans les préférences de stratégie de groupe

Tous les paramètres que vous pouvez configurer dans les préférences de stratégie de groupe ne sont pas activés par défaut. Si vous souhaitez par exemple configurer la page d'accueil Internet Explorer en utilisant les préférences de stratégie de groupe, ce réglage ne fonctionnera pas par défaut. Lorsque vous configurez un paramètre, vous pouvez voir une ligne rouge en pointillés, tandis que dans le même onglet le paramètre **Supprimer l'historique de navigation en quittant le navigateur** est marqué d'une ligne verte continue. Cela signifie que le paramètre est activé.

Vous pouvez activer et désactiver les paramètres dans un onglet en utilisant les touches **F5**, **F6**, **F7** et **F8**.

Les touches activent et désactivent les paramètres comme suit :

- F5 active tous les paramètres dans un onglet
- F6 active le paramètre sélectionné
- F7 désactive le paramètre sélectionné
- F8 désactive tous les paramètres dans un onglet.

Notez que les cases à cocher et les options sont entourées d'un cercle vert ou rouge pour montrer si le paramètre est activé ou non.

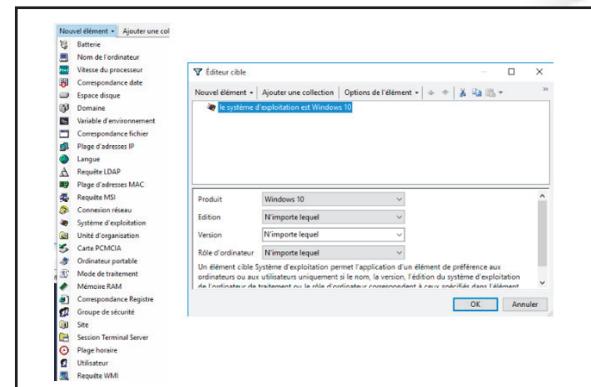
Options de ciblage au niveau élément

Le *ciblage au niveau élément* est une fonctionnalité qui permet de n'appliquer les paramètres des préférences de stratégie de groupe qu'à des ordinateurs ou des objets utilisateur correspondant aux critères définis. Cela rend possible le contrôle de ciblage avancé et permet aux administrateurs de stratégie de groupe de repérer exactement où et quand un paramètre doit s'appliquer. Le ciblage au niveau élément offre les fonctionnalités suivantes :

- Cibler 27 catégories différentes. Le ciblage au niveau élément peut utiliser 27 catégories différentes pour cibler les ordinateurs et les objets utilisateur. Cela permet un ciblage de précision.
- Combiner différentes catégories en utilisant la logique booléenne ET ou OU. Au lieu d'utiliser une seule catégorie pour le ciblage, vous pouvez utiliser plusieurs catégories.
- Actualiser le ciblage au niveau élément durant l'actualisation de fond de la stratégie de groupe. Cela signifie que la configuration des objets ordinateur et utilisateur en utilisant le ciblage au niveau élément est un moyen dynamique de gérer ces objets.

Les catégories suivantes sont disponibles dans le ciblage au niveau élément :

- Batterie
- Nom des ordinateurs
- Vitesse du processeur



- Correspondance de date
- Espace disque
- Domaine
- Variable d'environnement
- Correspondance fichier
- Plage d'adresses IP
- Langue
- Requête LDAP
- Plage d'adresses MAC
- Requête MSI
- Connexion réseau
- Système d'exploitation
- Unité d'organisation
- Carte PCMCIA
- Ordinateur portable
- Mode de traitement
- Mémoire vive
- Correspondance registre
- Groupe de sécurité
- Site
- Session Terminal Server
- Plage horaire
- Utilisateur
- Requête WMI

Scénarios pour la configuration en utilisant le ciblage au niveau élément

En utilisant les différentes catégories avec des expressions logiques booléennes, vous pouvez créer un ciblage précis au niveau élément pour chaque paramètre des préférences de stratégie de groupe que vous configurez.

La liste suivante présente quelques scénarios pour lesquels vous pourriez utiliser le ciblage au niveau élément :

- Restreindre les mappages de lecteurs à un groupe de sécurité Active Directory. Vous pouvez aller plus loin en limitant les mappages de lecteurs avec un contenu sensible à une plage d'adresses IP spécifique.
- Restreindre les mappages de lecteurs à des ordinateurs disposant d'un fichier (ou programme) spécifique seulement. Il n'est par exemple pas nécessaire de mapper un lecteur avec l'emplacement de stockage des données d'une application si celle-ci n'est pas présente sur l'ordinateur.
- Configurer des plans de puissance pour les ordinateurs portables et de bureau. Vous pouvez aller plus loin et baser le plan d'alimentation sur l'heure de la journée, de sorte que les ordinateurs clients passent en mode veille plus rapidement en dehors des heures de bureau.

- Mettre à disposition d'ordinateurs portables des imprimantes uniquement lorsque les utilisateurs sont membres d'un groupe spécifique. Vous pouvez aller plus loin en mettant à disposition un groupe d'imprimantes à des ordinateurs qui répondent à certains critères, par exemple : portables, utilisés par un membre d'un groupe spécifique et dans un sous-réseau IP spécifique. Vous pouvez ensuite mettre à disposition une autre série d'imprimantes lorsque le sous-réseau IP change.
- Copier des modèles Microsoft Office en fonction de la langue du système d'exploitation installé sur l'ordinateur.
- Créer un raccourci si l'utilisateur est membre d'un groupe spécifique, si l'ordinateur a un nom spécifique (par exemple W10-001), si les critères de temps correspondent à un moment précis (par exemple entre 8 heures et 17 heures) et si l'utilisateur est connecté à un serveur Terminal Server à partir d'un ordinateur client avec une adresse IP dans une plage spécifiée (par exemple 10.5.5.10 et 10.5.5.15).

Démonstration : Configuration des préférences de stratégie de groupe

Cette démonstration montre comment :

- Créer une imprimante avec les préférences de stratégie de groupe
- Cibler la préférence
- Configurer un plan d'alimentation avec les préférences de stratégie de groupe
- Cibler la préférence
- Tester les préférences.

Procédure de démonstration

Créer une imprimante avec les préférences de stratégie de groupe

1. Sur **LON-DC1**, ajoutez une nouvelle imprimante locale et partagée sous le nom **Brother** en utilisant le pilote **Brother Color Leg Type1 Class Driver**.
2. Lancez la **GPMC**.
3. Dans la GPMC, créez un nouveau GPO nommé **Prefs** et liez le GPO au domaine.
4. Ouvrez le GPO pour modification et allez à **Configuration utilisateur\Préférences\Paramètres du Panneau de configuration\Imprimantes**.
5. Créez une imprimante partagée en utilisant l'imprimante **\LON-DC1\Brother**.

Cibler la préférence

- Ciblez la préférence pour les adresses IP dans la plage **172.16.0.50 - 172.16.0.99**.

Configurer un plan d'alimentation avec les préférences de stratégie de groupe

1. Allez dans **Configuration ordinateur\Préférences\Paramètres du Panneau de configuration\Options d'alimentation**.
2. Créez un nouveau plan d'alimentation nommé **Plan d'alimentation Adatum** et faites-en le plan de puissance actif.

Cibler la préférence

- Ciblez cette préférence pour les ordinateurs sous **Windows 10**.

Tester les préférences

1. Basculez vers **LON-CL1** puis actualisez si nécessaire les stratégies de groupe à l'aide de la commande suivante dans l'invite de commandes :

```
gpupdate /force
```

2. Connectez-vous, puis vérifiez la présence à la fois de l'imprimante **Brother sur LON-DC1** et du **Plan d'alimentation Adatum**.

Testez vos connaissances

| Question |
|---|
| Quels sont les paramètres de préférences de stratégie de groupe que vous pouvez utiliser pour configurer l'expérience utilisateur de Internet Explorer ? (Choisissez toutes les réponses applicables) |
| Sélectionnez la réponse correcte. |
| <input type="checkbox"/> Internet Explorer |
| <input type="checkbox"/> Raccourcis |
| <input type="checkbox"/> Registre |
| <input type="checkbox"/> Options d'alimentation |
| <input type="checkbox"/> Options de dossier |

Confirmez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|---|--------------------------|
| Vous pouvez utiliser un ciblage niveau élément pour limiter les préférences de stratégie de groupe en fonction de la forêt AD DS à laquelle appartient l'utilisateur. | <input type="checkbox"/> |

Question : Dans quels scénarios avez-vous utilisé les préférences de stratégie de groupe et le ciblage au niveau élément ?

Atelier pratique : Gestion des paramètres de l'utilisateur avec la stratégie de groupe

Scénario

A. Datum Corporation a mis en place Microsoft Office 2016 et vous souhaitez utiliser la stratégie de groupe pour configurer les paramètres de certaines applications Office 2016. Le service informatique utilise des scripts d'ouverture de session pour fournir aux utilisateurs le mappage des lecteurs aux dossiers partagés. Cependant, le maintien de ces scripts est un problème permanent, car ils sont vastes et complexes. Votre gestionnaire vous a demandé de mettre en œuvre le mappage des lecteurs en utilisant les préférences de stratégie de groupe pour supprimer des scripts d'ouverture de session.

Votre directeur vous a également demandé de placer sur le bureau un raccourci vers l'application Bloc-notes pour tous les utilisateurs qui appartiennent au groupe IT Security. En outre, vous devez ajouter le groupe de sécurité d'un nouvel administrateur de l'ordinateur en tant qu'administrateur local sur tous les serveurs.

Pour aider à réduire les tailles des profils, vous devez également configurer la redirection de dossiers pour rediriger plusieurs dossiers de profils vers le lecteur de base de chaque utilisateur. Enfin, vous devez compléter la conception GPO pour gérer les postes de travail des utilisateurs et la sécurité du serveur.

Objectifs

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

- Utiliser des modèles d'administration pour gérer les paramètres utilisateur
- Mettre en œuvre des paramètres en utilisant les préférences de stratégie de groupe
- Configurer la redirection de dossiers.

Configuration de l'atelier pratique

Durée approximative : 45 minutes

Ordinateurs virtuels : **22742A-LON-DC1**, **22742A-LON-DC2** et **22742A-LON-CL1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**.

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-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 :
 - o Nom d'utilisateur : **Administrateur**
 - o Mot de passe : **Pa55w.rd**.
 - o Domaine : **Adatum**
5. Répétez les étapes 2 à 4 pour **22742A-LON-DC2**.
6. Répétez les étapes 2 à 4 pour **22742A-LON-CL1**.

Exercice 1 : Utilisation de modèles d'administration pour gérer les paramètres utilisateur

Scénario

Dans le cadre de la mise en œuvre de stratégie de groupe pour configurer les paramètres des applications Office 2016, vous devez maintenant importer des modèles d'administration personnalisés pour Office 2016 et configurer les paramètres.

Les tâches principales de cet exercice sont les suivantes :

1. Importer des modèles d'administration pour Microsoft Office 2016.
2. Configurer les paramètres de Office 2016.
3. Appliquer et vérifier les paramètres sur l'ordinateur client.

► Tâche 1 : Importer des modèles d'administration pour Microsoft Office 2016

1. Sur **LON-DC1**, double-cliquez sur le fichier **E:\LabFiles\Mod06\admintemplates_x64_4390-1000_en-us.exe** et extrayez les fichiers vers le Bureau.
2. Copiez tous les fichiers et sous-dossiers du répertoire **C:\Users\Administrator\Desktop\admx** vers **C:\Windows\PolicyDefinitions**.

► Tâche 2 : Configurer les paramètres de Office 2016

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, lancez la **Gestion des stratégies de groupe**.
2. Créez un nouveau GPO nommé **Paramètres Office 2016**.
3. Modifiez le GPO.
4. Localisez le nœud **Configuration utilisateur\Stratégies\Modèles d'administration\Microsoft Excel 2016**.
5. Dans **Options Excel\Personnaliser le ruban**, activez le paramètre **Afficher l'onglet Développeur dans le ruban**.
6. Dans **Options Excel\Save**, activez le paramètre **Emplacement du fichier par défaut** et définissez **%userprofile%\Bureau** comme emplacement par défaut des fichiers.
7. Fermez l'Éditeur de gestion des stratégies de groupe.
8. Liez les paramètres **Office 2016** au domaine **Adatum.com**.

► Tâche 3 : Appliquer et vérifier les paramètres sur l'ordinateur client

1. Basculez vers **LON-CL1** et actualisez la stratégie de groupe.
2. Démarrez **Microsoft Excel 2016**.
3. Créez un classeur vide.
4. Vérifiez que l'onglet **Développeur** s'affiche sur le ruban.
5. Si l'onglet **Développeur** ne s'affiche pas sur le ruban, procédez comme suit :
 - a. Redémarrez **LON-CL1**.
 - b. Connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
 - c. Effectuez à nouveau les étapes 2-4.
6. Enregistrez le fichier et vérifiez que l'emplacement du fichier par défaut est le Bureau de l'utilisateur.
7. Fermez **Excel 2016**.

Résultats : Une fois cette opération terminée, vous devriez avoir développé avec succès des modèles d'administration avec des modèles pour Office 2016 et configuré certains paramètres Office en utilisant la stratégie de groupe.

Exercice 2 : Mise en œuvre des paramètres en utilisant les préférences de stratégie de groupe

Scénario

Vous avez maintenant à mettre en œuvre le mappage des lecteurs en utilisant les préférences de stratégie de groupe pour supprimer des scripts d'ouverture de session qu'A. Datum utilise actuellement pour fournir aux utilisateurs le mappage des lecteurs aux dossiers partagés. Vous devez également placer un raccourci sur le bureau vers l'application Bloc-notes pour tous les utilisateurs qui appartiennent au groupe IT Security.

Les tâches principales de cet exercice sont les suivantes :

1. Mettre en place l'environnement actuel.
2. Tester un lecteur mappé pour les utilisateurs de la succursale 1.
3. Créer un GPO de préférences avec les préférences de stratégie de groupe requises.
4. Tester les préférences.

► Tâche 1 : Mettre en place l'environnement actuel

1. Basculez vers **LON-DC1**.
2. Sur **LON-DC1**, ouvrez l'**Explorateur de fichiers** puis accédez à **E:\Labfiles\Mod06**.
3. Exécutez le script Windows PowerShell **Mod06-1.ps1**.
4. Copiez le fichier **BranchScript.cmd** dans le Presse-papiers.
5. Fermez la **Gestion des stratégies de groupe**.
6. Ouvrez le GPO **Branch1** pour configurer un script d'ouverture de session.
7. Collez le script **BranchScript.cmd** dans le dossier des scripts.
8. Ajoutez le script **BranchScript.cmd** au paramètre scripts de connexion du GPO.

► Tâche 2 : Tester un lecteur mappé pour les utilisateurs de la succursale 1

1. Basculez vers **LON-CL1**.
2. Redémarrez l'ordinateur.
3. Après le redémarrage de l'ordinateur, connectez-vous en tant qu'**Adatum\Abbi** avec le mot de passe **Pa55w.rd**.
4. Ouvrez l'**Explorateur de fichiers** et vérifiez que le lecteur **S** s'affiche.
5. Si le lecteur S n'est pas disponible, procédez comme suit :
 - a. Actualisez la stratégie de groupe.
 - b. Redémarrez **LON-CL1**.
 - c. Connectez-vous en tant qu'**Adatum\Abbi** avec le mot de passe **Pa55w.rd**.
 - d. Le lecteur S doit maintenant s'afficher dans l'Explorateur de fichiers.

► Tâche 3 : Créer un GPO de préférences avec les préférences de stratégie de groupe requises

1. Basculez vers **LON-DC1**.
2. Sur **LON-DC1**, ouvrez **Utilisateurs et ordinateurs Active Directory**.
3. Dans l'UO **IT**, créez un nouveau groupe de sécurité globale nommé **Administrateurs de l'ordinateur**.
4. Dans la GPMC, sur l'**UO Branch 1**, supprimez le lien pour le GPO **Branch 1**.
5. Créez un nouveau GPO nommé **Préférences** et liez-le au domaine.
6. Allez à **Configuration utilisateur\Préférences\Paramètres Windows\Raccourcis**.
7. Créez un nouveau raccourci vers Notepad.exe avec les paramètres suivants :
 - Nom : **Bloc-notes**
 - Action : **Créer**
 - Emplacement : **Tous les utilisateurs Bureau**
 - Chemin cible : **C:\Windows\System32\Notepad.exe**
8. Dans l'onglet **Commun**, désactivez la case **Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de la stratégie utilisateur)**.
9. Ciblez la préférence vers les membres du groupe **IT Security**.
10. Allez à **Configuration utilisateur\Préférences\Paramètres Windows\Mappage de lecteur**.
11. Créez un nouveau lecteur mappé avec les paramètres suivants :
 - Action : **Mise à jour**
 - Emplacement : **\LON-DC1\Branch1**
 - Se reconnecter : **Sélectionné**
 - Nom : **Lecteur pour succursale 1**
 - Utilisation : **S**
12. Dans l'onglet **Commun**, décochez la case **Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de la stratégie utilisateur)**.
13. Ciblez la préférence vers les utilisateurs dans l'UO **Succursale 1**.
14. Allez à **Ordinateur Configuration\Préférences\Paramètres du Panneau de configuration\Utilisateurs et groupes locaux**.
15. Mettez à jour le groupe Administrateurs local en utilisant les paramètres suivants :
 - Action : **Mise à jour**
 - Nom : **Administrateurs**
 - Ajouter un nouveau membre du groupe local : **Administrateur de l'ordinateur**
16. Sur l'onglet **Commun**, désactivez la case **Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de la stratégie utilisateur)**.
17. Ciblez la préférence vers les ordinateurs avec le système d'exploitation **Windows Server 2016 Technical Preview 5**.

18. Fermez toutes les fenêtres ouvertes, à l'exception de la **Gestion des stratégies de groupe** et du **Gestionnaire de serveur**.

► **Tâche 4 : Tester les préférences**

1. Basculez vers et redémarrez **LON-CL1**.
2. Connectez-vous en tant qu'**Adatum\Abbi** avec le mot de passe **Pa55w.rd**.
3. Ouvrez l'**Explorateur de fichiers** et vérifiez que le lecteur **S** s'affiche.



Remarque : L'étiquette de lecteur est désormais **Lecteur pour succursale 1**, ce qui valide le mappage du lecteur via les préférences de la stratégie de groupe.

4. Sur le bureau, vérifiez qu'un raccourci vers le Bloc-notes s'affiche.
5. Si le raccourci vers le Bloc-notes n'est pas disponible, procédez comme suit :
 - a. Actualisez la stratégie de groupe.
 - b. Redémarrez **LON-CL1**.
 - c. Connectez-vous en tant qu'**Adatum\Abbi** avec le mot de passe **Pa55w.rd**.
 - d. Le raccourci vers le Bloc-notes doit maintenant s'afficher sur le bureau.
6. Ouvrez la **Gestion de l'ordinateur**.
7. Dans la **Gestion de l'ordinateur**, accédez au nœud **Outils système\Utilisateurs et groupes locaux\Groupes**.
8. Vérifiez que le groupe **Administrateurs de l'ordinateur** n'est pas membre du groupe **Administrateurs**, car le paramétrage des préférences s'applique uniquement aux serveurs.
9. Déconnectez-vous de **LON-CL1**.

Résultats : Après avoir terminé cette opération, vous devriez avoir retiré avec succès les scripts d'ouverture de session, les paramètres de préférence configurés, puis avoir attribué les paramètres en utilisant les GPO.

Exercice 3 : Configuration de la redirection de dossiers

Scénario

Pour aider à réduire la taille des profils, vous décidez de configurer la redirection de dossiers pour les utilisateurs de la succursale, en redirigeant plusieurs dossiers de profils vers le lecteur de base de chaque utilisateur.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un dossier partagé pour stocker les dossiers redirigés
2. Créer un nouveau GPO et le lier à l'unité organisationnelle (UO) Succursale 1
3. Modifier les paramètres de redirection de dossiers dans la stratégie
4. Tester les paramètres de redirection de dossiers.

► **Tâche 1 : Créer un dossier partagé pour stocker les dossiers redirigés**

- Sur **LON-DC1**, ouvrez l'**Explorateur de fichiers**, créez un nouveau dossier en utilisant les propriétés suivantes, puis partagez-le avec des **Personnes spécifiques** :
 - Chemin : **C:\Branch1Redirect**
 - Nom de partage : **Branch1Redirect**
 - Autorisations : **Tout le monde, Lecture/écriture**

► **Tâche 2 : Créer un nouveau GPO et le lier à l'unité organisationnelle (OU)**

Succursale 1

- Sur **LON-DC1**, ouvrez la **Gestion des stratégies de groupe**, puis créez et liez un nouveau GPO nommé **Redirection de dossiers** à l'OU **Succursale 1**.

► **Tâche 3 : Modifier les paramètres de redirection de dossiers dans la stratégie**

1. Ouvrez le GPO **Redirection de dossiers** pour le modifier.
2. En dessous de **Configuration utilisateur**, accédez à **Stratégies\Paramètres Windows\Redirectation de dossiers**.
3. Configurez les propriétés du dossier **Documents** de manière à utiliser le paramètre **De base - Rediriger les dossiers de tout le monde vers le même emplacement**.
4. Veillez à ce que l'**emplacement du dossier cible** soit paramétré sur **Créer un dossier pour chaque utilisateur sous le chemin d'accès racine**.
5. Indiquez le chemin de racine **\LON-DC1\Branch1Redirect**.
6. Configurez les dossiers **Images** et **Musique** de manière à les rediriger vers le dossier **Documents**.
7. Fermez toutes les fenêtres actives sur **LON-DC1**.

► **Tâche 4 : Tester les paramètres de redirection de dossiers**

1. Basculez vers **LON-CL1**.
2. Connectez-vous en tant qu'**Adatum\Abbi** avec le mot de passe **Pa55w.rd**.
3. Dans la fenêtre de l'**Invite de commandes**, entrez la commande suivante pour actualiser la stratégie de groupe puis appuyez sur Entrée :

```
gpupdate /force
```

4. Déconnectez-vous, puis reconnectez-vous à **LON-CL1** en tant qu'**Adatum\Abbi** avec le mot de passe **Pa55w.rd**.
5. Ouvrez l'**Explorateur de fichiers** et vérifiez que, dans la boîte de dialogue des propriétés de **Documents**, l'emplacement est **\LON-DC1\Branch1Redirect\Abbi**.
6. Dans le dossier **Documents**, vérifiez l'existence des deux sous-dossiers **Musique** et **Images**.



Remarque : Cela permet de vérifier que **Musique** et **Images** sont également redirigés.

7. Déconnectez-vous de **LON-CL1**.

Résultats : Une fois cette opération terminée, vous devriez avoir configuré avec succès la Redirection de dossiers vers un dossier partagé sur le serveur **LON-DC1**.

Exercice 4 : Planifier la stratégie de groupe (en option)

Scénario

Vous êtes chargé de la planification d'un modèle GPO pour l'infrastructure actuelle afin de gérer la sécurité pour les postes de travail des utilisateurs et les serveurs. Vous devez finaliser le modèle de délégation pour les tâches administratives et déterminer les administrateurs qui ont des droits sur les ordinateurs clients.

Le management d'A. Datum souhaite également configurer les paramètres de Windows Update et restreindre les outils d'administration pour les comptes ordinaires de l'utilisateur. En outre, l'une des exigences de sécurité est que la société dispose d'un avertissement de conformité lié à une mauvaise utilisation des ordinateurs de l'entreprise.

En tant qu'administrateur de A. Datum, vous êtes chargé de traduire les impératifs professionnels en paramètres GPO. Vous devez ensuite concevoir et mettre en œuvre les GPO aux niveaux appropriés de la conception pour l'UO.

Dans cet exercice, vous allez concevoir la stratégie GPO qui répond aux exigences commerciales et organisationnelles d'A. Datum.

Documentation fournie avec le produit

Beth Burke

De : Huong Tang [Huong@adatum.com]

Envoyé : 2 juillet 11h43

À : Beth@adatum.com

Objet : Conception du GPO

Bonjour,

Comme nous l'avons discuté lors de notre réunion d'hier, nous avons besoin de renforcer la sécurité des serveurs et de configurer les postes de travail des utilisateurs en fonction de la première conception initiale.

J'ai ajouté les notes de notre réunion dans le document de proposition ci-joint. Veuillez lire le document.

J'apprécierais beaucoup que vous me fassiez parvenir le document de proposition mis à jour d'ici la fin de cette semaine.

Merci beaucoup,

Huong

Proposition de stratégie GPO d'A. Datum

Numéro de référence du document : BS00918/1

| | |
|--------------------|------------|
| Auteur du document | Beth Burke |
| Date | 2 juillet |

Présentation des exigences

Concevoir une stratégie GPO qui réponde aux exigences suivantes :

Proposition de stratégie GPO d'A. Datum

- Tous les ordinateurs de l'organisation devraient disposer d'un groupe de paramètres GPO de base qui doivent être appliqués. Ces paramètres sont notamment :
 - Configuration des comptes d'administrateur local
 - Configuration des paramètres de stratégie de mise à jour
 - Restriction de certaines options, telles que l'accès à l'éditeur de registre.

Ces paramètres ne sont pas applicables aux postes de travail administrateur.
- Chaque bureau devrait avoir un groupe de paramètres de base applicables aux postes de travail. À partir de maintenant, vous devez mettre en œuvre ce qui suit :
 - Afficher un avertissement de sécurité avant la connexion de l'ordinateur indiquant que seuls les employés d'A. Datum peuvent utiliser les ordinateurs. Ce paramètre doit être appliqué dans chaque site, avec un affichage automatique dans d'autres langues pour les sites étrangers.
 - Tous les utilisateurs doivent disposer d'un ensemble de lecteurs mappés qui leur sont assignés par défaut. Vous devez baser la définition du lecteur mappé sur l'appartenance à un département.
 - Les administrateurs informatiques centraux à Londres doivent être en mesure de gérer tous les GPO et les paramètres de l'organisation. Les administrateurs de chaque bureau devraient être en mesure de gérer uniquement les GPO applicables à ce bureau.

Synthèse des informations

La structure d'UO en support comprend les éléments suivants :

- Les utilisateurs sont actuellement regroupés par département dans une UO de niveau haut.
- Les clients sont dans l'UO clients de niveau haut, qui est divisé par site sur le niveau suivant.

Propositions

- Quelle exigence nécessitera la création d'un ou de plusieurs GPO ?
- Pouvez-vous répondre à l'une des exigences sans créer de GPO ?
- Existe-t-il des exceptions à l'application GPO par défaut que vous devez prendre en compte ?
- Lister les GPO que vous devez créer pour répondre aux exigences du scénario de l'atelier pratique. Fournir les informations suivantes dans le tableau fourni :
 - Nom du GPO
 - Exigences remplies par le GPO
 - Paramètres de configuration (stratégies de l'utilisateur, stratégies de l'ordinateur, préférences de l'utilisateur, préférences de l'ordinateur) que le GPO contiendra
 - Conteneur (domaine, UO, site) auquel le GPO sera lié

| Nom | Exigences remplies | Paramètres de configuration | S'applique aux éléments ci-dessous |
|-----|--------------------|-----------------------------|------------------------------------|
| | | | |

Proposition de stratégie GPO d'A. Datum

| | | | |
|--|--|--|--|
| | | | |
| | | | |
| | | | |
| | | | |

- Listez d'autres tâches de configuration que vous devez effectuer au sein de la console de gestion des stratégies de groupe pour répondre aux exigences du scénario.

Les tâches principales de cet exercice sont les suivantes :

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

► **Tâche 1 : Lire la documentation fournie avec le produit**

- Lisez la documentation fournie.

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

- Répondez aux questions de la section Propositions du document Proposition de stratégie GPO pour A. Datum.

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

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

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

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

Résultats : À la fin de cet exercice, vous devrez avoir configuré une stratégie GPO.

► Tâche 5 : Préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 à 3 pour **22742A-LON-DC2** et **22742A-LON-CL1**.

Question : Quelles sont les options que vous pouvez utiliser pour séparer les dossiers redirigés des utilisateurs vers des serveurs différents ?

Question : Pouvez-vous nommer deux méthodes que vous pouvez utiliser pour attribuer un GPO à des objets sélectionnés au sein d'une UO ?

Question : Vous avez créé des préférences de stratégie de groupe pour configurer de nouvelles options d'alimentation. Comment pouvez-vous vous assurer qu'elles s'appliquent uniquement aux ordinateurs portables ?

Révision du module et éléments à retenir

Bonnes Pratiques

Meilleures pratiques en matière de gestion des stratégies de groupe :

- Lors de la configuration des paramètres dans un GPO, inclure des commentaires sur les paramètres GPO
- Utiliser un magasin central pour les modèles d'administration
- Utiliser les préférences de stratégie de groupe pour configurer les paramètres qui ne sont pas disponibles dans les paramètres de stratégie de groupe.

Problèmes courants et conseils de dépannage

| Problème courant | Conseil pour la résolution du problème |
|--|--|
| Vous avez configuré la redirection de dossiers pour une UO, mais aucun des dossiers des utilisateurs n'est redirigé vers l'emplacement réseau. Quand vous regardez dans le dossier racine, vous constatez que le sous-répertoire pour chaque utilisateur a été créé, mais qu'il est vide. | |
| Vous avez des ordinateurs fonctionnant sous Windows 7 et sous Windows 10. Après avoir configuré plusieurs paramètres dans les modèles d'administration d'un GPO, les utilisateurs sous les systèmes d'exploitation Windows 7 indiquent que certains paramètres s'appliquent et que d'autres ne s'appliquent pas. | |

| Problème courant | Conseil pour la résolution du problème |
|---|--|
| Les préférences de stratégie de groupe ne s'appliquent pas. | |

Questions de contrôle des acquis

Question : Pourquoi certains paramètres de stratégie de groupe nécessitent-ils deux signatures avant de prendre effet ?

Question : Quel est l'avantage d'utiliser un magasin central ?

Question : Quelle est la principale différence entre les paramètres de stratégie de groupe et les préférences de stratégie de groupe ?

Module 7

Sécurisation des services de domaine Active Directory

Sommaire :

| | |
|--|-------------|
| Vue d'ensemble du module | 7-1 |
| Leçon 1 : Sécurisation des contrôleurs de domaine | 7-2 |
| Leçon 2 : Implémentation de la sécurité du compte | 7-16 |
| Leçon 3 : Mise en œuvre d'authentification d'audit | 7-37 |
| Leçon 4 : Configuration des comptes de services administrés | 7-42 |
| Atelier pratique : sécurisation AD DS | 7-50 |
| Révision du module et Takeaways | 7-61 |

Vue d'ensemble du module

Dans l'infrastructure de la technologie informatique de votre organisation (IT), la sécurisation des contrôleurs de domaine Active Directory (AD DS) est une tâche critique. Les contrôleurs de domaine permettent d'accéder à de nombreuses ressources différentes et ils contiennent des informations sur les utilisateurs et leurs mots de passe. Si un contrôleur de domaine unique est compromis, tous les objets dans le même domaine Active Directory ou dans tout domaine approuvé sont à risque d'être compromis, aussi.

Le système d'exploitation Windows Server 2016 fournit des fonctionnalités et applications que vous pouvez utiliser pour aider à sécuriser votre réseau contre les menaces de sécurité. Le système d'exploitation fournit des mesures pour sécuriser les contrôleurs de domaine en minimisant leur surface d'attaque et en déterminant les placements du domaine-contrôleur. Le système d'exploitation détermine également les rôles AD DS qui sont utilisés pour l'administration, la conception et met en œuvre la sécurité des mots de passe, en plus de l'audit lorsque des attaques se produisent. Vous pouvez également utiliser les contrôleurs de domaine pour déployer des mesures de sécurité à d'autres clients et serveurs dans votre infrastructure Windows.

Les administrateurs AD DS doivent comprendre les menaces qui pèsent sur les contrôleurs de domaine et les méthodes qu'ils peuvent utiliser pour sécuriser AD DS et ses contrôleurs de domaine.

Objectifs

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

- Sécuriser les contrôleurs de domaine ;
- Mettre en œuvre la sécurité du compte ;
- Mettre en œuvre l'authentification de l'audit ;
- Configurer les comptes de service (MSA).

Leçon 1

Sécurisation des contrôleurs de domaine

Les contrôleurs de domaine de votre réseau sont au cœur de votre infrastructure AD DS. Ils contiennent toutes vos informations compte-utilisateur et, sans eux, les utilisateurs ne peuvent pas se connecter au réseau ou accéder aux ressources dont ils ont besoin pour effectuer leur travail. Lorsque les comptes d'utilisateurs sont compromis, d'autres comptes dans le même domaine et tout domaine approuvé aussi pourraient être compromis. Par conséquent, la sécurisation de vos contrôleurs de domaine est un élément essentiel dans la sécurisation de votre infrastructure informatique.

Objectifs des leçons

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

- Décrire les risques de sécurité qui peuvent affecter les contrôleurs de domaine ;
- Expliquer comment modifier les paramètres de sécurité des contrôleurs de domaine ;
- Mettre en œuvre une authentification sécurisée ;
- Sécuriser l'accès physique aux contrôleurs de domaine ;
- Décrire les contrôleurs de domaine (RODC) en lecture seule ;
- Déployer un RODC ;
- Planifier et configurer une stratégie de réPLICATION de mot de passe RODC ;
- Configurer une stratégie de réPLICATION de mot de passe ;
- Décrire la séparation des rôles pour les administrateurs locaux RODC.

Les risques de sécurité qui peuvent affecter les contrôleurs de domaine

Avant de définir les mesures de sécurité, vous devez déterminer les menaces contre lesquelles vous aurez besoin pour protéger votre réseau. Vous devez définir les limites de sécurité de votre organisation et vous devez identifier d'où les pirates ou les attaquants pourraient essayer de compromettre votre sécurité. Par exemple, vous aurez besoin de sécuriser votre réseau contre les attaques de l'extérieur de votre entreprise. Vous pourriez aussi avoir des régions, des départements ou des groupes où vous ne pouvez pas faire confiance aux employés de votre organisation de la même manière que vous faites confiance aux employés dans un environnement strictement contrôlé, comme votre bureau principal. Avez-vous des groupes d'administration dont vous n'avez pas confiance ? Avez-vous des sites ou services qui nécessitent un niveau de sécurité plus élevé ? Tous ces facteurs auront un impact sur votre planification de la sécurité.

- Les contrôleurs de domaine sont des cibles idéales pour les attaques et les ressources les plus importantes à sécuriser
- Les risques de sécurité comprennent :
 - La sécurité du réseau
 - Les attaques d'authentification
 - L'élevation de privilège
 - Les attaques DoS
 - Les attaques sur le système d'exploitation, les services ou les applications
 - Les risques opérationnels
 - Les menaces sur la sécurité physique

Pour sécuriser votre domaine Active Directory et les contrôleurs de domaine, vous devez gérer la sécurité en fonction des risques suivants :

- Sécurité Internet. Un attaquant doit avoir accès à votre réseau pour obtenir de plus amples informations. Par conséquent, vous devez vous assurer que le réseau des frontières, tels que les pare-feu et services exposés, sont très protégés. En outre, vous devez vous assurer que vos réseaux sans fil

sont fixés correctement et ne permettent pas d'appareils non sécurisés de se connecter à votre réseau interne. Utilisez des certificats pour les connexions sans fil et mettre en œuvre Network Access Protection (NAP) pour sécuriser l'accès au réseau.

- Attaques d'authentification. L'accès aux informations d'authentification, tels que les noms d'utilisateur et mots de passe, est la cible principale pour toute personne qui tente d'accéder à votre réseau et aux données. Les contrôleurs de domaine Active Directory stockent toutes les informations sur tous les utilisateurs et leurs mots de passe et ils ont besoin de sécurité suffisante pour protéger ces informations.
- Elévation de privilège Bien que régulièrement, les informations d'identification de l'utilisateur peuvent accéder à certaines informations, les administrateurs de domaine ou d'autres groupes d'administration ont élevé des priviléges, en donnant à ces comptes le contrôle de données. Dans de nombreux cas, les administrateurs peuvent s'accorder un accès supplémentaire aux ressources. En outre, ils peuvent configurer les mesures de sécurité. Si les attaquants peuvent accroître les pouvoirs qu'ils utilisent en mettant leurs comptes en groupes élevés dans les mêmes ou de confiance domaines, ils peuvent réduire les garanties de sécurité et potentiellement contourner l'audit ou les sauvegardes de sécurité.
- Attaque par déni de service. Un utilisateur ou des utilisateurs malveillants ne lancent pas d'attaques DoS pour accéder aux données, mais plutôt pour désactiver des services, des systèmes ou des infrastructures entières. Certaines mesures de sécurité, telles que les politiques de verrouillage de compte, pourraient être utiles pour protéger votre réseau contre certaines menaces, mais elles fournissent également une surface facilement accessible d'attaque DoS.
- Système d'exploitation, service ou application d'attaques. Les systèmes d'exploitation de réseau, en plus des services et des applications qui prennent en charge la communication sur les réseaux, sont vulnérables aux attaques de sécurité. Ces systèmes fournissent une communication sur un réseau et les attaquants vont essayer de tromper les communications attendues pour faire que ces services fassent quelque chose différemment de ce qui était prévu.
- Les risques opérationnels. Il est important de maintenir l'infrastructure de toute organisation correctement. Tout type de logiciel qui fonctionne sur des réseaux pourrait être une cible potentielle pour les attaquants. Pour renforcer la sécurité, les fournisseurs de logiciels et de matériel informatique doivent offrir des mises à jour régulièrement. Les administrateurs doivent garder leurs systèmes mis à jour et supprimer ou désactiver tous les comptes d'utilisateurs et d'ordinateurs inutilisés qui sont susceptibles d'avoir des mots de passe non sécurisés. Les autorisations accordées doivent être vérifiées et contrôlées régulièrement pour veiller à ce qu'elles ne laissent pas un réseau vulnérable.
- Menaces de sécurité physique. Il est important pour les contrôleurs de domaine Active Directory d'être physiquement sécurisé. Si quelqu'un obtient un accès physique à un serveur, il est plus facile de désactiver les mesures de sécurité et exécuter localement des logiciels malveillants pour récupérer tous les mots de passe dans un domaine.

Modification des paramètres de sécurité des contrôleurs de domaine

Un domaine Active Directory comprend habituellement plusieurs contrôleurs de domaine. Pour veiller à ce que tous les paramètres de sécurité s'appliquent systématiquement à tous les contrôleurs de domaine, vous devez configurer les paramètres de sécurité pour les contrôleurs de domaine Active Directory centralisée. Pour ce faire, utilisez l'objet de stratégie Contrôleurs de domaine par défaut de groupe (GPO), ou créer un nouveau GPO personnalisé qui est lié à l'unité d'organisation des contrôleurs de domaine (UO). Vous créez tous les comptes d'ordinateur de domaine contrôleur dans cette unité d'organisation, vous ne devriez pas les sortir de cette unité, car ils vont tomber hors du champ des contrôleurs de domaine par défaut.

- Utilisez un GPO pour appliquer les mêmes paramètres de sécurité à tous les contrôleurs de domaine
- Pensez à personnaliser les GPO liés aux contrôleurs de domaine UO
- Les options de sécurité comprennent :
 - Les stratégies de compte telles que les mots de passe et le verrouillage de compte
 - Les politiques locales telles que l'audit, les droits d'utilisateur et les options de sécurité
 - La configuration des journaux d'événements
 - Les groupes restreints
 - Les services de sécurité du système
 - Le pare-feu Windows avec fonctions avancées de sécurité
 - Les stratégies de clé publique
 - La vérification avancée

Certaines organisations préfèrent utiliser un autre GPO que la stratégie des contrôleurs de domaine par défaut. Lors de la configuration des paramètres de sécurité, il est possible d'appliquer des paramètres qui pourraient être trop sûrs. Par exemple, vous pouvez configurer les politiques qui verrouillent sur certains groupes ou des politiques administratives qui empêchent quiconque d'accéder au domaine. Bien qu'il soit simple de dissocier ou de désactiver un GPO personnalisé, vous ne devriez pas désactiver ou dissocier la Stratégie de Contrôleurs de Domaine par défaut. Pour cette raison, nous vous recommandons de créer un GPO personnalisé et un lien pour les contrôleurs de domaine OÜ au lieu de modifier la politique par défaut des contrôleurs de domaine.

Stratégie de domaine par défaut vs. Stratégie de Contrôleurs de domaine.

Il y a deux GPO par défaut, la Stratégie de Domaine par Défaut et la Stratégie des contrôleurs de Domaine par défaut et il est essentiel de comprendre les différences entre les deux :

- Stratégie de Domaine par Défaut GPO. Ce GPO est lié au domaine et il s'applique à tous les utilisateurs et les ordinateurs, y compris les ordinateurs clients, les contrôleurs de domaine et les serveurs du domaine. Vous devez utiliser cette politique et d'autres qui pointent vers un domaine avec soin. Cette politique ne doit contenir que les paramètres qui sont explicitement destinés à appliquer à tous les objets dans une organisation.
- Stratégie de contrôleurs de domaine par défaut Ce GPO est relié aux contrôleurs de domaine UO et il s'applique à tous les contrôleurs de domaine dans le domaine. Ceci est le GPO dans lequel vous configurez la plupart des paramètres de sécurité qui se rapportent aux contrôleurs de domaine.

Paramètres de sécurité disponibles dans les stratégies de groupe.

Voici quelques-uns des paramètres de sécurité les plus importants que vous pouvez configurer dans un GPO. Vous pouvez trouver les **paramètres de sécurité** dans tout **GPO sous Configuration ordinateur\Stratégies\Paramètres Windows** :

- **Stratégies de comptes** Sous ce nœud, vous pouvez configurer la politique de mot de passe, la politique de verrouillage de compte et la politique de Kerberos. Ces paramètres s'appliquent uniquement aux comptes d'utilisateurs locaux des ordinateurs auxquels la politique s'applique, sauf si vous configurez les paramètres de la stratégie par défaut de domaine. Seules les stratégies de compte que vous configurez dans le Default Domain Policy s'appliquent à tous les comptes de domaine.
- **Stratégies locales**. Ce nœud contient trois des plus importants nœuds pour la configuration de sécurité :
 - **Stratégie d'audit** Ces paramètres configurent l'audit des politiques qui s'appliquent à toutes les versions de système d'exploitation Windows. Toutefois, si vous avez Windows Server 2008 R2 et

Windows 7 ou plus récent déployés dans votre réseau, nous vous recommandons d'utiliser la configuration politique de vérification avancée à la place de ces politiques d'audit.

- **Attribution des droits utilisateur** Ces paramètres configurent de nombreux paramètres de sécurité applicables aux droits des utilisateurs. Par exemple, vous pouvez spécifier qui peut accéder à l'ordinateur à partir du réseau, qui peut se connecter localement ou via Remote Desktop Services (RDS), et qui est capable de changer le temps ou éteindre l'ordinateur. Pour les contrôleurs de domaine, vous pouvez également spécifier qui est capable de synchroniser les données des services d'annuaire.
- **Options de sécurité** Ces paramètres contiennent des paramètres de sécurité importants, y compris les options pour la gestion des comptes par défaut, tels que les comptes Clients et Administrateur et ces options portent également sur la gestion des périphériques, les contrôleurs de domaine, les protocoles de sécurité de domaine membre, les paramètres de sécurité d'ouverture de session, l'accès au réseau et les paramètres de sécurité parmi d'autres.
- **Journaux des événements.** Sous ce nœud, vous pouvez configurer des paramètres tels que la taille du journal des événements, la méthode de rétention et la durée de rétention pour l'application par défaut, la sécurité et les journaux d'événements du système. Il est important d'avoir tous les journaux de sécurité sur les contrôleurs de domaine configurés de manière identique. Si vous configurez le journal de sécurité sur un contrôleur de domaine pour conserver les journaux pendant six jours et un autre conserve les journaux pour seulement trois jours, vous recevez des résultats incohérents, en fonction du contrôleur de domaine sur lequel vous effectuez la recherche.
- **Groupes restreints** Sous ce nœud, vous pouvez définir deux propriétés pour les groupes sensibles à la sécurité (ou groupes restreints). Pour chaque groupe que vous ajoutez ici, vous pouvez définir les **Membres** et le **Membre** d'attributs. Pour les groupes que vous configurez comme restreints, vous ne pouvez pas modifier l'appartenance en utilisant d'autres outils, tels que les **utilisateurs et les ordinateurs Active Directory**.
- **Services système.** Sous ce nœud, vous pouvez définir des autorisations de comportement et de sécurité de démarrage pour les services système en utilisant les GPO. Cela vous permet de désactiver tous les services qui ne sont pas nécessaires pour un rôle de serveur spécifique, comme un contrôleur de domaine.
- **Pare-feu Windows avec fonctions avancées de sécurité.** Ce réglage vous permet d'administrer le pare-feu Windows avec sécurité avancée au centre. En utilisant un GPO pour configurer les paramètres du pare-feu Windows, vous pouvez vous assurer que tous les serveurs qui fournissent les mêmes services, tels que les contrôleurs de domaine, ont une configuration cohérente Pare-feu Windows.
- **Stratégies de clé publique** Sous ce nœud, vous configurez les paramètres qui reposent sur une infrastructure à clé publique (PKI), tels que le Encrypting File System (EFS) et sa clé de récupération, BitLocker Drive Encryption, les Paramètres de Demande de Certificat Automatique (auto-inscription) et les Autorités de Certification de Racine de Confiance, parmi d'autres.
- **Configuration de la stratégie avancée de vérification.** Les paramètres sous ce nœud permettent une stratégie de configuration plus étendue que la stratégie de vérification sous le nœud Stratégies locales. Lorsque vous ciblez Windows Server 2008 R2 ou plus récent, ou Windows 7 ordinateurs ou plus récent, nous vous recommandons d'utiliser les nouveaux paramètres de configuration avancée Policy Audit.

Mettre en œuvre une authentification sécurisée

Avoir un processus d'authentification sécurisé est l'un des composants de sécurité les plus importants de votre environnement de domaine et vous devez tenir compte des facteurs suivants lors de la mise en œuvre d'une authentification sécurisée :

- Sécuriser les comptes d'utilisateur et les mots de passe. Il est très important de sécuriser les comptes d'utilisateurs et mots de passe. Pour ce faire, la configuration et l'utilisation de composants techniques, telles que la configuration des politiques de mot de passe et des comptes et aussi l'éducation de vos utilisateurs sur la façon de créer et d'utiliser des mots de passe longs et complexes. Si vos applications prennent en charge les mots de passe longs, enseignez aux utilisateurs comment utiliser phrases clés pour remplacer les mots de passe.
- Sécuriser les groupes avec des autorisations élevées. Chaque organisation a des groupes avec des autorisations élevées. Ces groupes comprennent les Admins du domaine, Administrateurs du schéma et les Groupes Administrateurs de l'entreprise. La mise en œuvre des processus de gestion sécurisée pour ces groupes est important. Par exemple, vous pouvez limiter qui connaît les mots de passe pour les membres de ces groupes et veiller à ce que tous les administrateurs aient des comptes administratifs spéciaux et qu'ils signent dans seulement avec ces comptes lors de l'exécution des tâches administratives. Pour ces groupes, vous pouvez également utiliser le paramètre Groupes restreints dans la stratégie de groupe, qui une section ultérieure de ce module, les détails.
- Évaluer les modifications de l'objet de critiques. Pour suivre toutes les modifications apportées aux groupes administratifs critiques, tels que les comptes intégrés, les groupes intégrés et en particulier des groupes avec des autorisations élevées, configurer votre stratégie d'audit pour suivre toutes les modifications apportées à ces groupes. Si possible, veiller à ce que seuls les membres d'une équipe d'audit ont accès aux événements audités, ce qui va empêcher les administrateurs de supprimer des événements.
- Mettre en œuvre une authentification sécurisée L'authentification à deux facteurs est la clé pour atteindre une sécurité renforcée, au-delà de nom d'utilisateur et mot de passe des informations d'identification régulières. Il est courant d'utiliser des cartes à puce pour sécuriser l'authentification ou de mettre en œuvre l'authentification multi-facteur avec les téléphones mobiles. Les cartes à puce ont un certificat stocké qui agit comme les informations d'identification d'un utilisateur pour la connexion, plutôt que d'un nom d'utilisateur et mot de passe. Pour authentifier en utilisant une carte à puce, vous devez posséder la carte à puce et vous devez avoir le numéro d'identification personnel (NIP) ou mot de passe pour déverrouiller la clé privée. La combinaison de la clé publique, connu du contrôleur de domaine et la clé privée de la carte à puce, permet au contrôleur de domaine pour authentifier l'utilisateur. Vous pouvez également appliquer l'utilisation de cartes à puce si les utilisateurs veulent accéder à des applications supplémentaires et sur RDS. Si vous utilisez les téléphones intelligents comme un deuxième facteur d'authentification, vous pouvez obliger les utilisateurs à utiliser l'application, un message texte, ou par téléphone pour prouver leur identité.
- Sécurisation des activités du réseau. La sécurisation du réseau est nécessaire lors de la tentative de parvenir à une infrastructure client / serveur sécurisé. Si votre organisation prend en charge les réseaux sans fil, veiller à ce que tous les réseaux avec l'accès aux serveurs de votre organisation soient sécurisés, de préférence en utilisant des certificats. Si nécessaire, fournir des réseaux publics ou clients pour permettre à des clients, des partenaires ou d'autres non-employées d'avoir accès à Internet, plutôt que de leur permettre l'accès au réseau d'entreprise. Pour vos réseaux câblés, envisager un dispositif d'attestation sanitaire pour empêcher les périphériques inconnus de se connecter à votre

Tenez compte des facteurs suivants lors de la mise en œuvre d'une authentification sécurisée :

- Sécurisation des comptes et des mots de passe d'utilisateur
- Sécurisation des groupes avec autorisations élevées
- Audit des modifications d'objets critiques
- Déploiement d'une authentification sécurisée, à l'instar des cartes à puce ou des authentifications multi-facteurs
- Sécurisation de l'activité réseau
- Réalisation des processus de retrait et de nettoyage
- Sécurisation des ordinateurs clients

réseau. Pour les serveurs critiques qui hébergent des informations hautement confidentielles, envisager l'application de la sécurité du protocole Internet (IPsec) signatures ou cryptage pour sécuriser les communications réseau.

- Établir des processus de déprovisionnement et de nettoyage. Fondamentalement, le *provisionnement* autorise un nouvel employé en créant son compte, ses abonnements aux groupes, sa boîte aux lettres et d'autres composants dont il a besoin pour travailler dans votre organisation. Bien que l'approvisionnement est important, vous devez vous rappeler que le *déprovisionnement* souvent oublié est encore plus important. Vous devez définir et mettre en place des processus pour les employés qui démissionnent volontairement et plus important, involontairement. En outre, envisager d'autres raisons pour lesquelles un employé peut prendre un congé, comme le congé parental ou un congé sabatique. Définir quel type d'accès, le cas échéant, est nécessaire. En outre, vous devez décider de désactiver les comptes, supprimer des comptes, ou supprimer des comptes de certains groupes, tels que les listes de distribution généraux ou les ressources humaines critiques (RH) des applications et de décider d'autoriser ou d'empêcher l'accès par les utilisateurs qui sont à l'extérieur du réseau de votre entreprise.

Un processus de nettoyage est également nécessaire pour les membres du domaine, comme pour les ordinateurs clients, car ils sont également autorisés à authentifier sur le domaine, un utilisateur malveillant peut utiliser leurs pouvoirs afin de compromettre un réseau. De plus, assurez-vous qu'il n'y a pas des ordinateurs clients ou d'utilisateurs qui ont été créés, mais qui ne sont pas utilisés pour se connecter au domaine. Ceci est parce que leurs mots de passe sont par défaut, les mots de passe bien connu, qu'un utilisateur malveillant pourrait découvrir et utiliser.

- Ordinateurs clients NetBIOS Si vous souhaitez sécuriser vos AD DS et les contrôleurs de domaine Active Directory, vous devez sécuriser vos ordinateurs clients. Les ordinateurs clients mettent en cache les 10 dernières connexions, par défaut. Par conséquent, si un ordinateur client est perdu, vous devez avoir un processus par lequel vous suivez les comptes qui ont signé à l'intérieur de l'intervalle de changement de mot de passe et vous avez besoin de savoir comment faire pour réinitialiser les mots de passe après une perte est signalée. Vous devez également protéger votre réseau interne à partir d'ordinateurs clients qui se connectent à partir de réseaux filaires ou sans fil des maisons, des hôtels ou des aéroports. Pour protéger les ordinateurs clients, veiller à ce que les ordinateurs clients disposent de toutes les mises à jour de sécurité installés, qu'ils ont la protection antivirus actuelle et un pare-feu basé sur l'hôte et envisager d'utiliser le chiffrement de lecteur telles que le chiffrement de lecteur BitLocker.

Sécurisation de l'accès physique aux contrôleurs de domaine

La sécurité physique des contrôleurs de domaine est d'une importance cruciale. Les contrôleurs de domaine contiennent toutes les informations d'identification dans un domaine Active Directory de votre organisation. Si les attaquants obtiennent un accès physique à vos contrôleurs de domaine, ils peuvent contourner presque toutes les garanties que vous avez. Ils peuvent ensuite accéder à la plupart des mots de passe rapidement et ils peuvent utiliser cette information pour attaquer votre réseau.

Par conséquent, vous devez suivre les étapes suivantes pour sécuriser davantage vos contrôleurs de domaine Active Directory, y compris que vous :

Lors de la sécurisation de l'accès physique à vos contrôleurs de domaine, prenez en compte ceci :

- Déployez uniquement les contrôleurs de domaine pour lesquels la sécurité physique est assurée ;
- Utilisez les RODC ;
- Utilisez BitLocker sur les volumes de disques de contrôleurs de domaine ;
- Surveillez les systèmes de disques remplaçables à chaud, car ils peuvent conduire au vol du contrôleur de domaine ;
- Protégez les disques virtuels ; les administrateurs d'ordinateurs virtuels doivent être très fiables ;
- Stockez les sauvegardes dans en lieu sûr.

- Déployez uniquement les contrôleurs de domaine où l'on peut assurer la sécurité physique. Si vos emplacements de serveur ne sont pas des salles dédiées avec contrôle d'accès, ne mettez pas un contrôleur de domaine dans cet environnement.
- Utilisez des disques SSD dans la mesure du possible. Vous pouvez utiliser RODC comme contrôleurs de domaine dans des endroits avec une sécurité physique moindre parce que, par défaut, les RODC ne stockent pas secrets tels que les mots de passe. Une autre section pour les détails de cette leçon sur les RODC.
- Cliquez sur Chiffrement de lecteur BitLocker. Pour fournir un niveau supplémentaire de sécurité, envisager de chiffrer le domaine contrôleur de disques durs en utilisant BitLocker. Cela empêche les pirates d'accéder aux données sur les disques durs du serveur si elles sont retirées des serveurs. Windows Server 2016 prend en charge l'utilisation de BitLocker sur les volumes qui stockent les bases de données AD DS. Cependant, il ne supporte pas l'utilisation d'EFS pour protéger les fichiers de base de données AD DS.
- Surveillez les systèmes de disques hot swap. Généralement, les serveurs se déploient avec des systèmes de disques *hot swap*, qui vous permettent de changer un lecteur sans interruption du serveur en cas de panne matérielle. Si vous disposez d'une matrice redondante de disques indépendants (RAID) de niveau 1 dans vos serveurs, assurez-vous que la surveillance est en place, de sorte que vous savez si des disques ont été supprimés ou échangés. Sinon, il est simple de supprimer et éventuellement de remplacer un lecteur de votre contrôleur de domaine. Si quelqu'un possède le disque dur de votre contrôleur de domaine, il ou elle a la même capacité à exploiter le système comme ils le feraient si elles avaient tout contrôleur de domaine.
- Protéger les disques virtuels. De nombreuses organisations déploient des contrôleurs de domaine en tant que machines virtuelles. Les disques virtuels utilisés par les machines virtuelles doivent être aussi sûrs que les disques physiques et les administrateurs de votre infrastructure virtuelle doivent être aussi fiables que vos administrateurs de domaine. Parfois, la gestion d'une infrastructure virtuelle dédiée aux composants critiques tels que les contrôleurs de domaine répond à ces risques.
- Stockez les sauvegardes dans des endroits sûrs. Vos sauvegardes domaine-contrôleur contiennent toutes les mêmes informations que les contrôleurs de domaine. Assurez-vous que les sauvegardes sont stockées dans des endroits sûrs, dont seuls les administrateurs de confiance peuvent accéder.

À quoi servent les RODC ?

Les succursales présentent un défi unique pour le personnel informatique d'une organisation. Les succursales sont généralement de petits sites dans lesquels aucun centre de données n'existe. En outre, les succursales pourraient ne pas avoir une installation sûre dans laquelle loger les serveurs et qu'il pourrait ne pas y avoir assez, voire aucun personnel IT pour prendre en charge les serveurs. Si un lien réseau étendu (WAN) sépare une succursale de votre site pivot, en fonction du nombre d'utilisateurs et les services qui sont disponibles dans la succursale, vous devez décider

| Centre de traitement de données | Succursale |
|---|--|
| <ul style="list-style-type: none"> Windows Server 2008 réinscriptible ou contrôleur de domaine plus récent Stratégie de réplication du mot de passe : <ul style="list-style-type: none"> Indique l'utilisateur et les mots de passe d'ordinateur que le RODC peut mettre en cache  | <ul style="list-style-type: none"> RODC : <ul style="list-style-type: none"> Tous les objets Sous-ensemble d'attributs : <ul style="list-style-type: none"> Aucun secret Non accessible en écriture Connexion des utilisateurs : <ul style="list-style-type: none"> Le RODC transfère l'authentification Le mot de passe est mis en cache : <ul style="list-style-type: none"> Si la politique de réplication du mot de passe le permet Détient un groupe d'administrateurs locaux  |

si vous voulez placer un contrôleur de domaine dans la succursale. AD DS dans Windows Server 2008 et les versions plus récentes prennent en charge un nouveau type de contrôleur de domaine, *un contrôleur de domaine en lecture seule* ou RODC, qui se déploie dans ce type d'environnement.

Raisons pour le déploiement des RODC

Si vous ne déployez pas un contrôleur de domaine dans une succursale, vous devez utiliser un lien WAN pour diriger les activités d'authentification et d'un service de billets sur le site hub. Lorsqu'un utilisateur tente d'abord d'accéder à un service spécifique, le client de l'utilisateur demande un ticket de service à partir d'un contrôleur de domaine. Les utilisateurs se connectent généralement à plusieurs services au cours d'une journée de travail, de sorte que l'activité de service-ticket arrive régulièrement.

Authentification et activité de ticket de service sur une liaison WAN entre une succursale et un site hub peuvent entraîner un ralentissement des performances ou peu fiables.

Si vous placez un contrôleur de domaine dans une succursale, l'authentification se produit plus efficacement. Cependant, il y a plusieurs problèmes potentiellement importants, qui comprennent:

- Un contrôleur de domaine conserve une copie de tous les attributs de l'objet dans son domaine, y compris des informations sécurisées, telles que les mots de passe de l'utilisateur. Si un pirate accède ou vole un contrôleur de domaine, ou son disque dur ou un lecteur de sauvegarde, un utilisateur malveillant déterminé pourrait identifier les noms et mots de passe d'utilisateur valides. À ce moment, l'ensemble de votre domaine est compromis et vous auriez à réinitialiser les mots de passe pour chaque utilisateur et compte d'ordinateur dans le domaine. La sécurité du serveur dans les succursales est souvent pas idéale, donc un contrôleur de domaine d'une succursale constitue un risque de sécurité considérable.
- Les modifications apportées à la base de données Active Directory sur un contrôleur de domaine d'une succursale sont répliquées sur le site hub et à d'autres contrôleurs de domaine de cet environnement. Par conséquent, la corruption d'un contrôleur de domaine dans une succursale présente un risque pour l'intégrité des AD DS de l'organisation. Par exemple, un administrateur de la succursale qui effectue une restauration du contrôleur de domaine à partir d'une sauvegarde obsolète pourrait entraîner des répercussions importantes sur l'ensemble du domaine.
- Un contrôleur de domaine de la succursale pourrait exiger l'entretien, comme par exemple l'installation de nouveaux pilotes de périphérique. Pour effectuer la maintenance sur un contrôleur de domaine standard, vous devez vous connecter en tant que membre du groupe Administrateurs, qui signifie que vous êtes effectivement un administrateur du domaine. Il ne serait pas approprié d'accorder ce niveau de capacité à une équipe de soutien de la succursale.

Ces préoccupations peuvent laisser des organisations à une décision difficile. Pour cette raison, Microsoft a introduit le RODC, qui répond à ce scénario de la succursale. Un domaine en lecture seule est un contrôleur de domaine qui conserve une copie de tous les objets et les attributs dans le domaine, à l'exception des informations sécurisées telles que les propriétés liées aux mots de passe. Si vous ne configurez pas la mise en cache, un RODC reçoit des demandes des utilisateurs de succursales et les transmet à un contrôleur de domaine dans le site pivot pour l'authentification.

Vous pouvez configurer une stratégie de réPLICATION de mot de passe pour un domaine en lecture seule qui spécifie les comptes d'utilisateurs et d'ordinateurs pour lesquels les mots de passe peuvent être mis en cache sur le RODC. Si un utilisateur se connecte en utilisant l'aide d'un domaine en lecture seule, le RODC demande les informations d'identification de l'utilisateur à partir d'un contrôleur de domaine complet.

Lorsque l'utilisateur est un membre de la stratégie de réPLICATION de mot de passe qui s'applique à un RODC, le RODC peut récupérer le mot de passe et le contrôleur de domaine complet permet la réPLICATION du secret. Cela signifie que la prochaine fois que l'utilisateur demande l'authentification à partir du même domaine en lecture seule, le RODC peut effectuer la tâche au niveau local. Alors que les utilisateurs qui sont inclus dans la stratégie de réPLICATION de mot de passe se connectent, le RODC construit sa cachette des informations d'identification afin qu'il puisse effectuer une authentification localement pour les utilisateurs. Normalement, vous ajoutez des utilisateurs et des ordinateurs pour la stratégie de réPLICATION de mot de passe qui sont dans le même site physique que le domaine en lecture seule.

Parce que RODC maintient seulement un sous-ensemble des informations d'identification, l'exposition de sécurité est limitée si un RODC est compromis ou volé. Si un RODC est compromis, seuls les comptes utilisateur et ordinateur que le RODC avait cachés, doivent avoir leurs mots de passe réinitialisés.

Le processus de réPLICATION RODC améliore également la sécurité. Un domaine en lecture seule réplique les modifications à AD DS à partir de contrôleurS de domaine accessibles en écriture, mais il ne se réplique pas de données vers d'autres contrôleurS de domaine. Cela permet d'éliminer l'exposition des services Active Directory à la corruption en raison de modifications apportées à un contrôleur de domaine des sites distants compromise. Enfin, les RODC ont l'équivalent d'un groupe Administrateurs local. Vous pouvez donner à un ou plusieurs employés de soutien locale la capacité de maintenir un RODC entièrement sans leur accorder les équivalents des droits Admins du domaine.

Les limitations et les considérations RODC

Pour réduire les risques de sécurité et les coûts administratifs, certaines options de contrôleur de domaine qui sont disponibles pour les contrôleurS de domaine inscriptibleS ne sont pas disponibles sur RODC.

Avant de vous décider à déployer un RODC, vous devez être conscient des limites et des considérations suivantes :

- Les RODC ne peuvent pas être maître d'opérations et détenteurs de rôle. Les détenteurs de rôle de maître d'opérations doivent pouvoir écrire des informations dans la base de données Active Directory. Le maître d'opérations détenteurs de rôles doivent être en mesure d'écrire des informations dans la base de données Active Directory. En raison de la nature en lecture seule de la base de données Active Directory du domaine en lecture seule, elle ne peut pas agir en tant que maître d'opérations détenteur du rôle.
- RODC ne peut pas être des serveurs de tête de pont. Les serveurs Bridgehead répliquent spécifiquement des changements provenant d'autres sites. RODC effectue seulement la réPLICATION entrante, de sorte qu'ils ne peuvent pas agir en tant que serveur tête de pont pour un site.
- Vous devriez avoir un seul RODC par site et par domaine. Si vous avez plusieurs RODC, le comportement de la mise en cache est incompatible parce que les secrets partagés sont uniquement mis en cache si un utilisateur se connecte à ce RODC spécifique. Il est probable que l'un des RODC a les secrets partagés et une autre RODC dans le même site ne dispose pas du tout.
- Les RODC ne peuvent pas s'authentifier à travers le système de relations lorsqu'une connexion WAN n'est pas disponible. Si vos utilisateurs et les ordinateurS sont dans des domaines différents, ils ne peuvent pas effectuer des ouvertures de session lorsque le site de succursale utilise RODC et est déconnecté du site pivot.
- Etant donné que les changementS AD DS ne peuvent pas être écrites directement dans un domaine en lecture seule, aucun changement de réPLICATION ne peut provenir d'un RODC. Cela signifie que tout changement ou la corruption qu'un pirate pourrait faire dans les succursales ne peuvent pas répliquer à partir du RODC à la forêt. Cela réduit également la charge de travail des serveurs têtes de pont du hub et l'effort requis pour surveiller la réPLICATION. La réPLICATION unidirectionnelle de RODC s'applique à la fois aux AD DS et à la réPLICATION DFS (Distributed File System).
- RODC ne peut pas soutenir toute application appropriée qui doit mettre à jour AD DS interactive, tel que Microsoft Exchange Server. Si vous allez déployer Exchange Server ou des applications similaires à un site, vous devez également déployer un contrôleur de domaine accessible en écriture. En outre, si vous déployez Exchange Server sur un site, vous aussi devriez avoir un emplacement sécurisé pour vos serveurs.

- Vous pouvez installer le système de noms de domaine (DNS) de service de serveur sur RODC. Les RODC peuvent répliquer toutes les partitions d'annuaire d'application que le DNS utilise, y compris ForestDnsZones et DomainDnsZones. Si vous installez un serveur DNS sur un RODC, les clients peuvent interroger pour la résolution des noms comme ils le feraient avec tout autre serveur DNS. Tout comme les informations de domaine Active Directory sur un RODC, les informations de zone DNS sur un RODC sont en lecture seule et par conséquent, il ne supporte pas les mises à jour de client directement. Lorsque les ordinateurs clients tentent d'enregistrer un enregistrement de ressource dans une zone DNS hébergé sur un RODC, le RODC renvoie le nom d'un contrôleur de domaine complet qui contient une copie inscriptible de cette zone au client. Le client utilise le contrôleur de domaine complet pour enregistrer le dossier.

Déploiement d'un RODC

Avant de déployer dans votre base Windows Server 2016 AD DS, vous devez :

- Exécutez **ADPrep /RODCPrep** si vous avez mis à niveau votre domaine à partir de Windows Server 2003 ou versions antérieures.
- Assurez-vous que vous avez un nombre suffisant de contrôleurs de domaine pour soutenir vos RODC. RODC a besoin de Windows Server 2008 ou des contrôleurs de domaine inscriptibles récents comme partenaires de réPLICATION.
- Notez que si vous utilisez Windows Server 2012 ou plus récent comme des contrôleurs de domaine inscriptibles, vous ne disposez pas des conditions préalables supplémentaires pour RODC.

- Conditions préalables :
 - ADPrep /RODCPrep**
 - Windows Server 2008 compatible ou partenaires de réPLICATION plus récents pour les RODC
- Pour un déploiement en une seule étape, effectuez l'une des étapes suivantes :
 - Dans Gestionnaire de serveur, ouvrez Ajouter des rôles et des fonctionnalités, puis utilisez l'Assistant Configuration des services de domaine Active Directory
 - Windows PowerShell : **Install-ADDSDomainController -ReadOnlyReplica**
- Pour un déploiement en deux étapes, procédez comme suit :
 - Pré-configuration : Créez le compte en utilisant le Centre d'administration Active Directory ou **Add-ADDSReadOnlyDomainControllerAccount**
 - Promotion déléguée : Rejoindre le RODC en tant qu'admin délégué : Gestionnaire de serveur ou **Install-ADDSDomainController -ReadOnlyReplica**

Après avoir terminé les étapes préparatoires, vous pouvez installer un RODC. Un domaine en lecture seule peut être une installation complète ou Server Core de Windows Server 2016. Vous pouvez effectuer une installation RODC en une seule étape ou en deux étapes par prédéfinition du compte.

Installation d'un RODC en une seule étape

Vous pouvez utiliser l'**Assistant Configuration des services de domaine Active Directory**, même à distance, dans le **Gestionnaire de serveur** pour créer un RODC. Sur la page **Additional Domain Controller Options** de l'Assistant, vous n'avez qu'à cliquer sur **RODC**.

Vous pouvez également utiliser la cmdlet **Install-ADDSDomainController** avec le commutateur - **ReadOnlyReplica** pour installer un RODC.

Sur une installation Server Core de Windows Server 2016, nous vous recommandons d'utiliser le **gestionnaire de serveur** à distance ou d'utiliser l'applet de commande PowerShell de Windows **Installer-ADDSDomainController** interface ligne de commande à distance à l'aide de l'applet de commande **Invoke-Command**.

Installation d'un RODC en deux étapes : la prédéfinition et la promotion déléguée

Vous pouvez compléter l'installation d'un domaine en lecture seule en deux étapes ; un individu différent effectue chaque étape. La première étape de l'installation crée un compte pour un domaine en lecture seule dans AD DS. La deuxième étape de l'installation joint le serveur qui sera le domaine en lecture seule sur le compte qui a été créé pour elle auparavant. Vous pouvez déléguer la possibilité de joindre le serveur à un groupe non administratif ou un utilisateur, comme un administrateur de la succursale délégué.

Au cours de la première étape, l'**Assistant Configuration des Services de domaine Active Directory** enregistre toutes les données sur le RODC, comme son nom de compte de contrôleur de domaine et le site dans lequel il sera placé. La base de données répartie de l'Active Directory stocke ces informations. Un membre du groupe Domain Admins doit effectuer cette étape de l'installation.

L'administrateur qui crée le compte RODC peut également spécifier quels utilisateurs ou groupes peuvent compléter l'étape suivante de l'installation. Tout utilisateur ou un groupe dans la succursale qui a été délégué le droit de terminer l'installation peut effectuer l'étape suivante. Cette étape ne nécessite pas d'appartenance à des groupes intégrés, tels que le groupe Domain Admins. Si l'utilisateur qui crée le compte RODC ne spécifie aucun délégué pour terminer l'installation et l'administration du RODC, seul un membre des groupes Administrateurs du domaine ou Administrateurs de l'entreprise peut terminer l'installation.

Vous pouvez effectuer une installation de mise en scène d'un RODC en utilisant plusieurs approches. Vous pouvez créer préalablement un compte RODC à l'aide du **Centre d'administration Active Directory**, cela étant approprié pour un petit nombre de comptes. Vous pouvez également utiliser la **cmdlet Add-ADDSReadOnlyDomainControllerAccountavec** les commutateurs appropriés.

Planification et configuration d'une stratégie de réPLICATION de mot de passe RODC

Une stratégie de réPLICATION de mot de passe détermine quels utilisateurs ou des ordinateurs des pouvoirs qui met en cache un RODC spécifique. Si une stratégie de réPLICATION de mot de passe permet à un RODC de mettre en cache les informations d'identification d'un utilisateur, le RODC peut traiter l'authentification et le service-ticket activités de cet utilisateur. Si un RODC ne peut pas mettre en cache les informations d'identification d'un utilisateur, le RODC désigne les activités d'authentification et d'un service de billets à un contrôleur de domaine inscriptible.

- Une stratégie de réPLICATION de mot de passe détermine les informations d'identification des utilisateurs ou de l'ordinateur qu'un RODC spécifique met en cache
- Vous pouvez configurer ces informations avec :
 - Une stratégie de réPLICATION de mot de passe à l'échelle du domaine
 - Une stratégie de réPLICATION de mot de passe propre au RODC
 - Un ensemble d'attributs filtré par RODC

Deux attributs à plusieurs valeurs du compte de l'ordinateur RODC déterminent la stratégie de réPLICATION de mot de passe d'un RODC. Ces attributs sont la *liste autorisée* et la *liste refusée*. Si le compte d'un utilisateur est sur la liste autorisée, le RODC met en cache les informations d'identification de l'utilisateur. Vous pouvez inclure des groupes sur la liste autorisée, dans ce cas, le RODC met en cache tous les utilisateurs qui appartiennent au groupe. Si un utilisateur est à la fois sur la liste autorisée et la liste refusée, les informations d'identification de l'utilisateur ne sont pas mis en cache-la liste refusée est prioritaire.

Stratégie de réPLICATION de mot de passe à l'échelle du domaine

Pour faciliter la gestion de votre stratégie de réPLICATION de mot de passe, Windows Server 2008 ou des systèmes d'exploitation plus récents créer deux groupes de sécurité de domaine locale dans le conteneur utilisateurs au sein de AD DS :

- Groupe de réPLICATION de mot de passe ROC autorisé. Les membres de ce groupe sont inclus dans la liste autorisée de chaque nouveau domaine en lecture seule. Par défaut, ce groupe n'a pas de membres. Par conséquent, par défaut, un nouveau domaine en lecture seule ne met pas en cache les informations d'identification de tout utilisateur. Vous devez ajouter les utilisateurs pour lesquels vous souhaitez que tous les RODC de domaine pour mettre en cache des informations d'identification au mot de passe RODC admis groupe de réPLICATION.

- Groupe de réPLICATION de mot de passe ROC refusé. Les membres de ce groupe sont inclus dans la liste de numéros interdits de chaque nouveau domaine en lecture seule. Vous devez ajouter les utilisateurs pour lesquels vous souhaitez vous assurer ne soient jamais cachées par les RODC de domaine dans le groupe de réPLICATION de mot de passe ROOC refusé. Par défaut, ce groupe contient des comptes sensibles à la sécurité qui sont membres de groupes, y compris Domain Admins, Enterprise Admins et de stratégie de groupe Propriétaires créateurs.

 **Remarque :** Les utilisateurs ne sont pas les seuls générateurs d'authentification et de services d'activité de billets. Les ordinateurs dans une succursale exigent également une telle activité. Pour améliorer les performances du système et de veiller à ce que les ordinateurs puissent établir un canal sécurisé avec un contrôleur de domaine dans une succursale, pour permettre également la branche RODC de mettre en cache les informations d'identification de l'ordinateur. Lors d'une panne WAN, il faut savoir que les utilisateurs ne sont en mesure de se connecter lorsque l'ordinateur et les utilisateurs des informations d'identification sont mis en cache.

Stratégie de réPLICATION de mot de passe propre au RODC

Ces deux groupes vous permettent de gérer la politique de réPLICATION de mot de passe sur tous les RODC. Cependant, pour mieux soutenir un scénario de succursale, vous devez autoriser le RODC dans chaque bureau de succursale de mettre en cache dans cet endroit précis les informations d'identification utilisateur et ordinateur. Par conséquent, alors que vous pouvez utiliser la liste globale refusée, vous devez configurer une liste spécifique alloué pour chaque domaine en lecture seule.

Ensemble d'attributs filtré par RODC

Certaines applications qui utilisent AD DS comme un magasin de données peuvent utiliser des données des titres de compétences semblables, tels que les mots de passe, les informations d'identification et des clés de chiffrement, que vous ne voulez pas stocker sur un RODC, dans le cas où il devient compromis. Pour ces applications, vous pouvez configurer un ensemble d'attributs de schéma qui ne sera pas répliqué vers un RODC. Cet ensemble d'attributs est l'ensemble des attributs RODC filtré. Les attributs que vous définissez dans l'ensemble des attributs RODC filtré ne peut pas être répliqués à tout RODC dans la forêt. Vous ne pouvez pas ajouter des attributs critiques du système à l'ensemble des attributs RODC filtré. Un attribut est un système critique si les conditions suivantes l'obligent à fonctionner correctement :

- AD DS
- Autorité de sécurité locale
- Base de données SAM
- Interfaces de fournisseurs de sécurité spécifiques à Microsoft, tel que le protocole Kerberos version 5.

Si vous avez des applications que vous souhaitez utiliser l'ensemble des attributs filtrés RODC, vous devez vérifier auprès du vendeur de l'app s'ils le supportent. Alors que les demandes à un RODC reçoivent des renvois à un contrôleur de domaine complet, les applications qui demandent un RODC pour un attribut dans l'ensemble des attributs filtrés RODC le reçoivent vide. RODC connaît l'attribut, mais n'a pas reçu une valeur pour cela. L'application doit être consciente de cette fonctionnalité et savoir demander un contrôleur de domaine inscriptible lors de la lecture de l'ensemble des attributs filtrés RODC.

Démonstration : Configuration d'une stratégie de réPLICATION de mot de passe

Dans cette démonstration, vous allez apprendre à :

- Procéder à une installation déléguée d'un RODC.
- Voir la stratégie de réPLICATION de mot de passe d'un RODC.
- Configurer une stratégie de réPLICATION de mot de passe propre à un RODC.
- Vérifiez la stratégie de mot de passe qui en résulte.

Procédure de démonstration

Organiser l'installation déléguée d'un RODC

1. Sur **LON-DC1**, à partir du **Gestionnaire de serveur**, ouvrez **Active Directory Sites et Services**, créez un nouveau site nommé **Munich** et puis l'attribuer à la **DEFAULTIPSITELINK**.
2. Démarrez le **Centre d'administration Active Directory**, puis naviguez vers les **Contrôleurs de domaine** OU.
3. Créez au préalable un compte RODC avec le nom **MUC-RODC1** qui devrait également être un **serveur DNS** et un **catalogue global**.
4. Déléguer **Bill Norman** pour installer et administrer le RODC.
5. Terminer la pré-création du compte RODC.

Voir une stratégie de réPLICATION de mot de passe d'un RODC

1. Dans le **Centre d'administration Active Directory**, dans les **contrôleurs de domaine** OU, ouvrez les propriétés du compte d'ordinateur **MUC-RODC1**.
2. Dans la section **Extensions**, sélectionnez l'onglet **Stratégie de réPLICATION de mot de passe**, puis notez ses paramètres.

Configurer une stratégie de réPLICATION de mot de passe propre à un RODC

1. Basculez vers **Gestionnaire de serveur** et dans le menu **Outils**, démarrez **Utilisateurs et ordinateurs Active Directory**.
2. Accédez au conteneur **Utilisateurs**, puis créez un nouveau groupe nommé **Groupe de réPLICATION de mot de passe RODC autorisé par Munich**.
3. Ajouter **Ana Cantrell** au nouveau groupe.
4. Basculez vers le **Centre d'administration Active Directory**, puis ouvrez les propriétés de **MUC-RODC1**.
5. Dans la section **Extensions**, sous l'onglet **Stratégie de réPLICATION de mot de passe**, configurez le **Groupe de réPLICATION de mot de passe RODC autorisé par Munich** pour autoriser la réPLICATION de mot de passe, puis fermez les propriétés de **MUC-RODC1**.

Vérifiez la stratégie de mot de passe qui en résulte

1. Dans le **Centre d'administration Active Directory**, ouvrez les propriétés de **MUC-RODC1**, puis dans la section **Extensions**, sous l'onglet **Stratégie de réPLICATION de mot de passe**, cliquez sur **Avancé**.
2. Notez que cette boîte de dialogue affiche tous les comptes dont les mots de passe sont stockés dans le RODC.

3. Sélectionnez **Comptes authentifiés sur ce contrôleur de domaine en lecture seule**, puis notez que cette page affiche uniquement les comptes disposant des autorisations requises et que le contrôleur de domaine racine a été authentifié.
4. Sélectionnez l'onglet **Stratégie résultante**, puis ajoutez **Ana Cantrell**. Notez que Ana a un **paramètre résultant de Autoriser**.
5. Fermez toutes les boîtes de dialogue ouvertes.

Séparer l'administration locale RODC

Les RODC dans les succursales pourraient nécessiter une maintenance, comme les mises à jour de pilotes de périphériques. En outre, les petites succursales peuvent combiner le rôle d RODC avec un rôle de serveur de fichiers sur un seul système. Dans ce scénario, il sera important de sauvegarder le système. Les RODC supportent l'administration locale en utilisant la fonctionnalité de *séparation de rôle de l'administrateur*. Avec cette fonctionnalité, vous pouvez déléguer à tout utilisateur de domaine ou d'un groupe de sécurité le rôle d'administrateur local d'un RODC, sans accorder à cet utilisateur ou groupe les droits au domaine ou aux autres contrôleurs de domaine. Par conséquent, un administrateur délégué peut se connecter à un RODC pour effectuer des travaux d'entretien, tels que la mise à niveau d'un pilote sur le serveur. Toutefois, l'administrateur délégué ne peut pas se connecter à un autre contrôleur de domaine ou effectuer toute autre tâche administrative dans le domaine.

- La séparation des rôles de l'administrateur permet l'exécution des tâches administratives locales sur le RODC pour les administrateurs sans domaine
- Chaque RODC conserve une base de données locale de groupes du Gestionnaire de comptes de sécurité à des fins administratives spécifiques
- Configurez l'administrateur local par :
 - L'ajout de l'utilisateur ou du groupe lors de la pré-création ou de l'installation du RODC
 - L'ajout d'un utilisateur ou d'un groupe sur l'onglet Géré par dans les propriétés du compte RODC

Chaque RODC maintient une base de données locale des groupes à des fins administratives spécifiques. Vous pouvez ajouter un compte d'utilisateur de domaine à ces rôles locaux pour permettre l'appui à un RODC spécifique.

Vous pouvez configurer les administrateurs délégués pour un RODC lorsque vous pré-arez un compte d'ordinateur RODC ou lorsque vous installez le RODC. Vous pouvez ajouter un utilisateur ou un groupe dans la page **Délégation de l'installation et de l'administration du RODC** dans l'**Assistant d'installation des services de domaine Active Directory**. Vous pouvez également ajouter le compte d'utilisateur ou de groupe dans l'onglet **Géré par** des propriétés du compte RODC dans **Utilisateurs et ordinateurs Active Directory**.

Question : Comment pouvez-vous fournir une sécurité supplémentaire pour les disques durs dans les contrôleurs de domaine ?

Leçon 2

Implémentation de la sécurité du compte

En tant qu'administrateur, vous devez vous assurer que les comptes d'utilisateurs dans votre environnement sont conformes aux normes de sécurité définies par votre organisation. Pour ce faire, Windows Server 2016 vous permet d'utiliser des stratégies de compte pour configurer les paramètres de sécurité pour les comptes utilisateur. De plus, avec Windows Server 2016, vous pouvez configurer une sécurité supplémentaire avec des groupes protégés, les politiques d'authentification et les silos de la politique d'authentification. Cette leçon explique les paramètres qui sont disponibles pour la sécurité des comptes et les méthodes pour configurer ces paramètres.

Objectifs des leçons

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

- Décrire la sécurité de compte dans Windows Server 2016.
- Décrire les stratégies de mot de passe.
- Cliquez sur Stratégie de verrouillage du compte.
- Décrivez les stratégies Kerberos.
- Configuration des stratégies de compte de domaine
- Décrire la façon de protéger les groupes dans AD DS.
- Stratégies de mot de passe et de verrouillage affinées.
- Décrire les objets de paramétrage de mot de passe (PSO).
- Configuration d'une stratégie de mot de passe fine.
- Priorité PSO et PSO résultante.
- Options de sécurité du compte dans Windows Server 2016.
- Configuration des stratégies de compte d'utilisateur.
- Décrire la façon d'améliorer l'authentification par mot de passe avec Windows Bonjour et le service Microsoft Azure authentification multi-facteurs (MFA).

Sécurité de compte dans Windows Server 2016

Dans tout réseau basé sur l'authentification, il est extrêmement important de sécuriser les informations d'identification du compte, telles que les noms d'utilisateur et les mots de passe. Pour assurer la sécurité du compte, Windows Server 2016 propose plusieurs options, y compris :

- Les politiques de mot de passe pour configurer plusieurs exigences, telles que l'âge du mot de passe, la longueur et la complexité, éléments que les mots de passe des utilisateurs doivent respecter.

Les caractéristiques de sécurité de compte dans Windows Server 2016 comprennent :

- Stratégies de mot de passe
- Stratégies de verrouillage de comptes
- Stratégies de mot de passe affinées
- Utilisateurs protégés
- Stratégies d'authentification
- Cloisonnements de la stratégie d'authentification

- Les politiques de verrouillage de compte qui vous permettent de configurer qu'un compte doit se verrouiller lorsque les mauvais mots de passe sont entrés.
- Les politiques affinées de mot de passe qui offrent la possibilité de spécifier les différentes politiques de mot de passe et les politiques de verrouillage de compte pour les différents groupes d'utilisateurs, tels que les cadres, les administrateurs, les comptes de service, ou les utilisateurs réguliers.
- Les utilisateurs protégés qui vous permet de spécifier les comptes critiques qui devraient être davantage sécurisés.
- Les stratégies d'authentification et les silos de politique d'authentification qui vous offrent la possibilité d'utiliser des règles basées sur les revendications pour spécifier quels utilisateurs sont en mesure de se connecter à quels ordinateurs.
- Les stratégies Kerberos qui déterminent les paramètres liés à Kerberos, tels que la durée de vie des billets et de l'application.

Cette leçon explique ces options plus en détail.

Stratégies de mot de passe

Les stratégies de compte dans AD DS définissent les paramètres par défaut pour les attributs liés à la sécurité qui sont affectés à des objets utilisateur. Dans AD DS, les politiques de compte sont classés en trois groupes de paramètres différents : la politique de mot de passe, le verrouillage de compte et la stratégie de Kerberos. Vous pouvez configurer la politique de mot de passe et les paramètres de verrouillage de compte dans les paramètres de stratégie locale pour un individu de serveur Windows Server 2016, ou vous pouvez configurer tous les trois groupes de paramètres pour l'ensemble du domaine en utilisant la console de gestion des stratégies de groupe dans AD DS. Lorsque les paramètres de stratégie locale et la stratégie de groupe des paramètres sont en conflit, les paramètres de stratégie de groupe remplacent les paramètres de stratégie locale.

Définissez les exigences de mot de passe en utilisant les paramètres suivants :

- Appliquer l'historique des mots de passe
- Âge de mot de passe maximal
- Âge de mot de passe minimal
- Longueur de mot de passe minimale
- Renforcement de la complexité des mots de passe :
 - Ne contient pas de nom ou nom d'utilisateur
 - Il doit comporter au moins 6 caractères
 - Il contient des caractères de trois des quatre groupes suivants : majuscules, minuscules, caractères numériques et caractères spéciaux

Dans la gestion de stratégie de groupe au sein de AD DS, la plupart des paramètres de stratégie peuvent s'appliquer à différents niveaux au sein de la structure AD DS : domaine, site ou OU (unité d'organisation). Cependant, les stratégies de compte pour les comptes de domaine ne peuvent s'appliquer qu'à un niveau dans AD DS - à l'ensemble du domaine. Par conséquent, un seul ensemble de paramètres de stratégie de compte peut s'appliquer à un domaine AD DS.

La politique de mot de passe est l'une des politiques les plus importants lors de la sécurisation des comptes utilisateurs AD DS. Utilisez la stratégie de mot de passe pour configurer les propriétés des mots de passe que les utilisateurs peuvent choisir. Vous utilisez ces paramètres pour veiller à ce que les utilisateurs ne peuvent pas utiliser des mots de passe simples, qui offrent une protection insuffisante contre les attaques de mot de passe.

Vous définissez la politique de mot de passe en utilisant les paramètres suivants :

- **Appliquer l'historique des mots de passe.** Ceci est le nombre de nouveaux mots de passe uniques qui sont à associer à un compte d'utilisateur avant qu'un ancien mot de passe peut être réutilisé. Le réglage par défaut est de 24 mots de passe précédents. Lorsque vous utilisez ce paramètre avec le paramètre de l'âge de mot de passe minimale, l'historique de mot de passe mis en œuvre empêche la réutilisation constante du même mot de passe.

- **Âge maximal du mot de passe :** Ceci est le nombre de jours durant lesquels l'utilisateur peut utiliser un mot de passe avant de devoir changer. Changer régulièrement les mots de passe permet d'éviter le compromis des mots de passe. Cependant, vous devez équilibrer cette considération de la sécurité contre les considérations logistiques qui résultent de la demande faite aux utilisateurs de changer les mots de passe très souvent. Le réglage par défaut de 42 jours est appropriée pour la plupart des organisations.
- **Âge minimal du mot de passe :** Ceci est le nombre de jours pendant lesquels un mot de passe doit être utilisé avant que l'utilisateur peut modifier. La valeur par défaut est un jour, ce qui est approprié si vous appliquez l'historique du mot de passe. Vous pouvez restreindre l'utilisation constante du même mot de passe si vous utilisez ce paramètre avec le paramètre de l'historique de mot de passe mis en œuvre.
- **Longueur de mot de passe minimale :** Ceci est le nombre minimal de caractères du mot de passe d'un utilisateur doit contenir. La valeur par défaut est Oui. Ce défaut est un minimum largement utilisé, mais vous devriez envisager d'augmenter la longueur du mot de passe à au moins 10 caractères pour améliorer la sécurité.
- **Exigences de complexité :** Windows Server comprend un filtre de mot de passe par défaut qui est activé par défaut et vous ne devriez pas le désactiver. Le filtre nécessite qu'un mot de passe possède les caractéristiques suivantes :
 - Ne contient pas votre nom ou votre nom d'utilisateur
 - Contient au moins six caractères
 - Contient des caractères de trois des quatre groupes suivants :
 - Les lettres majuscules [A-Z]
 - Les lettres minuscules [a-z]
 - 0 - 9
 - Caractères spéciaux non-alphanumériques, tels que ! @ #) (* & ^%

Stratégies de verrouillage de comptes

En plus des politiques de mot de passe, la plupart des organisations configurent les politiques de verrouillage de compte. Alors que les politiques de mot de passe précisent que les utilisateurs ont besoin d'utiliser des mots de passe sécurisés, les stratégies de verrouillage vous permettent de définir si les comptes doivent être verrouillés s'il y a trop de tentatives de se connecter avec des mots de passe invalides.

Vous pouvez définir les seuils pour un verrouillage de compte, la durée du verrouillage et un moyen de déverrouiller les comptes. Les seuils pour un verrouillage de compte stipulent que les comptes deviennent inutilisables après un certain nombre de tentatives de connexion en échec au cours d'une certaine période de temps. Les stratégies de verrouillage de compte permettent de détecter et de prévenir les attaques par force brute sur les mots de passe. Les paramètres disponibles sont les suivants :

- **Durée du verrouillage de comptes :** Définit le nombre de minutes pendant lesquelles un compte verrouillé reste verrouillé. Après le nombre spécifié de minutes, le compte se déverrouille

- Les stratégies de verrouillage de compte déterminent si les comptes doivent être verrouillés automatiquement après plusieurs tentatives infructueuses de connexion
- Pour configurer ces paramètres de stratégie, vous devez prendre en compte :
 - La durée de verrouillage du compte
 - Le seuil de verrouillage du compte
 - Réinitialiser le compteur de verrouillage de compte après
- Les stratégies de verrouillage de compte offrent un certain niveau de sécurité, mais présentent aussi des occasions pour les attaques DoS

automatiquement. Pour spécifier qu'un administrateur doit déverrouiller le compte, définissez la valeur à 0. Envisagez d'utiliser des politiques de mot de passe affinés pour exiger aux administrateurs de déverrouiller les comptes de haute sécurité, puis la configuration de ce paramètre pour 30 minutes pour les utilisateurs normaux.

- **Seuil du verrouillage de comptes** : Détermine le nombre de tentatives de connexion en échec qui sont autorisés avant un compte d'utilisateur est verrouillé. Une valeur de 0 signifie que le compte n'est jamais verrouillé. Vous devez définir cette valeur suffisamment élevée pour permettre des mots de passe mal orthographiés, mais suffisamment faible pour assurer l'échec des tentatives de force brute pour deviner un mot de passe. Des valeurs communes pour cette plage de réglage de trois à cinq.
- **Réinitialiser le compteur de verrouillage de compte après** : Détermine le nombre de minutes qui doivent être respecté après qu'une tentative de connexion a échoué avant que le compteur d'connexion est remis à 0. Ce réglage est valable lorsque l'utilisateur a tapé un mot de passe incorrect, mais l'utilisateur n'a pas dépassé le seuil de verrouillage du compte. Envisager de mettre cette valeur à 30 minutes.

La plupart des organisations mettent en œuvre des politiques de verrouillage de compte pour empêcher les attaquants d'utiliser des techniques de passe-devinettes pour avoir accès à un réseau. Bien que cette approche fournit un niveau de sécurité, il expose également votre organisation à une attaque DoS parce que les attaquants peuvent exécuter des scripts pour deviner les mots de passe de l'utilisateur et verrouiller tous les comptes d'utilisateurs. Cela empêche la bonne personne d'être en mesure d'accéder à son compte. Si vous choisissez de ne pas mettre en œuvre les politiques de verrouillage de compte, il est essentiel que vous surveillez les tentatives infructueuses de présences en temps réel, pour empêcher les attaquants de prendre avantage de cette configuration.

Stratégies Kerberos

Vous déployez les paramètres de stratégie Kerberos pour l'ensemble du domaine de la stratégie par défaut de domaine. Cette politique est pour les comptes d'utilisateurs de domaine et de l'informatique et détermine les paramètres liés à Kerberos, tels que la durée de vie des billets et de l'application. Les stratégies Kerberos n'existent pas dans la Stratégie Ordinateur local.

Les options de configuration de la stratégie de Kerberos contiennent des paramètres pour le protocole d'authentification le ticket d'octroi de Kerberos (TGT), la durée de vie des billets de session et les paramètres d'horodatage. Pour la plupart des organisations, les paramètres par défaut sont appropriés. Vous trouverez la stratégie Kerberos dans l'Éditeur d'objets de stratégie de groupe dans la section **Stratégie de compte** du nœud **Configuration de l'ordinateur**, la page **Paramètres de sécurité**, sous les stratégies **Mot de passe et Verrouillage de compte**.

- Les paramètres de stratégie Kerberos déterminent le calendrier pour les tickets Kerberos et autres événements

| Paramètre | Valeur par défaut |
|---|-------------------|
| Appliquer les restrictions sur l'ouverture de session utilisateur | Activé |
| Durée de vie maximale du ticket de service | 600 minutes |
| Durée de vie maximale du ticket utilisateur | 10 heures |
| Durée de vie maximale pour le renouvellement du ticket utilisateur | 7 jours |
| Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur | 5 minutes |

- Les réclamations Kerberos et l'authentification composée pour DAC nécessitent Windows Server 2012 ou des contrôleurs de domaine récents

Kerberos est un protocole d'authentification qui émet des tickets d'identité, qui permettent aux entités de prouver qui ils sont à d'autres entités d'une manière sécurisée. Kerberos a plusieurs avantages uniques en tant que protocole d'authentification. Il a la capacité de fournir une authentification déléguée en permettant aux services du système d'exploitation Windows de faire passer pour un ordinateur client lorsque l'accès aux ressources pour cela. Kerberos fournit l'authentification unique pour les utilisateurs de domaine et des ordinateurs par l'émission TGT qu'ils peuvent échanger contre des billets de session pour accéder aux sessions de serveur spécifiques. Kerberos a l'interopérabilité étendue avec d'autres composants de réseau parce que Kerberos fait partie de la suite de protocoles non-propriétaires TCP/IP. Kerberos offre une authentification plus efficace avec les serveurs parce que vous utilisez des tickets de session Kerberos présentées par les services au niveau de l'utilisateur pour l'accès approuvé aux ressources du serveur. Enfin, Kerberos offre une authentification mutuelle parce que le serveur présente ses lettres de créance vers les services de niveau utilisateur.

Stratégies Kerberos

Vous pouvez utiliser la stratégie Kerberos dans un GPO pour appliquer le signe de l'utilisateur dans les restrictions et de définir des seuils pour le service maximum et utilisateur billet à vie, un maximum de renouvellement durée de vie du ticket utilisateur et les maximales horloges des ordinateurs de temps peuvent être hors de synchronisation. Les paramètres disponibles sont les suivants :

- **Appliquer les restrictions sur l'ouverture de session utilisateur.** Détermine si le Centre de distribution de clés de la Kerberos (KDC) permettra de valider chaque demande de ticket de session contre la politique du compte d'utilisateur des droits d'utilisateur. Cela peut ajouter une sécurité supplémentaire, mais cela n'est pas nécessaire. Le choix de faire respecter les restrictions pour l'ouverture de session peut ralentir l'accès des services aux ressources du réseau. Ce paramètre est activé par défaut.
- **Durée de vie maximale du ticket de service.** Définit la durée maximale d'un ticket de service est valable pour authentifier l'accès des clients à un service particulier. Si le ticket de service expire avant que le client demande la connexion au serveur, le serveur répond avec une erreur et le client redirige les requêtes vers le KDC pour recevoir un nouveau ticket de service. Cette durée de vie maximale doit être d'au moins 10 minutes mais pas plus grande que la durée de vie maximale pour un billet de l'utilisateur. Par défaut, la durée de vie maximale de ticket de service est de 600 minutes, ou 10 heures.
- **Durée de vie maximale du ticket utilisateur** Définit la quantité de temps TGT d'un compte d'utilisateur est valide. La valeur par défaut est 10 heures.
- **Durée de vie maximale pour le renouvellement du ticket utilisateur.** Définit la quantité de temps, en jours, pour lesquels TGT du compte d'utilisateur peut être renouvelé.
- **La valeur par défaut est de sept jours.** Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur. Détermine la quantité de temps que les horloges des ordinateurs clients peuvent être en décalage avec le contrôleur de domaine. Le rôle de maître d'opération d'émulateur du contrôleur de domaine principal (PDC) sur un domaine détermine l'heure correcte pour l'ensemble du domaine. Les paquets de réPLICATION de domaine de TGT et de services billets sont horodatés et les temps sur les différents billets et les paquets sont dignes de confiance entre les ordinateurs correspondants. Cependant, il est possible pour tous les deux ordinateurs pour être hors de synchronisation sur leurs horloges. Les administrateurs peuvent définir la quantité de temps par lequel les horloges peuvent être désynchronisé. La valeur par défaut de cet intervalle est de 10 minutes.

Vous pouvez créer un contrôle d'accès basé sur les revendications et l'authentification du composé en déployant Dynamic Access Control (DAC). Vous devez vous assurer que vous avez suffisamment de Windows Server 2008 ou nouveaux contrôleurs de domaine disponibles qui utilisent ces nouveaux types d'autorisation. Le paramètre de **stratégie de modèle administratif KDC** vous permet de configurer un contrôleur de domaine pour prendre en charge les revendications et l'authentification composée pour le blindage DAC et Kerberos. En outre, le contrôleur Windows Server 2012 ou plus récent domaine est

nécessaire pour les clients Kerberos exécutant Windows 10, Windows 8.1, ou Windows 8 systèmes d'exploitation pour soutenir les revendications et l'authentification du composé en utilisant l'authentification Kerberos.



Remarque : Les périphériques qui exécutent Windows 8 et les systèmes d'exploitation plus récents vont échouer l'authentification si elles ne peuvent pas trouver un contrôleur de domaine qui exécute Windows Server 2012 ou plus récent. Vous devez vous assurer qu'il y a des contrôleurs de domaine suffisants qui exécutent Windows Server 2012 ou plus récent pour tous les domaines compte, de référence et les ressources qui sont pris en charge.

Démonstration : Configuration des stratégies de compte de domaine

Dans cette démonstration, vous allez apprendre à configurer les stratégies de mot de passe et de verrouillage de compte.

Procédure de démonstration

Configurer une stratégie de mot de passe basée sur le domaine

1. Sur **LON-DC1**, à partir du **Gestionnaire de serveur**, ouvrez la console **Gestion des stratégies de groupe**.
2. Modifiez le défaut Stratégie de domaine, puis configurer les paramètres suivants de la politique compte de mot de passe :
 - o Historique des mots de passe : **20 mots de passe**
 - o Âge maximal du mot de passe : **45 jours**
 - o Âge minimal du mot de passe : **1 jour**
 - o Longueur du MDP : **10 caractères**
 - o Complexité activé : **Oui**

Configurer une stratégie de verrouillage du compte

1. Dans la fenêtre **Éditeur de gestion de stratégie de groupe**, configurez les paramètres de stratégie de verrouillage de compte suivants pour la stratégie de domaine par défaut :
 - o Durée du verrouillage de comptes : **30 minutes**
 - o Seuil du verrouillage de comptes : **5 tentatives**
 - o Réinitialiser le compteur de verrouillage de compte après : **15 minutes**
2. Fermez la fenêtre **Éditeur de gestion de stratégie de groupe** et la **Console de Gestion de stratégie de groupe**.

Protection des groupes dans AD DS

Dans la plupart des déploiements AD DS, certains groupes de sécurité sont considérées comme essentielles à la sécurité. Windows Server 2016 fournit la fonctionnalité Groupes restreints et les groupes de sécurité des utilisateurs protégés disposent pour fournir une protection supplémentaire pour ces groupes.

Groupes restreints

Pour les groupes locaux de sécurité critiques sur des serveurs ou des postes de travail, vous pouvez utiliser la fonctionnalité Groupes restreints disponibles dans la stratégie de groupe pour contrôler l'appartenance à ces groupes et l'appartenance à ces groupes.

Groupes restreints vous permettent de sélectionner un groupe de sécurité locale et de définir deux attributs : **Membres** et **membre de**.

Lors de la définition de l'attribut **Membres**, vous spécifiez qui doit et ne doit pas appartenir au groupe restreint configuré. Lorsque vous configurez l'attribut **Membres**, tout membre en cours d'un groupe restreint qui n'est pas répertorié comme membre est supprimé automatiquement, à l'exception de l'administrateur dans le groupe Administrateurs. En outre, tout utilisateur qui est répertorié en tant que membre, qui ne sont pas actuellement membre du groupe restreint, est ajouté automatiquement.

Lorsque vous utilisez l'attribut **Membre de** d'un groupe restreint, assurez-vous que le groupe restreint est un membre de groupes qui sont répertoriés dans la zone de texte **Membre de**. Vous ne pouvez pas utiliser cet attribut pour supprimer le groupe restreint de tout autre groupe.

Pour configurer des groupes restreints, ouvrez l'Éditeur de gestion des stratégies de groupe et accédez au nœud **Configuration de l'ordinateur\Paramètres\Paramètres Windows\Paramètres de sécurité**.

Un exemple de quand vous voudrez peut-être utiliser Groupes restreints est si vous voulez contrôler l'appartenance au groupe Administrateur local sur les postes de travail de votre organisation.



Remarque : Vous ne pouvez pas utiliser cette fonction pour gérer les groupes de domaine dans AD DS. Vous devez utiliser les Groupes restreints disposent seulement avec des groupes locaux sur client ou serveur ordinateurs.

Groupe Utilisateurs protégés :

Windows Server 2012 R2 introduit le utilisateurs groupe de sécurité protégé, ce qui génère une protection non configurable sur :

- Les appareils et les ordinateurs qui exécutent des systèmes d'exploitation plus récents Windows Server 2012 R2 et Windows 8.1 ou.
- Les contrôleurs de domaine dans les domaines avec un contrôleur de domaine principal qui exécutent Windows Server 2012 R2 ou plus récent.

Cela réduit sensiblement l'empreinte mémoire d'informations d'identification lorsque les utilisateurs se connectent à des ordinateurs sur le réseau à partir d'un ordinateur sans compromis. Considérez les points suivants lors de l'utilisation des groupes d'utilisateurs protégés :

- L'appartenance au groupe Utilisateurs protégés ne peut pas authentifier en utilisant NTLM, l'authentication Digest ou le Credential Security Support Provider (un mécanisme d'authentification

également connu sous le nom de *CredSSP*). Sur les appareils fonctionnant sous Windows 8.1 et plus récent, les mots de passe ne sont pas mis en cache, de sorte que le dispositif qui utilise l'un de ces fournisseurs de support de sécurité (SSP) ne parviendra pas à authentifier à un domaine où le compte est membre du groupe de l'utilisateur protégé.

- Le protocole Kerberos ne pas utiliser le plus faible Data Encryption Standard (DES) ou de types de chiffrement RC4 dans le processus de pré-authentification. Par conséquent, vous devez configurer le domaine pour prendre en charge au moins la suite de chiffrement AES (Advanced Encryption Standard).
- Vous ne pouvez pas déléguer le compte de l'utilisateur avec Kerberos délégation contrainte ou sans contrainte. Cela peut provoquer des anciens liens avec d'autres systèmes d'échouer si l'utilisateur est dans le groupe des utilisateurs protégés.
- Le paramètre de **durée de vie Kerberos TGTs** par défaut de quatre heures peut être configuré en utilisant les **stratégies d'authentification et les silos**, auxquels vous pouvez accéder via le **Centre d'administration Active Directory**. Cela signifie que l'utilisateur doit être authentifié à nouveau au bout de quatre heures.

Stratégies de mot de passe et de verrouillage affinées

À partir de Windows Server 2008, les administrateurs peuvent définir plus d'une politique de mot de passe dans un seul domaine en mettant en œuvre des politiques de mots de passe affinés. Ceux-ci vous donnera un contrôle individuel sur les exigences de mot de passe de l'utilisateur et vous pouvez avoir des exigences différentes de mot de passe pour différents utilisateurs ou groupes. Ceci est bénéfique pour l'application des paramètres de mot de passe plus restrictives pour les administrateurs, les comptes de service, ou les utilisateurs avec des fonctions commerciales très critiques.

• Vous pouvez utiliser des stratégies de mot de passe à grains fins pour spécifier les stratégies de mots de passe multiples au sein d'un domaine unique

• Stratégies de mot de passe affiné :

- Appliquez-les uniquement aux objets utilisateur, aux objets **InetOrgPerson** ou aux groupes de sécurité globale
- Ne les appliquez pas directement à une UO
- Ne les faites pas interférer avec les filtres de mot de passe personnalisés que vous pouvez utiliser dans le même domaine

Pour prendre en charge la fonction fine politique de mot de passe, AD DS dans Windows Server 2008 et plus récents comprennent deux types d'objets :

- Password Settings Container. Windows Server crée ce conteneur par défaut et vous pouvez le voir dans le conteneur système du domaine. Le conteneur stocke les PSO que vous créez et un lien vers les groupes de sécurité globaux ou à des utilisateurs.
- PSO. Les membres du groupe Domain Admins créer PSO puis définir les paramètres spécifiques de mot de passe et de verrouillage de compte pour lier à un groupe de sécurité spécifique ou un utilisateur.

Les stratégies de mots de passe affinés ne s'appliquent qu'aux objets utilisateur, aux objets **InetOrgPerson** ou aux groupes de sécurité globaux. En liant un PSO à un utilisateur ou un groupe, vous modifiez un attribut appelé **msDS-PSOApplied** qui est vide par défaut. Cette approche traite maintenant les paramètres de mot de passe et de verrouillage de compte pas que les exigences de l'ensemble du domaine, mais comme attributs d'un utilisateur spécifique ou un groupe. Par exemple, pour configurer une stratégie de mot de passe stricte des comptes d'administration, de créer un groupe de sécurité global, ajoutez les comptes d'administrateur en tant que membres, puis lier un PSO au groupe. L'application des politiques de mot de passe affiné à un groupe de cette manière est plus facile à gérer que d'appliquer des politiques pour chaque compte d'utilisateur individuel. Si vous créez un nouveau compte de service, il vous suffit de l'ajouter à un groupe et le PSO gère le compte.

Par défaut, seuls les membres du groupe Admins du domaine peuvent créer et appliquer des politiques de mot de passe affiné. Cependant, vous pouvez également déléguer la possibilité de définir ces politiques à d'autres utilisateurs sur une base domaine par domaine.

Configuration d'une stratégie de mot de passe affiné

Vous ne pouvez pas appliquer une politique de mot de passe affiné directement à un OU. Pour appliquer une politique de mot de passe affiné aux utilisateurs des OU, vous pouvez utiliser un *groupe d'ombre*. Un groupe d'ombre est un groupe de sécurité globale qui mappe logiquement à une unité d'organisation et applique une politique de mot de passe affiné. Vous pouvez ajouter des utilisateurs d'une unité d'organisation en tant que membres du groupe de l'ombre nouvellement créé et puis vous pouvez appliquer la politique à grain fin mot de passe pour ce groupe d'ombre. Si vous déplacez un utilisateur d'une unité d'organisation à l'autre, vous devez mettre à jour la composition des groupes d'ombre correspondants.

Les paramètres gérés par les stratégies de mots de passe affinés sont identiques à ceux des noeuds **Stratégie de mot de passe** et **Stratégies de comptes** d'un GPO. Cependant, vous ne mettrez en œuvre des politiques de mot de passe affiné dans le cadre de la stratégie de groupe ne sont-ils appliqués dans le cadre d'un GPO. Au lieu de cela, le PSO est une catégorie distincte d'objet dans AD DS qui maintient les paramètres de la politique de mot de passe affiné. En outre, les politiques de mot de passe affiné ne pas interférer avec les paramètres de mot de passe personnalisés ou les filtres que vous pourriez avoir mis en œuvre.

Vous pouvez créer un ou plusieurs PSO dans votre domaine. Chacun contient un ensemble complet de mots de passe et de la politique de verrouillage des paramètres et chacun permet les mêmes options de configuration qui sont disponibles dans le mot de passe et verrouillage des paramètres de domaine. Vous appliquez une PSO en l'associant à un ou plusieurs groupes de sécurité globaux ou des utilisateurs.

Pour utiliser une politique à grain fin mot de passe, votre niveau fonctionnel du domaine doit être au moins Windows Server 2008, ce qui signifie que tous vos contrôleurs de domaine dans le domaine doivent exécuter au moins Windows Server 2008. Pour répondre à cette condition, vous devez augmenter le niveau fonctionnel de domaine au moins Windows Server 2008.

Pour confirmer et modifier le niveau fonctionnel du domaine, utilisez la procédure suivante :

1. Ouvrez les **domaines et les approbations Active Directory**.
2. Dans l'arborescence de la console, développez **Domaines et approbations Active Directory**, puis développez l'arborescence jusqu'à ce que vous voyez le domaine.
3. Cliquez avec le bouton droit sur le domaine et puis cliquez sur **Augmenter le niveau fonctionnel du domaine**.

Outils pour la création PSO

PSO sont les éléments clés pour la mise en œuvre des politiques de mot de passe affiné.

Le tableau suivant met en évidence certains paramètres que PSO peut contenir.

Windows Server 2012 et les systèmes d'exploitation récents fournissent deux outils de configuration des PSO :

- Les applets de commande Windows PowerShell :
 - **New-ADFineGrainedPasswordPolicy**
 - **Add-FineGrainedPasswordPolicySubject**
- Centre d'administration Active Directory

| Paramètre | Valeurs | Description |
|--|---------------------------------|---|
| Paramètres du mot de passe | | |
| Nom | String | Nom du GPO Assurez-vous de mettre en œuvre une stratégie de nommage pour les PSO. |
| ComplexityEnabled | Vrai ou faux | Définit si le PSO impose l'utilisation de mots de passe complexes. |
| MinPasswordLength | Nombre entier | Longueur minimale du mot de passe. |
| MaxPasswordAge | Temps : <i>jj.hh: mm: ss</i> | Montant maximal de jours avant que les utilisateurs devront changer leurs mots de passe. |
| MinPasswordAge | Temps : <i>jj.hh: mm: ss</i> | Montant minimum de temps avant que les utilisateurs sont en mesure de changer leurs mots de passe. Vous utilisez souvent PasswordHistoryCount pour empêcher les utilisateurs de modifier leurs mots de passe plusieurs fois immédiatement pour réutiliser leurs anciens mots de passe. |
| PasswordHistoryCount | Nombre entier | Nombre de mots de passe qui ne peuvent pas être réutilisés. |
| ReversibleEncryptionEnabled | Vrai ou faux | Définit si le chiffrement réversible est autorisé. Vous devez le définir sur Faux sauf si vous avez des raisons spécifiques pour permettre le cryptage réversible. |
| Seuil de verrouillage du compte | | |
| LockoutThreshold | Nombre entier | Nombre d'ouvertures de session de mots de passe erronés qui conduisent à un compte verrouillé. |
| LockoutObservationWindow | Temps : <i>hh:mm:ss</i> | Période au cours de laquelle le nombre de mots de passe erronés va bloquer votre compte. |
| LockoutDuration | Temps : <i>hh:mm:ss</i> | Durée après laquelle le compte se déverrouille automatiquement. Si non configuré, un administrateur doit déverrouiller le compte. |
| Paramètres généraux | | |
| Priorité | Nombre entier | Nombre qui définit la priorité du PSO. Si différents PSO appliquent au même utilisateur, la priorité définit que l'on va appliquer. |
| PSOApplied | Liste de valeurs multiples | Mesdames et Messieurs les noms des utilisateurs ou groupes de sécurité globaux |

| Paramètre | Valeurs | Description |
|---|------------------|--|
| | noms distinctifs | auxquels le PSO doit s'appliquer. |
| Protégé d'une suppression accidentelle | Vrai ou faux | Définit si le PSO doit être protégé contre toute suppression accidentelle. |

Vous pouvez créer et appliquer les PSO dans le Windows Server 2012 et plus récents environnement en utilisant l'un des outils suivants :

- Windows PowerShell
- **Centre d'administration Active Directory**

La configuration IPv4 à l'aide de Windows PowerShell

Dans Windows Server 2012 et plus récents, vous pouvez utiliser les cmdlets de commande suivantes dans le module Active Directory pour Windows PowerShell pour créer et gérer des PSO dans votre domaine.

- **New-ADFineGrainedPasswordPolicy.** Ce cmdlet crée une nouvelle PSO et définit ses paramètres. Par exemple, la commande suivante crée un nouveau PSO nommé **TestPwd**, puis spécifie ses paramètres :

```
New-ADFineGrainedPasswordPolicy TestPwd -ComplexityEnabled: $ true -LockoutDuration: "00:30:00" -LockoutObservationWindow: "00:30:00" -LockoutThreshold: -MaxPasswordAge "0": "42.00: 00: 00" -MinPasswordAge: "1.00 : 00: 00" -MinPasswordLength:" 7 "- PasswordHistoryCount:" 24 1 "-ReversibleEncryptionEnabled: $ false - ProtectedFromAccidentalDeletion: $ true
```

- **Add-FineGrainedPasswordPolicySubject.** Cette commande vous permet de lier un utilisateur ou un groupe à un PSO existant. Par exemple, la commande suivante lie le PSO de **TestPwd** au groupe AD DS nommé **Marketing** :

```
Add-ADFineGrainedPasswordPolicySubject testpwd -Subjects marketing
```

Configuration PSO en utilisant le Centre d'administration Active Directory

Le **Centre d'administration Active Directory** fournit une interface graphique pour la création et la gestion des PSO. Pour gérer les PSO dans le **Centre d'administration Active Directory**, suivez cette procédure :

1. Ouvrez le **Centre d'administration Active Directory**.
2. Cliquez sur **Gérer**, sur **Ajouter des nœuds de navigation**, dans la boîte de dialogue **Ajouter un nœud de navigation**, sélectionnez le domaine cible approprié, puis cliquez sur **OK**.
3. Dans le volet de navigation **Centre d'administration Active Directory**, ouvrez le conteneur **Système**, puis cliquez sur **Conteneur de paramètres de mot de passe**.
4. Dans le volet **Tâches**, cliquez sur **Nouveau**, puis cliquez sur **Paramètres du mot de passe**.
5. Configurez les paramètres de la nouvelle PSO.
6. Sous **Appliquez directement à**, cliquez sur **Ajouter**, tapez **Marketing**, puis cliquez sur **OK**.
Cela associe l'objet **Stratégie de mot de passe** aux membres du groupe global que vous avez créé pour l'environnement de test.
7. Cliquez sur **OK** pour soumettre la création du PSO.



Remarque : L'interface du **Centre d'administration Active Directory** pour la gestion PSO utilise les cmdlets de commande Windows PowerShell mentionnés précédemment pour effectuer la création et la gestion des PSO.

Démonstration : Configuration d'une stratégie de mot de passe affiné

Dans cette démonstration, vous allez apprendre à créer et à déployer une stratégie de mot de passe affiné.

Procédure de démonstration

1. Sur **LON-DC1**, ouvrez le **Centre d'administration Active Directory**.
2. Modifiez la portée de groupe pour le groupe **Gestionnaires** à **Global**.



Remarque : Assurez-vous que vous ouvrez la boîte de dialogue **Propriétés** pour le groupe Managers, et non Managers OU.

3. Dans le **Centre d'administration Active Directory**, configurez une stratégie de mots de passe précis pour le groupe **Adatum\Managers** avec les paramètres suivants :
 - o Nom : **ManagersPSO**
 - o Priorité : **10**
 - o Longueur du MDP : **15 caractères**
 - o Historique des mots de passe : **20 mots de passe**
 - o Complexité activé : **Oui**
 - o Âge minimal du mot de passe : **1 jour**
 - o Âge maximal du mot de passe : **30 jours**
 - o Nombre d'échecs de tentatives de connexion autorisées : **3 tentatives**
 - o Réinitialiser l'échec des tentatives d'ouverture de session compte après : **30 minutes**
 - o Sélectionnez **Jusqu'à ce qu'un administrateur déverrouille manuellement le compte**.
4. Fermez le **Centre d'administration Active Directory**.

Priorité PSO et PSO résultante

Vous pouvez lier plus d'un PSO à un utilisateur ou un groupe de sécurité. Cela se produit quand un utilisateur est membre de plusieurs groupes de sécurité qui pourraient avoir chacun déjà un PSO cédé ou lorsque vous affectez plusieurs PSO directement à un objet utilisateur. Dans les deux cas, un seul PSO peut être la politique de mot de passe efficace. Si vous affectez plusieurs PSO à un utilisateur ou un groupe, l'attribut **msDS-PasswordSettingsPrecedence** permet de déterminer la PSO résultante. Un PSO avec une valeur inférieure a la priorité sur un PSO avec une valeur plus élevée.

msDS-PasswordSettingsPrecedence permet de déterminer la PSO résultante. Un PSO avec une valeur inférieure a la priorité sur un PSO avec une valeur plus élevée.

- Si des PSO multiples s'appliquent à un utilisateur :
 - Les PSO que vous appliquez directement prennent priorité sur les PSO que vous appliquez à l'aide d'adhésions du groupe
 - Le PSO avec la priorité la plus basse l'emporte
 - Si deux PSO ont la même priorité, le plus petit objectGUID l'emporte
- Pour évaluer un objet utilisateur et voir quel PSO a été appliqué, vous pouvez utiliser l'attribut Active Directory **msDS-ResultantPSO**
- Pour afficher le PSO efficace que l'AD DS applique à un utilisateur :
 1. Ouvrez Utilisateurs et ordinateurs Active Directory, et dans le menu **Affichage**, veillez à ce que les Fonctionnalités avancées sont activées
 2. Ouvrez les propriétés d'un compte d'utilisateur
 3. Dans l'onglet **Éditeur d'attributs**, visualisez l'attribut **msDS-ResultantPSO** si vous avez configuré l'option **Afficher les attributs construits** sous les options de **Filtre**

Le processus suivant décrit comment AD DS détermine la PSO résultante si vous liez plusieurs PSO à un utilisateur ou un groupe :

1. Tout PSO que vous liez directement à un objet utilisateur est le PSO résultant. Si vous reliez plusieurs PSO directement à l'objet utilisateur, le PSO avec la valeur **msDS-PasswordSettingsPrecedence** la plus faible est le PSO résultant. Si deux PSO ont la même priorité, le PSO avec le plus petit mathématiquement objectGUID est le PSO résultant.
2. Si vous ne liez pas les PSO directement à l'objet utilisateur, AD DS compare les PSO pour tous les groupes de sécurité globaux qui contiennent l'objet utilisateur. Le PSO avec la plus faible valeur **msDS-PasswordSettingsPrecedence** est le PSO résultant. Si vous appliquez plusieurs PSO au même utilisateur et qu'ils possèdent la même valeur **msDS-PasswordSettingsPrecedence**, AD DS applique le PSO avec l'objectGUID mathématiquement le plus petit.
3. Si vous ne liez pas PSO à l'objet utilisateur, que ce soit directement ou indirectement par l'appartenance au groupe, AD DS applique la stratégie par défaut de domaine.

Tous les objets utilisateur contiennent un nouvel attribut appelé **msDS-ResultantPSO**. Vous pouvez utiliser cet attribut pour déterminer le nom unique du PSO que AD DS applique à l'objet de l'utilisateur. Si vous ne liez pas un PSO à l'objet de l'utilisateur, cet attribut ne contient pas de valeur et par défaut Stratégie de domaine contient la politique de mot de passe efficace. Pour afficher le PSO efficace que AD DS applique à un utilisateur, ouvrez **Utilisateurs et ordinateurs Active Directory** et, dans le menu **Affichage**, assurez-vous que les **fonctionnalités avancées** sont activées. Vous devez alors ouvrir les propriétés d'un compte d'utilisateur et afficher l'attribut **msDS-ResultantPSO** dans l'onglet **Éditeur d'attributs** si vous avez configuré l'option **Afficher les attributs construits** sous les options **Filtre**.



Remarque : Alors que vous devez définir les PSO à partir d'un groupe très privilégié, comme Domain Admins, vous devez former les help-desk administrateurs pour évaluer les PSO efficaces pour un utilisateur. Cela aide les administrateurs à répondre aux questions des utilisateurs quand ils ne comprennent pas quels sont les paramètres de mot de passe à appliquer.

Options de sécurité du compte dans Windows Server 2016

Les comptes sécurisés créent une infrastructure de domaine et de forêt AD DS sécurisée. Par défaut, tous les comptes qui se connectent à un client ou à un serveur relié au domaine sont mis en cache localement sur cet ordinateur. L'ordinateur maintient, par défaut, les 10 derniers profils d'utilisateurs et leurs informations d'identification associées. Ce problème peut se produire dans les situations suivantes :

- Prenez un compte administratif qui est utilisé pour dépanner ou aider les utilisateurs à l'aide d'une connexion locale au périphérique d'un utilisateur classique. Le profil de compte d'utilisateur et ses informations d'identification sont stockés dans le système. Si le propriétaire du système a des droits locaux plus élevés, il peut se servir d'outils pour récupérer les informations d'identification administratives, puis les utiliser pour accéder à d'autres informations sur le réseau.
- Certains comptes d'utilisateurs et ordinateurs contiennent des informations très importantes sur votre organisation. Par conséquent, veillez à ce que seuls les utilisateurs autorisés puissent se connecter à leurs stations de travail, et faites en sorte que d'autres utilisateurs ne puissent pas accéder aux mêmes ordinateurs.

Vous devez configurer les comptes de services hautement fiables pour l'autorisation que sur un certain ensemble d'ordinateurs.

Pour fournir aux administrateurs la possibilité de remédier à ces risques et de répondre à ces exigences, Windows Server 2016 et Windows Server 2012 R2 incluent de nouvelles fonctionnalités pour la protection et la gestion des informations d'identification :

- Utilisateurs protégés
- Stratégies d'authentification
- Silos de la stratégie d'authentification

Utilisateurs protégés

Le groupe de sécurité des Utilisateurs protégés empêche les comptes très sensibles d'être mis en cache localement sur les ordinateurs membres du domaine. Il requiert une authentification du contrôleur de domaine pour ces comptes à chaque connexion.

Les Utilisateurs protégés forment un nouveau groupe que vous pouvez utiliser pour configurer des comptes très sensibles et que vous pouvez trouver dans le conteneur Utilisateurs de AD DS. Pour activer les Utilisateurs protégés, un administrateur ajoute simplement les comptes hautement fiables au groupe de sécurité Utilisateurs protégés. La fonctionnalité Utilisateurs protégés ne nécessite pas de contrôleurs de domaine Windows Server 2012 R2. Cependant, ce groupe est uniquement créé lorsqu'un contrôleur de domaine Windows Server 2012 R2 ou versions plus récentes reçoit le rôle de maître d'opérations émulateur de PDC. Pour encore plus utiliser cette fonctionnalité, il n'est pas nécessaire de laisser le maître d'opérations émulateur de PDC sur le contrôleur de domaine Windows Server 2012 R2 ni de garder le contrôleur de domaine. Cependant, compte tenu du fait que le contrôleur de domaine peut uniquement être promu lorsque le schéma a été étendu, l'extension de schéma pour Windows Server 2012 R2 ou les versions plus récentes doit être en place, même si la fonctionnalité ne l'exige pas.

Le groupe Utilisateurs protégés :

- Protège les utilisateurs dans le groupe des utilisateurs protégés
- Bloque les profils d'utilisateur et les informations d'identification localement mis en cache
- Nécessite l'authentification Kerberos, limite le ticket TGT à quatre heures
- Aucune connexion hors ligne
- Membres des domaines Windows 8.1, Windows 10, Windows Server 2012 R2 ou Windows Server 2016 uniquement

Stratégies d'authentification :

- Configurées comme objet de stratégie d'authentification dans AD DS, s'appliquent à l'utilisateur, au service ou aux comptes d'ordinateur
- Personnaliser le ticket TGT
- Utilise les réclamations (DAC) pour personnaliser les conditions

Cloisonnements de la stratégie d'authentification :

- Objet AD DS
- Appliquez des stratégies d'authentification à plusieurs objets, de façon centralisée
- Une revendication supplémentaire permet aux administrateurs de configurer l'accès aux fichiers par silo

La fonctionnalité Utilisateurs protégés est une fonctionnalité côté client qui protège les comptes de domaine sur les ordinateurs membres du domaine. Les Utilisateurs protégés dépendent du système d'exploitation du membre du domaine et sont disponibles sur les systèmes d'exploitation suivants :

- Windows 8.1 ou versions plus récentes
- Windows Server 2012 R2 ou versions plus récentes

Les systèmes d'exploitation plus anciens ne prendront pas en charge cette fonctionnalité et n'empêcheront pas les comptes du groupe Utilisateurs protégés d'être mis en cache localement. Pour garantir que les comptes au sein du groupe Utilisateurs protégés ne sont pas compromis sur les systèmes d'exploitation plus anciens, utilisez les autres méthodes telles que le paramètre de sécurité **Refuser une ouverture de session locale** le cas échéant.

Les Utilisateurs protégés qui se connectent à un ordinateur membre du domaine possédant un système d'exploitation pris en charge ne pourront pas utiliser les protocoles suivants :

- Délégation des informations d'identification par défaut ou fournisseur de support de sécurité des informations d'identification (CredSSP)
- Authentification condensée
- NTLM

Une sécurité supplémentaire est fournie lorsque tous les contrôleurs de domaine du domaine de connexion sont basés sur Windows Server 2012 R2 et que le niveau fonctionnel du domaine est mis au niveau de Windows Server 2012 R2. En raison de cette sécurité supplémentaire, les utilisateurs ne peuvent pas :

- Utiliser le cryptage DES ou RC4 dans la préauthentification Kerberos.
- Être délégués avec la délégation contrainte ou non contrainte.
- Renouveler leur Kerberos TGT sans contact avec le contrôleur de domaine.

Les conditions suivantes s'appliquent lorsqu'un utilisateur est membre du groupe de sécurité Utilisateurs protégés :

- L'utilisateur doit être en mesure d'utiliser l'authentification basée sur le cryptage AES. Par conséquent, tous les contrôleurs de domaine doivent être mis au niveau de Windows Server 2008 ou de ses versions plus récentes.
- Le mot de passe d'un compte du groupe Utilisateurs protégés doit avoir été changé auprès d'un contrôleur de domaine Windows Server 2008 ou versions plus récentes pour garantir que le mot de passe a été chiffré en utilisant AES.
- Sur les membres du domaine pris en charge, tels que Windows 10 et Windows Server 2016, les informations d'identification de l'utilisateur ne seront pas mises en cache.
- L'utilisateur pourra seulement se connecter aux membres du domaine qui peuvent s'authentifier auprès d'un contrôleur de domaine. L'ouverture de session hors connexion ne fonctionnera pas pour ces comptes. Le démarrage des services qui utilisent un compte membre du groupe Utilisateurs protégés échouera lorsque le membre du domaine sera déconnecté.
- La durée de vie maximale d'un TGT Kerberos émis ainsi que la durée de vie maximale de renouvellement d'un ticket sont limitées à 240 minutes (quatre heures). Même si les administrateurs configurent tous les autres comptes en utilisant les paramètres de stratégie de domaine, qui sont définis par défaut à 10 heures pour le ticket et à sept jours pour le renouvellement, quatre heures sont codées en dur pour les Utilisateurs protégés.

La fonctionnalité Utilisateurs protégés est un paramètre de sécurité qui est global dans le domaine. Ce paramètre ne vous permet pas de protéger certains utilisateurs uniquement sur certains périphériques. Par conséquent, utilisez la fonctionnalité Utilisateurs protégés avec prudence et testez-la avant de vous en remettre à elle.

Stratégies d'authentification

Avec les stratégies d'authentification, vous pouvez configurer des paramètres Kerberos plus restrictifs pour les comptes utilisateur ou service spécifiques. En outre, vous pouvez utiliser des revendications DAC pour définir les conditions devant être remplies par les utilisateurs, les comptes de service et/ou les périphériques lors de la connexion.

Stratégies d'authentification à mettre en œuvre à l'aide d'une nouvelle classe d'objets nommée **stratégie d'authentification** dans AD DS.

Pour mettre en œuvre des stratégies d'authentification, vous devez vous assurer que vous répondez aux conditions suivantes, y compris que :

- Tous les contrôleurs de domaine dans le domaine sont basés sur Windows Server 2012 R2 ou versions plus récentes.
- Le niveau fonctionnel du domaine est Windows Server 2016 ou Windows Server 2012 R2.
- Les contrôleurs de domaine sont configurés pour prendre en charge le DAC.
- Les membres des domaines Windows 10, Windows 8.1, Windows 8, Windows Server 2016, Windows Server 2012 R2, ou Windows Server 2012 sont configurés pour prendre en charge le DAC, notamment les revendications mixtes Kerberos (revendications de périphériques).

Lors de la configuration d'une stratégie d'authentification dans le **Centre d'administration Active Directory**, vous pouvez configurer les paramètres suivants :

- Le nom d'affichage de la stratégie d'authentification.
- La description.
- Si la stratégie doit être appliquée (par défaut), ou si vous souhaitez valider uniquement la stratégie par des restrictions de stratégie d'audit.
- Les comptes sur lesquels la stratégie doit être appliquée. Les comptes se trouvent dans les paramètres de stratégie d'authentification ; sachez toutefois que vous les configurez sur le compte, contrairement aux silos de la stratégie d'authentification, pour lesquels les comptes sont configurés dans le silo.
- Pour l'utilisateur, le service, et les comptes d'ordinateurs, vous pouvez définir séparément les paramètres suivants :
 - La durée de vie des TGT du compte.
 - Les conditions de contrôle d'accès à l'aide des revendications DAC qui définissent les utilisateurs ou les services capables de fonctionner sur tels périphériques.

Vous pouvez configurer ces paramètres pour les comptes d'utilisateurs dans la fenêtre des propriétés de l'utilisateur du **Centre d'administration Active Directory**, ou dans la fenêtre des propriétés de la stratégie d'authentification. Peu importe où vous configurez ces paramètres, ils sont écrits sur la stratégie d'authentification. Après avoir configuré ces paramètres, vous pourrez vous connecter à un périphérique, ou vous recevrez le message : « Votre compte est configuré pour vous empêcher d'utiliser ce PC ». Dans les deux cas, un événement est enregistré.



Remarque : Même si les systèmes d'exploitation plus anciens avaient des options pour empêcher certains utilisateurs de se connecter à des périphériques spécifiques, ils étaient faciles à contourner. Les stratégies d'authentification, les silos de la stratégie d'authentification basés sur Kerberos (en dépit des noms uniquement), ainsi que les revendications DAC fournissent une méthode sécurisée pour garantir que seuls certains utilisateurs peuvent se connecter à certains périphériques.



Remarque : Les stratégies d'authentification n'empêchent pas les utilisateurs de se connecter à l'aide de NTLM. Quand un membre de domaine est entièrement capable de communiquer en utilisant Kerberos, il est probable que les règles configurées dans la stratégie d'authentification fonctionnent comme prévu. Cependant, il pourrait y avoir des scénarios dans lesquels le NTLM est utilisé. Pour éviter cela, envisagez de combiner la fonctionnalité Utilisateurs protégés avec les stratégies de compte.

Silos de la stratégie d'authentification

Les silos de la stratégie d'authentification permettent aux administrateurs de configurer les utilisateurs, les comptes de service, et les ordinateurs dans un même périmètre de sécurité pour appliquer la même stratégie d'authentification. Les stratégies d'authentification permettent aux administrateurs de sélectionner une stratégie d'authentification distincte pour chaque type d'entité de sécurité : les comptes d'utilisateurs, de services, ou d'ordinateurs. Le système ajoute ensuite une revendication supplémentaire aux entités d'un silo, ce qui permet aux administrateurs de serveurs de fichiers de restreindre l'accès à certains fichiers pour les entités de sécurité des silos de la stratégie d'authentification spécifiques.

Les conditions préalables des silos de la stratégie d'authentification sont les mêmes que pour les stratégies d'authentification. Vous devez les utiliser comme un moyen alternatif pour charger l'utilisateur, le service, ou les comptes d'ordinateurs d'utiliser certaines stratégies d'authentification. En utilisant la délégation Active Directory, vous êtes en mesure d'attribuer différents rôles pour créer des stratégies d'authentification puis affecter ces stratégies aux entités de sécurité à l'aide des silos de la stratégie d'authentification.

Comme pour les stratégies d'authentification, vous pouvez configurer des silos de stratégie d'authentification à appliquer ou en mode audit. Les stratégies d'authentification sont appliquées par défaut, tandis que les silos de la stratégie d'authentification sont configurés en mode audit. En outre, les silos de stratégie d'authentification ont une priorité plus élevée que les stratégies d'authentification.

De même, les silos de la stratégie d'authentification fournissent une revendication et un administrateur peut l'utiliser pour faire en sorte que certains fichiers ou certaines structures de fichiers soient uniquement accessibles lorsque les utilisateurs ou les ordinateurs ont été validés par un silo de la stratégie d'authentification.



Lectures supplémentaires : pour plus d'informations sur la protection des informations d'identification et la gestion, consultez le site suivant : <http://aka.ms/R5bfid>

Configuration des stratégies de compte d'utilisateur

Plusieurs options sont disponibles pour configurer les stratégies de compte d'utilisateur lorsque vous administrez un environnement AD DS.

Paramètres de stratégie locale avec Secpol.msc

Chaque ordinateur Windows Server 2016 individuel a son propre ensemble de stratégies de compte, applicables aux comptes créés et administrés sur l'ordinateur local. Pour configurer ces paramètres de stratégie, ouvrez la **Console de stratégie de sécurité locale** en exécutant **secpol.msc** à l'invite de commande. Vous pouvez trouver les paramètres de la stratégie de mot de passe et de la stratégie de compte dans la **Console de stratégie de sécurité locale** en développant les **Paramètres de sécurité**, puis les **Stratégies de compte**.

- Paramètres de compte de stratégie de sécurité locale :
 - Configurez avec **secpol.msc**
 - Appliquez aux comptes d'utilisateurs locaux
- Paramètres de compte de stratégie de groupe :
 - Configurez avec la console de gestion des stratégies de groupe
 - Appliquez à tous les comptes dans AD DS et comptes locaux sur les ordinateurs reliés au domaine
 - Ne peut s'appliquer qu'une seule fois dans un domaine et dans un seul GPO
 - Prend la préséance sur les paramètres de stratégie de sécurité locale

Stratégie de groupe avec la gestion de stratégie de groupe

Dans l'environnement de domaine AD DS, vous pouvez configurer les paramètres de stratégie de compte au niveau du domaine au sein de l'Éditeur de gestion de stratégie de groupe. Pour trouver les paramètres de stratégie de compte au niveau du domaine appartenant aux paramètres, développez le nœud **Configuration de l'ordinateur**, puis le nœud **Stratégies**, puis le nœud **Paramètres Windows**, puis le nœud **Paramètres de sécurité** et enfin le nœud **Stratégies de compte**.

Les paramètres trouvés dans le nœud **Stratégies de compte** sont les mêmes que ceux trouvés dans la stratégie de sécurité locale, auxquels s'ajoutent les paramètres de stratégie Kerberos applicables à l'authentification de domaine.

Les paramètres de stratégie de compte de la stratégie de groupe existent dans le modèle de chaque GPO que vous créez dans la console de gestion des stratégies de groupe. Cependant, vous pouvez appliquer une stratégie de compte qu'une seule fois dans un domaine et dans un seul GPO. Ceci est la stratégie de domaine par défaut, et elle est reliée à la racine du domaine AD DS. Par conséquent, les paramètres de stratégie de compte dans la stratégie de domaine par défaut s'appliquent à chaque ordinateur associé au domaine.



Remarque : Si les paramètres de stratégie de compte de la stratégie de sécurité locale entrent en conflit avec les paramètres de stratégie de compte du GPO de la stratégie de domaine par défaut, les paramètres de stratégie de domaine par défaut sont alors prioritaires.

Lorsque vous commencez par installer un système d'exploitation Windows, tel que Windows 8.1, Windows 10, ou Windows Server 2016, l'ordinateur possède une stratégie de mot de passe avec des paramètres configurés et mis en place par défaut, contrairement à la stratégie de verrouillage de compte dont les paramètres ne sont pas configurés. Lorsque vous installez un domaine, la stratégie de domaine par défaut créée contient les trois stratégies. Vous pouvez apporter des modifications à ces stratégies, notamment configurer les paramètres de la stratégie de verrouillage de compte. Cependant, vous devez examiner attentivement les conséquences de cette action avant de la réaliser.

Dans la plupart des cas, votre organisation aura déjà mis en place des domaines et des systèmes informatiques qui ont ces paramètres configurés. La plupart des organisations ont aussi de nombreuses stratégies de sécurité écrites qui dictent les normes pour les stratégies de verrouillage des mots de passe et des comptes. Dans ce cas, vous ne pouvez pas apporter de modifications sans approbation ou réponse aux stratégies de sécurité écrites.

Amélioration de l'authentification par mot de passe avec Windows Hello et MFA

Comme les identités des utilisateurs deviennent plus critiques, il est nécessaire de développer de nouvelles technologies pour protéger les identités ainsi que le processus de vérification ou d'authentification des identités. Microsoft fournit des technologies d'authentification améliorées qui combinent plusieurs facteurs dans les nouvelles versions de systèmes d'exploitation et les services de cloud.

Windows Bonjour et Microsoft Passport

Pour améliorer la sécurité côté client, et sécuriser encore plus le processus d'authentification,

Microsoft a mis en œuvre les technologies Microsoft Passport et Windows Hello dans le système d'exploitation Windows 10. Ces technologies vous permettent d'utiliser des méthodes différentes ou supplémentaires d'authentification, à la place de la traditionnelle combinaison d'un nom d'utilisateur et d'un mot de passe.

Windows Hello est la technologie biométrique qui permet aux utilisateurs de se connecter à Windows à l'aide de leurs empreintes digitales, de la reconnaissance faciale, ou du balayage de l'iris. De nombreux ordinateurs portables d'entreprise intègrent aujourd'hui des lecteurs d'empreintes digitales, et Windows Hello prend en charge la plupart des matériels de lecture d'empreintes digitales existants. En outre, sur certains appareils mobiles, tels que le Microsoft Lumia 950, une caméra de balayage de l'iris est disponible, et Windows Hello est utilisé pour reconnaître un utilisateur et lui permettre de se connecter.

La technologie Windows Hello vous permet d'utiliser des méthodes alternatives et plus sûres pour vous connecter à votre ordinateur ou à votre périphérique portable. De plus, compte tenu du fait que la technologie Windows Hello est extensible, elle sera compatible avec les nouveaux matériels qui ne sont pas encore disponibles sur le marché.

Microsoft Passport est une technologie qui complète Windows Hello. Microsoft Passport fournit une authentification à deux facteurs en combinant les données biométriques de Windows Hello avec les clés de cryptage prises à partir du périphérique. Microsoft Passport vous permet également d'établir un code PIN que vous pouvez utiliser pour vous connecter à un périphérique Windows 10, au lieu d'utiliser un mot de passe. L'utilisation d'un code PIN à la place d'un mot de passe est plus sûre, car le code PIN est lié au périphérique que vous utilisez. Vous pouvez établir un code PIN différent pour chaque périphérique que vous utilisez, mais vous serez toujours connecté avec un même compte d'utilisateur.

Microsoft Passport est une technologie qui utilise intensivement les processeurs du Module de plateforme sécurisée (TPM). TPM offre la possibilité de stocker des clés d'authentification en toute sécurité. Lorsque l'utilisateur s'authentifie sur Windows Hello en utilisant le mécanisme de la biométrie, Microsoft Passport récupère les données d'authentification et les utilise pour que le processeur TPM puisse générer un ensemble de clés publiques et privées.

Sur chaque périphérique Windows 10 (portable, bureau, et ordinateur portable), vous pouvez configurer plusieurs méthodes d'authentification. Par exemple, vous pouvez configurer un code PIN mais aussi utiliser votre empreinte digitale pour vous connecter à votre ordinateur Windows 10. De plus à chaque connexion, vous pouvez choisir la méthode vous allez utiliser. De même, sur votre appareil mobile Windows 10, tel que le Lumia 950, vous pouvez utiliser un code PIN ou le balayage de l'iris pour déverrouiller l'appareil.

Pour améliorer la sécurité du processus d'authentification, vous pouvez utiliser :

- Windows Hello :
 - Pour une connexion biométrique à Windows
- Microsoft Passport :
 - Pour exploiter Windows Hello et TPM
- Azure Multi-Factor Authentication :
 - Pour améliorer la sécurité de compte en ajoutant un deuxième facteur de vérification
 - Peut être utilisé dans le cloud ou pour des applications sur site



Windows Hello est la technologie que vous pouvez utiliser non seulement pour vous authentifier sur le système d'exploitation mais également sur votre application. Les développeurs peuvent utiliser Windows Hello pour renforcer la sécurité de leurs applications qui nécessitent une authentification.

Authentification multifacteurs Microsoft Azure

Le but de l'Authentification multifacteurs (MFA) est de renforcer la sécurité. L'authentification classique et habituelle exige de connaître les informations d'identification de connexion, qui se composent généralement d'un nom d'utilisateur associé à un mot de passe. L'authentification multifacteurs ajoute une vérification supplémentaire qui repose sur l'accès à un dispositif qui est vraisemblablement en possession du propriétaire légitime ou les caractéristiques physiques de cette personne, comme c'est le cas pour la biométrie. Cette exigence supplémentaire permet de rendre le processus d'authentification beaucoup plus difficile à compromettre par une personne non autorisée.

L'authentification multifacteurs est intégrée dans Azure Active Directory (Azure AD). Elle permet d'utiliser un téléphone comme un périphérique physique qui fournit les moyens de confirmer l'identité d'un utilisateur. Le processus de mise en œuvre de l'Authentification multifacteurs pour un compte d'utilisateur Azure AD commence quand un utilisateur possédant le rôle d'administrateur global active le compte pour l'Authentification multifacteurs à partir du portail Azure. Lors de la prochaine tentative de connexion, l'utilisateur est invité à mettre en place un système d'authentification en sélectionnant l'une des options suivantes :

- Téléphone mobile. Requiert que l'utilisateur donne un numéro de téléphone portable. La vérification peut se faire sous la forme d'un message texte ou d'un appel téléphonique, à la fin duquel l'utilisateur doit appuyer sur la touche dièse (#).
- Téléphone du bureau. Requiert la spécification de l'entrée TÉLÉPHONE DU BUREAU des informations de contact de l'utilisateur dans Azure AD. Un administrateur doit préconfigurer cette entrée, et l'utilisateur ne peut pas modifier ou fournir cette entrée au moment de la vérification.
- Application mobile. Requiert que l'utilisateur dispose d'un smartphone sur lequel il a installé et configuré l'application de téléphone mobile.

Un utilisateur peut également générer des mots de passe d'application dans le cadre du processus de vérification, car l'Authentification multifacteurs est limitée à l'authentification de l'accès aux applications et services à partir d'un navigateur. En effet, elle ne s'applique pas aux applications traditionnelles de bureau, aux applications modernes telles qu'Outlook, Skype Entreprise, ou aux applications mobiles pour les e-mails. Un utilisateur peut alors utiliser les paramètres de configuration de ces applications pour attribuer des mots de passe d'application aléatoirement générés aux applications individuelles.

Néanmoins, les mots de passe d'application peuvent être vulnérables aux attaques. Par conséquent, en tant qu'administrateur, vous pouvez empêcher tous les utilisateurs d'annuaire de créer des mots de passe d'application. Vous pouvez également annuler tous les mots de passe d'application pour un utilisateur individuel si l'ordinateur ou le périphérique sur lequel les applications sont installées est compromis.

Une fois le processus de vérification terminé, l'état de l'Authentification multifacteurs pour l'utilisateur change et passe de l'état activé à appliqué. Le même processus de vérification est répété lors de chaque tentative d'authentification ultérieure. L'option de vérification de sécurité supplémentaire apparaît dans le Panneau d'accès, qui reflète le changement d'état. Dans le Panneau d'accès, vous pouvez choisir et configurer un mécanisme de vérification différent et générer des mots de passe d'application. La génération de mots de passe d'application est particulièrement importante, car sans mots de passe d'application attribués, les applications de bureau et les applications modernes qui dépendent de l'accès authentifié à Azure AD ne parviendront pas à se connecter au service de cloud Azure.

Vous pouvez utiliser l'Authentification multifacteurs pour protéger des ressources locales grâce au serveur d'Authentification multifacteurs Azure. Le serveur d'Authentification multifacteurs s'intègre à l'authentification Internet Information Services (IIS) pour sécuriser les applications Web Microsoft IIS,

l'authentification du protocole RADIUS (Remote Authentication Dial-In User Service), l'authentification du protocole LDAP (Lightweight Directory Access Protocol) et l'authentification Windows.

Avant de pouvoir utiliser le serveur de l'Authentification multifacteurs, vous devez le télécharger et l'activer. Le téléchargement est disponible via un lien sur le portail de gestion de l'Authentification multifacteurs. Le portail utilisateur de l'Authentification multifacteurs Azure est un site web Internet Information Services (IIS) sur lequel les utilisateurs peuvent s'inscrire à l'Authentification multifacteurs Azure et gérer leurs comptes d'Authentification multifacteurs.

L'inscription et l'autogestion des utilisateurs impliquent qu'ils remplissent leur inscription, par exemple en sélectionnant une méthode d'authentification si l'administrateur n'en a pas préspécifié.

Question : Quelle technologie vous permet d'utiliser la fonctionnalité biométrique pour vous connecter à des périphériques Windows ?

Leçon 3

Mise en œuvre d'authentification d'audit

L'audit est un élément important de la sécurité. Les contrôleurs de domaine Windows Server 2016 ainsi que d'autres serveurs enregistrent les événements liés à la sécurité dans le journal de sécurité, que vous pouvez utiliser pour surveiller et identifier les problèmes pouvant justifier un examen plus approfondi. L'audit peut enregistrer les activités réussies pour fournir des documents sur les changements apportés. Il peut également enregistrer les tentatives ratées et potentiellement malveillantes visant à accéder aux ressources de l'entreprise. L'audit se compose de trois étapes de gestion au maximum : la configuration d'une stratégie d'audit, la configuration des paramètres d'audit sur les objets, et l'affichage des événements dans le journal de sécurité. Dans cette leçon, vous apprendrez à configurer l'audit pour répondre à plusieurs scénarios fréquents.

Objectifs de la leçon

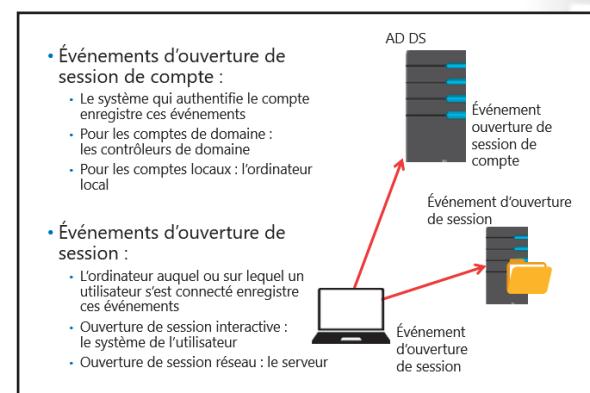
À la fin de cette leçon, vous serez à même de :

- Décrire la connexion au compte et les événements de connexion
- Configurer des stratégies d'audit liées à l'authentification.
- Décrire la portée des stratégies d'audit.
- Afficher des événements d'ouverture de session.

Connexion au compte et événements de connexion

Avant de configurer l'audit, vous devez d'abord comprendre la différence qui existe entre deux paramètres de stratégie portant des noms similaires : **Audit des événements de connexion au compte** et **Audit des événements de connexion**.

Lorsqu'un utilisateur se connecte à un ordinateur dans le domaine en utilisant un compte d'utilisateur du domaine, un contrôleur de domaine authentifie cette tentative. Cela génère un événement de connexion au compte sur le contrôleur de domaine.



L'ordinateur sur lequel l'utilisateur s'est connecté, par exemple, l'ordinateur portable de l'utilisateur, génère un événement de connexion. L'ordinateur n'a pas authentifié l'utilisateur d'après le compte, mais a plutôt passé le compte à un contrôleur de domaine pour validation. Toutefois, l'ordinateur a permis à l'utilisateur de se connecter de manière interactive à l'ordinateur. Par conséquent, l'événement est un événement de connexion.

Lorsqu'un utilisateur se connecte à un dossier sur un serveur du domaine, ce serveur autorise une ouverture de session réseau à l'utilisateur, c'est-à-dire un type de connexion. Encore une fois, le serveur n'authentifie pas l'utilisateur. Au contraire, il se base sur le ticket que le contrôleur de domaine a donné à l'utilisateur. La connexion de l'utilisateur génère toutefois un événement de connexion sur le serveur.

Stratégies d'audit avancées

Dans les versions précédentes de Windows Server, telles que Windows Server 2008, il n'y a que neuf catégories d'audit. Les administrateurs peuvent configurer chaque catégorie pour effectuer l'audit et

surveiller la réussite, l'échec, ou à la fois la réussite et l'échec de tâches et événements spécifiques. Ces événements ont une portée assez étendue et peuvent être déclenchés par une multitude d'actions similaires, dont certains peuvent générer un grand nombre d'entrées dans le journal des événements.

Dans Windows Server 2012 et Windows Server 2016, le nombre d'événements vérifiables est passé de neuf à 53, permettant ainsi aux administrateurs d'être plus sélectifs quant au nombre et au type d'événements à auditer.

Ces nouvelles stratégies d'audit avancées permettent aux administrateurs de rassembler les règles d'entreprise et les stratégies d'audit. Cela donne beaucoup plus de contrôle aux administrateurs sur le processus d'ouverture de session et leur permet d'obtenir des informations sur des événements très spécifiques qui se produisent au cours des processus d'ouverture ou de fermeture de session.

Pour un événement de connexion au compte, vous pouvez maintenant définir quatre paramètres d'audit différents :

- **Validation des informations d'identification.** Vérifie les événements générés par les tests de validation sur les informations d'identification de connexion au compte d'utilisateur.
- **Opérations de ticket de service Kerberos.** Vérifie les événements générés par les demandes de ticket de service Kerberos.
- **Autres événements de connexion au compte.** Vérifie les événements générés en réponse aux demandes d'informations d'identification qui ne sont pas des demandes de tickets Kerberos ou de validation d'informations d'identification.
- **Service d'authentification Kerberos.** Vérifie les événements générés par les demandes TGT d'authentification Kerberos.

Vous pouvez vérifier les événements de connexion et de déconnexion suivants :

- **Connexion.** Vérifie les événements générés par les tentatives de connexion à un compte d'utilisateur sur un ordinateur.
- **Déconnexion.** Vérifie les événements générés par la fermeture d'une session ouverte. Ces événements se produisent sur l'ordinateur accessible, et pour une connexion interactive, l'événement d'audit de sécurité est généré sur l'ordinateur auquel le compte d'utilisateur est connecté.
- **Verrouillage de compte.** Vérifie les événements générés par une tentative ratée de se connecter à un compte verrouillé.
- **Mode principal IPsec.** Vérifie les événements générés par le protocole IKE (Internet Key Exchange) et le protocole Internet authentifié (AuthIP) pendant les principales négociations de mode.
- **Mode rapide IPsec.** Vérifie les événements générés par IKE et AuthIP au cours des négociations de mode rapide.
- **Mode étendu IPsec.** Vérifie les événements générés par IKE et AuthIP au cours des négociations de mode étendu.
- **Ouverture de session spéciale.** Vérifie les événements générés par des connexions spéciales.
- **Autres événements de connexion et de déconnexion.** Vérifie d'autres événements liés à l'ouverture et à la fermeture de session qui ne sont pas inclus dans les paramètres de **Connexion** et de **Déconnexion**.
- **Serveur NPS (Network Policy Server).** Vérifie les événements générés par les demandes d'accès des utilisateurs RADIUS, du service d'authentification Internet, et NAP. Ces demandes peuvent être Accordées, Refusées, Jetées, Mises en quarantaine, Verrouillées et Déverrouillées.

Stratégies d'audit de base contre stratégies d'audit avancées

Les paramètres de la stratégie d'audit de base en matière de sécurité se trouvent dans **Paramètres de sécurité\Stratégies locales\Stratégie d'audit**, alors que les paramètres de la stratégie d'audit avancée en matière de sécurité se trouvent dans **Paramètres de sécurité\Configuration de la stratégie d'audit avancée\Stratégies d'audit**. Même si les paramètres des stratégies d'audit de base et avancée en matière de sécurité semblent se chevaucher, elles sont enregistrées et appliquées différemment.

Le nouvel ensemble de stratégies d'audit avancées permet aux administrateurs d'être plus sélectifs quant au nombre et aux types d'événements à auditer. Par exemple, pour se connecter à un compte, la stratégie d'audit de base propose un seul paramètre alors que la stratégie d'audit avancée en fournit quatre.

L'activation du seul paramètre de connexion au compte de base revient à configurer les quatre paramètres de connexion au compte avancés. À titre de comparaison, la configuration d'un seul paramètre de stratégie d'audit avancée ne génère pas d'événements d'audit pour les activités qui ne vous intéressent pas. Par exemple, si vous activez l'audit de réussite pour le paramètre de stratégie de base **Audit des événements de connexion au compte**, seuls les événements réussis seront enregistrés pour tous les comportements liés à la connexion au compte. En comparaison, vous pouvez configurer un audit de réussite pour un seul paramètre de connexion au compte avancé, un audit d'échec pour un deuxième paramètre de connexion au compte avancé, un audit de réussite et d'échec pour un troisième paramètre de connexion au compte avancé, ou aucun audit, en fonction des besoins de votre organisation.



Remarque : Utiliser à la fois les paramètres de base et avancés peut provoquer des résultats inattendus. Par conséquent, ne combinez pas les deux ensembles de paramètres de stratégies d'audit. Si vous utilisez les paramètres de la **Configuration de la stratégie d'audit avancée**, vous devez activer le paramètre de stratégie **Audit : Forcer les paramètres de la sous-catégorie de la stratégie d'audit (Windows Vista ou version ultérieure) à remplacer les paramètres de la catégorie de la stratégie d'audit** sous **Stratégies locales\Options de sécurité**. Cela permettra d'éviter les conflits entre des paramètres similaires en obligeant à faire abstraction de l'audit de sécurité de base.

Démonstration : Configuration des stratégies d'audit liées à l'authentification

Au cours de cette démonstration, vous allez apprendre à configurer les stratégies d'audit liées à l'authentification.

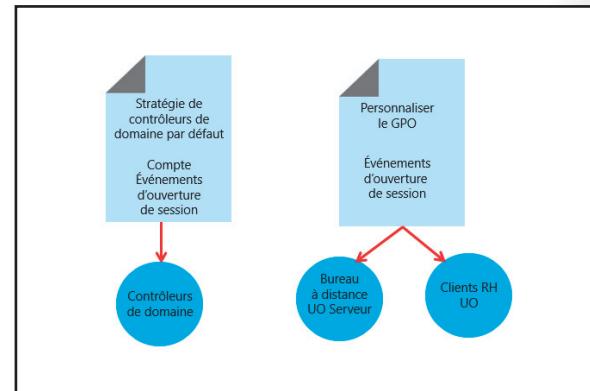
Étapes de démonstration

- Sur **LON-DC1**, dans le **Gestionnaire de serveur**, ouvrez la **console de Gestion des stratégies de groupe**.
- Naviguez vers la **Stratégie des contrôleurs de domaine par défaut**, puis modifiez la stratégie.
- Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, naviguez vers **Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Stratégie d'audit**.
- Expliquez les neuf catégories de stratégies existantes qui figurent dans le volet d'informations.
- Naviguez vers **Configuration de l'ordinateur\Stratégies\Paramètres Windows\Stratégies de sécurité\Configuration de la stratégie d'audit avancée\Stratégies d'audit**.
- Affichez les dix principales catégories sous les stratégies d'audit avancées, puis cliquez sur **Connexion au compte** et **Connexion/Déconnexion** pour afficher les sous-catégories disponibles.

7. Sous **Connexion au compte**, ouvrez les propriétés de la stratégie d'**Audit du service d'authentification Kerberos**.
8. Notez que vous pouvez activer la stratégie pour enregistrer un événement qui est une Réussite ou un Échec. Activez la stratégie et sélectionnez **Réussite** et **Échec**.
9. Cliquez sur l'onglet **Expliquer** pour afficher les informations détaillées sur l'événement, les paramètres d'enregistrement par défaut, et le volume d'audit prévu.
10. Appliquez la stratégie changée, puis cliquez sur **OK** pour fermer le paramètre de stratégie.

Définition de la portée des stratégies d'audit

Comme pour tous les paramètres de stratégie, vous devez définir soigneusement la portée des GPO qui appliquent vos stratégies d'audit afin que les paramètres soient affectés aux bons systèmes. Par exemple, si vous souhaitez vérifier les tentatives de connexion aux serveurs de bureau distants de votre entreprise par des utilisateurs, vous pouvez configurer l'audit des événements de connexion dans un GPO associé à l'unité d'organisation contenant vos serveurs de bureau distants. Néanmoins, si vous voulez vérifier les connexions au bureau par les utilisateurs de votre service des Ressources Humaines, vous pouvez configurer l'audit des événements de connexion dans un GPO associé à l'unité d'organisation contenant des objets informatiques des Ressources humaines. Rappelez-vous qu'un utilisateur de domaine qui se connecte à un ordinateur client ou à un serveur génère un événement de connexion, et non un événement de connexion au compte, sur ce système.



Seuls les contrôleurs de domaine génèrent des événements de connexion au compte pour les utilisateurs de domaine. Rappelez-vous qu'un événement de connexion au compte se produit sur le contrôleur de domaine qui authentifie un utilisateur de domaine, peu importe l'endroit où l'utilisateur se connecte. Si vous voulez vérifier les connexions aux comptes de domaine, vous devez vous assurer que l'audit des événements de connexion au compte affecte tous les contrôleurs de domaine. Le GPO des contrôleurs de domaine par défaut qui est créé lorsque vous installez votre premier contrôleur de domaine est un GPO idéal pour configurer des stratégies d'audit de connexion au compte.

Démonstration : Affichage des événements d'ouverture de session

Au cours de cette démonstration, vous allez apprendre à afficher les événements d'ouverture de session

Étapes de démonstration

1. Sur **LON-DC1**, exécutez **gpupdate/force**.
2. Déconnectez-vous.
3. Tentez de vous connecter en tant que **Adatum\Aidan** avec le mot de passe **123456**.
4. Connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
5. À partir du **Gestionnaire de serveur**, dans le menu **Outils**, ouvrez **Observateur d'événements**.
6. Naviguez vers le journal de **sécurité**.

7. Affichez l'événement **Audit d'échec** avec l'ID d'événement 4771, puis affichez ensuite l'événement **Audit de réussite** avec l'ID d'événement 4768.

Vérifiez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|---|---------|
| Lorsqu'un utilisateur se connecte à un contrôleur de domaine, un événement d'ouverture de session est généré. | |

Leçon 4

Configuration des comptes de services administrés

La création de comptes d'utilisateurs pour fournir une authentification destinée aux applications, aux services système et aux processus en arrière-plan est une pratique courante dans l'environnement Windows. Jusqu'ici, vous deviez créer des comptes et les nommer pour être utilisés par un service spécifique. Windows Server 2016 prend en charge les objets similaires à AD DS, connus sous le nom de *comptes de service administrés* (MSA), qui facilitent l'administration des comptes de service et qui présentent un risque moins élevé pour la sécurité de votre environnement.

Cette leçon vous fera découvrir les MSA et les nouvelles fonctionnalités associées aux MSA intégrées dans Windows Server 2016.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même de :

- Décrire les comptes de service.
- Identifier les défis liés à l'utilisation des comptes d'utilisateurs standards pour les services.
- Décrire les MSA.
- Décrire les MSA de groupe.
- Configurer les MSA de groupe.
- Décrire la délégation Kerberos et les noms des entités de service (SPN).

Aperçu des comptes de service

Dans le système d'exploitation Windows, les applications nécessitent parfois un accès administratif aux ressources locales et réseau. Auparavant, il était courant d'octroyer ces autorisations de comptes administratifs d'applications aux ressources. Par exemple, un serveur SQL Microsoft a besoin de gérer ses bases de données et pourrait donc avoir besoin d'un accès administratif local pour ce faire. Dans un environnement serveur SQL distribué, avec plusieurs serveurs SQL hébergeant chacun de nombreuses bases de données, le serveur peut avoir besoin d'un accès administratif pour chacune d'entre elles. Pour cette raison, un administrateur a besoin de créer un compte pour le serveur SQL appartenant au groupe Admins du domaine, ou au moins au groupe Administrateurs local des ordinateurs, avec un mot de passe configuré pour ne pas jamais expirer. Les administrateurs ont besoin de se souvenir de changer régulièrement et manuellement le mot de passe pour chaque service de serveur sur lequel ce mot de passe est saisi. Ce type de compte peut présenter des problèmes de sécurité et, s'il est compromis, peut mettre en danger un domaine entier.

- Les applications nécessitent parfois l'accès aux ressources :

- à cet effet, vous pouvez créer un domaine ou des comptes pour gérer cet accès. Toutefois, cela pourrait compromettre la sécurité

- Utilisez les comptes de service suivants à la place :

- Local System (Système local) :

- Privilégiés pour la plupart, toujours vulnérables si compromis

- Service local :

- Le moins privilégié, peut ne pas avoir suffisamment d'autorisations pour accéder à toutes les ressources nécessaires

- Service de réseau :

- Peut accéder aux ressources de réseau avec des informations d'identification correctes

En raison des problèmes de sécurité éventuels, vous pourriez donc envisager d'exécuter le programme ou le service en utilisant un compte local intégré. Les systèmes d'exploitation Windows ont trois comptes locaux intégrés pour permettre aux programmes et services d'accéder aux ressources. Ces comptes sont plus liés à l'ordinateur individuel qu'à un compte d'utilisateur, et ce comme indiqué ci-dessous :

- Système local. A des priviléges étendus sur le système local et agit comme l'ordinateur sur le réseau. Il s'agit d'un compte intégré très privilégié. Le nom du compte est AUTORITÉ NT\SYSTÈME.
- Service local. A le même niveau d'accès aux ressources et aux objets que les membres du groupe Utilisateurs locaux. Cet accès limité permet de protéger le système si des services ou des processus individuels sont compromis. Les services qui fonctionnent comme le compte de service local accéderont aux ressources du réseau sous la forme d'une session invalide sans aucune information d'identification. Le nom du compte est AUTORITÉ NT\SERVICE LOCAL.
- Service réseau. A plus accès aux ressources et aux objets que les membres du groupe Utilisateurs, tels que le compte de service local. Les services qui fonctionnent comme le compte de service réseau accèdent aux ressources du réseau en utilisant les informations d'identification du compte d'ordinateur. Le nom du compte est AUTORITÉ NT\SERVICE RÉSEAU.

Vous devez savoir que l'utilisation du compte de système local pourrait encore compromettre votre sécurité, si l'on considère le niveau de priviléges élevé sous lequel il opère. Par conséquent, vous devez prendre des précautions supplémentaires lorsque vous utilisez ce compte pour accéder au programme. Par ailleurs, le compte de service local ne peut pas avoir assez de priviléges pour accéder à toutes les ressources requises par le programme. Si le programme a besoin de ressources sur d'autres ordinateurs, vous pouvez utiliser le compte Service réseau. Cependant, vous devez ajouter le compte de l'ordinateur à un groupe du domaine ou individuellement sur les autres ordinateurs. Dans tous les cas, vous devrez faire une analyse approfondie de la sécurité pour vous assurer que vous examinez tous les aspects de l'utilisation des comptes de service.

Défis liés à l'utilisation de comptes de service

De nombreux programmes tels que le serveur SQL ou IIS contiennent des services que vous devez installer sur le serveur qui héberge le programme. Ces services fonctionnent généralement au démarrage du serveur ou sont déclenchés par d'autres événements. Les services fonctionnent souvent en arrière-plan et ne nécessitent aucune intervention de l'utilisateur.

Pour démarrer et authentifier un service, vous utilisez un compte de service. Un compte de service peut être un compte local sur l'ordinateur, tel que le système local intégré, le service local, ou les comptes de services réseau. Vous pouvez également configurer un compte de service pour utiliser un compte basé sur le domaine situé dans AD DS.

- Effort administratif supplémentaire pour gérer le mot de passe de compte de service
- Difficulté à déterminer où un compte basé sur le domaine est utilisé comme un compte de service
- Effort administratif supplémentaire pour gérer le SPN

- Pour aider à la centralisation de l'administration de et de répondre aux exigences du programme, de nombreuses organisations choisissent d'utiliser un compte de domaine pour exécuter les services du programme. Bien que cela fournit un certain avantage concernant l'utilisation d'un compte local, plusieurs défis y sont associés, à savoir :

Un effort d'administration supplémentaire peut être nécessaire pour gérer le mot de passe du compte de service en toute sécurité. Cela inclut des tâches telles que la modification du mot de passe et la résolution de situations qui débouchent sur un verrouillage de compte. Les comptes de service sont

aussi généralement configurés pour avoir des mots de passe qui n'expirent pas, ce qui peut aller à l'encontre des politiques de sécurité de votre entreprise.

- La difficulté à déterminer les situations où un compte de domaine est utilisé comme un compte de service. Vous pouvez utiliser un compte d'utilisateur standard pour plusieurs services sur différents serveurs à travers l'environnement. Une tâche simple, comme la modification du mot de passe, peut provoquer des problèmes d'authentification pour certaines applications. Il est important de savoir où et comment utiliser un compte d'utilisateur standard quand il est associé à un service de programme.
- Un effort d'administration supplémentaire peut être nécessaire pour gérer le nom principal de service (SPN). L'utilisation d'un compte d'utilisateur standard peut nécessiter une administration manuelle du SPN. Si le compte d'ouverture de session du service est modifié, le nom d'ordinateur est modifié. Par ailleurs, si une propriété du nom d'hôte DNS est modifiée, vous devrez peut-être modifier les enregistrements SPN manuellement pour refléter ce changement. Un SPN mal configuré entraîne des problèmes d'authentification avec le service de programme.

Windows Server 2016 prend en charge un objet AD DS, nommé *Compte de service administré (MSA)*, à utiliser pour faciliter la gestion des comptes de service. Les rubriques suivantes fournissent des informations sur les exigences et l'utilisation des MSA dans Windows Server 2016.

Aperçu des comptes de services gérés

Un MSA est une classe d'objets AD DS qui permet une simplification du mot de passe et de la gestion SPN pour les comptes de service. Les MSA ont été introduits dans Windows 7 et Windows Server 2008 R2.

De nombreux programmes basés sur le réseau utilisent un compte pour gérer des services ou pour fournir une authentification. Par exemple, un programme sur un ordinateur local peut utiliser les comptes de Service local, de Service réseau ou de Système local. Ces comptes de service peuvent fonctionner correctement.

Cependant, ils sont généralement partagés entre plusieurs programmes et services, ce qui les rend difficiles à gérer pour un programme spécifique. En outre, vous ne pouvez pas gérer ces comptes de services locaux au niveau du domaine.

Sinon, il est assez fréquent qu'un programme utilise un compte de domaine standard que vous configurez spécifiquement pour le programme. Toutefois, le principal inconvénient est que vous devez gérer les mots de passe manuellement, ce qui augmente l'effort d'administration. Un compte de service administré peut fournir un programme avec son propre compte unique, tout en éliminant la nécessité d'avoir un administrateur pour gérer manuellement les informations d'identification du compte.

Comment fonctionne un MSA ?

Les MSA sont stockés dans AD DS comme des objets **msDS-managedserviceaccount**. Cette classe hérite des aspects structurels de la classe d'ordinateur, qu'elle hérite de la classe d'utilisateur. Ceci permet à un MSA de remplir les fonctions semblables à celles de l'utilisateur, comme la fourniture d'authentification et de contexte de sécurité pour un service en cours d'exécution. Cela permet également à un MSA d'utiliser le mécanisme de mise à jour du mot de passe utilisé par les objets d'ordinateur dans AD DS et qui est un processus ne nécessitant aucune intervention de l'utilisateur.

Les MSA fournissent les avantages suivants pour simplifier l'administration :

- Utilisez les MSA pour automatiser le mot de passe et la gestion du SPN pour les comptes de services utilisés par les services et les applications
- Nécessite Windows Server 2008 R2 ou plus récent installé avec :
 - .NET Framework 3.5x
 - Module Active Directory pour Windows PowerShell
- Recommandé pour fonctionner avec AD DS configuré au niveau fonctionnel de Windows Server 2008 R2 ou à un supérieur

- Une gestion de mot de passe automatique. Un MSA gère automatiquement son propre mot de passe, y compris les changements du mot de passe.
- Une gestion SPN simplifiée. La gestion SPN se produit automatiquement si vous configurez votre domaine au niveau fonctionnel de domaine Windows Server 2008 R2 ou à un niveau supérieur.

Les MSA sont stockés dans le conteneur **CN=comptes de service administrés, DC=<domaine>, DC=<com>** Conteneur. Vous pouvez voir ceci en activant l'option **Fonctionnalités avancées** dans le menu **Affichage** dans **Utilisateurs et ordinateurs Active Directory**. Ce conteneur est visible par défaut dans le **Centre d'administration Active Directory**.

Conditions requises pour utiliser les MSA

Pour utiliser un MSA, le serveur qui exécute le service ou le programme doit exécuter Windows Server 2008 R2 ou un système d'exploitation plus récent. Vous devez également veiller à ce que Microsoft.NET Framework 3.5.x et le module Active Directory pour Windows PowerShell soient tous deux installés sur le serveur.



Remarque : vous ne pouvez pas partager un MSA standard entre plusieurs ordinateurs ou celui que vous utilisez dans les clusters de serveurs lorsque le service est répliqué entre les nœuds. En outre, vous ne pouvez pas utiliser les MSA pour les tâches planifiées sans surveillance.

Pour simplifier et fournir un mot de passe entièrement automatisé et une gestion SPN, nous recommandons fortement que le domaine AD DS soit au niveau fonctionnel Windows Server 2008 R2 ou à un niveau supérieur. Toutefois, si vous avez un contrôleur de domaine qui exécute Windows Server 2008, vous pouvez mettre à jour le schéma Active Directory à Windows Server 2008 R2 pour prendre en charge cette fonctionnalité. Le seul inconvénient est que l'administrateur de domaine doit configurer les données SPN manuellement pour les MSA.

Utilisation de MSA sur les contrôleurs de domaine Windows Server 2016

Dans Windows Server 2016, vous créez des MSA comme nouveau type d'objet de compte de service administré en groupe par défaut. Cependant, sur un contrôleur de domaine Windows Server 2016, vous pouvez vous adapter en créant une clé racine de Service de distribution de clés (KDS) pour le domaine. Pour créer la clé racine, vous devez exécuter l'applet de commande suivante à partir du module Active Directory pour Windows PowerShell :

```
Add-KDSRootKey -EffectiveTime ((Get-Date).AddHours(-10))
```

Le sujet suivant traite des groupes MSA plus en détail, y compris en fournissant des explications supplémentaires sur la façon dont vous pouvez créer une clé racine KDS et l'applet de commande **Add-KDSRootKey**.

Que sont les MSA de groupe ?

Les MSA de groupe vous permettent d'étendre les capacités des MSA standards à plus d'un serveur dans votre domaine. Dans les scénarios de batterie de serveurs avec des clusters ou des serveurs IIS d'équilibrage de charge réseau (NLB), vous devez souvent exécuter les services de système ou de programme sous le même compte de service. Les MSA standards ne peuvent pas fournir de fonctionnalités MSA aux services qui sont en cours d'exécution sur plus d'un serveur. Cependant, en utilisant les MSA de groupe, vous pouvez configurer plusieurs serveurs pour utiliser le même MSA et toujours conserver les avantages offerts par les MSA, comme l'entretien automatique du mot de passe et une gestion SPN simplifiée.

- Les MSA de groupe étendent les capacités des MSA standards à travers :
 - L'autorisation d'utiliser les MSA sur plus d'un ordinateur dans le domaine
 - Le stockage des informations d'authentification MSA sur les contrôleurs de domaine
- Pour soutenir le MSA de groupe, votre environnement doit :
 - Avoir au moins Windows Server 2012 ou un contrôleur de domaine plus récent
 - Avoir une clé racine KDS créée pour le domaine

Conditions requises pour les MSA de groupe

Votre environnement doit répondre aux exigences suivantes si vous souhaitez prendre en charge la fonctionnalité de MSA de groupe, notamment :

- Au moins un contrôleur de domaine doit exécuter Windows Server 2012 ou une version plus récente pour stocker des informations gérées concernant le mot de passe.
- Les ordinateurs clients utilisant des MSA de groupe doivent disposer de Windows 8 ou d'une version plus récente et les ordinateurs basés sur le serveur doivent avoir Windows Server 2012 ou une version plus récente.
- Vous devez créer une clé racine KDS sur l'un des contrôleurs de domaine du domaine. Pour créer la clé racine KDS, vous devez exécuter la commande suivante à partir du module Active Directory pour Windows PowerShell sur un contrôleur de domaine Windows Server 2016 :

```
Add-KdsRootKey -EffectiveImmediately
```



Remarque : le commutateur **-EffectiveImmediately** utilise l'heure actuelle pour établir l'horodatage qui marque la clé comme valide. Cependant, en utilisant le commutateur **--EffectiveImmediately**, le temps effectif réel est fixé à 10 heures plus tard que l'heure actuelle. Cette différence de 10 heures vise à permettre une réplication AD DS pour répliquer les modifications à d'autres contrôleurs de domaine dans le domaine. À des fins de test, vous pouvez contourner cette fonctionnalité en définissant le paramètre **-EffectiveTime** à 10 heures avant l'heure actuelle en exécutant la commande suivante :

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

Fonctionnalité MSA de groupe

Les MSA de groupe activent la fonctionnalité de compte de service administré sur plusieurs serveurs en déléguant la gestion des informations concernant le mot de passe MSA aux contrôleurs de domaine de Windows Server 2016. Ce faisant, la gestion des mots de passe ne dépend plus de la relation entre un serveur unique et AD DS, mais est entièrement contrôlée par AD DS.

L'objet de compte de service de groupe géré contient une liste des entités, ordinateurs ou groupes AD DS, qui sont autorisées à récupérer les informations concernant le mot de passe de MSA de groupe à partir de AD DS. Les entités peuvent ensuite utiliser le groupe compte de service administré pour l'authentification pour les services.

Créez des MSA de groupe en utilisant les mêmes applets de commande que vous avez utilisés pour créer le MSA standard du module Active Directory pour Windows PowerShell. Autrement dit, les applets de commande utilisés pour la gestion des comptes de service administrés créent des MSA de groupe par défaut.

Sur un contrôleur de domaine Windows Server 2016, créez un nouvel MSA en utilisant l'applet de commande **New-ADServiceAccount** avec le paramètre **-PrincipalsAllowedToRetrieveManagedPassword**.

Ce paramètre accepte un ou plusieurs comptes d'ordinateur séparés par des virgules ou des groupes AD DS qui sont autorisés à obtenir des informations concernant le mot de passe pour le MSA de groupe qui est stocké dans AD DS sur les contrôleurs de domaine de Windows Server 2016.

Par exemple, l'applet de commande suivant crée un nouvel MSA de groupe appelé SQLFarm, et permet aux hôtes LON-SQL1, LON-SQL2 et LON-SQL3 d'utiliser le MSA de groupe :

```
New-ADServiceAccount -Name LondonSQLFarm -PrincipalsAllowedToRetrieveManagedPassword LON-SQL1, LON-SQL2, LON-SQL3
```

Une fois que vous avez ajouté un ordinateur pour utiliser le paramètre **PrincipalsAllowedToRetrieveManagedPassword**, vous pouvez affecter le MSA de groupe aux services en utilisant le même processus d'attribution que pour les MSA standards.

Utiliser des groupes d'AD DS pour gérer les MSA de groupe

Vous pouvez utiliser des groupes de sécurité AD DS pour identifier les MSA de groupe. Lorsque vous utilisez un groupe d'AD DS pour le paramètre **PrincipalsAllowedToRetrieveManagedPassword**, tous les ordinateurs qui sont membres de ce groupe seront autorisés à récupérer le mot de passe et utiliser la fonctionnalité MSA de groupe. Lorsque vous utilisez un groupe AD DS comme entité pouvant récupérer un mot de passe administré, tous les comptes membres du groupe auront également la même capacité.

Démonstration : configuration des MSA de groupe

Au cours de cette démonstration, vous allez apprendre à configurer des MSA de groupe.

Étapes de démonstration

Créer la racine principale KDS pour le domaine

1. Dans **LON-DC1**, à partir du **Gestionnaire de serveur**, ouvrez la console **Module Active Directory pour Windows PowerShell**.
2. Utilisez l'applet de commande **Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))** pour créer la clé racine KDS de domaine.

Créer et associer un MSA

1. Utilisez l'applet de commande **New-ADServiceAccount** pour créer un MSA.
2. Utilisez l'applet de commande **Add-ADComputerServiceAccount** pour associer le MSA avec **LON-SVR1**.
3. Utilisez l'**applet de commande Get-ADServiceAccount** pour afficher le MSA nouvellement créé et pour confirmer la bonne configuration.

Installer un MSA

1. Dans **LON-SVR1**, ouvrez la console **Module Active Directory pour Windows PowerShell**.
2. Utilisez l'applet de commande **Installez-ADServiceAccount** pour installer le MSA sur **LON-SVR1**.
3. Ouvrez le **Gestionnaire de serveur** et démarrez la console **Services**.
4. Ouvrez les pages de **Propriétés** pour le service de partage de données puis sélectionnez l'onglet **Connexion**.
5. Configurez le Service de partage de données pour utiliser **Adatum\SampleApp_SVR1\$**.
6. Effacez le mot de passe pour les cases **Mot de passe** et **Confirmer mot de passe**.

Délégation SPN et Kerberos

Dans certains scénarios, un programme pour un service peut avoir besoin d'établir un lien avec les services d'un autre serveur au nom du client. Par exemple, lorsqu'un client utilise un serveur frontal qui établit une connexion à un serveur principal, cette connexion nécessite une authentification. Kerberos utilise la délégation d'authentification pour de tels scénarios. Le service demandeur, qui est un client dans cet exemple, demande que le KDC autorise un deuxième service à agir en son nom. Le deuxième service peut alors déléguer l'authentification à un troisième service. Toutefois, dans Windows Server 2008 ou une version plus récente, Microsoft a ajouté le modèle de délégation contrainte pour limiter la portée des services qui peuvent être délégués de cette façon, en particulier les services de troisième niveau et au-delà. Ce modèle fournit une forme plus sûre de délégation pour les services à utiliser.

- Délégation d'authentification Kerberos :
 - Les services peuvent déléguer des tickets de service qui leur sont délivrés par le KDC à un autre service
- Délégation contrainte :
 - Permet aux administrateurs de définir quels services peuvent utiliser les tickets de service émis à d'autres services
- Les SPN permettent d'identifier exclusivement les services
- Windows Server 2016 autorise :
 - La délégation contrainte à travers les domaines
 - Les administrateurs de services à configurer la délégation contrainte

Lorsque vous utilisez une délégation contrainte, vous pouvez configurer une délégation de compte de service à des ensembles spécifiques de comptes de service. Vous pouvez configurer un compte de service particulier à approuver pour la délégation à une instance spécifique d'un service en cours d'exécution sur un ordinateur spécifique ou à un ensemble d'instances spécifiques de services en cours d'exécution sur des ordinateurs spécifiés.

Un SPN est un identificateur unique pour chaque instance d'un service en cours d'exécution sur un ordinateur. Lorsque vous utilisez l'authentification Kerberos, un SPN défini pour un service permet aux clients d'identifier cette instance du service sur le réseau. Le SPN est enregistré dans AD DS et est associé au compte du service que le SPN spécifie. Lorsqu'un service doit authentifier un autre service, il utilise le SPN de ce service afin de le distinguer des autres services sur cet ordinateur. Un service peut utiliser une délégation contrainte si elle peut obtenir un ticket de service Kerberos pour lui-même au nom de l'utilisateur en cours de délégation, soit un autre service dans ce cas. Lors de l'utilisation de la délégation contrainte, l'utilisateur peut obtenir le ticket de service directement par l'authentification par le biais des rôles de limite ou le service peut obtenir le ticket de service pour le compte de l'utilisateur.

Un problème posé par ce modèle est que lorsqu'un administrateur de domaine configure le service pour la délégation contrainte, l'administrateur du service ne sait pas quel service frontal a été délégué aux services de ressources détenus. Dans Windows Server 2016, ce problème est résolu en permettant également à l'administrateur du service de configurer la délégation contrainte d'un service. Cela signifie que l'administrateur du service frontal peut autoriser ou refuser l'accès par les services frontaux.

Windows Server 2012 et Windows Server 2016 utilisent de nouvelles extensions pour la délégation contrainte. Par exemple, l'extension « Service for User to Proxy », connue sous le nom de *S4U2Proxy*, permet à un service d'utiliser son ticket de service Kerberos pour qu'un utilisateur obtienne un ticket de service du KDC à un service frontal. Un administrateur de service peut configurer la délégation contrainte sur le compte de service frontal, même dans un autre domaine. Vous pouvez configurer les services frontaux, tels que Microsoft Office Outlook sur le Web et Microsoft SharePoint Server, pour la délégation contrainte aux serveurs frontaux sur d'autres domaines. Cela améliore votre capacité à soutenir des solutions de services à travers des domaines en utilisant vos mécanismes existants d'authentification Kerberos.

Question : En quoi les MSA de groupe sont-ils différent des MSA standards ?

Atelier pratique : sécurisation AD DS

Scénario

L'équipe de sécurité d'A. Datum Corporation a examiné les problèmes de sécurité potentiels dans l'organisation en se concentrant sur AD DS. L'équipe de sécurité est particulièrement préoccupée par l'authentification AD DS et par la sécurité des contrôleurs de domaine des succursales.

Vous devez aider à améliorer la sécurité et la surveillance de l'authentification envers le domaine AD DS de l'entreprise. En outre, la direction d'A. Datum a mis en place une stratégie de mot de passe, et vous devez l'appliquer pour tous les comptes d'utilisateurs et développer une stratégie de mot de passe plus stricte pour les comptes administratifs sensibles en matière de sécurité. Il est également important que vous mettiez en œuvre une piste de vérification appropriée pour aider à surveiller les tentatives d'authentification dans AD DS.

La deuxième partie de votre mission comprend le déploiement et la configuration des RODC pour soutenir l'authentification AD DS dans une succursale. Enfin, vous devez évaluer l'utilisation d'un MSA de groupe en le déployant sur le serveur de test.

Objectifs

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

- Mise en œuvre des stratégies de sécurité pour les comptes, mots de passe et groupes d'administration ;
- Déploiement et configuration d'un RODC ;
- Création et association d'un MSA de groupe ;

Configurer l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels : **22742A-LON-DC1**, **22742A-LON-DC2**, **22742A-LON-SVR1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-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 : **Pa55w.rd**
5. Répétez les étapes 2 à 4 pour **22742A-LON-DC2** et **22742A-LON-SVR1**.

Exercice 1 : Mise en œuvre des stratégies de sécurité pour les comptes, mots de passe et groupes d'administration

Scénario

La direction d'A. Datum a indiqué qu'il est important que tous les processus de gestion soient aussi sécurisés que possible pour aider à lutter contre une brèche de sécurité. Les équipes de sécurité et de gestion de l'entreprise ont identifié ses besoins commerciaux par rapport à la connexion de compte et la sécurité du mot de passe. Dans cet exercice, vous allez définir et mettre en œuvre les paramètres de stratégie de groupe pour répondre aux besoins de l'entreprise.

Documentation fournie avec le produit

| Proposition de stratégie GPO d'A. Datum | |
|--|--|
| Présentation des exigences | |
| <p>A. Datum a identifié les exigences suivantes en ce qui concerne les stratégies de connexion de compte et mot de passe :</p> <ul style="list-style-type: none"> Tous les utilisateurs doivent utiliser un mot de passe qui contient au moins huit caractères. Pour les administrateurs, la longueur minimale doit être de 10 caractères. Les mots de passe pour tous les utilisateurs doivent être complexes et stockés en toute sécurité. Tous les utilisateurs, sauf les administrateurs, doivent changer leur mot de passe tous les 60 jours au plus tard. Les administrateurs informatiques doivent changer leur mot de passe tous les 30 jours au plus tard. Si les utilisateurs entrent un mot de passe incorrect plus de cinq fois en 20 minutes, leurs comptes doivent être verrouillés. Pour les utilisateurs normaux, les comptes sont déverrouillés automatiquement après une heure. Pour les administrateurs, les comptes doivent être verrouillés après trois tentatives d'authentification incorrectes. Les comptes des administrateurs informatiques ne sont jamais déverrouillés automatiquement. Un administrateur doit déverrouiller le compte. Les comptes des administrateurs informatiques comprennent tous les membres du groupe informatique et du groupe admins du domaine. Aucun utilisateur ne devrait être en mesure d'utiliser au moins 10 de leurs mots de passe précédents. La liste des membres du groupe administrateurs locaux sur tous les serveurs membres doit être limitée au compte administrateur local, au groupe admins du domaine et au groupe informatique seulement. Le groupe admins domaine doit comprendre le compte administrateur seulement. Les groupes administrateurs de l'entreprise et le schéma admins doivent être vides pendant les opérations normales. Les utilisateurs doivent être ajoutés explicitement à ces groupes seulement quand ils ont besoin d'effectuer des tâches qui exigent ce niveau de droits d'administration. D'autres groupes intégrés, tels que les opérateurs de compte et les opérateurs de serveur, ne doivent contenir aucun membre. Si des utilisateurs sont ajoutés à l'un de ces groupes, ils doivent être automatiquement retirés du groupe. Toutes les modifications apportées aux objets utilisateur et aux groupes de sécurité dans AD DS doivent être vérifiées. | |
| Propositions | |

Propositions

Dressez une liste des paramètres que vous devez configurer pour répondre aux exigences d'A. Datum concernant les politiques de mot de passe et le verrouillage de compte.

| Paramètres | Configuration pour tous les utilisateurs | Configuration pour les administrateurs informatiques |
|------------|--|--|
| | | |

| | | |
|--|--|--|
| Appliquer l'historique des mots de passe | | |
| Durée de vie maximale du mot de passe | | |
| Durée de vie minimale du mot de passe | | |
| Longueur minimale du mot de passe | | |
| Les mots de passe doivent répondre à des exigences de complexité | | |
| Stocker le mot de passe en utilisant le chiffrage réversible | | |
| Durée de verrouillage du compte | | |
| Seuil de verrouillage du compte | | |
| Réinitialiser le compteur de verrouillage de compte après | | |

1. Comment pouvez-vous faire une configuration pour que les administrateurs informatiques aient des paramètres de verrouillage de compte et de mot de passe différents de ceux des utilisateurs habituels ?
2. Comment pouvez-vous identifier les administrateurs informatiques en termes de paramètres de verrouillage de compte et de mot de passe plus restreints ?
3. Comment pouvez-vous répondre à l'exigence de limiter la liste des membres des groupes d'administrateurs locaux sur tous les serveurs membres uniquement au compte de l'administrateur local, au groupe des administrateurs de domaine et au groupe informatique ?
4. Comment pouvez-vous répondre à l'exigence selon laquelle le groupe des administrateurs de domaine doit comprendre uniquement le compte Administrateur et les Admins de l'entreprise et les groupes Schema Admins doivent être vides pendant le fonctionnement normal ?
5. Comment pouvez-vous répondre à l'exigence selon laquelle les autres groupes intégrés, tels que les opérateurs de compte et opérateurs de serveur ne doivent pas contenir de membres ?
6. Comment pouvez-vous répondre à l'exigence selon laquelle vous devez vérifier toutes les modifications apportées à AD DS ?

Les tâches principales de cet exercice sont les suivantes :

1. Identifier les paramètres requis ;
2. Configurer les paramètres de mot de passe pour tous les utilisateurs ;
3. Configurer un PSO pour les administrateurs informatiques ;
4. Mettre en œuvre des politiques de sécurité administratives ;
5. Mettre en œuvre la vérification administrative.

► **Tâche 1 : Identifier les paramètres requis**

1. Lisez la documentation fournie.
2. Remplissez le tableau des paramètres en fonction des exigences de A. Datum Corporation.
3. Répondez aux questions supplémentaires du document de proposition.

► **Tâche 2 : Configurer les paramètres de mot de passe pour tous les utilisateurs**

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, ouvrez la **console de Gestion des stratégies de groupe**.
2. Accédez à la **Stratégie de domaine par défaut**, puis cliquez sur **Modifier**.
3. Dans la fenêtre **Éditeur de gestion de la stratégie de groupe**, accédez à **Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de compte** puis cliquez sur **Stratégie de mot de passe**.
4. Configurez les paramètres de stratégie suivants :
 - o Appliquer l'historique des mots de passe : **dix mots de passe mémorisés**
 - o Durée de vie maximale du mot de passe : **60 jours**
 - o Durée de vie minimale du mot de passe : **1 jour**
 - o Le mot de passe doit répondre à des exigences de complexité : **activé**
 - o Longueur du MDP : **8 caractères**
 - o Stocker le mot de passe en utilisant le chiffrage réversible : **désactivé**
5. Sélectionnez **Stratégie de verrouillage de compte**, puis définissez et configurez les paramètres de stratégie suivants :
 - o Durée du verrouillage de comptes : **60 minutes**
 - o Acceptez le changement de valeur suggéré
 - o Seuil du verrouillage de comptes : **5 tentatives de connexion non valides**
 - o Réinitialiser le compteur de verrouillage de compte après : **20 minutes**
6. Fermez la fenêtre **Éditeur de gestion des stratégies de groupe** et la **Console de gestion des stratégies de groupe**.

► **Tâche 3 : Configurer un PSO pour les administrateurs informatiques**

1. Dans **LON-DC1**, depuis le **Gestionnaire de serveur**, ouvrez le **Centre d'administration Active Directory**.
2. Accédez à **Adatum (local)\Système\Conteneur de paramètres de mot de passe**.
3. Créez un nouveau PSO avec les caractéristiques suivantes :
 - o Nom : **Paramètres de mot de passe administrateurs Adatum**

- Priorité : **10**
- Appliquer la longueur minimale du mot de passe : **sélectionné, longueur du mot de passe de dix caractères minimale**
- Appliquer l'historique des mots de passe : **sélectionné, dix mots de passe mémorisés**
- Le mot de passe doit répondre à des exigences de complexité : **sélectionné**
- Stocker le mot de passe en utilisant le chiffrage réversible : **non sélectionné**

Options de durée de vie du mot de passe :

- Durée de vie minimale du mot de passe : **sélectionné**
- L'utilisateur ne peut pas changer le mot de passe avant (jours) : **1**
- Appliquer la durée de vie maximale du mot de passe : **sélectionné**
- L'utilisateur doit changer le mot de passe après (jours) : **30**

Options de verrouillage de compte :

- Appliquer la stratégie de verrouillage du compte : **sélectionné**
- Nombre d'échecs de tentatives de connexion autorisés : **3**
- Réinitialiser le compteur d'échecs des tentatives d'ouverture de session compte après (minutes) : **20**
- Le compte sera verrouillé : **jusqu'à ce qu'un administrateur déverrouiller le compte manuellement.**

4. Dans la section **S'applique directement à**, configurez le PSO à appliquer au groupe **informatique**.
5. Le groupe informatique ne fonctionnera pas car c'est un groupe global. Ouvrez Windows PowerShell, puis vérifiez la portée du groupe informatique avec la commande suivante :

```
Get-ADGroup IT
```

6. Modifiez la portée du groupe en utilisant la commande suivante :

```
Set-ADGroup IT -GroupScope Global
```

7. Dans la section **S'applique directement à**, configurez le PSO à appliquer aux groupes suivants :

- **Informatique**
- **Administrateurs du domaine**

8. Créez le PSO.
9. Dans le **Centre d'administration Active Directory**, passez à la page **Vue d'ensemble** et dans la case **Recherche globale**, recherchez **Abbi Skinner**. Utilisez les **Paramètres d'affichage des mots de passe résultants** pour vérifier que le PSO **Paramètres de mot de passe Adatum** s'applique à **Abbi** ; il est dans le groupe informatique.

10. Répétez l'étape neuf pour vérifier l'utilisateur **Adam Hobbs**. Il n'est pas dans un groupe informatique, et les paramètres de stratégie de domaine par défaut s'appliquent à lui.

11. Fermez le **Centre d'administration Active Directory** et **Windows PowerShell**.

► Tâche 4 : Mettre en œuvre des politiques de sécurité administratives

1. Dans **LON-DC1**, ouvrez le **Centre d'administration Active Directory** et créez une unité d'organisation de haut niveau nommée **Serveurs Adatum**.

2. Déplacez **LON-SVR1** et **LON-SVR2** vers l'UO **Serveurs Adatum**.
 3. Ouvrez la **Console de stratégie de gestion de groupe**, puis créez et reliez une stratégie nommée **Administrateurs restreints sur les serveurs membres** à l'UO **Serveurs Adatum**.
 4. Modifiez le GPO pour restreindre le groupe des administrateurs locaux au compte **Administrateur**, au groupe **Administrateurs de domaine** et au groupe **informatique**.
 5. Basculez vers **LON-SVR1** et actualiser la stratégie de groupe.
 6. Vérifiez que la stratégie s'applique à **LON-SVR1** et qu'elle a restreint le groupe Administrateurs locaux.
 7. Rebasquez vers **LON-DC1**.
 8. Modifiez la **stratégie de contrôleurs de domaine par défaut**.
 9. Configurez le GPO avec les **Groupes restreints**. Ajoutez les groupes **Opérateurs de compte** et **Opérateurs de serveur** et configurez les deux pour qu'ils ne contiennent aucun membre.
 10. Fermez la **console Gestion de stratégie de groupe**.
- **Tâche 5 : Mettre en œuvre la vérification administrative**
1. Dans **LON-DC1**, dans le **Gestionnaire de serveur**, ouvrez la **console de Gestion des stratégies de groupe**.
 2. Recherchez et modifiez la **Stratégie de contrôleurs de domaine par défaut**.
 3. Configurez la stratégie de contrôleurs de domaine par défaut Stratégie des contrôleurs pour permettre la **Réussite** de la vérification des **modifications de Directory Service** sous de **ConfigurationOrdinateur\Stratégies\ParamètresWindows\ParamètresDeSécurité\ParamètresAvancésStratégiesD'audit\StratégiesD'audit\AccèsDS**.
 4. Dans la Stratégie de contrôleurs de domaine par défaut, activez la **Réussite** de la vérification de **l'Appartenance au groupe de sécurité** sous **ConfigurationOrdinateur\Stratégies\ParamètresDeSécurité\ParamètresAvancésDeStratégieD'audit\StratégiesD'audit\GestionDeCompte**.
 5. Dans la stratégie de contrôleurs de domaine par défaut, activez la stratégie **Vérification : paramètres de sous-catégorie de stratégie d'audit (Windows Vista ou version ultérieure) prévalent sur les paramètres de catégorie de stratégie d'audit** sous **ConfigurationOrdinateur\Stratégies\ParamètresWindows\ParamètresDeSécurité\StratégiesLocales\OptionsDeSécurité**.
 6. À l'invite de commandes, saisissez **gpupdate /force**, puis appuyez sur Entrée.
 7. Ouvrez **Utilisateurs et ordinateurs Active Directory** et activez l'affichage **Fonctionnalités avancées**. Dans la boîte de dialogue des propriétés **Adatum.com**, sous **Paramètres de sécurité avancés**, dans **Vérification**, recherchez la **réussite** de l'entrée d'audit pour **Tout le monde** avec un accès **Spécial**, qui s'applique à **Cet objet uniquement**.
 8. Ouvrez et modifiez l'entrée d'audit à appliquer à **Cet objet et tous les objets descendants**.
 9. Dans **Utilisateurs et ordinateurs Active Directory**, ajoutez l'utilisateur **Abbi** au groupe **Administrateurs de domaine**.
 10. Recherchez l'utilisateur **Ada Russel** dans l'UO **Marketing**, puis changez la ville de **Londres** à **Birmingham**.
 11. Ouvrez l'**Observateur d'événements**, allez dans le journal **Sécurité** puis ouvrez l'**ID d'événement 4728** le plus récent. Dans les propriétés, notez que **ADATUM\Administrateur** a ajouté **ADATUM\Abbi** aux groupes **Administrateurs de domaine** groupes.

12. Dans l'**Observateur d'événements**, ouvrez l'**ID d'événement 5136** le plus récent et notez que **ADATUM\Administrateur** a modifié l'objet utilisateur **cn=Ada Russel** et supprimé la valeur **Londres**.
13. Déplacez et ouvrez l'événement suivant dans la page Détails **Propriétés de l'événement** et notez que **ADATUM\Administrateur** a modifié **Ada Russel** et a ajouté la valeur **Birmingham**.
14. Fermez toutes les fenêtres actives exceptée **Gestionnaire de serveurs**.

Résultats : Après cette opération, vous devriez avoir identifié et configuré les stratégies de sécurité pour A. Datum.

Exercice 2 : Déploiement et configuration d'un RODC

Scénario

Dans cet exercice, vous allez apprendre à configurer le serveur **LON-SVR1** comme un RODC dans la succursale éloignée. Pour éviter les frais de déplacement, vous décidez de faire la conversion à distance, en collaboration avec un technicien de support de bureau et avec le seul membre du personnel IT de la succursale. Cet utilisateur a déjà installé un ordinateur avec serveur Windows Server 2016 nommé **LON-SVR1**. Vous allez organiser une étape d'installation d'un RODC pour que cet utilisateur administratif puisse terminer l'installation. Une fois le déploiement terminé, vous configurerez une stratégie de réPLICATION de mot de passe à l'échelle de domaine et la stratégie de réPLICATION de mot de passe spécifique à l'ordinateur **LON-SVR1**.

Les tâches principales de cet exercice sont les suivantes :

1. Procéder à une installation déléguée d'un RODC ;
2. Exécuter l'Assistant d'installation Active Directory Domain Services sur un RODC pour terminer le processus de déploiement ;
3. Configurer la stratégie de réPLICATION de mot de passe à l'échelle du domaine ;
4. Créer un groupe pour gérer la réPLICATION de mot de passe au RODC de la filiale ;
5. Evaluer la stratégie de réPLICATION de mot de passe qui en résulte.

► Tâche 1 : Organiser l'installation déléguée d'un RODC

Préparation

Pour prédéfinir un compte RODC, le nom de l'ordinateur ne doit pas être en cours d'utilisation dans le domaine. Par conséquent, vous devez d'abord retirer **LON-SVR1** du domaine via les étapes suivantes :

1. Retirez **LON-SVR1** du domaine, ajoutez-le au groupe de travail **MUNICH** puis redémarrez le serveur.
2. Connexion en tant que :
 - o Nom d'utilisateur : **Administrateur**
 - o Mot de passe : **Pa55w.rd**
3. Basculez vers **LON-DC2**.
4. À partir du **Gestionnaire de serveur**, démarrez **Utilisateurs et ordinateurs Active Directory**, accédez à l'UO **Serveurs Adatum** puis supprimez **LON-SVR1**. Confirmez la suppression.

Organiser l'installation déléguée d'un RODC

1. Dans **Sites et services Active Directory**, créez un nouveau site nommé **Munich**, puis affectez-le à **DEFAULTSITELINK**.
2. Lancez le **Centre d'administration Active Directory** puis naviguez vers l'unité d'organisation **Contrôleurs de domaine**.
3. Créez au préalable un compte RODC avec le nom **LON-SVR1** qui soit également un **Serveur DNS** et un **Catalogue global**.
4. Déléquez **Nestor Fiore** pour installer et administrer le RODC.
5. Terminez la pré-création du compte RODC.

► **Tâche 2 : Exécuter l'Assistant d'installation Active Directory Domain Services sur un RODC pour terminer le processus de déploiement**

1. Basculez vers **LON-SVR1**. À partir du **Gestionnaire de serveur**, lancez l'**Assistant Ajout de rôles et fonctionnalités**.
2. Utilisez l'assistant pour installer les **Services de domaine Active Directory** sur **LON-SVR1**. Acceptez l'installation des fonctionnalités et des outils de gestion.
3. Une fois l'installation terminée, cliquez dans la zone de notification du **Gestionnaire de serveur** pour promouvoir ce serveur à un contrôleur de domaine.
4. Configurez-le pour ajouter le serveur comme contrôleur de domaine à un domaine existant. Cliquez sur **Modifier** et fournissez les informations suivantes :
 - Nom d'utilisateur : **Adatum\Nestor**
 - Mot de passe : **Pa55w.rd**
5. Sélectionnez **Adatum.com** comme domaine, puis poursuivez.
6. Notez que l'**Assistant d'installation Active Directory Domain Services** trouve le compte créé au préalable. Acceptez toutes les autres valeurs par défaut dans l'assistant pour utiliser ce compte, puis configurez AD DS.

► **Tâche 3 : Configurer la stratégie de réPLICATION de mot de passe à l'échelle du domaine**

1. Basculez vers **LON-DC2**. À partir du **Gestionnaire de serveur**, démarrez le **Centre d'administration Active Directory**.
2. Faites du groupe informatique, trouvé dans l'UO informatique, un membre du **Groupe de stratégie de réPLICATION de mot de passe RODC refusé**.



Remarque : les membres du groupe informatique ont des autorisations élevées, donc stocker leur mot de passe sur un RODC représenterait un risque de sécurité. Par conséquent, ajoutez le groupe Informatique à la liste globale de refus, qui s'applique à tous les RODC dans le domaine.

► **Tâche 4 : Créer un groupe pour gérer la réPLICATION de mot de passe au RODC de la filiale**

1. Basculez vers le **Gestionnaire de serveur** et, à partir du menu **Outils**, lancez **Utilisateurs et Ordinateurs Active Directory**.
2. Accédez au conteneur **Utilisateurs** puis créez un nouveau groupe nommé **Groupe de réPLICATION de mot de passe RODC autorisé de Munich**.
3. Ajoutez **Ana Cantrell** au nouveau groupe.
4. Dans le **Centre d'administration Active Directory**, à partir de l'UO **Contrôleurs de domaine**, visualisez les propriétés de **LON-SVR1**.
5. Dans la section **Extensions**, dans l'onglet **Stratégie de réPLICATION de mot de passe**, configurez le **Groupe de réPLICATION de mot de passe RODC autorisé de Munich** pour permettre la réPLICATION du mot de passe. Fermez les Propriétés pour **LON-SVR1**.

► **Tâche 5 : Évaluer la stratégie de réPLICATION de mot de passe qui en résulte**

1. Dans le **Centre d'administration Active Directory**, ouvrez les propriétés de **LON-SVR1**, puis dans la section **Extensions**, dans l'onglet **Stratégie de réPLICATION de mot de passe**, cliquez sur **Avancé**.

Notez que cette boîte de dialogue affiche tous les comptes dont les mots de passe sont stockés dans le RODC.

2. Sélectionnez les **Comptes authentifiés sur ce contrôleur de domaine en lecture seule**, puis notez que ceci ne montre que les comptes disposant des autorisations et ayant déjà été authentifiés par ce RODC.
3. Cliquez sur l'onglet **Stratégie résultante**, puis ajoutez **Ana Cantrell**. Notez qu'Ana Cantrell a une stratégie résultante d'**Autoriser**.
4. Fermez toutes les boîtes de dialogue ouvertes.

Résultats : à la fin de cet exercice, vous devez avoir déployé et configuré un RODC.

Exercice 3 : Créer et associer un MSA de groupe

Scénario

Vous devez configurer un MSA de groupe pour soutenir une nouvelle application basée sur le Web et en cours de déploiement. L'utilisation d'un MSA de groupe contribuera à maintenir les exigences de sécurité du mot de passe pour le compte.

Les tâches principales de cet exercice sont les suivantes :

1. Créer et associer un MSA ;
2. Installer un groupe MSA ;
3. Préparer le module suivant.

► Tâche 1 : Créer et associer un MSA

1. Dans **LON-DC1**, ouvrez la console **Module Active Directory pour Windows PowerShell**.
2. Créez la clé racine KDS en utilisant l'applet de commande **Add-KdsRootKey**. Définissez un temps effectif d'au moins 10 heures, pour que la clé soit immédiatement active.
3. Créez le nouveau compte de service nommé **Service Web** pour l'hôte **LON-DC1**.
4. Associez le MSA **Service Web** avec **LON-DC1**.
5. Vérifiez que le MSA de groupe a été créé en utilisant l'applet de commande **Get-ADServiceAccount**.

► Tâche 2 : Installer un groupe MSA

1. Dans **LON-DC1**, installez le compte de Service Web en utilisant la commande suivante :


```
Install-ADServiceAccount -Identity Webservice
```
2. Depuis le menu **Outils** dans le **Gestionnaire de serveur**, ouvrez le **Gestionnaire des services Internet (IIS)**.
3. Développez **LON-DC1 (Adatum\Administrateur)**, puis cliquez sur **Pools d'applications**.
4. Dans le volet Actions **DefaultAppPool**, dans la boîte de dialogue **Paramètres avancés**, configurez **DefaultAppPool** pour utiliser le compte **Webservice\$** comme l'identité. Notez que vous pouvez cliquer sur **ellipses (...)** par le nom d'identité pour ajouter le compte **Webservice\$** comme un compte personnalisé.
5. Arrêtez puis démarrez le pool d'applications.

Résultats : à la fin de cet exercice, vous devez avoir configuré un compte de service administré (MSA, Managed Service Account).

► Tâche 3 : Préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 à 3 pour **22742A-LON-DC2** et **22742A-LON-SVR1**.

Question : Dans le laboratoire, vous avez configuré les paramètres de mot de passe pour tous les utilisateurs au sein de la stratégie de domaine par défaut et vous avez configuré les paramètres de mot de passe pour les administrateurs dans un PSO. Quelles autres options étaient-elles disponibles pour vous aider à atteindre la solution ?

Question : Dans le laboratoire, vous utilisez la priorité pour le PSO administratif d'une valeur de 10. Pourquoi faire cela ?

Révision du module et Takeaways

Questions de contrôle des acquis

Question : Pourquoi la sécurité physique est-elle si importante, en particulier pour les contrôleurs de domaine AD DS ?

Question : Vous avez besoin de mettre en œuvre des stratégies de vérification pour l'authentification de domaine et les changements des services de répertoire. Quelle est la meilleure façon de mettre en œuvre ces paramètres de vérification ?

Question : Votre organisation vous oblige à maintenir une infrastructure AD DS très fiable et sécurisée. Elle exige également que les utilisateurs puissent accéder aux e-mails d'entreprise à partir d'Internet en utilisant Outlook Web Access. Vous envisagez de mettre en œuvre les paramètres de verrouillage de compte. Que devez-vous prendre en considération ?

Problèmes courants et conseils de dépannage

| Problème courant | Conseil pour la résolution du problème |
|--|--|
| Vous avez configuré les paramètres avancés de la stratégie de vérification, mais ils ne s'appliquent pas. | |
| Vous avez configuré la vérification du compte de connexion et des changements des services de répertoire. Maintenant, vous les testez, mais vous ne pouvez pas trouver les événements dans le journal des événements de votre serveur. | |

Outils

Le tableau suivant répertorie les outils référencés par ce module.

| Outil | Utilisation | Emplacement |
|---|---|--------------------------------|
| Utilisateurs et ordinateurs Active Directory | Gestion des objets dans AD DS, tels que les utilisateurs, les groupes et les ordinateurs. | Gestionnaire de serveur |
| Centre d'administration Active Directory | Gestion des objets dans AD DS, tels que les utilisateurs, les groupes et les ordinateurs. | Gestionnaire de serveur |
| Gestion des stratégies de groupe | Gestion, rapports, sauvegarde et restauration des GPO. | Gestionnaire de serveur |
| Gpupdate.exe | Mise à jour manuelle des GPO des machines locales. | Ligne de commande |

Module 8

Déploiement et gestion AD CS

Sommaire :

| | |
|--|------|
| Vue d'ensemble du module | 8-1 |
| Leçon 1 : Déploiement des AC | 8-2 |
| Leçon 2 : Administration des AC | 8-12 |
| Leçon 3 : Dépannage et maintien des AC | 8-23 |
| Atelier pratique : Déploiement et configuration d'une hiérarchie AC à deux niveaux | 8-31 |
| Contrôle des acquis et éléments à retenir | 8-35 |

Vue d'ensemble du module

L'infrastructure à clé publique (PKI) est constituée de plusieurs composants, tels que l'autorité de certification (AC), qui vous aident à sécuriser les communications et transactions d'entreprise. Vous pouvez utiliser les AC pour gérer, distribuer et valider les certificats numériques que vous utilisez pour sécuriser des informations. Vous pouvez installer les services de certificats Active Directory (AD CS) comme une AC racine ou une AC secondaire dans votre organisation. Dans ce module, vous apprendrez à déployer et à gérer des AC.

Objectifs

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

- Déployer les AC.
- Administrer Les AC.
- Dépanner et maintenir les AC.

Leçon 1

Déploiement des AC

Pour utiliser des certificats dans votre infrastructure Services de domaine Active Directory (AD DS), vous devez utiliser des certificats fournis par l'extérieur ou déployer et configurer au moins une AC. La première AC que vous déployez est une autorité de certification racine. Après avoir installé l'AC racine, vous pouvez installer une AC secondaire pour appliquer des restrictions de stratégie et pour émettre des certificats. Vous pouvez également utiliser un fichier CAPolicy.inf pour automatiser les installations d'AC racine et pour fournir des paramètres de configuration supplémentaires qui ne sont pas disponibles avec des installations basées sur l'interface graphique standard. Dans cette leçon, vous allez apprendre comment déployer des AC dans l'environnement de système d'exploitation Windows Server 2016.

Objectifs de la leçon

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

- Décrire AD CS.
- Décrire les options pour mettre en œuvre des hiérarchies d'AC ;
- Décrire les différences entre les AC autonomes et d'entreprises ;
- Décrire les considérations pour le déploiement d'une AC racine ;
- Déployer une AC racine d'entreprise ;
- Décrire les considérations pour le déploiement d'une AC secondaire ;
- Expliquer comment utiliser le fichier CAPolicy.inf pour installer une AC.

Qu'est-ce qu'AD CS ?

AD CS est une technologie d'identité au sein de Windows Server 2016 qui vous permet de mettre en œuvre PKI, de sorte que vous pouvez facilement émettre et gérer des certificats pour répondre aux besoins de votre organisation.

Vue d'ensemble de PKI

PKI est la combinaison de logiciels, technologies de chiffrement, de processus et de services qui permettent à une organisation de sécuriser ses communications et ses transactions commerciales. PKI repose sur l'échange de certificats numériques entre utilisateurs authentifiés et sur des ressources de confiance. Vous utilisez des certificats pour sécuriser des données et gérer les informations d'identification des utilisateurs et des ordinateurs à la fois à l'intérieur et à l'extérieur de votre organisation.

Vous pouvez concevoir une solution de PKI en utilisant AD CS pour répondre aux exigences techniques et de sécurité suivantes de votre organisation :

- Confidentialité. PKI vous donne la possibilité de crypter les données stockées et transmises. Par exemple, vous pouvez utiliser un système de fichiers EFS PKI pour crypter et sécuriser les données. Vous pouvez également maintenir la confidentialité des données transmises sur les réseaux publics en utilisant une sécurité du protocole Internet ICP (IPsec) activé avec PKI.

- Il permet d'implémenter une PKI pour votre organisation
 - Émettre et gérer des certificats
- Services de rôle AD CS sur Windows Server 2016
 - AC
 - Inscription par le Web de l'autorité de certification
 - Répondeur en ligne
 - Service d'inscription de périphérique réseau
 - Service Web Inscription de certificats
 - Service Web Stratégie d'inscription de certificats

- **Intégrité.** Vous pouvez utiliser des certificats pour signer numériquement des données. Une signature numérique détermine si des données ont été modifiées lors de la communication des informations. Par exemple, un message électronique signé numériquement veille à ce que le contenu du message ne soit pas modifié pendant le transit. En outre, dans une infrastructure PKI, l'AC émettrice signe numériquement les certificats qui sont émis aux utilisateurs et aux ordinateurs, ce qui prouve l'intégrité des certificats émis.
- **Authenticité.** Une PKI fournit plusieurs mécanismes d'authenticité. Les données d'authentification passent par des algorithmes de hachage, comme Secure Hash Algorithm 2 (SHA-2) pour produire une synthèse du message. La synthèse du message est ensuite signée numériquement en utilisant la clé privée de l'expéditeur à partir du certificat pour prouver que l'expéditeur a produit la synthèse du message.
- **Non-répudiation.** Lorsque les données sont signées numériquement avec un certificat de l'auteur, la signature numérique fournit à la fois la preuve de l'intégrité des données signées et la preuve de l'origine des données. L'intégrité et l'origine des données à tout moment et le propriétaire du certificat qui a signé numériquement les données ne peut pas les révoquer.
- **Disponibilité.** Vous pouvez installer plusieurs AC dans votre hiérarchie AC pour émettre des certificats. Si une AC n'est pas disponible dans une hiérarchie d'AC, d'autres AC peuvent continuer à émettre des certificats.

AD CS dans Windows Server 2016

Windows Server 2016 déploie tous les composants liés à PKI en tant que services de rôle du rôle de serveur AD CS. Chaque service de rôle est responsable d'une partie spécifique de l'infrastructure de certificat tout en travaillant ensemble pour former une solution complète.

Les services de rôle du rôle AD CS dans Windows Server 2016 sont les suivants :

- **Autorité de certification.** Les principaux objectifs des AC sont d'émettre des certificats, de révoquer les certificats et de publier des accès à l'information de l'autorité (AIA) et des informations de révocation. Lorsque vous installez la première AC, elle établit la PKI dans votre organisation. Vous pouvez avoir une ou plusieurs AC dans un seul réseau, mais une seule AC peut être au plus haut point dans la hiérarchie AC. L'AC racine est l'AC située au point le plus haut dans la hiérarchie. Cependant, vous pouvez avoir plus d'une hiérarchie d'AC, ce qui vous permet d'avoir plus d'une AC racine. Après qu'une autorité de certification racine ait émis un certificat pour elle-même, les AC secondaires inférieures dans la hiérarchie reçoivent des certificats de l'autorité de certification racine.
- **Inscription de l'autorité de certification via le Web.** Ce composant fournit une méthode pour émettre et renouveler les certificats pour les utilisateurs, les ordinateurs et les périphériques qui ne sont pas joints au domaine, ne sont pas connectés directement au réseau ou sont pour les utilisateurs d'autres systèmes d'exploitation que Windows.
- **Répondeur en ligne.** Vous pouvez utiliser ce composant pour configurer et gérer la vérification de la validation et de la répudiation du protocole OCSP (Online Certificate Status Protocol). Un répondeur en ligne décode des demandes de révocation de statut pour des certificats spécifiques, évalue l'état de ces certificats et renvoie une réponse signée contenant les informations d'état de certificat demandées. Les données de révocation de certificats peuvent provenir d'une AC sur un ordinateur qui exécute Windows Server 2003 ou une version plus récente.
- **Service d'inscription de périphérique réseau.** Avec ce composant, les routeurs, les commutateurs et autres périphériques réseau peuvent obtenir des certificats de la part d'AD CS.
- **Service Web Inscription de certificats (CES).** Ce composant fonctionne comme un client proxy entre l'ordinateur (sous Windows 7 ou supérieur) et l'AC. Windows Server 2008 R2 a introduit cette composante et elle exige que la forêt Active Directory soit au moins au niveau de Windows Server 2008 R2. Il permet aux utilisateurs, aux ordinateurs ou aux applications de se connecter à une AC en utilisant des services Web pour effectuer les actions suivantes :

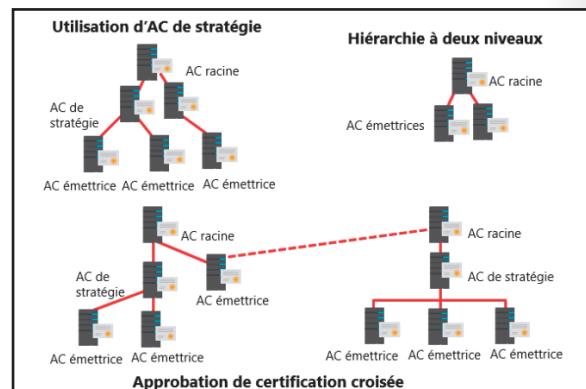
- Demander, renouveler et installer les certificats émis ;
- Récupérer des listes de révocation de certificats (CRL) ;
- Télécharger un certificat racine ;
- S'inscrire sur Internet ou à travers des forêts ;
- Renouveler automatiquement des certificats pour les ordinateurs qui font partie de domaines AD DS non approuvés ou ne sont pas liés à un domaine.
- Service Web Stratégie d'inscription de certificats. Ce composant permet aux utilisateurs d'obtenir des informations sur la stratégie d'inscription de certificats. Combiné avec CES, il permet l'inscription à base de certificats basés sur la stratégie lorsque l'ordinateur client n'est pas un membre d'un domaine ou lorsqu'un membre de domaine n'est pas connecté au domaine.

Le rôle de serveur AD CS, en plus de tous les services de rôle liés, peut fonctionner sur Windows Server 2016 avec une expérience de bureau complet ou sur une installation minimale. Cependant, les rôles AD CS ne peuvent pas fonctionner sur Nano Server. Vous pouvez déployer les services de rôle AD CS dans Windows Server 2016 à l'aide du Gestionnaire de serveur ou des applets de commande dans l'interface de ligne de commande Windows PowerShell. En outre, vous pouvez déployer les services de rôle tout en travaillant localement sur l'ordinateur ou à distance sur le réseau.

AD CS dans Windows Server 2016 a maintenant un soutien accru pour l'attestation de clé du Module de plateforme sécurisée (TPM). Bien que le support client existe pour les clés privées protégées par le TPM depuis Windows 8, AD CS dans Windows Server 2012 R2 ne pouvait effectuer que des attestations de clé TPM en utilisant le fournisseur de chiffrement de la Microsoft. AD CS vous permet maintenant d'utiliser le fournisseur stockage de clé à carte à puce Microsoft (KSP) pour l'attestation de clé TPM afin que les périphériques qui ne sont pas joints au domaine puissent s'inscrire pour des certificats concernant une clé privée protégée par TPM en utilisant une inscription NDES.

Options pour la mise en œuvre des hiérarchies CA

Lorsque vous décidez de mettre en œuvre AD CS dans votre organisation, l'une des premières décisions que vous devez faire est la façon de concevoir votre hiérarchie d'AC. La hiérarchie d'AC détermine la conception de base de votre PKI interne et détermine le but de chaque AC au sein de la hiérarchie. Chaque hiérarchie d'AC comprend habituellement deux ou plusieurs AC. Habituellement, la deuxième AC et toutes les autres après sont déployées dans un but précis. Seule l'AC racine est obligatoire.



Remarque : il n'est pas obligatoire d'avoir une hiérarchie multi-niveau d'AC déployée pour utiliser PKI et les certificats. Pour les environnements plus petits et plus simples, vous pouvez avoir une hiérarchie d'AC avec une seule AC déployée. Cette AC est généralement déployée comme une AC racine d'entreprise. En outre, vous pouvez choisir de ne pas déployer d'autorité de certification interne du tout et d'utiliser des certificats fournis à l'extérieur.

Si vous décidez de mettre en œuvre une hiérarchie d'AC et avez déjà déployé une AC racine, vous devez décider quels rôles assigner aux AC sur les deuxième et troisième niveaux. En général, nous ne recommandons pas la construction d'une hiérarchie d'AC supérieure à trois niveaux, à moins qu'elle ne soit dans un environnement complexe et distribué.

Le plus souvent, les hiérarchies d'AC ont deux niveaux, avec l'autorité de certification racine au niveau supérieur et l'AC émettrice secondaire au deuxième niveau. L'AC racine est généralement mise hors ligne tandis que les AC secondaires émettent et gèrent des certificats pour tous les clients. Toutefois, dans certains scénarios plus complexes, vous pouvez également déployer d'autres types de hiérarchies d'AC.

En général, les hiérarchies d'AC appartiennent à l'une des catégories suivantes :

- Hiérarchies d'AC avec AC de stratégie. Les AC de stratégie sont un type d'AC secondaires qui se trouvent directement sous l'AC racine dans une hiérarchie d'AC. Vous utilisez des AC de stratégie pour émettre des certificats d'AC à des AC secondaires qui se trouvent directement sous l'AC de stratégie dans la hiérarchie. Le rôle d'une AC de stratégie est de décrire les stratégies et procédures que l'organisation met en œuvre pour sécuriser son PKI, les processus qui valident l'identité des détenteurs de certificats et les processus qui appliquent les procédures qui gèrent les certificats. Une AC de stratégie n'émet de certificats qu'aux autres autorités de certification. Les AC qui reçoivent ces certificats doivent respecter et appliquer les stratégies que l'AC de stratégie définit. Il est obligatoire d'utiliser les AC de stratégie sauf si différents secteurs, divisions ou lieux de votre organisation exigent des stratégies et des procédures d'émission différentes. Toutefois, si votre organisation exige des stratégies et des procédures d'émission différentes, vous devez ajouter les AC de stratégie à la hiérarchie pour définir chaque stratégie unique. Par exemple, une organisation peut mettre en œuvre une AC de stratégie pour tous les certificats qu'elle émet en interne pour les employés et une autre AC de stratégie pour tous les certificats qu'elle émet à des utilisateurs qui ne sont pas employés.
- Hiérarchies d'AC avec confiance à certification croisée. Dans ce scénario, deux hiérarchies d'AC indépendantes interagissent quand une AC dans une hiérarchie émet un certificat d'autorité de certification en certification croisée à une AC dans une autre hiérarchie. Lorsque vous faites cela, vous établissez la confiance mutuelle entre différentes hiérarchies d'AC.
- AC avec une hiérarchie à deux niveaux. Dans une hiérarchie à deux niveaux, il y a une autorité de certification racine et au moins une autorité de certification secondaire. Dans ce scénario, l'AC secondaire est responsable des stratégies et de l'émission des certificats aux demandeurs.

AC d'entreprise contre AC autonomes

Dans Windows Server 2016 AD CS, vous pouvez déployer deux types d'AC : des AC autonomes et d'entreprises. Ces types ne sont pas une question de hiérarchie, mais de fonctionnalité et de stockage de configuration. La différence la plus importante entre ces deux types d'AC est l'intégration et la dépendance AD DS. Une AC autonome peut fonctionner sans AD DS et n'en dépend pas en aucune façon. Une AC d'entreprise nécessite AD DS, mais fournit également plusieurs avantages, y compris l'inscription automatique. La fonction d'inscription automatique permet aux utilisateurs et périphériques associés à un domaine de s'inscrire automatiquement pour les certificats si vous avez activé l'inscription automatique de certificat par la stratégie de groupe.

| AC autonomes | AC d'entreprise |
|---|---|
| Doit être utilisée si une AC (racine / intermédiaire / stratégie) est hors connexion, car une AC autonome n'est pas liée à un domaine AD DS | Nécessite l'utilisation d'AD DS et stocke les informations dans AD DS |
| Les utilisateurs doivent fournir des informations d'identification et spécifier le type de certificat | Peut utiliser la stratégie de groupe pour propager des certificats au stockage de certificat AC racine approuvé |
| Ne supporte pas les modèles de certificats | Publie les certificats utilisateur et CRL à AD DS |
| Toutes les demandes de certificat sont mises en attente jusqu'à l'autorisation de l'administrateur | Délivre des certificats basés sur un modèle de certificat |
| | Prend en charge l'inscription automatique pour l'émission des certificats |

Le tableau suivant détaille les différences les plus importantes entre les AC autonomes et d'entreprises.

| Caractéristique | AC autonome | AC d'entreprise |
|-----------------------------------|---|--|
| Usage typique | Vous utilisez généralement une AC autonome pour des AC hors ligne, mais vous pouvez également l'utiliser pour une AC qui est toujours disponible sur le réseau. | Vous utilisez généralement une AC d'entreprise pour émettre des certificats aux utilisateurs, aux ordinateurs et aux services et vous ne pouvez pas l'utiliser comme une AC hors-ligne. |
| Dépendance à AD DS | Une AC autonome ne dépend pas d'AD DS et vous pouvez la déployer dans des environnements autres qu'AD DS. | Une AC d'entreprise nécessite AD DS, que vous utilisez comme base de données de configuration et d'enregistrement. Une AC d'entreprise fournit également un point de publication pour les certificats émis aux utilisateurs et ordinateurs. |
| Méthodes de demande du certificat | Les utilisateurs peuvent demander des certificats uniquement à partir d'une AC autonome en utilisant une procédure manuelle ou une inscription Web. | Les utilisateurs peuvent demander des certificats à une AC d'entreprise en utilisant les méthodes suivantes : <ul style="list-style-type: none"> • Inscription manuelle • Inscription Web • Auto-inscription • Inscription au nom • Services Internet |
| Méthodes d'émission du certificat | Un administrateur de certificat doit approuver toutes les demandes manuellement. | Les demandes peuvent être émises ou refusées automatiquement en fonction des paramètres émission-exigences. |

Le plus souvent, vous déployez l'AC racine, qui est la première AC à être déployée en tant qu'AC autonome et elle est mise hors ligne après avoir émis un certificat pour elle-même et pour une AC secondaire

Considérations pour le déploiement d'une autorité de certification racine

Avant de déployer une AC racine, vous devez décider plusieurs aspects. D'abord, vous devez déterminer si vous avez besoin de déployer une AC racine hors connexion. Sur la base de cette décision, vous devez également décider si vous allez déployer une AC racine autonome ou une AC racine d'entreprise

Habituellement, si vous déployez une hiérarchie d'AC sur une seule couche, ce qui signifie que vous déployez une seule AC, il est plus courant de choisir une AC racine d'entreprise. Cependant, si vous déployez une hiérarchie à deux couches avec une AC secondaire, le scénario le plus courant est de déployer une AC racine autonome. Cela rend l'AC racine plus sûre et permet de la mettre hors ligne, sauf quand elle doit émettre des certificats pour les nouvelles AC secondaires.

- Le nom de l'ordinateur et l'appartenance au domaine ne peuvent pas changer
- Lorsque vous planifiez la configuration de clés privées, considérez ce qui suit :
 - CSP
 - La longueur de caractères clés avec une valeur par défaut de 2048
 - L'algorithme de hachage qui est utilisé pour signer les certificats émis par une autorité de certification
- Lorsque vous planifiez une AC racine, tenez compte de ce qui suit :
 - Nom et configuration
 - Base de données de certificat et l'emplacement du journal
 - Période de validité

L'autre facteur à considérer est le type d'installation du système d'exploitation. Tant l'expérience utilisateur que les installations minimales prennent en charge AD CS. L'installation minimale offre une surface d'attaque plus petite et un traitement moins administratif et donc, vous devriez l'envisager pour AD CS dans un environnement d'entreprise. Dans Windows Server 2016, vous pouvez également utiliser Windows PowerShell pour déployer et gérer le rôle AD CS.

Vous devez être conscient que vous ne pouvez pas modifier les noms d'ordinateur, nom de domaine ou les adhésions de domaine de l'ordinateur après avoir déployé une AC de tout type sur cet ordinateur. Par conséquent, il est important de déterminer ces attributs avant d'installer une AC.

Le tableau suivant détaille les considérations supplémentaires.

| Considération | Description |
|---|--|
| Un fournisseur de services cryptographiques (CSP) qui est utilisé pour générer une nouvelle clé | <ul style="list-style-type: none"> Le CSP par défaut est le fournisseur de stockage de clé RSA#Microsoft. Tout fournisseur dont le nom contient un signe dièse (#) est un fournisseur Cryptography Next Generation (CNG). |
| La longueur de caractère de la clé | La longueur de la clé par défaut pour le Strong Cryptographic Provider Microsoft est de 2,048 caractères. Ceci est la valeur minimale recommandée pour une AC racine, mais il est recommandé de choisir une clé de 4.096 bits. |
| L'algorithme de hachage qui est utilisé pour signer les certificats émis par une AC | L'algorithme de hachage par défaut est SHA-256. Dans les versions précédentes de Windows Server, l'algorithme de hachage par défaut est SHA-1. Bien que l'AD CS de Windows Server 2016 prend toujours en charge SHA-1, vous devriez l'éviter, sauf si vous en avez besoin spécifiquement pour prendre en charge d'anciennes versions de Windows. SHA-1 n'est plus considéré comme sûr et de nombreux navigateurs Web arrêteront de le prendre en charge en 2017. |
| La période de validité des certificats émis par une autorité de certification | Les modèles définissent la valeur par défaut pour les certificats. Vous pouvez choisir différentes périodes de validité sur les différents modèles de certificats. |
| L'état du serveur racine (hors ligne ou en ligne) | Vous devez déployer le serveur racine comme une AC autonome hors ligne, si possible. Cela améliore la sécurité et protège le certificat racine en le rendant indisponible aux attaques venant du réseau. |

Si vous décidez de déployer une AC racine autonome hors-ligne, il y a des considérations spécifiques que vous devez garder à l'esprit :

- Avant d'émettre un certificat secondaire depuis l'AC racine, assurez-vous que vous fournissez au moins un point de distribution de liste de révocation de certificats (CDP) et un emplacement AIA qui sera disponible à tous les clients. En effet, par défaut, une autorité de certification racine autonome a le CDP et AIA situé sur lui-même. Par conséquent, lorsque vous déconnectez l'AC racine du réseau, une vérification de révocation échoue parce que les emplacements CDP et AIA sont inaccessibles. Lorsque vous définissez ces emplacements, vous devez copier les informations des listes de révocation des certificats et AIA manuellement à cet emplacement.

- Définissez une période de validité pour les listes de révocation des certificats que l'AC racine publie sur une longue période de temps, par exemple, un an. Cela signifie que vous devez activer l'AC racine une fois par an pour publier une nouvelle liste de révocation des certificats, puis la copiez à un endroit qui est à la disposition des clients. Si vous ne le faites pas, après l'expiration de la liste de révocation des certificats sur l'AC racine, la vérification de révocation pour tous les certificats échoue également.
- Utilisez la stratégie de groupe pour publier le certificat de l'AC racine sur une AC racine de confiance sur toutes les machines serveur et client. Vous devez le faire manuellement, car une AC autonome ne peut pas le faire automatiquement, contrairement à une AC d'entreprise. Vous pouvez également publier le certificat d'autorité de certification racine sur AD DS en utilisant l'outil de ligne de commande certutil.

Démonstration : Déploiement d'une AC racine d'entreprise

Étapes de la démonstration

Déployer une AC racine d'entreprise

1. Dans **Gestionnaire de serveur**, ajoutez le rôle **Services de certificats Active Directory**.
2. Sélectionnez le service de rôle **Autorité de certification**.
3. Une fois l'installation terminée avec succès, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination**.
4. Sélectionnez cette option pour installer une AC racine d'entreprise.
5. Réglez la longueur de la clé sur **4096**.
6. Nommez l'AC **AdatumACRacine**.

Considérations pour le déploiement d'une AC secondaire

Vous pouvez utiliser une AC secondaire pour mettre en œuvre des restrictions de stratégie pour PKI et pour émettre des certificats aux clients.

Après l'installation d'une autorité de certification racine pour l'organisation, vous pouvez installer une ou plusieurs autorités de certification secondaires.

Lorsque vous utilisez une AC secondaire pour émettre des certificats à des utilisateurs ou des ordinateurs qui ont un compte dans un environnement AD DS, vous pouvez installer l'AC secondaire comme une AC d'entreprise. Ensuite,

vous pouvez utiliser les données des comptes clients dans AD DS pour émettre et gérer des certificats et pour publier des certificats dans AD DS. Cependant, pour compléter cette procédure, vous devez être membre du groupe Administrateurs local ou avoir des autorisations équivalentes. Si l'AC secondaire est une AC d'entreprise, vous devez également être membre du groupe Administrateurs du domaine ou avoir des autorisations équivalentes. Du point de vue de la sécurité, un scénario recommandé serait d'avoir une AC racine autonome hors-ligne et une AC secondaire d'entreprise.

- Le nom de l'ordinateur et l'appartenance au domaine ne peuvent pas changer
- Lorsque vous planifiez la configuration de clés privées, considérez ce qui suit :
 - CSP
 - La longueur de caractères clés avec une valeur par défaut de 2048
 - L'algorithme de hachage qui est utilisé pour signer les certificats émis par une autorité de certification
- Lorsque vous planifiez une AC racine, tenez compte de ce qui suit :
 - Nom et configuration
 - Base de données de certificat et l'emplacement du journal
 - Période de validité

Une AC secondaire est généralement déployée pour remplir certaines des fonctionnalités suivantes :

- Utilisation. Vous pouvez émettre des certificats pour un certain nombre d'objectifs, tels que les protocoles Secure/Multipurpose Internet Mail Extensions (S/MIME), EFS ou l'accès à distance. La politique d'émission pour ces différentes utilisations pourrait être distincte et la séparation fournit une base pour l'administration de ces stratégies.
- Divisions organisationnelles. Vous pourriez avoir des stratégies différentes pour l'émission de certificats qui dépendent du rôle d'une entité dans l'organisation. Vous pouvez créer des AC secondaires pour séparer et administrer ces stratégies.
- Divisions géographiques. Les organisations ont souvent des entités situées sur différents sites physiques. Une connectivité réseau limitée entre ces sites pourrait exiger des AC secondaires individuelles pour plusieurs sites ou pour tous.
- Équilibrage de charge. Si vous utilisez votre PKI pour émettre et gérer un grand nombre de certificats et n'avez qu'une seule AC, cela peut résulter en une charge réseau considérable pour cette unique AC. L'utilisation de plusieurs AC secondaires pour émettre le même genre de certificats divise la charge du réseau entre les AC.
- Sauvegarde et tolérance aux pannes. Des AC multiples augmentent la possibilité que votre réseau dispose d'AC opérationnelles disponibles pour répondre aux demandes des utilisateurs.

Comment utiliser le fichier StratégieAC.inf pour l'installation d'une AC

Vous pouvez utiliser le fichier CAPolicy.inf si vous souhaitez déployer une AC racine ou secondaire et que vous voulez définir des valeurs et des paramètres pendant ou après l'installation. Le fichier CAPolicy.inf est un fichier texte qui contient divers paramètres que vous pouvez utiliser lorsque vous installez le rôle AD CS ou lorsque vous renouvez le certificat AC. Le fichier CAPolicy.inf n'est pas nécessaire pour installer AD CS, mais sans lui, les paramètres par défaut sont appliqués. Dans de nombreux cas, les paramètres par défaut ne sont pas suffisants pour des déploiements plus complexes.

Vous pouvez utiliser le fichier CAPolicy.inf pour configurer les AC dans des déploiements plus complexes.

Chaque fichier CAPolicy.inf est divisé en sections et a une structure simple, décrite comme suit :

- Une *section* est une zone dans le fichier.inf qui contient un groupe logique de clés. Une section apparaît toujours entre crochets dans le fichier.inf.
- Une *clé* est le paramètre qui se trouve à gauche du signe égal (=).
- Une *valeur* est le paramètre qui est à la droite du signe égal (=).

Par exemple, si vous souhaitez spécifier un point AIA dans le fichier CAPolicy.inf, vous utilisez la syntaxe suivante :

```
[AuthorityInformationAccess]
URL=http://pki.adatum.com/CertData/adatumCA.crt
```

- Le fichier CAPolicy.inf est stocké dans le dossier %Windir% de l'AC racine ou secondaire
- Le fichier CAPolicy.inf définit les éléments suivants :
 - L'emplacement du CPS ;
 - L'identificateur d'objet ;
 - Les intervalles de publication de la liste CRL ;
 - Les paramètres de renouvellement de l'AC ;
 - La longueur de clé ;
 - La période de validité du certificat ;
 - Les chemins CDP et AIA.

Dans cet exemple, AuthorityInformationAccess est une section, l'URL est la clé et <http://pki.adatum.com/CertData/adatumCA.crt> est la valeur.

Vous pouvez également spécifier certains paramètres du serveur d'AC dans le fichier CAPolicy.inf. Un exemple de la section qui définit ces paramètres est :

```
[certsrv_server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=5
CRLPeriod=Days
CRLPeriodUnits=2
CRLDeltaPeriod=Hours
CRLDeltaPeriodUnits=4
ClockSkewMinutes=20
LoadDefaultTemplates=True
AlternateSignatureAlgorithm=0
ForceUTF8=0
EnableKeyCounting=0
```



Remarque : Tous les paramètres des exemples précédents sont facultatifs.

Vous pouvez également utiliser le fichier CAPolicy.inf lors de l'installation d'AD CS pour définir ce qui suit :

- Certification practice statement (CPS). Décrit les pratiques que l'AC utilise pour émettre des certificats. Cela inclut les types de certificats émis, les informations sur l'émission, le renouvellement et la récupération des certificats et d'autres détails sur la configuration de l'AC.
- L'identificateur d'objet. Identifie un objet ou un attribut spécifique.
- Intervalles de publication de la liste de révocation des certificats. Définit l'intervalle entre les publications pour la liste de révocation de certificats de base.
- Paramètres de renouvellement de l'AC. Vous pouvez définir les paramètres de renouvellement comme suit :
 - Longueur de clé. Définit la longueur de la paire de clés utilisée lors d'un renouvellement d'une AC racine.
 - Période de validité du certificat. Définit la période de validité d'un certificat d'une AC racine.
 - Chemins CDP et AIA. Fournit le chemin utilisé pour les installations et les renouvellements d'AC racine.

Après avoir créé votre fichier CAPolicy.inf, vous devez le copier dans le dossier %SystemRoot% de votre serveur (par exemple, C:\Windows) avant d'installer le rôle AD CS ou avant de renouveler le certificat AC.



Remarque : le fichier CAPolicy.inf est utilisé à la fois pour les installations et les renouvellements d'AC racines et secondaires.

Testez vos connaissances

| Question | |
|--|---|
| Lesquelles des options suivantes décrivent les avantages du déploiement d'une AC d'entreprise au lieu d'une AC autonome ? | |
| Sélectionnez la réponse correcte. | |
| | Fournit plusieurs façons pour les utilisateurs et les périphériques de recevoir des certificats. |
| | Ne nécessite pas AD DS. |
| | Les demandes de certificats peuvent être délivrées ou refusées automatiquement en fonction de la stratégie. |
| | Peut être mis hors ligne pour éviter les compromis. |
| | Peut utiliser des modèles pour émettre des certificats basés sur les données dans AD DS. |

Testez vos connaissances

| Question | |
|---|---|
| Lesquelles des options suivantes sont des raisons pour déployer plusieurs AC secondaires ? | |
| Sélectionnez la réponse correcte. | |
| | Vous voulez segmenter l'émission de certificats sur la base de stratégies d'utilisation uniques. |
| | Vous avez plusieurs domaines dans votre environnement AD DS et chaque domaine exige sa propre AC secondaire. |
| | Vous voulez segmenter l'émission de certificats sur base de la division organisationnelle ou de la région géographique. |
| | Vous voulez plusieurs AC secondaires pour la haute disponibilité et l'équilibrage de charge des demandes. |
| | Vous avez besoin de publier plusieurs modèles de certificat et chaque modèle nécessite sa propre AC secondaire. |

Leçon 2

Administration des AC

Après avoir conçu et déployé une hiérarchie d'AC, vous devez configurer différentes options pour les AC. Vous devez disposer de méthodes efficaces pour la gestion de la hiérarchie d'AC et pour la configuration des options de sécurité, l'audit et le suivi. AD CS propose plusieurs méthodes pour la gestion de la hiérarchie d'AC. Dans cette leçon, vous allez apprendre à administrer et gérer la hiérarchie d'AC et les AC.

Objectifs de la leçon

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

- Expliquer comment gérer les AC ;
- Décrire comment configurer la sécurité des AC ;
- Décrire comment configurer les rôles de sécurité pour l'administration des AC ;
- Décrire comment configurer la stratégie de l'AC et les modules de sortie ;
- Décrire comment configurer les emplacements CDP et AIA ;
- Configurer les propriétés des AC.

Gestion des AC

Après avoir déployé une AC, il y a plusieurs tâches que vous devez effectuer pour la configurer et, par après, pour la gérer correctement. Une AC est un service très important, donc vous devez la gérer avec soin.

Après qu'une hiérarchie d'AC a été déployée, vous devez vérifier la configuration de sécurité de l'AC pour vérifier quels utilisateurs et groupes sont autorisés à effectuer des tâches administratives sur cette AC. En outre, il est important que vous configuriez les options de journalisation et de surveillance pour une AC, afin d'enregistrer toutes les tâches et activités importantes.

Vous pouvez configurer les options de gestion d'AC les plus courantes si vous utilisez la console de gestion d'AC. Cependant, vous pouvez également utiliser Windows PowerShell et l'utilitaire de ligne de commande certutil pour gérer différentes options d'AC avancées et pour effectuer certaines tâches qui ne sont pas disponibles dans une console graphique.

- Pour la gestion de la hiérarchie d'AC, vous pouvez utiliser :
 - La console de gestion de l'autorité de confiance ;
 - Windows PowerShell ;
 - L'utilitaire de ligne de commande Certutil.
- Certutil fournit une interface pour AC avancée et la configuration et de gestion de PKI
- Les options de PKI peuvent être gérées via la stratégie de groupe, si vous utilisez ce qui suit :
 - Les Informations d'identification itinérantes ;
 - L'inscription automatique des certificats ;
 - La validation du chemin d'accès du certificat ;
 - La distribution de certificat.

Applets de commande Windows PowerShell pour le déploiement et l'administration d'une AC

Windows Server 2016 fournit plusieurs applets de commande Windows PowerShell pour le déploiement et l'administration d'AD CS. Dans Windows Server 2016, les modules Windows PowerShell **ADCSDeployment** et **ADCSAdministration** sont disponibles pour déployer et administrer les AC. Si vous avez déjà installé les fichiers binaires AD CS, vous pouvez importer les modules destinés à être utilisés dans Windows PowerShell en exécutant les commandes suivantes :

```
Import-Module ADCSDeployment  
Import-Module ADCSAdministration
```

Si vous voulez voir tous les applets de commande disponibles pour le déploiement et l'administration des AC, vous pouvez exécuter la commande suivante dans Windows PowerShell :

```
Get-Command -Module ADCS*
```

La liste suivante décrit certains applets de commande pour l'administration des AC :

- **Add-CATemplate.** Ajoute un modèle de certificat à l'AC
- **Add-CACrlDistributionPoint.** Ajoute un Uniform Resource Identifier (URI) CDP dans lequel l'AC publie des révocations de certification.
- **Add-CAAuthorityInformationAccess.** Configure un URI AIA ou OCSP sur une AC.
- **Get-CATemplate.** Obtient la liste des modèles établis sur l'AC pour l'émission de certificats.
- **Get-CACrlDistributionPoint.** Obtient tous les endroits indiqués sur l'extension CDP des propriétés d'AC.
- **Get-CAAuthorityInformationAccess.** Obtient les informations URI AIA et OCSP mises sur l'extension AIA des propriétés d'AC.
- **Remove-CATemplate.** Supprime les modèles de l'AC qui ont été réglés pour l'émission de certificats.
- **Remove-CACrlDistributionPoint.** Supprime l'URI pour le CDP de l'AC.
- **Remove-CAAuthorityInformationAccess.** Supprime l'URI AIA ou OCSP de l'extension AIA définie sur l'AC.



Lectures supplémentaires : Pour plus d'informations, consultez :

- « Applets de commande pour le déploiement d'AD CS dans Windows PowerShell » à l'adresse : <http://aka.ms/Giih2g>
- « Applets de commandes pour l'administration d'AD CS dans Windows PowerShell » à l'adresse : <http://aka.ms/Dekm5i>

Utilisation de certutil pour administrer une AC

Alors que Windows PowerShell ne fournit pas de gestion complète d'AD CS, certutil offre une gestion complète. Certutil.exe est un utilitaire de ligne de commande qui est installé dans le cadre d'AD CS. Certutil.exe peut afficher des informations de configuration d'une AC, configurer AD CS, sauvegarder et restaurer des composants d'AC et vérifier les certificats, les paires de clés et les chaînes de certificats.

Pour les tâches courantes de configuration et de gestion d'AC, vous ne devez pas utiliser certutil. Cependant, pour des tâches plus avancées, certutil peut être votre seul choix.

Par exemple, si vous voulez passer en revue tous les paramètres de configuration pour l'AC, vous pouvez le faire en exécutant les commandes suivantes :

```
Certutil -dump
Certutil -getreg
Certutil -getreg CA
```

Cette commande fournit beaucoup plus d'informations sur votre configuration AC. Cela inclut le type d'information qui est fixé par CAPolicy.inf ou après l'installation en exécutant des scripts de post-configuration. Vous ne pouvez pas accéder à toutes les informations en n'utilisant que la console d'administration de l'AC.

Pour afficher le contenu du conteneur AIA dans AD DS pour un domaine nommé adatum.com, exécutez la commande suivante :

```
certutil -viewstore "ldap:///CN=AIA,CN=Public Key  
Services,CN=Services,CN=Configuration,DC=adatum,DC=com?  
cACertificate?base?objectclass=certificationAuthority"
```

Gestion de PKI avec la stratégie de groupe

Une fois votre PKI en place, vous aurez besoin de vous tourner vers la stratégie de groupe pour automatiser la distribution et pour définir les options de configuration. Vous pouvez utiliser la stratégie de groupe pour les domaines suivants liés à AD CS :

- Informations d'identification itinérantes. Les informations d'identification itinérantes permettent aux utilisateurs de conserver leurs certificats avec AD DS sur plusieurs ordinateurs. Cela supprime l'obligation de gérer plusieurs certificats clients et les clés privées sur plusieurs postes de travail clients pour un seul utilisateur.
- Inscription automatique des certificats. L'inscription automatique simplifie l'émission de certificats en permettant aux ordinateurs clients de demander et renouveler les certificats automatiquement. L'inscription automatique nécessite une AC d'entreprise et l'utilisation de la stratégie de groupe pour permettre aux ordinateurs et aux utilisateurs de votre environnement AD DS d'utiliser l'inscription automatique.
- Validation du chemin d'accès du certificat. Avec la validation de chemin d'accès du certificat, vous pouvez gérer les certificats utilisés pour la signature de code, le déploiement de certificats d'AC secondaires, le blocage des certificats qui ne sont pas approuvés et la configuration des paramètres de récupération pour les certificats et les listes de révocation des certificats.
- Distribution de certificat. En règle générale, vous utilisez la stratégie de groupe pour la distribution automatisée de certificats ou pour spécifier les paramètres liés à l'inscription.

Configuration de la sécurité d'une autorité de confiance

Pour gérer et configurer la sécurité sur l'AC, vous pouvez utiliser l'onglet **Sécurité** pour afficher les propriétés d'une AC dans la console d'autorité de certification (certsrv.msc). Vous pouvez définir les autorisations de sécurité suivantes sur une AC :

- Lecture. Les entités de sécurité affectées de cette autorisation peuvent localiser cette AC dans AD DS ou y accéder en utilisant la console Web ou les services Web si vous avez déployé l'AC comme une AC autonome.
- Émettre et gérer des certificats. Les entités de sécurité affectées de cette autorisation peuvent approuver ou refuser les demandes de certificats qui sont en attente. Elles peuvent également révoquer un certificat émis, spécifier un motif de révocation et effectuer une non-révocation. Les entités de sécurité peuvent également lire tous les certificats émis et les exporter vers des fichiers.
- Gérer une AC. Les entités de sécurité affectées de cette autorisation peuvent gérer et configurer toutes les options de l'AC. Elles ne peuvent pas gérer les certificats par défaut, mais peuvent se donner ce droit.

• Vous pouvez attribuer les autorisations suivantes sur un objet d'AC :

- Lecture
- Émission et gestion des certificats
- Gestion d'une AC
- Demande de certificats

• Les principes de sécurité avec la permission d'émission et de gestion des certificats peuvent être limités à un modèle spécifique

- L'onglet Gestionnaires de certificats sur les propriétés de l'objet d'AC

- Demander des certificats. Les entités de sécurité affectées de cette autorisation peuvent effectuer des demandes de certificats contre cette AC. Toutefois, cela ne signifie pas qu'elles peuvent s'inscrire pour un certificat. Le modèle de certificat contrôle les autorisations d'inscription.

En plus de définir des autorisations de sécurité sur la liste de contrôle d'accès (ACL) de l'objet AC, vous pouvez également utiliser l'onglet **Gestionnaires de certificats** dans les propriétés de l'AC pour limiter d'autres entités de sécurité contenant l'autorisation **Émettre et gérer des certificats**.

Par exemple, si vous souhaitez déléguer l'autorisation **Émettre et gérer des certificats** pour un modèle spécifique, vous devez :

- Accorder au directeur de la sécurité l'autorisation **Émettre et gérer des certificats** sur l'onglet **Sécurité** des propriétés de l'AC ;
- Sur l'onglet **Gestionnaires de certificats** des propriétés de l'AC, sélectionnez **Restreindre les gestionnaires de certificats** ;
- Sélectionnez l'entité de sécurité que vous souhaitez restreindre et modifiez les modèles que vous souhaitez que l'entité de sécurité gère.

En utilisant l'onglet **Gestionnaires de certificats** des propriétés de l'AC, vous pouvez déléguer des droits à un modèle de certificat spécifique sans donner à une entité de sécurité le droit **Émettre et gérer des certificats** sur tous les modèles publiés sur l'AC.

Rôles de sécurité pour l'administration de l'AC

L'administration basée sur les rôles dans AD CS offre la possibilité de déléguer les autorisations prédéfinies disponibles sur une AC à des groupes que vous créez soit dans AD DS (pour les AC d'entreprises), soit dans la base de données du Gestionnaire de compte de sécurité local (pour les AC autonomes qui ne sont pas associées à un domaine). Bien que vous puissiez attribuer des autorisations d'AC à un objet utilisateur spécifique, nous vous recommandons de ne déléguer des autorisations qu'à un groupe.

Déléguer à un groupe réduit l'effort administratif nécessaire et assure la transparence des autorisations que vous avez attribuées.

- Administration basée sur les rôles :
 - Accorder des autorisations d'AC prédéfinies à un groupe de sécurité
 - Doit être configuré manuellement ; les rôles ne sont pas créés automatiquement
- Des rôles typiques pour AD CS seraient :
 - Administrateur d'AC
 - Gestionnaire de certificats
 - Opérateur de sauvegarde
 - Vérificateur
 - Candidat
- Les rôles peuvent être uniques pour chaque déploiement AD CS

Chaque rôle que vous créez ne devrait être en mesure que d'effectuer une tâche ou une série de tâches prédéterminées que vous attribuez à un groupe de sécurité. Le tableau suivant présente le détail des rôles et des groupes généralement impliqués dans l'administration basée sur les rôles d'un déploiement AD CS.

| Rôle/groupe | Autorisations | Description |
|-----------------------------|--|--|
| Administrateur d'AC | Gérer une AC Émettre et gérer des certificats | Assigné dans la console de l'AC. Les utilisateurs dans ce rôle peuvent configurer tous les aspects de l'AC et affecter d'autres rôles si nécessaire. |
| Gestionnaire de certificats | Émettre et gérer des certificats | Assigné dans la console de l'AC. |

| Rôle/groupe | Autorisations | Description |
|-------------------------|--|--|
| Opérateur de sauvegarde | Sauvegarde des fichiers et des répertoires Restaure des fichiers et des répertoires | Ce rôle est un rôle de système d'exploitation, que l'adhésion au groupe de sécurité local Opérateurs de sauvegarde définit. |
| Vérificateur | Gère les journaux d'audit et de sécurité | Ce rôle est un rôle de système d'exploitation, que la politique de sécurité locale sur l'AC définit. |

| Rôle/groupe | Autorisations | Description |
|--------------|--|---|
| Participants | Demande des certificats (définis sur l'objet AC) Participe (défini sur le modèle de certificat) | Ce rôle est un rôle d'AC, qui donne aux utilisateurs affectés la capacité de voir l'AC et de demander des certificats. Cela ne signifie pas que les utilisateurs affectés ont des autorisations pour s'inscrire parce que l'autorisation est attribuée sur un modèle de certificat. Par défaut, l'entité de sécurité Utilisateurs identifiés dispose d'autorisations Demander des certificats sur une AC. Cependant, vous pourriez avoir des rôles plus spécifiques, qui attribuent des autorisations d'inscription pour chaque modèle unique exigé par votre organisation. |



Remarque : Le groupe **Administrateurs** local sur une AC dispose par défaut des autorisations **Gérer l'autorité de certification** et **Émettre et gérer des certificats**. Sur les AC d'entreprise, ces autorisations s'étendent également aux groupes **Administrateurs du domaine** et **Administrateurs de l'entreprise**. Sur les AC autonomes jointes à un domaine, les membres du groupe **Administrateurs du domaine** disposent aussi de droits administratifs complets sur l'AC.

Créer des rôles de sécurité pour l'administration d'AD CS

Vous devez être conscient qu'AD CS ne crée automatiquement pas les rôles et les groupes énumérés dans le tableau ci-dessus lorsque vous installez AD CS. Les rôles mentionnés ci-dessus sont représentatifs d'un déploiement AD CS typique où vous désirez une administration basée sur les rôles. L'administration basée sur les rôles peut être unique à chaque déploiement AD CS. Par conséquent, vous devez planifier et créer uniquement les rôles nécessaires à votre organisation. Lisez le scénario suivant et réfléchissez à la façon dont vous pourriez configurer l'administration basée sur les rôles pour répondre à ces exigences.

Scénario : Vous êtes l'administrateur AD CS pour A. Datum. Vous avez déployé une AC racine autonome qui est jointe au domaine et deux AC d'entreprises secondaires. Une AC secondaire émet des certificats d'utilisateur et l'autre AC secondaire émet des certificats d'ordinateur. Vous voulez mettre en place une administration basée sur les rôles afin d'avoir les rôles suivants :

- Un rôle qui a les droits **Gérer l'autorité de certification** et **Émettre et gérer des certificats** sur toutes les AC dans la hiérarchie ;
- Un rôle qui a les droits **Gérer l'autorité de certification** et **Émettre et gérer des certificats** sur les AC secondaires uniquement ;

- Un rôle qui a les droits **Émettre et gérer des certificats** pour le modèle de certificat **Utilisateur** ;
- Un rôle qui a les droits **Émettre et gérer des certificats** pour le modèle de certificat **Ordinateur**.

Vous configureriez l'administration d'AD CS basée sur les rôles en suivant les étapes ci-dessous.

1. Créez un groupe de sécurité dans AD DS qui s'aligne sur chaque rôle que vous souhaitez attribuer dans AD CS. Sur la base des exigences ci-dessus, vous devez créer les groupes suivants pour chaque rôle nécessaire.
 - Administrateurs PKI de l'entreprise
 - Administrateurs d'AC secondaires
 - Gestionnaires de certificats d'utilisateur
 - Gestionnaires de certificats d'ordinateur
2. Sur chaque AC dans la hiérarchie, vous affectez au groupe **Administrateurs PKI de l'entreprise** les autorisations **Gérer l'autorité de certification** et **Émettre et gérer des certificats** dans la console Autorité de certification.
3. Sur chaque AC secondaire, vous affectez au groupe **Administrateurs d'AC secondaires** les autorisations **Gérer l'autorité de certification** et **Émettre et gérer des certificats** dans la console Autorité de certification.
4. Sur l'AC secondaire qui émet des certificats d'utilisateur, vous affectez au groupe **Gestionnaires de certificats d'utilisateur** l'autorisation **Émettre et gérer des certificats** dans la console Autorité de certification. Sur l'onglet **Gestionnaires de certificats** des propriétés de l'AC, vous limitez le groupe **Gestionnaires de certificats d'utilisateur** au modèle de certificat **Utilisateur**.
5. Sur l'AC secondaire qui émet des certificats d'ordinateur, vous affectez au groupe **Gestionnaires de certificats d'ordinateur** l'autorisation **Émettre et gérer des certificats** dans la console Autorité de certification. Sur l'onglet **Gestionnaires de certificats** des propriétés de l'AC, vous limitez le groupe **Gestionnaires de certificats d'ordinateur** au modèle de certificat **Ordinateur**.

Configuration de la stratégie de l'AC et des modules de sortie

Des déploiements plus avancés de hiérarchies d'AC ou des scénarios dans lesquelles une AC avec un autre service en lien avec le PKI, nécessitent que vous configureriez et gériez des *modules de stratégie et de sortie* sur votre AC. Les modules de stratégie et de sortie existent sur toutes les AC, autonomes ou d'entreprise. Chaque AC a des modules de stratégie et de sortie par défaut et dans la plupart des scénarios, vous ne devez pas configurer ces modules. Vous pouvez gérer à la fois les modules de stratégie et de sortie si vous utilisez la console Administrateur AC. Pour une configuration plus complexe, cependant, vous devez utiliser l'outil de ligne de commande certutil.

- Le module de stratégie détermine l'action qui est effectuée après la réception de la demande de certificat
- Le module de sortie détermine ce qui se passe avec un certificat après son attribution
- Chaque AC est configurée avec la stratégie par défaut et les modules de sortie
- MIM 2016 et sa gestion de certificats déploie une stratégie personnalisée et des modules de sortie
- Le module de sortie peut envoyer un courrier électronique ou publier un certificat à un système de fichiers
- Vous devez utiliser certutil pour spécifier ces paramètres, car ils ne sont pas disponibles dans la console d'administration d'AC

Qu'est-ce qu'un module de stratégie ?

Un module de stratégie détermine l'action que l'AC effectue après avoir reçu la demande de certificat. Vous pouvez configurer un module de stratégie par défaut pour mettre chaque demande de certificat dans un état d'attente jusqu'à ce qu'un administrateur l'approuve ou la refuse. Le comportement du module de stratégie par défaut est d'émettre un certificat si les paramètres du modèle de certificat le permettent. Toutefois, vous pouvez installer un module de stratégie personnalisé pour faire d'autres tâches lorsque l'AC reçoit la demande de certificat.

Par exemple, si vous installez Microsoft Identity Manager (MIM) 2016 et sa gestion des certificats dans votre PKI interne, vous devrez déployer le module de stratégie MIM de gestion des certificats sur votre AC qui émet des certificats. MIM 2016 peut gérer l'émission de certificats par le biais des flux de travail. Le module de stratégie de gestion des certificats MIM transmet chaque demande d'un certificat géré par la gestion des certificats de MIM 2016 à la gestion de certificat MIM 2016 lorsqu'une AC reçoit une demande. Après que le flux de travail MIM a traité la demande, il émet le certificat ou refuse la demande. Le module de stratégie de gestion des certificats MIM spécifie également l'empreinte numérique du certificat de signature pour un agent qui a passé des demandes de certificats d'utilisateurs à une AC. Chaque demande que les AC marquent d'une empreinte numérique spécifiée dans le module de stratégie de gestion des certificats MIM est passée au flux de travail MIM avant qu'il n'émette le certificat. Ceci est un exemple de l'utilisation du module de stratégie personnalisé, mais il y a aussi d'autres applications tierces qui pourraient utiliser des modules de stratégie personnalisés.

Qu'est-ce qu'un module de sortie ?

Contrairement au module de stratégie, le module de sortie détermine ce qui se passe avec un certificat après que l'AC l'a émis. Les actions les plus courantes sont d'envoyer un e-mail ou de publier un certificat sur un système de fichiers. Ces actions sont possibles même avec un module de sortie par défaut sur chaque AC.

Cependant, vous pouvez également déployer un module de stratégie personnalisé. Pour utiliser le même exemple qu'avec le module de stratégie, si vous déployez Microsoft Identity Manager (MIM) 2016 et sa gestion des certificats dans votre environnement, vous aurez également à déployer un module de sortie personnalisé sur votre AC. Le module de sortie transfère des données sur chaque certificat émis à un Microsoft SQL Server spécifié dans le module de sortie. Si vous écrivez des informations sur les certificats émis à un ordinateur qui exécute SQL Server, la gestion des certificats MIM peut visualiser et contrôler les certificats émis sans interaction directe avec la base de données AC. Une AC peut utiliser simultanément des modules de sortie multiples, contrairement au module de stratégie, où vous ne pouvez avoir qu'un seul module de stratégie actif à la fois.

Par exemple, si vous souhaitez envoyer un courriel à une adresse spécifique à chaque fois que l'AC émet un certificat, vous devez utiliser certutil pour spécifier ces paramètres, car ils ne sont pas disponibles dans la console de l'administrateur AC.

Tout d'abord, vous devez spécifier le serveur de protocole SMTP qui est utilisé pour envoyer des courriels, ce que vous pouvez faire en exécutant la commande certutil suivante :

```
certutil -setreg exit\smtp\<smtpServerName>
```

Vous devez entrer le nom de domaine complet de votre serveur de messagerie au lieu de la variable <smtpServerName>. Après cela, vous devez indiquer l'adresse de l'événement et le courrier électronique à laquelle la notification est envoyée en exécutant la commande suivante :

```
certutil -setreg exit\smtp\CRLIssued\To<E-mailString>
```



Remarque : le module de sortie sur l'AC qui est configuré pour envoyer des e-mails sur un événement n'utilise pas l'authentification SMTP. Si votre serveur SMTP requiert une authentification, vous devez la configurer du côté de l'AC en tapant la commande suivante :

```
certutil -setreg exit\smtp\SMTPAuthenticate 1
certutil -setsmtpprofile<UserName>
```

Le <Nom d'utilisateur> spécifie le nom d'utilisateur d'un compte valide sur le serveur SMTP. Vous serez invité à fournir le mot de passe pour ce nom d'utilisateur.

Outre l'envoi d'e-mails de notification lorsque l'AC émet un certificat, vous pouvez également configurer un module de sortie pour envoyer des notifications pour les événements suivants :

- Demande de certificat en attente ;
- Demande de certificat refusée ;
- Certificat révoqué ;
- Une liste de révocation des certificats est émise ;
- Démarrage du service AC ;
- Arrêt du service AC.

Si vous souhaitez configurer un module de sortie pour publier des certificats dans le système de fichiers, vous pouvez utiliser la console d'administration AC pour ouvrir les propriétés du module de sortie. Après avoir activé l'option **Autoriser les certificats à être publiés sur le système de fichiers** et redémarrez l'AC, les certificats émis à partir de cette AC sont copiés dans le fichier.cer dans le dossier C:\Windows\System32\CertEnroll sur l'AC. Cependant, pour que cela se produise, les demandeurs de certificats doivent inclure un attribut **certfile:true** dans leur demande.

Si vous déployez des modules de sortie personnalisés, leur configuration pourrait être possible via la console d'administration AC ou avec un autre utilitaire.

Configuration de CDP et d'emplacements AIA

Pour vous assurer qu'un environnement PKI fonctionne correctement, vous devez configurer les extensions de certificat Accès aux informations de l'autorité (AIA) et points de distribution de liste de révocation des certificats (CDP) pour chaque AC. Cela permet d'assurer qu'elle rencontre le moins d'échecs possible lorsque les applications ou les services tentent de valider le statut de la chaîne d'approbation ou de la révocation d'un certificat.

- Les adresses AIA sont des URL qui indiquent à un vérificateur de certificat l'emplacement du certificat d'autorité de certification. Les adresses AIA sont nécessaires pour que les applications et services utilisant un certificat puissent établir à la fois la validité de l'AC et d'une chaîne d'approbation dans une AC auquel le vérificateur fait explicitement confiance (s'il ne fait pas explicitement confiance au CA qui a directement émis le certificat).

- L'AIA spécifie où récupérer le certificat de l'AC
- La CDP spécifie à partir de quel emplacement la CRL d'une AC peut être récupérée
- Emplacements de publication pour AIA et CDP :
 - AD DS (LDAP) ;
 - Serveurs Web (HTTP) ;
 - Serveurs FTP ;
 - Serveur de fichiers.
- Assurez-vous de configurer correctement les emplacements de CRL et d'AIA pour les AC hors connexion et autonomes
- Assurez-vous que la CRL n'expire pas pour une AC racine hors connexion

- Les adresses CDP sont les URL qui indiquent à un vérificateur de certificat l'emplacement de la liste des certificats révoqués (CRL) maintenus par l'AC. Les adresses CDP sont nécessaires pour que les applications et services qui utilisent un certificat puissent établir l'état de révocation d'un certificat.

Chaque certificat que vous émettez à partir de votre AC contient les URL AIA et CDP que vous avez configuré sur l'AC au moment où elle a émis le certificat. Les extensions AIA et CDP doivent contenir chacune au moins une URL accessible ou le vérificateur pourrait supposer que le certificat n'est pas valide, ce qui rend le certificat inutilisable.

 **Remarque :** les URL pour les emplacements AIA et CDP peuvent être HTTP, protocole FTP, Protocole LDAP ou des adresses de fichiers.

Considérations d'édition AIA et CDP

Si vous utilisez une AC d'entreprise, les valeurs d'extension AIA et CDP sont automatiquement configurées de telle sorte que le certificat d'autorité de certification et la liste de révocation des certificats sont disponibles dans la partition de configuration AD DS répliquée sur tous les contrôleurs de domaine dans la forêt AD DS. Toutefois, si vous souhaitez déployer une CA autonome ou hors connexion ou si vous allez utiliser les certificats émis par votre AC en dehors de votre environnement AD DS, il y a d'autres choses que vous devez prendre en considération.

- AC autonomes ou hors connexion. Étant donné que les AC hors connexion et autonomes ne s'intègrent pas dans AD DS, vous devrez vous assurer de l'accessibilité AIA et CDP manuellement en publiant le certificat AC hors connexion ou autonome et la liste de révocation des certificats dans AD DS en utilisant la commande certutil. Ceci fournit les mêmes avantages qu'une AC d'entreprise et rend les URL AIA et CDP accessibles aux clients AD DS dans la forêt, mais vous devez publier manuellement les informations et configurer manuellement les extensions d'AC avec l'URL correcte LDAP.

 **Remarque :** outre la configuration des points de publication CDP et AIA, vous devez également vous assurer que la liste de révocation des certificats est valide. Une AC en ligne renouvelle la liste de révocation des certificats périodiquement, mais une AC hors connexion ne le fera pas. Si la liste de révocation des certificats d'une AC hors connexion expire, les contrôles de révocation échouent. Pour éviter tout échec, assurez-vous que vous configurez une période de validité de la liste de révocation des certificats d'une AC hors connexion assez longue et définissez un rappel pour activer cette AC et émettre une nouvelle liste de révocation des certificats avant que l'ancienne n'arrive à expiration.

- Les clients qui ne sont pas joints au domaine. Les clients internes qui ne sont pas joints au domaine ne seront pas en mesure d'accéder à l'URL AIA ou CDP LDAP, qui font référence à la partition de configuration AD DS. Dans ce cas, vous devez placer le certificat d'autorité de certification et la liste de révocation des certificats sur un serveur Web accessible en interne et configurer une URL HTTP valide pour les extensions AIA et CDP. Vous pouvez également choisir d'utiliser des URL FTP ou FILE, mais nous vous recommandons d'utiliser uniquement HTTP dans ce scénario pour une interopérabilité et une flexibilité maximale.
- Clients externes. Les clients qui sont externes à votre réseau (y compris les clients de domaine sur un réseau externe) ne seront pas non plus en mesure d'accéder à l'URL AIA ou CDP LDAP, qui référence votre environnement AD DS interne. En outre, ils pourraient ne pas être en mesure d'accéder aux URL HTTP internes sans un VPN ou une connexion DirectAccess. Si les clients externes doivent valider les certificats émis par votre AC interne, vous pourriez avoir besoin de prendre les mesures suivantes :
 - Publier les URL HTTP internes à l'extérieur en utilisant le Service proxy d'application Web de Windows Server 2016 du rôle d'accès à distance. Vous pouvez éventuellement utiliser une

solution proxy inverse tiers. Si les URL internes et externes ne correspondent pas, vous devrez configurer une URL supplémentaire HTTP AIA/CDP sur l'AC.

- Les clients externes ne faisant pas partie de votre domaine AD DS auront besoin d'avoir votre certificat d'autorité de certification importé manuellement dans les autorités de certification racines de confiance ou les magasins intermédiaires autorités de certification. Cela peut être nécessaire étant donné que le client externe ne fera autrement pas confiance aux certificats qui ont été émis par votre AC interne.



Remarque : L'ordre dans lequel vous répertoriez les URL CDP et AIA est important parce que le moteur de chaînage des certificats recherche les URL séquentiellement. Si vos certificats sont principalement utilisés en interne dans un environnement AD DS, placez l'URL LDAP en premier sur la liste. Classez les autres URL basées selon la probabilité que l'URL est disponible pour les clients internes ou externes.



Remarque : Si vous déclassez les URL AIA ou CDP présentes sur les certificats émis (en les retirant de l'AC), vous devez vous assurer que tous les certificats contenant une URL déclassée ont expiré, été révoqués ou contiennent une URL supplémentaire qui est toujours valide et accessible.

Démonstration : Configuration des propriétés de l'AC

Étapes de la démonstration

1. Sur **LON-SVR1**, ouvrez la console **Autorité de certification**, puis ouvrez les **Propriétés** de **AdatumRootCA**
2. Affichez le certificat **Autorité de certification**
3. Vérifiez les paramètres du module de stratégie actif
4. Vérifiez les paramètres du module de sortie
5. Passez en revue les valeurs fournies sur l'onglet **Extension**
6. Vérifiez les paramètres **Sécurité** de l'AC
7. Vérifiez les paramètres **Gestionnaires de certificats**

Testez vos connaissances

| Question | |
|---|--|
| Lesquelles des options suivantes sont des affirmations exactes concernant l'administration basée sur les rôles de votre déploiement AD CS ? | |
| Sélectionnez la réponse correcte. | |
| | AD CS crée automatiquement trois rôles intégrés et groupes pour l'administrateur AC, le gestionnaire de certificats et la personne inscrite. |
| | Vous pouvez accorder aux groupes de rôle AD CS l'une ou plusieurs des AC suivantes : Gérer AC, émettre et gérer des certificats, lire, demander des certificats. |
| | Vous pouvez limiter l'autorisation d'émission et de gestion des certificats AC à un modèle spécifique ou à un ensemble de modèles. |
| | Vous pouvez créer des groupes de rôles AD CS sur la base des besoins spécifiques de votre organisation. |
| | Le directeur de la sécurité des utilisateurs authentifiés peut s'inscrire pour n'importe quel certificat publié sur une AC. |

Testez vos connaissances

| Question | |
|--|---|
| Lesquelles des affirmations suivantes sont correctes par rapport à l'extension AIA et CDP d'une AC ? | |
| Sélectionnez la réponse correcte. | |
| | Chaque extension nécessite un minimum de deux URL valides et accessibles pour que la validation du certificat fonctionne correctement. |
| | Vous pouvez publier manuellement des certificats AC hors connexion et autonomes et des listes de révocation des certificats dans un environnement AD DS. |
| | L'ordre dans lequel vous spécifiez les URL AIA et CDP n'est pas important étant donné que le moteur de chaînage de certificat classe automatiquement les emplacements en fonction de la connexion la plus rapide. |
| | Afin de faciliter la validation du certificat pour les clients externes, vous devez publier des URL AIA et CDP externes en utilisant HTTP au moyen d'un Service proxy d'application Windows Server 2016. |
| | Si vous utilisez une AC d'entreprise, la validation du certificat interne fonctionnera sans aucune configuration supplémentaire. |

Leçon 3

Dépannage et maintien des AC

La résolution des problèmes et le maintien des hiérarchies d'AC est une partie très importante d'un déploiement PKI interne. Vous devez utiliser les techniques, outils et méthodes disponibles pour assurer la maintenance et résoudre les problèmes de l'ensemble de votre PKI de façon efficace et proactive. AD CS fournit plusieurs outils que vous pouvez utiliser pour assurer la maintenance et résoudre les problèmes d'une hiérarchie d'AC. Dans cette leçon, vous apprendrez à résoudre les problèmes et à assurer la maintenance des AC.

Objectifs de la leçon

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

- Expliquer comment résoudre les problèmes des AC ;
- Expliquer comment renouveler un certificat d'autorité de certification ;
- Décrire comment déplacer une AC racine vers un autre ordinateur ;
- Décrire comment surveiller les opérations d'AC ;
- Décrire comment sauvegarder et récupérer une AC.

Résolution des problèmes des AC

Résoudre les problèmes dans AD CS commence avec les outils intégrés qui donnent aux administrateurs une vue détaillée des conditions actuelles des services de rôle AD CS.

La liste suivante décrit quelques outils que vous pouvez utiliser :

- Composant logiciel enfichable Certificats. Utilisez ce composant logiciel enfichable pour afficher et gérer les magasins de certificats pour un ordinateur, un utilisateur ou un service.
- Outil PKIView. Utilisez cet outil pour surveiller plusieurs AC, listes de révocation des certificats et emplacements AIA et pour gérer les objets AD CS qu'il publie dans AD DS.
- Composant logiciel enfichable AC. Utilisez ce composant logiciel enfichable pour administrer une AC et pour révoquer et inscrire un certificat. Le composant logiciel enfichable AC vous permet également de gérer les modèles de certificats disponibles sur un AC.
- Certutil.exe. Utilisez cet outil de ligne de commande pour afficher les informations de configuration CA, configurer AD CS, sauvegarder et restaurer des composants d'AC et vérifier les certificats, les paires de clés et les chaînes de certificats.
- Composant logiciel enfichable modèles de certificats. Utilisez ce composant logiciel enfichable pour analyser et gérer les modèles de certificats dans AD DS et pour configurer leurs autorisations.

- Outils pour la gestion des AC :
 - Composant logiciel enfichable Certificats ;
 - Outil PKIView ;
 - AC enfichable ;
 - Certutil.exe ;
 - Composant logiciel enfichable Modèles de certificats.
- Problèmes courants avec AD CS :
 - Problèmes d'inscription automatique des clients ;
 - Option d'AC d'entreprise indisponible ;
 - Erreur d'accès aux pages Web d'AC ;
 - Restriction de l'agent d'inscription.

- Windows PowerShell Vous pouvez utiliser les modules ADCSDeployment, ADCSAdministration et PKI dans Windows PowerShell en remplacement ou en complément des outils énumérés ci-dessus. En tirant parti de la fonctionnalité dans les modules Windows PowerShell disponibles, vous pouvez écrire des scripts pour tester automatiquement ou vérifier votre configuration AD CS.
- La console de gestion stratégie de groupe et les outils gpresult.exe peuvent vous aider à vérifier la bonne application des objets de stratégie de groupe (GPO), qui configurent l'inscription automatique ou d'autres paramètres liés à PKI.

Problèmes courants AD CS

La liste suivante décrit des problèmes courants AD CS que vous pourriez rencontrer :

- Les utilisateurs ou les ordinateurs ne s'inscrivent pas automatiquement pour les certificats comme prévu.
 - Parce que vous activez l'inscription automatique via la stratégie de groupe, vous devez vérifier que les GPO qui permettent l'inscription automatique pour l'utilisateur et l'ordinateur appliquent l'inscription automatique correctement et que l'utilisateur ou l'ordinateur n'est pas dans une unité d'organisation (UO) où l'héritage de la stratégie a été bloqué ou annulé par un autre GPO. Tant l'utilisateur et l'ordinateur doivent être activés séparément, bien que les deux paramètres puissent résider dans le même GPO.
 - Vous devez vérifier que AD CS publie le modèle de certificat à une AC d'entreprise, qui peut être consultée par l'ordinateur ou l'utilisateur.
 - Vous devez vérifier que l'ordinateur ou l'utilisateur disposent d'une autorisation **Demandeur des certificats** sur l'AC et d'une autorisation **Inscription automatique** sur le modèle de certificat en question.
 - Vous devez vérifier que le modèle de certificat demandé ne nécessite pas d'informations qui ne peuvent être fournies automatiquement par AD DS.
- Impossible de configurer les autorisations d'inscription automatique sur un modèle. Pour configurer l'inscription automatique auprès d'un certificat, le modèle doit être en version 2 ou plus récente. Les modèles de version 2 ne peuvent être ajoutés qu'à une AC exécutant Windows Server 2008 Enterprise ou version ultérieure.
- Option AC d'entreprise non disponible. Ce problème se produit lorsqu'un utilisateur qui n'est pas membre du groupe Administrateurs de l'entreprise ou Administrateurs du domaine installe une AC ; en tant que tel, l'AC pourrait ne pas être installée comme une AC d'entreprise. Dans ce cas, l'option AC d'entreprise est indisponible et des informations sur l'AC ne peuvent pas automatiquement être publiées sur l'AD DS.
- Erreur lors de l'accès aux pages d'inscription Webde l'AC. Cette erreur se produit lors de l'accès aux pages Web de l'AC. Dans ce cas, vous devez vous assurer que l'utilisateur est un membre du groupe Administrateurs ou Utilisateurs avec pouvoir sur l'ordinateur client.
- Restriction de l'agent d'inscription. Cette restriction se produit lorsqu'un agent d'inscription ne peut pas s'inscrire au nom d'un utilisateur pour un modèle de certificat précis. Cela peut se produire en raison des restrictions configurées sur l'agent d'inscription ou du manque d'autorisations d'inscription sur le modèle de certificat.

Résolution des problèmes de validation

Tous les certificats ont une durée de validité. Après l'expiration de la période de validité, le certificat n'est plus une information d'identification acceptable. Les ordinateurs clients peuvent ne pas être en mesure de se connecter à des ressources qui exigent des certificats si des problèmes de validation de certificat se produisent. Les services AD CS peuvent s'arrêter ou ne pas parvenir à s'exécuter, s'il y a des problèmes de disponibilité, de validité et de validation de la chaîne pour le certificat d'autorité de certification. Vous pouvez utiliser l'utilitaire PKIView pour vérifier que les emplacements et les certificats des AIA et des listes

de révocation des certificats CDP sont valides. En outre, vous pouvez utiliser le composant logiciel enfichable AC pour installer de nouveaux certificats.

Renouvellement d'un certificat de l'AC

Une AC a également son propre certificat. Une AC racine émet un certificat pour elle-même, un certificat autosigné, alors que les AC secondaires obtiennent leurs certificats d'une AC racine.

Chaque certificat d'autorité de certification a une période de validité. Habituellement, lors du déploiement d'une AC racine, les administrateurs choisissent de définir la période de validité du certificat de l'AC racine à cinq ans ou plus. Vous devez renouveler un certificat d'autorité de certification lorsque la période de validité s'approche de la date d'expiration. Une AC avec un certificat expiré ne peut pas fonctionner, par conséquent, vous ne devriez pas laisser le certificat d'autorité de certification expirer.

- Le certificat d'AC doit être renouvelé lorsque la période de validité du certificat d'AC est proche de sa date d'expiration
- L'AC ne délivre jamais un certificat qui a une période de validité plus longue que son propre certificat
- Considérations pour le renouvellement d'un certificat d'AC racine :
 - Longueur de la clé ;
 - Période de validité.
- Considérations pour le renouvellement d'un certificat pour une CA émettrice :
 - Nouvelle paire de clés ;
 - CRL plus petits.
- Procédure pour le renouvellement d'un certificat d'AC

La période de validité du certificat d'autorité de certification est également importante pour les certificats que l'AC émet. Une AC n'émet jamais un certificat qui a un temps de validité plus long que celui de son propre certificat. Ceci est utile si vous choisissez de ne pas renouveler l'AC dans le cas où vous voulez la déclasser. Par exemple, lorsque le certificat d'autorité de certification atteint la fin de sa durée de vie, tous les certificats que l'AC maintenant expirée a émis ne peuvent plus être utilisés comme des informations d'identification de sécurité valides.

Cela peut aussi avoir des effets secondaires. Lorsque la durée de vie du certificat d'autorité de certification se rapproche de l'expiration, l'AC va commencer à réduire la durée de vie des certificats qu'elle émet. Par exemple, supposons que votre AC émettrice dispose d'un certificat avec cinq ans de temps de validité et émet des certificats avec une durée de vie de deux ans. Pour les trois premières années de sa durée de vie, il n'y aura aucun problème. Cependant, au bout de trois ans, cette AC émettra des certificats avec une période de validité de moins de deux ans.

Renouvellement des certificats d'AC racine

Une AC racine a généralement un certificat avec une longue période de validité. Contrairement à une AC secondaire, qui par défaut peut avoir une durée de validité de cinq ans maximum, vous pouvez définir un temps de validité beaucoup plus long pour un certificat d'autorité de certification racine lors de l'installation. Vous devez aussi sélectionner une longueur de clé plus élevée pour la paire de clé privée et publique de l'AC racine. Si vous utilisez une longue longueur de clé, ce qui rend la clé plus sûre contre les attaques par force brute, vous augmentez la durée pendant laquelle l'AC peut utiliser la même clé privée. En règle générale, créez une AC racine avec une durée de validité plus courte que la durée de vie estimée de la clé.

Avec cela à l'esprit, une stratégie raisonnable est de créer une clé RSA de 4.096 bits pendant une installation d'AC racine, ce qui réduit la nécessité d'un renouvellement fréquent. Compte tenu de l'état actuel de la technologie informatique, une clé privée de 4.096 bits est protégée contre les attaques par force brute pour environ 15-20 ans. Si vous choisissez une clé de 4.096 bits lors de la configuration de l'AC racine, vous pouvez alors créer un certificat racine en utilisant la clé 4.096 bits qui est valable pour cinq ans. Par la suite, vous devez renouveler le certificat de l'AC tous les quatre ans, un an avant l'expiration de la période de validité, chaque fois avec un certificat de validité de cinq ans. Chaque fois que vous renouvelez le certificat d'autorité de certification, nous vous recommandons d'évaluer si la même clé, compte tenu de la technologie informatique alors actuelle et d'autres considérations de sécurité, peut être utilisée en confiance pour les cinq prochaines années.

Renouvellement des certificats d'AC secondaires

Pour une AC secondaire qui émet des certificats pour des utilisateurs finaux et des périphériques, la stratégie recommandée serait de renouveler le certificat d'autorité de certification régulièrement avec une nouvelle clé 6 à 12 mois avant la fin de la période de validité de l'AC. Cela rend une attaque sur une des clés moins intéressante car toute clé compromise aurait une durée de vie relativement limitée.

La gestion de la liste de révocation des certificats est un autre avantage de renouveler une AC secondaire à l'aide d'une nouvelle clé. Lorsque vous renouvelez une AC avec une nouvelle clé, elle commence à publier une liste de révocation distincte pour les certificats révoqués qu'elle a émis. L'AC continue de publier la liste de révocation des certificats signés avec l'ancienne clé aussi longtemps que la période de validité de ces certificats est valide. Toutefois, cela peut réduire la taille d'une seule liste de révocation de certificats grandement et cela permettra de réduire la taille de la liste de révocation de certificats que le vérificateur de certificat doit télécharger lorsque lui est présenté un certificat d'une autorité de certification émettrice.

Vous pouvez compléter la procédure de renouvellement de certificat d'autorité de certification depuis la console d'administration AC. Vous devez arrêter un service d'AC avant de commencer la procédure de renouvellement. Lorsque vous commencez le renouvellement d'une procédure de certificat d'autorité de certification depuis la console d'administration AC, vous devez choisir si vous voulez générer un nouveau jeu de clés ou réutiliser le jeu existant. La procédure de renouvellement commence après avoir choisi quelle clé utiliser. Si vous choisissez l'AC racine, elle va renouveler son certificat après la procédure de renouvellement. Pour des AC secondaires, vous devez présenter une demande de renouvellement à l'Autorité de certification parente, de la même façon que quand vous avez émis le premier certificat.

Déplacement d'une AC racine à un autre ordinateur

Comme indiqué dans la rubrique précédente, les AC sont conçues et configurées pour fonctionner pendant de nombreuses années, au cours desquels vous pourriez avoir envie de mettre à niveau le système d'exploitation et le matériel qui prend en charge les AC. Ces scénarios exigent habituellement que vous déplacez une AC d'un ordinateur à un autre.

Une AC n'est pas comme d'autres services que vous pouvez simplement installer sur un nouvel ordinateur avant de continuer à travailler. Lorsque vous déplacez une AC d'un ordinateur à un autre, il est très important que vous gardiez l'identité de l'AC au cours de ce processus afin qu'elle puisse continuer à travailler sur le nouveau matériel ou système d'exploitation avec la même identité.

D'une manière générale, la procédure de déplacement d'une autorité de certification peut être divisée en deux phases :

- Sauvegarde d'une AC ;
- Restauration d'une AC.

- Pour déplacer une CA d'un ordinateur à un autre, vous devez faire une sauvegarde et une restauration :
- Pour restaurer un ordinateur, suivez cette procédure :
 - Notez les noms des modèles de certificats ;
 - Sauvegardez une AC dans la console d'administration AC ;
 - Exportez la sous-clé de registre ;
 - Désinstallez le rôle de l'AC ;
 - Confirmez les emplacements du dossier %SystemRoot% ;
 - Retirez l'ancienne AC du domaine.
- Pour restaurer, suivez cette procédure :
 - Installez AD CS ;
 - Utilisez la clé privée existante ;
 - Restaurez le fichier de registre ;
 - Restaurez la base de données et les paramètres de l'AC ;
 - Restaurez les modèles de certificats.

Exécution d'une sauvegarde d'une AC avant un déplacement

Vous devriez avoir une sauvegarde AC même si vous ne déplacez pas l'AC vers un autre ordinateur. Une sauvegarde AC est différente des scénarios de sauvegarde ordinaires. Pour effectuer une sauvegarde d'une AC avant de déplacer une AC sur un autre ordinateur, vous devez effectuer la procédure suivante :

1. Si vous sauvegardez une AC d'entreprise, cliquez sur l'élément **Modèles de certificats** dans la console d'AC, puis enregistrez les noms des modèles de certificats répertoriés. Ces modèles sont dans AD DS, de sorte que vous n'avez pas à les sauvegarder. Vous devez noter les modèles que vous avez publiés sur l'AC que vous déplacez étant donné que vous devrez les ajouter manuellement après avoir déplacé l'AC.
2. Dans le composant logiciel enfichable AC, faites un clic droit sur **nom d'AC**, cliquez sur **Toutes les tâches**, puis sur **sauvegarde d'AC** pour démarrer l'Assistant Sauvegarde d'autorité de certification. Dans l'assistant de sauvegarde, vous devez sélectionner l'option pour effectuer la sauvegarde de l'AC une clé privée, un certificat d'autorité de certification, une base de données de certificat et le journal de la base de données de certificats. Vous devez également fournir un emplacement approprié pour le contenu de la sauvegarde. Vous devez protéger une clé privée d'AC avec un mot de passe pour des raisons de sécurité.
3. Une fois la sauvegarde terminée, ouvrez l'Éditeur du Registre.
4. Recherchez et exportez la sous-clé de Registre suivante, située dans :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration.

 **Remarque :** nous vous recommandons de sauvegarder cette clé de Registre dans un fichier au sein du même dossier que la sauvegarde de l'AC de l'étape précédente.

5. Désinstallez l'AC de l'ancien serveur, puis renommez l'ancien serveur ou déconnectez-le de façon permanente du réseau.

Avant de commencer la procédure de restauration, confirmez que le dossier *%SystemRoot%* du serveur cible correspond au dossier *%SystemRoot%* sur le serveur à partir duquel vous avez pris la sauvegarde. En outre, l'emplacement de la restauration d'une AC doit correspondre à l'emplacement de la sauvegarde de l'AC. Par exemple, si vous sauvegardez l'AC dans le dossier *D:\WINNT\System32\Certlog*, vous devez restaurer la sauvegarde dans le dossier *D:\WINNT\System32\Certlog*. Après avoir restauré la sauvegarde, vous pouvez déplacer les fichiers de la base de données AC vers un autre emplacement.

Exécution d'une restauration d'AC sur un nouvel ordinateur

Après avoir complété avec succès la procédure de sauvegarde, vous devez restaurer l'AC sur un autre ordinateur. La nouvelle AC doit avoir le même nom que l'ancienne AC. Pour restaurer l'AC, procédez comme suit :

1. Installez AD CS sur l'ordinateur cible. Choisissez d'installer soit **Autonome** ou **Entreprise**, selon le type d'AC que vous déplacez. Lorsque vous arrivez sur la page **Configurer la clé privée**, cliquez sur **Utilisez la clé privée existante**. Choisissez ensuite de sélectionner un certificat et d'utiliser sa clé privée associée. Cela vous donne la possibilité d'utiliser un certificat existant d'une ancienne AC.
2. Sur la page **Sélectionnez le certificat existant**, cliquez sur **Importer**, entrez le chemin du fichier.p12 dans le dossier de sauvegarde, entrez le mot de passe que vous avez choisi dans la procédure précédente pour protéger le fichier de sauvegarde, puis cliquez sur **OK**. Lorsque vous êtes invité dans **Paire de clés publiques et privées**, vérifiez que l'option **Utilisez les clés existantes** est sélectionnée. Ceci est très important, car il faut garder le même certificat d'autorité de certification racine.

3. Lorsque vous y êtes invité sur la page **Base de données de certificat**, spécifiez le même emplacement pour la base de données de certificat et le journal de base de données de certificat comme sur l'ordinateur AC précédent. Après avoir sélectionné toutes ces options, attendez que la configuration d'AC se termine.
4. Une fois l'installation terminée, ouvrez le composant logiciel enfichable du Service pour arrêter le service AD CS. Vous faites cela pour restaurer les paramètres de l'ancienne AC.
5. Localisez le fichier de Registre que vous avez enregistré durant la procédure de sauvegarde, puis double-cliquez dessus pour importer les paramètres de Registre.
6. Après avoir restauré les paramètres du registre, ouvrez la console de gestion d'AC, cliquez avec le bouton droit sur **Nom d'AC**, cliquez sur **Toutes les tâches** puis sur **Restaurer l'AC**. Cela lance l'Assistant Restauration d'autorité de certification. Dans l'Assistant, cochez les cases **Clé privée et certificat d'Autorité de certification** et **Base de données de certificat et journal de base de données de certificat**. Ceci indique que vous souhaitez restaurer ces objets à partir de sauvegarde. Ensuite, fournissez un emplacement de dossier de sauvegarde et vérifiez les paramètres de la restauration. Les paramètres **Journal des émissions** et **demandes en attente** doivent être affichés.
7. Lorsque le processus de restauration est terminé, choisissez de redémarrer le service AD CS.
8. Si vous avez restauré une AC d'entreprise, restaurez les modèles de certificats d'AD DS que vous avez enregistrés dans la procédure précédente.

Suivi des opérations de l'AC

Étant donné que l'AC est un service essentiel pour chaque PKI activée, il est très important d'établir des techniques pour surveiller et assurer la maintenance de chaque objet d'AC, en plus des certificats, listes de révocation des certificats et d'autres objets liés à la PKI. Lorsque vous installez AD CS et le rôle AC, vous pouvez utiliser certains des outils de gestion, de suivi et d'audit.

Console PKIView

Windows Server 2016 inclut la console PKIView, qui est un outil de gestion, lorsque vous installez le rôle AD CS. Elle fournit une vue synthétique de l'état de la PKI d'entreprise. La console PKIView vous permet également d'afficher plusieurs AC et leur état d'intégrité actuel, mais vous ne pouvez pas voir les AC autonomes. Vous pouvez utiliser PKIView pour accéder à des conteneurs AD DS liés à PKI et pour gérer leur contenu, y compris les modèles de certificats. Vous pouvez démarrer la console PKIView lorsque vous entrez **pkiview.msc** à l'invite de commande ou dans Windows PowerShell.

PKIView affiche tous les AC et leur état d'intégrité au moyen d'une petite icône. Voici les états d'intégrité disponibles :

- Evaluation de l'état d'intégrité de l'AC (point d'interrogation) ;
- l'AC n'a pas de problèmes (indicateur vert) ;
- l'AC a un problème non critique (indicateur jaune) ;
- l'AC a un problème critique (indicateur rouge) ;
- l'AC est déconnectée (croix rouge sur l'indicateur AC).

- Pour la surveillance et la maintenance d'une hiérarchie d'AC, vous pouvez utiliser PKIView et CA auditing
- Avec PKIView, vous pouvez :
 - Accéder et gérer les conteneurs liés à la PKI d'AD DS ;
 - Surveiller les AC et leur état d'intégrité ;
 - Vérifier l'état des certificats d'AC ;
 - Vérifier l'état des emplacements de l'AIA ;
 - Vérifier l'état des CRL ;
 - Vérifier l'état des CDP ;
 - Évaluer l'état du répondeur en ligne.
- CA audit fournit la journalisation pour divers événements qui se produisent sur l'AC

PKIView affiche également un rapide résumé de l'intégrité des domaines suivants en indiquant que leurs options de statut sont OK ou Impossible de télécharger :

- Certificats AC ;
- Emplacements AIA ;
- Listes de révocation des certificats et listes de révocation des certificats delta ;
- CDP ;
- Emplacements OCSP.

PKIView évalue le statut AIA ou CDP pour chaque emplacement défini sur chaque AC. Par exemple, vous pouvez facilement voir si un emplacement CDP ou AIA n'est pas accessible ou si un de ces emplacements contient une liste de révocation des certificats qui a expiré. PKIView est également en mesure d'évaluer l'état du répondeur en ligne, si vous avez déployé ce service de rôle.

Audit d'évènements AC

Outre le suivi et l'examen de l'ensemble de la hiérarchie d'AC avec la console de PKIView, vous pouvez également utiliser les options d'audit au niveau de l'AC dans la console Autorité de certification pour surveiller les évènements qui se produisent sur chaque AC. Pour accéder aux options d'audit, vous devez ouvrir la fenêtre **Propriétés d'AC** et aller à l'onglet **Audit**. Vous pouvez configurer cet onglet pour surveiller les évènements suivants :

- Sauvegarde et restauration de la base de données ;
- Changement de la configuration de l'AC ;
- Changement des paramètres de sécurité de l'AC ;
- Gestion des demandes de certificats ;
- Révocation des certificats et publication des listes de révocation des certificats ;
- Stockage et récupération des clés archivées ;
- Démarrage et arrêt du service l'AD CS.

La console Autorité de certification ne configure aucune de ces options par défaut, ce qui signifie qu'elle ne permet pas automatiquement l'audit sur AC. Si vous voulez commencer l'enregistrement des évènements de l'AC, vous devez activer manuellement une ou plusieurs de ces options.

Testez vos connaissances

| Question | |
|---|---|
| Laquelle des questions suivantes pourrait empêcher l'inscription automatique de fonctionner correctement dans AD CS ? | |
| Sélectionnez la réponse correcte. | |
| | L'ordinateur que vous êtes supposé inscrire automatiquement pour un certificat est dans une UO AD DS où la succession de la stratégie est bloquée. |
| | L'utilisateur que vous êtes supposé inscrire automatiquement pour un certificat est dans une UO AD DS où les paramètres de stratégie de groupe nécessaires ne sont pas liés ou hérités. |
| | L'AC est une AC autonome. |

| Question | |
|----------|--|
| | Le modèle de certificat n'est pas publié sur une AC. |
| | L'URL AIA n'est pas configurée correctement sur l'onglet des extensions de l'AC. |

Testez vos connaissances

| Question | |
|---|--|
| Lesquelles des affirmations suivantes sont exactes au sujet de l'outil PKIView ? | |
| Sélectionnez la réponse correcte. | |
| | PKIView affiche tous vos AC d'entreprise et leur état d'intégrité actuel. |
| | Vous pouvez utiliser PKIView pour ajouter manuellement des AC autonomes. |
| | Vous pouvez utiliser PKIView pour configurer l'inscription automatique pour les utilisateurs et les ordinateurs. |
| | PKIView évalue le statut AIA ou CDP pour chaque emplacement défini sur chaque AC. |
| | PKIView peut évaluer l'état du service de rôle AD CS répondeur en ligne. |

Atelier pratique : Déploiement et configuration d'une hiérarchie AC à deux niveaux

Scénario

A. Datum Corporation est en croissance et donc ses exigences de sécurité augmentent aussi. Le service de sécurité souhaite vraiment permettre un accès sécurisé aux sites essentiels et fournir une sécurité supplémentaire pour les fonctionnalités. Pour répondre à ces questions et à d'autres exigences en matière de sécurité, A. Datum a décidé de mettre en œuvre une PKI en utilisant le rôle AD CS dans Windows Server 2016. En tant qu'administrateur réseau principal chez A. Datum, vous êtes responsable de la mise en œuvre du déploiement AD CS.

Objectifs

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

- Déployer une AC racine hors ligne ;
- Déployer une AC secondaire d'entreprise.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels. **22742A-LON-DC1**, **22742A-LON-DC2**, **22742A-LON-SVR1**, **22742A-CA-SVR1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-LON-DC1**, et dans le volet **Actions**, cliquez sur **Démarrer**.
3. Dans le volet d'**Actions**, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
 - o Nom d'utilisateur : **Adatum\Administrateur**
 - o Mot de passe : **Pa55w.rd**
5. Répétez les étapes 2 à 4 pour **22742A-LON-DC2** et **22742A-LON-SVR1**.
6. Répétez les étapes 2 et 3 pour **22742A-CA-SVR1**. Ne vous connectez pas à **22742A-CA-SVR1** tant qu'il ne vous a pas été demandé de le faire.

Exercice 1 : Déploiement d'une AC racine hors ligne

Scénario

A. Datum veut utiliser des certificats à des fins diverses. Vous devez installer l'infrastructure de l'AC appropriée. Vous avez décidé de mettre en œuvre le rôle AD CS car A. Datum utilise Windows Server 2016 AD DS. Lorsque vous avez examiné les modèles disponibles, vous avez décidé de mettre en œuvre une AC racine autonome. Cette AC sera mise hors ligne après avoir délivrer un certificat pour une autorité de certification secondaire. Après l'installation, vous devez vous assurer que vous avez configuré correctement le CDP et les emplacements AIA. Vous devez également vous assurer que vous avez un enregistrement du Système de nom de domaine (DNS) pour l'AC racine hors ligne afin d'être accessible depuis le réseau.

Les tâches principales de cet exercice sont les suivantes :

1. Créer des exceptions au partage de fichiers et d'imprimantes ;
2. Installer et configurer AD CS sur CA-SVR1 ;
3. Créer un enregistrement DNS (Domain Name System) pour une AC racine hors connexion.

► Tâche 1 : Créer des exceptions au partage de fichiers et d'imprimantes

1. Connectez-vous à **CA-SVR1** en tant qu'**Administrateur** avec le mot de passe **Pa55w.rd**.
2. Sur **CA-SVR1**, depuis le Centre Réseau et partage, activez le partage de fichiers et d'imprimantes sur les réseaux clients et publics.
3. Sur **LON-SVR1**, depuis le Centre Réseau et partage, activez le partage de fichiers et d'imprimante sur le réseau client/public.

► Tâche 2 : Installer et configurer AD CS sur CA-SVR1

1. Basculez vers **CA-SVR1** puis démarrez le **Gestionnaire de serveur**.
2. Utilisez l'**Assistant Ajout de rôles et de fonctionnalités** pour installer le rôle **services de certificats Active Directory**.
3. Une fois l'installation terminée, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination**.
4. Configurez le rôle AD CS en tant qu'AC racine autonome avec le nom **AdatumROOTCA**.
5. Réglez la longueur de clé sur **4.096**, puis acceptez toutes les autres valeurs par défaut.
6. Dans **CA-SVR1**, ouvrez la console **Autorité de certification**.
7. Ouvrez la boîte de dialogue **Propriétés d'AdatumROOTCA**.
8. Configurez les nouveaux emplacements pour la CDP comme **http://lon-svr1.adatum.com/CertData/<NomAutoritéCertification><SuffixeNomListeRévocationCertificats><ListeRévocationCertificatsDeltaAutorisée>.crl**
9. Sélectionnez les options suivantes :
 - **Inclure dans le CDP l'extension de certificats émis**
 - **Inclure dans les CRL. Les clients utilisent ceci pour trouver des emplacements Delta CRL**
10. Configurez de nouveaux emplacements pour qu'AIA se trouve sur **http://lon-svr1.adatum.com/CertData/<Nom du serveur DNS>_<NomAutoritéCertification><NomCertificat>.crt**
11. Cochez la case **Inclure des extensions de certificats émis dans AIA**.
12. Publier la liste de révocation sur **CA-SVR1**.
13. Exportez le certificat d'autorité de certification racine puis copiez le fichier.cer dans **\\\Lon-SVR1\C\$**.

14. Copiez le contenu du dossier **C:\Windows\System32\CertSrv\CertEnroll** dans **\\\Lon-SVR1\C\$**.

► **Tâche 3 : Créer un enregistrement DNS (Domain Name System) pour une AC racine hors ligne**

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, ouvrez la console de gestion DNS.
2. Créez un enregistrement d'hôte pour **CA-SVR1** dans la zone de recherche directe **Adatum.com**.
3. Utilisez l'adresse IP **172.16.0.40** pour l'enregistrement d'hôte **CA-SVR1**.

Résultats : à la fin de cet exercice, vous devez avoir installé et configuré avec succès le rôle de l'AC racine autonome sur le serveur **CA-SVR1**. En outre, vous devez avoir créé un enregistrement DNS approprié dans Active Directory Domain Services (AD DS) pour que d'autres serveurs puissent se connecter à **CA-SVR1**.

Exercice 2 : Déploiement d'une AC secondaire d'entreprise

Scénario

Après avoir déployé l'AC racine autonome, l'étape suivante consiste à déployer une AC d'entreprise secondaire. A. Datum veut utiliser une AC d'entreprise secondaire pour utiliser l'intégration AD DS. En outre, étant donné que la CA racine est une CA autonome, vous souhaitez publier son certificat à tous les clients.

Les tâches principales de cet exercice sont les suivantes :

1. Installer et configurer AD CS sur LON-SVR1 ;
2. Installer un certificat d'autorité de certification secondaire ;
3. Publier un certificat d'autorité de certification racine par la stratégie de groupe ;
4. Préparez le module suivant.

► **Tâche 1 : Installer et configurer AD CS sur LON-SVR1**

1. Sur **LON-SVR1**, dans le **Gestionnaire de serveur**, installez le rôle **services de certificats Active Directory**. Incluez les services de rôle **Autorité de certification** et **Inscription de l'autorité de certification via le Web**.
2. Une fois l'installation complétée avec succès, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination**.
3. Sélectionnez les services de rôle **Autorité de certification** et **Inscription de l'autorité de certification via le Web**.
4. Configurez **LON-SVR1** pour être une **AC d'entreprise**.
5. Configurez le type d'AC pour être une **AC secondaire**.
6. Comme Nom d'AC, entrez **Adatum-IssuingCA**.
7. Enregistrez le fichier de demande sur le disque local.

► **Tâche 2 : Installer un certificat d'autorité de certification subordonné**

1. Sur **LON-SVR1**, installez le certificat **C:\RootCA.cer** dans le magasin de l'autorité de certification racine de confiance.
2. Allez dans le **Disque local (C:)** puis copiez les fichiers **AdatumROOTCA.crl** et **CA-SVR1_AdatumROOTCA.crt** dans **C:\inetpub\wwwroot\CertData**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

3. Copiez le fichier de demande **LON-SVR1.Adatum.com_Adatum-LON-SVR1-CA.req** dans **\\\CA-SVR1\C\$**.
4. Basculez vers **CA-SVR1**.
5. Dans la console **Autorité de certification** sur **CA-SVR1**, soumettez une nouvelle demande de certificat en utilisant le fichier.req que vous avez copié à l'étape 3.
6. Émettez le certificat, puis exportez-le en format.p7b avec une chaîne complète. Enregistrez le fichier dans **\\\lon-svr1\apps\SubCA.p7b**.
7. Basculez vers **LON-SVR1**.
8. Installez le certificat d'autorité de certification secondaire sur **LON-SVR1** en utilisant la console **Autorité de certification**.
9. Démarrez le service. Assurez-vous que le service AD CS démarre correctement.
10. Basculez vers **CA-SVR1** puis fermez le serveur.

► **Tâche 3 : Publier un certificat AC racine via la stratégie de groupe**

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, ouvrez la **console de Gestion des stratégies de groupe**.
2. Modifiez la Stratégie de domaine par défaut.
3. Publiez le fichier **RootCA.cer** depuis **\\\Lon-SVR1\C\$** vers le magasin Autorités de certification racine de confiance situé dans **Ordinateur Configuration\Stratégies\Windows \Paramètres\Sécurité Paramètres \Clé publique Stratégies**.

Résultats : À la fin de cet exercice, vous devriez avoir déployé et configuré avec succès une autorité de confiance d'entreprise. Vous devez également avoir un certificat d'autorité de certification subordonné émis par une AC racine installée sur **LON-SVR1**. Pour établir la confiance entre l'AC racine et les clients joints à un domaine, vous allez utiliser la stratégie de groupe pour déployer un certificat AC racine.

► **Tâche 4 : Préparer le module suivant**

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-SVR1**, **22742A-LON-DC2** et **22742A-CA-SVR1**.

Question : Pourquoi n'est-il pas recommandé d'installer seulement une AC racine d'entreprise ?

Question : Quelles sont les raisons pour lesquelles une organisation utiliserait une AC racine d'entreprise ?

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quelles sont les raisons pour lesquelles une organisation utiliserait une PKI ?

Question : Pourquoi voudriez-vous déployer une stratégie personnalisée et des modules de sortie ?

Méthode conseillée

- Lors du déploiement d'une infrastructure d'AC, déployez une CA racine autonome (non reliée au domaine) et une AC d'entreprise secondaire (AC émettrice). Une fois que l'AC d'entreprise secondaire a reçu un certificat de l'AC racine, mettez l'AC racine hors ligne.
- Passez en revue le temps de validation des listes de révocation de certificats (CRL) de l'AC racine.
- Fournir plus d'un emplacement pour AIA et CRL.

Problèmes courants et conseils de résolution des problèmes

| Problème courant | Conseil pour la résolution du problème |
|---|--|
| L'emplacement du certificat de l'AC qui est spécifié dans l'extension AIA n'est pas configuré pour inclure le suffixe du nom de certificat. Les clients pourraient ne pas être en mesure de localiser la version correcte du certificat de l'AC émettrice pour construire une chaîne de certificats, et la validation du certificat pourrait échouer. | |
| L'AC est pas configurée pour inclure des emplacements CDP dans les extensions de certificats délivrés. Les clients pourraient ne pas être en mesure de localiser une CRL pour vérifier l'état de révocation d'un certificat, et la validation du certificat pourrait échouer. | |

Outils

- Console d'administration de l'autorité de confiance
- Utilité de ligne de commande Certutil
- Interface de ligne de commande Windows PowerShell
- Pkiview.msc
- Gestionnaire de serveur

Module 9

Déploiement et gestion de certificats

Sommaire :

| | |
|---|------|
| Vue d'ensemble du module | 9-1 |
| Leçon 1 : Déploiement et gestion de modèles de certificats | 9-2 |
| Leçon 2 : Gestion du déploiement, de la révocation et de la récupération de certificats | 9-9 |
| Leçon 3 : Utilisation de certificats dans un contexte commercial | 9-20 |
| Leçon 4 : Mise en œuvre et gestion des cartes à puce | 9-29 |
| Atelier pratique : Déploiement et utilisation de certificats | 9-36 |
| Révision du module et Takeaways | 9-43 |

Vue d'ensemble du module

Après avoir conçu et déployé la hiérarchie d'autorité de certification (AC), il est très important de créer correctement les modèles de certificats, de définir leur utilisation et de mettre en œuvre des techniques de sauvegarde et de récupération.

Dans ce module, vous apprendrez à déployer et à gérer les certificats, à configurer les modèles de certificats et à gérer le processus d'inscription. Vous apprendrez également à utiliser les certificats dans des contextes professionnels, mais aussi à déployer et à gérer les cartes à puce.

Objectifs

Au terme de ce module, vous saurez :

- Déployer et gérer des modèles de certificats ;
- Gérer le déploiement, la révocation et la récupération de certificats ;
- Utiliser des certificats dans un environnement commercial ;
- Mettre en œuvre et gérer des cartes à puce.

Leçon 1

Déploiement et gestion de modèles de certificats

Les modèles de certificats définissent comment un certificat est demandé et utilisé, par exemple pour chiffrer des fichiers ou signer le courrier électronique. Vous configurez des modèles au niveau de l'autorité de certification. Les modèles sont ensuite stockés dans la base de données des services de domaine Active Directory (AD DS). Plusieurs versions de modèles sont associées au système d'exploitation de l'autorité de certification. Le système d'exploitation Windows Server 2012 propose des modèles de version 4 tout en continuant à prendre en charge les trois versions précédentes.

Il existe deux types de catégories de certificats : les modèles de certificats utilisateur et les modèles de certificats ordinateur. Vous pouvez utiliser ces deux types de modèles à des fins diverses. Ainsi, vous pouvez affecter des autorisations à des modèles de certificats pour définir qui peut les gérer et qui peut effectuer l'inscription ou l'inscription automatique. Vous pouvez également mettre à jour les modèles de certificats en modifiant le modèle de certificat d'origine, en copiant un modèle ou en remplaçant les modèles de certificats existants. Dans cette leçon, vous apprendrez à gérer et à déployer des modèles de certificats.

Objectifs de la leçon

Au terme de cette leçon, vous saurez :

- Expliquer ce qu'est un certificat et un modèle de certificat ;
- Indiquer les versions de modèles de certificats disponibles dans Windows Server 2016 ;
- Expliquer comment configurer les autorisations des modèles de certificats ;
- Expliquer comment configurer les paramètres des modèles de certificats ;
- Indiquer les options disponibles pour mettre à jour un modèle de certificat ;
- Modifier et activer un modèle de certificat.

Que sont les certificats et les modèles de certificats ?

Un *certificat* est un petit fichier contenant plusieurs informations sur son propriétaire. Ces informations peuvent inclure le nom et l'adresse e-mail du propriétaire, le type d'utilisation du certificat et sa période de validité, les URL d'accès aux informations de l'autorité (AIA) et les URL du point de distribution de la liste de révocation de certificats (CDP). Un certificat contient également la *paire de clés*, c'est-à-dire la clé privée et la clé publique qui lui est associée. Ces clés sont utilisées pour la vérification d'identité, le chiffrement et les signatures numériques. La paire de clés générée pour chaque certificat fonctionne dans les conditions suivantes :

- Quand le contenu est crypté avec la clé publique, il peut être déchiffré uniquement avec la clé privée.
- Quand le contenu est crypté avec la clé privée, il ne peut pas être déchiffré avec la clé publique.
- Aucune autre clé n'est impliquée outre la paire de clés.

Un certificat contient des informations sur les utilisateurs, les appareils, l'utilisation, la validité et une paire de clés

Un modèle de certificat détermine :

- Le format et le contenu d'un certificat ;
- Le processus de création et de présentation d'une demande de certificat valide ;
- Les principes de sécurité autorisés à lire, à inscrire, ou à inscrire automatiquement les certificats basés sur le modèle ;
- Les autorisations nécessaires pour modifier un modèle de certificat.

- La clé privée ne peut pas être devinée dans un délai raisonnable à partir d'une clé publique et vice versa.

Pendant le processus d'inscription, le client génère une clé privée et l'AC génère une clé publique correspondante. Les certificats fournissent un mécanisme permettant de valider la relation entre une clé publique et l'entité qui possède la clé privée correspondante.

Un certificat fonctionne un peu comme un permis de conduire. De nombreuses entreprises acceptent le permis de conduire comme preuve d'identification parce qu'elles acceptent l'organisme émetteur (l'institution gouvernementale en question) comme étant digne de confiance. Connaissant le processus d'obtention d'un permis de conduire, ces entreprises ont confiance que l'organisme émetteur a bien vérifié l'identité de la personne à qui il a délivré ce permis. Ainsi, le permis de conduire est accepté comme preuve d'identité valide. Le processus d'approbation d'un certificat fonctionne de la même manière.

Modèles de certificats

Les modèles de certificats permettent aux administrateurs de personnaliser la méthode de distribution des certificats et de définir leurs objectifs ainsi que le type d'utilisation qu'ils autorisent. Les administrateurs peuvent créer des modèles, puis les déployer rapidement dans une entreprise à l'aide d'une interface graphique utilisateur (GUI) intégrée ou d'un utilitaire de ligne de commande.

Chaque modèle de certificat est associé à une liste de contrôle d'accès discrétionnaire (DACL). Cette liste définit les entités de sécurité qui sont autorisées à lire et à configurer le modèle et celles qui peuvent s'inscrire à des certificats ou utiliser l'inscription automatique sur la base du modèle de certificat. Les modèles de certificats et leurs autorisations sont définies et restent valides dans la forêt AD DS. Si plus d'une autorité de certification d'entreprise est présente dans la forêt AD DS, les modifications des autorisations les affecteront toutes.

Quand vous définissez un modèle de certificat, cette définition doit être disponible pour toutes les AC présentes dans la forêt. Pour cela, vous devez stocker les informations de modèle de certificat dans le contexte d'appellation de configuration de l'AD DS. Toute réplication de ces informations dépend de la planification de réplication AD DS. Par ailleurs, le modèle de certificat peut ne pas être disponible pour toutes les AC avant la fin de la réplication. Le stockage et la réplication des modèles se produisent automatiquement.

Versions de modèles de certificats dans Windows Server 2016

Dans Windows Server 2016, l'autorité de certification (AC) des services de certificats Active Directory (AD CS) prend en charge quatre versions de modèles de certificats. Outre le fait qu'elles correspondent aux versions du système d'exploitation Windows Server, les versions des modèles de certificats présentent également quelques différences fonctionnelles. Ces différences sont, entre autres, les suivantes :

- Modèles version 1. La seule modification permise aux modèles version 1 est celle de modifier les autorisations de lecture, d'écriture et d'inscription. Quand vous installez une AC, les modèles de certificats version 1 sont créés par défaut.

- Version 1
 - Crée par défaut lors de l'installation de l'autorité de certification
 - Ne peut pas être modifié (sauf en cas d'autorisation) ou supprimé
 - Peut être dupliqué pour créer des modèles de version 2 ou de version 3
- Version 2
 - Permet de personnaliser la plupart des paramètres du modèle
 - Prend en charge l'inscription automatique
- Version 3
 - Prend en charge les paramètres de chiffrement Suite B
 - Comprend des options avancées pour le chiffrement, les signatures numériques, l'échange de clés, et le hachage
- Version 4
 - Prend en charge les fournisseurs de services de chiffrement et les fournisseurs de stockage de clés
 - Prend en charge le renouvellement avec la même clé

- Modèles version 2. Plusieurs paramètres peuvent être personnalisés dans les modèles version 2. Par défaut, une installation AD CS fournit plusieurs versions préconfigurées des modèles version 2. Vous pouvez également créer des modèles version 2 en fonction des besoins de votre organisation. Autrement, vous pouvez dupliquer un modèle de certificat version 1 pour créer un nouveau modèle version 2. Vous pouvez ensuite modifier et sécuriser le modèle version 2 nouvellement créé. L'inscription automatique est prise en charge à partir de la version 2.
- Modèles version 3. Les modèles de certificats version 3 prennent en charge le chiffrement de nouvelle génération (CNG). Le CNG offre la prise en charge d'algorithmes de chiffrement Suite B, tel que le chiffrement à courbe elliptique. Vous pouvez dupliquer les modèles version 1 et version 2 par défaut pour les faire passer à la version 3. Avec les modèles de certificats version 3, vous pouvez utiliser le chiffrement CNG et les algorithmes de hachage pour modifier des demandes de certificats ou des certificats déjà émis et protéger les clés privées dans le cas d'un échange ou d'un archivage de clés.
- Modèles version 4. Les modèles version 4 sont pris en charge seulement par Windows Server 2012, Windows 8 ou ultérieur. Pour aider les administrateurs à vérifier quelles fonctions sont prises en charge par chaque version de Windows, l'onglet **Compatibilité** a été ajouté à l'onglet **Propriétés** du modèle de certificat. Cet onglet affiche les options non disponibles, en fonction des versions de systèmes d'exploitation sélectionnées pour un certificat client ou une AC donnés. Par ailleurs, les modèles de certificats de version 4 prennent en charge les fournisseurs de services de chiffrement (CSP) et les fournisseurs de stockage de clés. Ils peuvent également être configurés pour nécessiter d'être renouvelés en utilisant la même clé.

Configuration des autorisations de modèle de certificat

Pour configurer les autorisations des modèles de certificats, vous devez définir le DACL sur l'onglet **Sécurité** pour chacun d'eux. Les autorisations attribuées à un modèle définissent quels utilisateurs ou groupes peuvent lire ou modifier un modèle de certificat et s'ils peuvent s'y inscrire ou utiliser l'inscription automatique en fonction du modèle.

Vous pouvez affecter les autorisations suivantes aux modèles de certificats :

- Contrôle total. L'autorisation Contrôle total permet à une entité de sécurité de modifier tous les attributs d'un modèle de certificat, y compris les autorisations du modèle lui-même. Cela inclut également l'autorisation de modifier le descripteur de sécurité du modèle de certificat.
- Lecture. L'autorisation de lecture permet à un utilisateur ou à un ordinateur d'accéder au modèle de certificat pendant l'inscription de certificats. Le serveur de certificats nécessite l'autorisation de lecture pour trouver des modèles de certificats dans l'AD DS.
- Écriture. L'autorisation d'écriture permet à un utilisateur ou à un ordinateur de modifier les attributs d'un modèle de certificat.
- Inscription. L'autorisation d'inscription permet à un utilisateur ou à un ordinateur de s'inscrire à un certificat basé sur le modèle de certificat. Cependant, pour s'inscrire à un certificat, vous devez également disposer d'une autorisation de lecture pour le modèle de certificat.

| Autorisation | Description |
|-------------------------|---|
| Contrôle total | Permet à un utilisateur, groupe ou ordinateur désigné de modifier tous les attributs, y compris la propriété et les autorisations |
| Lecture | Permet à un utilisateur, groupe ou ordinateur désigné de lire le certificat dans AD DS lors de l'inscription |
| Écriture | Permet à un utilisateur, groupe ou ordinateur désigné de modifier tous les attributs, sauf les autorisations |
| Inscription | Permet à un utilisateur, groupe ou ordinateur désigné de s'inscrire au modèle de certificat |
| Inscription automatique | Permet à un utilisateur, groupe ou ordinateur désigné de recevoir un certificat via le processus d'inscription automatique |

- **Inscription automatique.** Cette autorisation permet à un utilisateur ou à un ordinateur d'obtenir un certificat par le biais du processus d'inscription automatique. Afin d'utiliser l'autorisation d'inscription automatique, l'utilisateur ou l'ordinateur doivent toutefois disposer également des autorisations de lecture et d'inscription pour un modèle de certificat.

Il est recommandé d'affecter les autorisations de modèle de certificat uniquement à des groupes globaux ou universels. En effet, les objets des modèles de certificats sont stockés dans le contexte d'appellation de configuration de l'AD DS. Évitez d'affecter des autorisations de modèle de certificat à des utilisateurs individuels ou à des comptes d'ordinateur.

Il est recommandé de toujours permettre l'accès au groupe **Utilisateurs authentifiés**. Les autorisations de lecture permettent à tous les utilisateurs et ordinateurs d'accéder aux modèles de certificats dans l'AD DS. Cette affectation d'autorisations permet également à l'AC, qui se situe dans le contexte système d'un compte d'ordinateur, d'accéder aux modèles de certificats lors de l'attribution de certificats. Cette autorisation ne donne pas pour autant de droits d'inscription, elle peut donc être attribuée sans aucun risque.

Configuration des paramètres de modèle de certificat

Outre les paramètres de sécurité, vous pouvez configurer plusieurs autres paramètres sur chaque modèle de certificat. N'oubliez pas cependant que le nombre d'options qu'il est possible de configurer dépend de la version du modèle de certificat. Ainsi, vous ne pouvez pas modifier les paramètres des modèles version 1 outre les réglages de sécurité. Par contre, vous pouvez utiliser des modèles de certificats de versions ultérieures pour configurer la plupart des options disponibles.

Pour chaque modèle de certificat, vous pouvez personnaliser plusieurs paramètres, comme le temps de validité, le but, le CSP, l'exportabilité de clé privée et les exigences d'émission

| Catégorie | Exemple d'usage unique | Exemple de multi-usages |
|--------------|---|--|
| Utilisateurs | <ul style="list-style-type: none"> • EFS basique • Session authentifiée • Connexion carte à puce | <ul style="list-style-type: none"> • Administrateur • Utilisateur • Utilisateur de carte à puce |
| Ordinateurs | <ul style="list-style-type: none"> • Serveur web • IPsec | <ul style="list-style-type: none"> • Ordinateur • Contrôleur de domaine |

Comme les versions précédentes, Windows Server 2016 fournit plusieurs modèles de certificats par défaut qui peuvent être utilisés à des fins diverses. Cela inclut entre autres la signature numérique du code, le chiffrement de données au moyen du système de fichiers EFS et la connexion par cartes à puces. Si vous souhaitez personnaliser un modèle de certificat pour votre organisation, vous pouvez le dupliquer, puis modifier la configuration du certificat.

Pour configurer des modèles, vous devez :

- Déterminer le format et le contenu du certificat selon son utilisation prévue ;
- Déterminer le processus à suivre pour créer et soumettre une demande de certificat valide ;
- Déterminer quel CSP est pris en charge ;
- Définir la longueur de la clé ;
- Définir la période de validité ;
- Déterminer le processus ou les exigences d'inscription.

 **Remarque :** L'utilisation d'un certificat peut concerner des utilisateurs ou des ordinateurs en fonction des types d'implémentations de sécurité requis pour utiliser l'infrastructure de clés publiques (PKI).

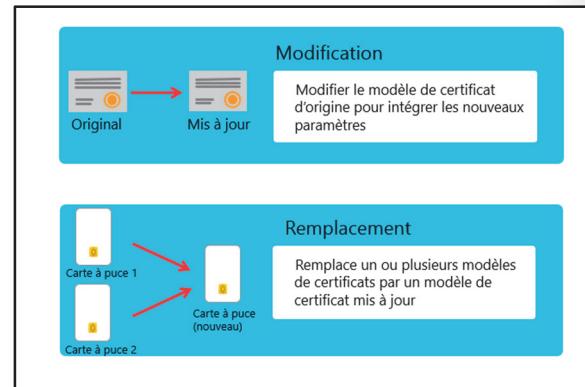
Vous pouvez également définir la fonction d'un certificat dans ses paramètres. Les modèles de certificats peuvent être :

- À usage unique. Un certificat à usage unique sert une seule fonction, par exemple permettre aux utilisateurs de se connecter au moyen d'une carte à puce. Les organisations utilisent des certificats à usage unique quand la configuration du certificat diffère de celle des autres certificats déployés. Supposons par exemple que tous les utilisateurs reçoivent un certificat pour se connecter avec une carte à puce, mais que seuls quelques groupes nécessitent un certificat EFS. Dans ce cas, les organisations gardent généralement ces certificats et modèles séparés, pour garantir qu'ils seront attribués seulement aux utilisateurs qui en ont besoin.
- À usage multiple. Un certificat à usage multiple sert plus d'un objectif à la fois, souvent sans rapport l'un avec l'autre. Alors que certains modèles, comme le modèle utilisateur, prévoient certaines fonctions par défaut, les organisations les modifient souvent pour ajouter des fonctions supplémentaires. Si, par exemple, une entreprise souhaite émettre des certificats pour servir trois objectifs, ceux-ci peuvent être combinés en un seul modèle de certificat pour réduire les efforts administratifs et la maintenance.

Options de mise à jour d'un modèle de certificat

Dans la plupart des organisations, la hiérarchie de l'AC prévoit un modèle de certificat pour chaque type de fonction. Ainsi, il peut y avoir un modèle de certificat pour le chiffrement de fichiers et un autre pour la signature du code. Par ailleurs, quelques modèles supplémentaires peuvent couvrir des fonctions pour la plupart des sujets communs.

En tant qu'administrateur informatique, vous aurez peut-être besoin de modifier un modèle de certificat existant à cause de paramètres mal configurés ou d'autres problèmes présents dans le modèle de certificat d'origine. Vous pouvez également avoir besoin de fusionner plusieurs modèles de certificats existants en un seul modèle.



Pour mettre à jour un modèle de certificat, vous pouvez soit le modifier, soit le remplacer par un nouveau.

- Modifier le modèle de certificat d'origine. Pour modifier un modèle de certificat des versions 2, 3 ou 4, vous devez apporter des modifications, puis les appliquer à ce modèle. À partir de ce point, tout certificat émis par une autorité de certification basée sur ce modèle comprendra vos modifications.
- Remplacer des modèles de certificats existants. La hiérarchie de l'AC d'une organisation peut avoir plusieurs modèles de certificats offrant des fonctionnalités identiques ou similaires. Dans un tel scénario, vous pouvez remplacer plusieurs modèles de certificats par un seul. Vous pouvez effectuer ce remplacement dans la console **Modèles de certificats** en indiquant que le nouveau modèle de certificat remplace les modèles de certificats existants. À partir de ce point, tous les utilisateurs disposant des certificats basés sur des modèles périmés en recevront de nouveaux basés sur le modèle de remplacement.

Démonstration : Modification et autorisation d'un modèle de certificat

Dans cette démonstration, vous allez apprendre comment modifier et activer un modèle de certificat.

Procédure de démonstration

1. Sur **LON-DC1**, dans **Gestionnaire de serveur**, ouvrez **Autorité de certification**.
2. Dans **Autorité de certification**, ouvrez la console **Modèles de certificats**.
3. Passez en revue la liste des modèles disponibles.
4. Ouvrez les propriétés du modèle de certificat **IPsec**, puis consultez les paramètres disponibles.
5. Dupliquez le modèle de certificat de l'**Utilisateur Exchange**. Nommez-le **Utilisateur Exchange Test1**, puis configurez-le pour qu'il remplace le modèle **Utilisateur Exchange**.
6. Permettez aux **Utilisateurs authentifiés** de s'inscrire et de s'inscrire automatiquement au modèle **Utilisateur Exchange Test1**.
7. Déployez le modèle **Utilisateur Exchange Test1** sur **LON-DC1**.

Testez vos connaissances

| Question |
|--|
| Lesquels des énoncés suivants sont vrais au sujet des modèles de certificats version 2 dans AD CS ? (Choisissez toutes les réponses qui s'appliquent.) |
| Sélectionnez la bonne réponse. |
| Les modèles version 2 prennent en charge l'inscription automatique. |
| Vous pouvez modifier uniquement l'onglet Sécurité dans un modèle version 2. |
| Vous pouvez passer à un modèle version 2 en dupliquant un modèle version 1. |
| Les modèles version 2 sont uniquement pris en charge dans Windows Server 2008, Windows Vista ou ultérieur. |
| Les modèles version 2 sont uniquement pris en charge dans Windows Server 2012, Windows 8 ou ultérieur. |

Testez vos connaissances

| Question | |
|----------|--|
| | <p>You êtes l'administrateur AD DS pour A. Datum Corporation. Plusieurs utilisateurs de votre environnement AD DS ont fait appel à l'inscription automatique pour obtenir un certificat utilisateur. Vous voulez raccourcir la période de validité du certificat utilisateur et devez veiller à ce que les utilisateurs obtiennent un nouveau certificat immédiatement, sans subir d'interruption de validité du certificat existant. Lesquelles des actions suivantes devriez-vous effectuer ? (Choisissez toutes les réponses qui s'appliquent.)</p> |
| | Sélectionnez la bonne réponse. |
| | Duplicer le modèle existant et indiquer un nouveau nom de modèle. Modifier la période de validité du nouveau modèle. |
| | Modifier la période de validité du modèle existant. |
| | Modifier les paramètres d'inscription automatique du modèle existant. |
| | Révoquer tous les certificats utilisateur émis à partir du modèle existant. |
| | Modifier le nouveau modèle pour qu'il remplace le modèle existant. Publier le nouveau modèle. |

Leçon 2

Gestion du déploiement, de la révocation et de la récupération de certificats

L'une des étapes du déploiement d'une PKI dans votre organisation est de définir les modalités de distribution des certificats et les modalités d'inscription. Pendant le processus de gestion des certificats, vous pouvez également avoir besoin de révoquer des certificats. Les motifs de révocation d'un certificat peuvent inclure une clé compromise ou un utilisateur quittant l'organisation. Vous devez vous assurer que les clients réseau peuvent déterminer quels certificats sont révoqués avant d'accepter les demandes d'authentification. Révoquer un certificat ou une clé représente l'une des tâches de gestion les plus importantes dans le cycle de vie d'un certificat. Si vous perdez vos clés publiques et privées, vous pouvez utiliser un agent d'archivage et de récupération de clé pour récupérer vos données. En outre, vous pouvez utiliser des méthodes de récupération d'archives et de clés automatiques ou manuelles pour vous assurer de pouvoir accéder aux données si jamais vous perdez vos clés.

Objectifs de la leçon

Au terme de cette leçon, vous saurez :

- Décrire les méthodes d'inscription d'un certificat ;
- Décrire l'inscription automatique d'un certificat ;
- Expliquer ce qu'est un agent d'inscription ;
- Décrire comment révoquer un certificat ;
- Décrire l'archivage et de la récupération d'une clé ;
- Décrire comment configurer l'archivage automatique des clés ;
- Configurer une autorité de certification (AC) pour l'archivage des clés.

Méthodes d'inscription du certificat

Dans Windows Server 2016, vous pouvez utiliser plusieurs méthodes d'inscription à un certificat utilisateur ou ordinateur. La méthode que vous choisissez dépend de votre scénario spécifique. Par exemple, vous pouvez utiliser l'inscription automatique pour déployer en masse des certificats à un grand nombre d'utilisateurs ou d'ordinateurs. Toutefois, vous pouvez choisir d'utiliser l'inscription manuelle de certificats dédiés à des entités de sécurité spécifiques. La liste suivante décrit les différentes méthodes d'inscription et précise dans quel cas les utiliser :

| Méthode | Utilisation |
|--|--|
| Inscription automatique | <ul style="list-style-type: none"> • Pour automatiser la demande, la récupération et le stockage des certificats pour les ordinateurs basés sur un domaine |
| Inscription manuelle | <ul style="list-style-type: none"> • Pour demander des certificats via la console Certificats ou Certreq.exe lorsque le demandeur ne peut pas communiquer directement avec l'autorité de certification |
| Inscription Web de l'autorité de certification | <ul style="list-style-type: none"> • Pour demander des certificats à partir d'un site Web qui se trouve sur une autorité de certification • Pour délivrer des certificats lorsque l'inscription automatique n'est pas disponible |
| S'inscrire au nom de | <ul style="list-style-type: none"> • Fournir le personnel informatique avec le droit de demander des certificats au nom d'un autre utilisateur (Agent d'inscription) |

- Inscription automatique. Quand vous utilisez cette méthode, l'administrateur définit les autorisations et la configuration d'un modèle de certificat. Ces définitions aident le demandeur à requérir, à récupérer et à renouveler automatiquement les certificats sans interaction nécessaire de la part de l'utilisateur final. Cette méthode est communément utilisée pour les ordinateurs de domaine AD DS. L'inscription automatique du certificat doit être configurée au moyen de la stratégie de groupe. Cette méthode est décrite plus en détail dans la rubrique suivante.

- **Inscription manuelle.** En utilisant ce procédé, la clé privée ainsi qu'une demande de certificat sont générées à partir d'un périphérique, tel qu'un service Web ou un ordinateur. La demande de certificat est ensuite transmise à l'autorité de certification pour générer le certificat demandé. Le certificat est alors transmis au périphérique pour y être installé. Utilisez cette méthode quand le demandeur ne peut pas communiquer directement avec l'AC ou si le périphérique en question ne prend pas en charge l'inscription automatique. Cette méthode est utilisée lors de l'achat d'un certificat public. Vous pouvez utiliser cette méthode au moyen du composant logiciel enfichable Certificats ou de l'outil Certreq.exe.
- **Inscription via le site Web de l'AC.** En utilisant cette méthode, vous pouvez activer l'AC sur un site Web pour permettre aux utilisateurs d'obtenir des certificats. Pour utiliser l'inscription via le site Web de l'autorité de certification, vous devez installer Internet Information Services (IIS) et le rôle AC pour l'inscription via le Web. Pour obtenir un certificat, le demandeur doit se connecter sur le site, choisir le modèle de certificat approprié, puis soumettre une demande. Le certificat est émis automatiquement si l'utilisateur dispose des autorisations nécessaires pour s'inscrire afin d'obtenir le certificat. Utilisez cette méthode pour délivrer des certificats quand vous ne pouvez pas appliquer l'inscription automatique. Cela peut arriver dans le cas d'une demande de certificat avancée.
- **Inscription pour le compte du demandeur.** Pour utiliser cette méthode, vous devez d'abord créer un agent d'inscription. L'*Agent d'inscription* est un compte utilisateur employé pour demander des certificats au nom d'un autre compte utilisateur. Un modèle de certificat spécifique est appliqué à un Agent d'inscription qui accorde les autorisations requises. Vous pouvez utiliser cette méthode si, par exemple, vous avez besoin de permettre à un gestionnaire de précharger les certificats d'ouverture de session sur les cartes à puce destinées aux nouveaux employés.

Aperçu de l'inscription automatique de certificat

Dans les situations où il n'est pas efficace d'utiliser l'inscription manuelle, vous pouvez configurer des modèles de certificats qui permettent au demandeur de s'inscrire à des certificats et les renouveler automatiquement sans interaction nécessaire de la part de l'utilisateur final.

Exemple de situation où l'inscription manuelle n'est pas efficace : Quand vous avez besoin de délivrer un certificat à chaque utilisateur et ordinateur de votre organisation. Une méthode courante et très efficace de s'y prendre est d'utiliser *l'inscription automatique*. Cette méthode vous fournit un moyen automatisé pour déployer des certificats aux utilisateurs et aux ordinateurs qui se trouvent au sein de votre organisation AD DS. Cependant, il est important de noter que vous ne pouvez pas utiliser l'inscription automatique avec une autorité de certification autonome. Vous devez disposer d'une AC d'entreprise disponible pour utiliser l'inscription automatique.

- Un modèle de certificat est configuré pour appliquer les autorisations d'Autorisation, d'Inscription et d'Inscription automatique des utilisateurs qui reçoivent les certificats
- L'autorité de certification est configurée pour émettre le modèle
- L'inscription automatique nécessite la création d'un objet de stratégie de groupe (GPO) AD DS
- Le GPO doit être lié au site, au domaine ou à l'unité d'organisation (OU) approprié(e)
- L'utilisateur ou l'ordinateur reçoit les certificats au cours du prochain intervalle d'actualisation de la stratégie de groupe

L'autorisation d'inscription automatique n'est pas disponible pour les modèles de certificats version 1. C'est pourquoi vous devez dans ce cas dupliquer un modèle de certificat, puis configurer les autorisations pour permettre la lecture, l'inscription et l'inscription automatique des utilisateurs ou des ordinateurs qui recevront les certificats. Ensuite, une stratégie de groupe basée sur un domaine vous aidera à activer et à gérer l'inscription automatique grâce à des stratégies basées sur l'utilisateur et sur l'ordinateur.



Remarque : Par défaut, la stratégie de groupe basée sur l'ordinateur est appliquée au démarrage et la stratégie de groupe basée sur l'utilisateur est traitée à l'ouverture de session. La stratégie de groupe actualise également les membres du domaine environ toutes les 90 minutes. Le paramètre de stratégie de groupe permettant l'inscription automatique des ordinateurs et des utilisateurs est nommé **Client des services de certificats - Incription automatique**.

Ce paramètre doit être activé tant pour l'ordinateur que pour l'objet utilisateur. Si vous activez l'inscription automatique uniquement pour une stratégie basée sur l'ordinateur, le processus d'inscription automatique n'est pas invoqué pour les utilisateurs qui se connectent à celui-ci.

Une minuterie interne déclenche l'inscription automatique toutes les huit heures depuis la dernière activation. Toutefois, un certificat n'est pas délivré chaque fois que la minuterie est déclenchée. Si l'utilisateur ou l'ordinateur s'est déjà inscrit à des certificats attribués par le biais de l'inscription automatique, aucune action n'est alors effectuée. Si le modèle de certificat nécessite une interaction utilisateur pour traiter la demande d'inscription, une fenêtre indépendante s'affiche environ 60 secondes après l'ouverture de session.

Pour configurer et activer l'inscription automatique de certificats dans un environnement de domaine, vous devez :

- Faire partie du groupe Administrateurs du domaine ou Administrateurs de l'entreprise ;
- Configurer un modèle de certificat avec l'autorisation d'inscription automatique ;
- Configurer une stratégie d'inscription automatique et l'appliquer aux utilisateurs du domaine et aux ordinateurs qui la nécessitent.

Qu'est-ce que l'itinérance avec authentification par informations d'identification ?

L'*itinérance avec authentification par informations d'identification* (Credential Roaming) est une fonctionnalité qui permet aux utilisateurs d'accéder à leurs informations d'identification à distance. L'itinérance avec authentification par informations d'identification permet à un utilisateur qui se connecte à un ordinateur exécutant Windows Server et pouvant appartenir à n'importe quel domaine d'obtenir et d'utiliser localement, de façon transparente et sans intervention nécessaire, tous ses identifiants (certificats et clés privées). L'intégrité des identifiants est conservée en toutes circonstances, par exemple quand les certificats sont mis à jour ou encore quand les utilisateurs se connectent à plus d'un ordinateur à la fois. Cela permet d'éviter l'hypothèse selon laquelle un utilisateur est en mesure d'obtenir automatiquement un certificat sur chaque nouvelle machine où il se connecte.

L'itinérance avec authentification par informations d'identification intervient dans certaines situations, par exemple quand une clé privée ou un certificat sont modifiés dans le magasin de certificats locaux de l'utilisateur, quand l'utilisateur verrouille ou déverrouille l'ordinateur ou encore quand la stratégie de groupe est actualisée. Toutes les communications basées sur les certificats sont signées et cryptées, qu'elles se déroulent entre les composants de l'ordinateur local ou entre l'ordinateur local et l'AD DS. Windows 7 et les systèmes d'exploitation ultérieurs prennent en charge l'itinérance avec authentification par informations d'identification.

Qu'est-ce qu'un agent d'inscription ?

Dans Windows Server 2016 CA, vous pouvez configurer l'inscription de certificats pour autoriser des utilisateurs désignés à inscrire d'autres utilisateurs à votre organisation en leur nom. Les utilisateurs désignés sont ce qu'on appelle un *Agent d'inscription*, c'est-à-dire un compte utilisateur employé pour demander des certificats au nom d'un autre compte utilisateur. Pour permettre l'inscription au compte d'un autre utilisateur, l'agent d'inscription doit posséder un certificat basé sur le modèle **Agent d'inscription**. Contrairement à un gestionnaire de certificats, un agent d'inscription peut uniquement traiter la demande d'inscription et ne peut pas approuver les demandes en attente ou révoquer les certificats déjà délivrés.

- Un *Agent d'inscription* est un compte d'utilisateur utilisé pour demander des certificats au nom d'un autre compte d'utilisateur
- Un agent d'inscription doit posséder un certificat basé sur le modèle **Agent d'inscription**
- Les agents d'inscription sont généralement des membres des services de sécurité informatique ou de l'entreprise
- Le champ d'application d'un agent d'inscription peut se limiter à :
 - Des utilisateurs ou des groupes de sécurité spécifiques ;
 - Des modèles de certificats spécifiques.



Remarque : Étant donné qu'un utilisateur possédant un certificat Agent d'inscription peut se faire passer pour d'autres utilisateurs, le modèle **Agent d'inscription** doit être sécurisé correctement. Il est recommandé de publier le modèle Agent d'inscription sur une autorité de certification uniquement s'il est nécessaire de désigner un agent d'inscription pour votre organisation. Une fois que l'agent d'inscription a reçu le certificat nécessaire, vous devez retirer le modèle Agent d'inscription de toutes les AC où il a été publié.

Windows Server 2016 comprend trois modèles de certificats permettant différents types d'agents d'inscription :

- Agent d'inscription. Il est utilisé pour demander des certificats au nom d'un autre sujet.
- Agent d'inscription (ordinateur). Il est utilisé pour demander des certificats pour le compte d'un autre sujet ordinateur.
- Agent d'inscription Exchange (demande hors connexion). Il est utilisé pour demander des certificats pour le compte d'un autre sujet et fournir le nom du sujet dans la demande. Le Service d'inscription de périphérique réseau (NDES) utilise ce modèle pour ses certificats d'agents d'inscription.

En règle générale, une ou plusieurs personnes autorisées au sein d'une organisation sont désignées comme agents d'inscription. Les agents d'inscription sont souvent choisis parmi les membres des équipes de sécurité, de sécurité informatique ou du service d'assistance de l'entreprise, car ce type de personnes se voient déjà confier la protection de ressources précieuses. Dans certaines organisations, telles que les banques disposant de plusieurs branches, les membres du service d'assistance et du personnel de sécurité peuvent ne pas être idéalement situés pour effectuer cette tâche. Dans ce cas, désigner un directeur de succursale ou un autre employé de confiance pour agir à titre d'agent d'inscription peut être nécessaire afin de permettre l'émission des identifiants de cartes à puce en des lieux multiples.

Quand vous créez un agent d'inscription, vous pouvez restreindre sa capacité à enregistrer des certificats pour le compte d'autres demandeurs en limitant leur champ d'application à un groupe de sécurité spécifique et à des modèles de certificats spécifiques. Ainsi, vous pouvez décider de mettre en œuvre une restriction pour faire en sorte que l'agent d'inscription puisse effectuer l'inscription de certificats d'ouverture de session par carte à puce uniquement au nom d'utilisateurs appartenant à un groupe spécifique de l'équipe de sécurité du département. Avant Windows Server 2008 Enterprise, il n'était pas possible de limiter la portée d'un agent d'inscription AD CS. Par conséquent, chaque utilisateur possédant un certificat Agent d'inscription était en mesure d'inscrire un utilisateur dans une organisation pour

n'importe quel modèle de certificat. Avec les versions AD CS plus récentes, la portée de l'agent d'inscription peut être limitée à des groupes et modèles de certificats spécifiques. Pour chaque modèle de certificat, vous pouvez choisir les utilisateurs ou groupes de sécurité au nom desquels un agent d'inscription peut s'inscrire.

 **Remarque :** Vous ne pouvez pas limiter un agent d'inscription sur la base d'unités organisationnelles ou de conteneurs AD DS spécifiques. L'inscription pour le compte d'autres utilisateurs ne peut être limitée à des utilisateurs ou à des groupes de sécurité spécifiques dans l'AD DS.

 **Remarque :** Restreindre la portée d'un agent d'inscription peut affecter la performance de l'AC. Pour optimiser la sécurité et les performances, vous devez réduire le nombre de comptes désignés comme agents d'inscription en modifiant la liste de contrôle d'accès dans le modèle Agent d'inscription.

Comment fonctionne la révocation de certificats ?

La *révocation* est un processus à l'aide duquel vous désactivez la validité d'un ou plusieurs certificats. En lançant le processus de révocation, vous publiez l'empreinte numérique du certificat dans la liste de révocation de certificats (CRL) correspondante. Cette action annonce qu'un certificat spécifique n'est plus valide.

Voici une vue d'ensemble du processus de révocation d'un certificat :

1. Un certificat est révoqué du composant logiciel enfichable Microsoft Management Console (MMC) dans l'AC. Spécifiez un code de motif ainsi que qu'une date et heure pendant la révocation. Cela est facultatif, mais recommandé.
2. Selon la valeur configurée, la liste de révocation de certificats annonce la révocation en utilisant la console de l'AC ou elle est publiée automatiquement. Les listes de révocation de certificats peuvent publier dans l'AD DS, dans un emplacement de dossier partagé ou encore sur un site Web.
3. Quand les ordinateurs clients exécutant Windows reçoivent un certificat, ils utilisent un processus pour vérifier son état de révocation en interrogeant l'AC émettrice et l'emplacement du CDP. Cela permet de déterminer si le certificat est révoqué, puis de fournir cette information à l'application qui a demandé la vérification. L'ordinateur client exécutant Windows utilise l'un des emplacements de liste de révocation de certificats indiqués dans le certificat pour vérifier sa validité.

Voici les étapes à suivre pour révoquer un certificat :

1. Un certificat est révoqué
2. Une liste de révocation de certificats est publiée
3. Un ordinateur client vérifie la validité et la révocation du certificat

Les systèmes d'exploitation Windows incluent le composant CryptoAPI, qui est responsable pour la révocation des certificats et des processus de vérification du statut. CryptoAPI utilise les phases suivantes pour le processus de vérification de certificats :

- Découverte de certificats. Pendant cette phase, CryptoAPI recueille les certificats de l'AC, les informations AIA des certificats délivrés et les détails du processus d'inscription de certificat.
- Validation du chemin d'accès. La *validation du chemin d'accès* est le processus de vérification du certificat via la chaîne d'autorité de certification ou *chemin d'accès* jusqu'à remonter à l'emplacement du certificat AC racine.

- Vérification de la révocation. Chaque certificat de la chaîne de certification est vérifié pour garantir qu'aucun certificat n'est révoqué.
- Récupération du réseau et mise en cache. La récupération du réseau est effectuée par le biais du protocole OCSP. CryptoAPI est chargé de vérifier le cache local pour obtenir des informations de révocation. Si aucune correspondance n'est trouvée, CryptoAPI lance un appel en utilisant le protocole OCSP, qui se base sur l'URL fournie par le certificat délivré.

Qu'est-ce qu'un service Répondeur en ligne ?

Vous pouvez également faire appel à un *service Répondeur en ligne*, qui est un moyen plus efficace pour vérifier l'état de révocation d'un certificat. Le service Répondeur en ligne utilise le protocole OCSP pour offrir aux clients un moyen efficace de déterminer l'état de révocation d'un certificat. L'OCSP soumet des demandes de statut de certificat en utilisant le protocole HTTP.

Les clients accèdent aux listes de révocation de certificats pour déterminer l'état de révocation d'un certificat. Si les listes de révocation de certificats sont volumineuses, les clients peuvent nécessiter beaucoup de temps pour effectuer la recherche. Un service Répondeur en ligne peut rechercher ces listes de révocation dynamiquement pour le compte des clients et leur fournir l'état du certificat demandé. Vous pouvez faire appel à un Répondeur en ligne pour déterminer l'état de révocation des certificats émis par une seule ou plusieurs autorités de certification. Vous pouvez également utiliser plus d'un Répondeur en ligne pour distribuer les informations sur l'état de révocation.

Vous devez installer un Répondeur en ligne et une autorité de certification sur différents ordinateurs. En outre, vous devez configurer l'AC pour qu'elle inclut l'URL du Répondeur en ligne dans l'extension AIA des certificats délivrés. Le client OCSP utilise cette URL pour valider l'état du certificat. Vous devez également émettre le modèle de certificat **Signature de réponse OCSP**, afin que le Répondeur en ligne puisse inscrire également ce certificat.

Vue d'ensemble de l'archivage et de la récupération de clé

Dans certains cas, il est crucial de protéger le certificat et la paire de clés correspondante. Si par exemple vous utilisez un certificat pour effectuer le chiffrement du contenu des e-mails ou des documents et que vous perdez vos clés publiques et privées, vous ne serez pas en mesure d'accéder aux données cryptées en utilisant la clé publique du certificat. Ces données peuvent comprendre des fichiers chiffrés EFS et des e-mails chiffrés S/MIME. L'archivage et la récupération des clés publiques et privées sont donc d'une grande importance. Vous pouvez archiver ou sauvegarder votre clé privée en exportant un certificat contenant la clé privée et le stocker dans un endroit sûr, tel qu'un support alternatif ou un espace de stockage en ligne. Cette approche nécessite cependant que chaque utilisateur sauvegarde sa clé privée, ce qui en général n'est pas une méthode de sauvegarde fiable. Une autre méthode consiste à centraliser l'archivage des clés privées sur l'AC.

- Les clés privées peuvent être perdues quand :
 - Un profil d'utilisateur est supprimé
 - Un système d'exploitation est réinstallé
 - Un disque est endommagé
 - Un ordinateur est perdu ou volé
- Vous devez impérativement archiver les clés privées des certificats utilisés pour le chiffrement
- La récupération de clé nécessite un KRA
- L'archivage de clé doit être configuré sur la CA et sur le modèle de certificat
- La récupération de clés se déroule en deux parties :
 1. Extraction de la clé
 2. Récupération de la clé
- Le certificat KRA doit être protégé



Remarque : lors des opérations normales, l'AC n'a pas accès à la clé privée d'un utilisateur, car elle est générée du côté du client. Pour cette raison, vous devez activer explicitement l'archivage des clés privées sur chaque modèle de certificat où vous voulez avoir cette fonctionnalité.

Conditions de perte de clés

Vous risquez de perdre des paires de clés dans les conditions suivantes :

- Un profil utilisateur est supprimé ou endommagé. Un CSP chiffre une clé privée et stocke la clé privée chiffrée dans le système de fichiers local ainsi que dans le registre du dossier de profil utilisateur. La suppression ou la corruption du profil provoque la perte des éléments de la clé privée ;
- Un système d'exploitation est réinstallé. Lorsque vous réinstallez le système d'exploitation, les installations précédentes des profils utilisateur sont perdues, y compris les éléments de la clé privée. Dans ce scénario, les certificats de l'ordinateur sont également perdus ;
- Un disque est endommagé. Si un disque dur est endommagé et le profil utilisateur est indisponible, les éléments de la clé privée sont perdus automatiquement, en plus des certificats d'ordinateur installés ;
- Un ordinateur est perdu ou volé. Si l'ordinateur d'un utilisateur est perdu ou volé, le profil utilisateur avec les éléments de la clé privée est indisponible.



Remarque : la perte d'une paire de clés (certificat) n'est pas toujours critique. Par exemple, si vous perdez un certificat utilisé pour la signature ou la journalisation numérique, vous pouvez tout simplement en émettre un nouveau et aucune donnée ne sera affectée. Toutefois, la perte d'un certificat qui a été utilisé pour le chiffrement des données rendra impossible l'accès aux données. C'est pour cette raison que l'archivage et la récupération sont essentiels.

Agents d'archivage et de récupération de clé

Pour utiliser l'archivage des clés privées, vous devez activer cette fonctionnalité sur l'AC et sur les modèles de certificat spécifiques, tels qu'EFS. Cette fonctionnalité est désactivée par défaut sur l'AC ou sur n'importe quel modèle de certificat. Pour être en mesure d'archiver les clés privées des certificats, vous devez également définir un agent de récupération de clé (KRA).



Remarque : l'archivage des clés sur l'AC fonctionne à partir du moment où il est entièrement configuré. Cependant, il ne concerne pas des certificats qui ont été émis avant son activation.

Vous utilisez l'archivage des clés et le KRA pour la récupération de données dans les scénarios où la clé privée est perdue. Le KRA est un utilisateur avec un certificat KRA émis qui est capable de déchiffrer les clés privées stockées dans une base de données AD CS. Lorsque l'archivage des clés est activé sur l'AC et sur les modèles de certificats, chaque clé privée est chiffrée avec la clé publique d'un KRA puis stockée dans la base de données AC. Par conséquent, la clé privée d'un KRA doit être utilisée pour déchiffrer la clé privée sur n'importe quel utilisateur. Les KRA sont désignés pour les utilisateurs qui sont en mesure de récupérer le certificat d'origine, la clé privée et la clé publique qui ont été utilisés pour chiffrer les données.



Remarque : Ne confondez pas le KRA avec l'agent de récupération de données. L'agent de récupération de données est capable de déchiffrer directement les données chiffrées avec EFS lorsque la clé privée de l'utilisateur d'origine n'est pas disponible. Sinon, le KRA ne déchiffre aucune donnée directement : il déchiffre uniquement les clés privées archivées. La fonctionnalité agent de récupération de données est abordée plus loin dans ce module.

Pour devenir un KRA, vous devez vous inscrire pour un certificat basé sur le modèle KRA. Une fois ce certificat délivré à l'utilisateur désigné, une clé publique du certificat du KRA est importée sur l'AC et l'archivage des clés est activé. À partir de ce moment, chaque certificat délivré sur la base d'un modèle où

l'archivage des clés est activé aura sa clé privée stockée dans la base de données AC et chiffrée avec la clé publique du KRA.

Pendant le processus de récupération de clés, le gestionnaire de certificats ou l'administrateur AC récupère le fichier chiffré qui contient le certificat et la clé privée de la base de données AC. Ensuite, un KRA utilise sa clé privée pour déchiffrer la clé privée du fichier chiffré, puis retourne le certificat et la clé privée à l'utilisateur.



Remarque : la récupération de clés est un processus en deux phases. Premièrement, la clé chiffrée est récupérée dans la base de données AC. Deuxièmement, le KRA déchiffre la clé et le certificat. Pour des raisons de sécurité, il est préférable que des personnes différentes réalisent les deux phases. Par défaut, le KRA n'a pas la permission pour récupérer des clés chiffrées à partir d'une base de données AC.

Sécurité pour l'archivage de clés

Lorsque vous avez un CA configuré pour délivrer un certificat KRA, tout utilisateur disposant d'autorisations de lecture et d'inscription sur le modèle de certificat KRA peut s'inscrire et devenir un KRA. Les membres des groupes Administrateurs du domaine et Administrateurs de l'entreprise reçoivent ces autorisations par défaut. Cependant, vous devez vous assurer que :

- Seuls les utilisateurs approuvés sont autorisés à s'inscrire à ce certificat ;
- La clé privée du KRA est stockée de manière sécurisée ;
- Le serveur sur lequel les clés sont archivées est dans un endroit séparé et sécurisé physiquement.

Une fois le certificat KRA délivré, nous vous recommandons de supprimer ce modèle de l'AC. De plus, nous vous recommandons d'importer le certificat KRA seulement quand une procédure de récupération de clé doit être effectuée.

Compréhension de l'archivage et de la récupération des clés

La récupération de clés implique que la partie clé privée d'une paire de clés publique et privée peut être archivée et récupérée. La récupération de clés privées ne récupère aucune donnée ni aucun message. Elle permet simplement à un utilisateur de récupérer des clés perdues ou endommagées ou à un administrateur d'assumer le rôle d'un utilisateur afin d'accéder ou de récupérer des données. Dans de nombreuses applications, la récupération de clés doit d'abord être effectuée avant de pouvoir récupérer les données. La procédure de récupération de clés est la suivante :

1. Un utilisateur demande un certificat d'une AC et fournit une copie de la clé privée dans le cadre de la demande. La AC, qui traite la demande, archive la clé privée chiffrée dans la base de données AC et délivre un certificat à l'utilisateur demandeur.
2. Une application telle qu'EFS peut utiliser le certificat délivré pour chiffrer des fichiers sensibles.
3. Si, à un moment donné, la clé privée est perdue ou endommagée, l'utilisateur peut contacter le gestionnaire de certificats de l'organisation pour récupérer la clé privée. Le gestionnaire de certificats, avec l'aide du KRA, récupère la clé privée, la stocke dans un format de fichier protégé, puis l'envoie à l'utilisateur.
4. Une fois que l'utilisateur a stocké la clé privée récupérée dans le magasin de clés locales de l'utilisateur, une application telle qu'EFS peut utiliser encore une fois la clé pour déchiffrer les fichiers déjà chiffrés ou pour en chiffrer de nouveaux.

Configuration de l'archivage principal automatique

Avant de pouvoir utiliser l'archivage de clés, vous devez réaliser plusieurs étapes de configuration. La fonctionnalité d'archivage de clés n'est pas activée par défaut, et vous devez configurer l'AC et les modèles de certificats applicables pour l'archivage de clés et récupération de clés.

Les étapes suivantes décrivent la procédure d'archivage automatique des clés :

1. Configurer le modèle de certificat KRA. Par défaut, seuls les membres des groupes Administrateurs de l'entreprise ou Administrateurs du domaine peuvent demander un certificat KRA. Si vous souhaitez autoriser d'autres utilisateurs à s'inscrire pour un certificat KRA, vous devez le spécifier sur la liste de contrôle d'accès du modèle KRA.
2. Les agents de récupération de clés désignés s'inscrivent pour un certificat KRA. Les utilisateurs qui ont été désignés comme un agent de récupération de clés doivent s'inscrire pour un certificat KRA de l'AC. Une fois que tous les certificats KRA nécessaires ont été délivrés, le modèle de certificat KRA devrait être retiré de l'AC.
3. Activer les agents de récupération de clés sur l'AC :
 - a. Connectez-vous en tant qu'administrateur du serveur ou administrateur de l'AC si la séparation des rôles est activée ;
 - b. Dans la console AC, cliquez avec le bouton droit sur le nom d'AC, puis cliquez sur **Propriétés**. Pour activer l'archivage de clés, sur l'onglet **Agents de récupération**, cliquez sur **Archiver la clé** ;
 - c. Par défaut, l'AC utilise un KRA. Cependant, vous devez d'abord sélectionner le certificat KRA pour l'AC en cliquant **Ajouter**, afin de commencer l'archivage ;
 - d. Le système trouve les certificats KRA valides qui ont été émis, puis affiche les certificats KRA disponibles. Ceux-ci sont généralement publiés sur AD DS par une AC d'entreprise lors de l'inscription. Les certificats KRA sont stockés dans le conteneur KRA de la branche Public Key Services de la partition de configuration dans AD DS. Une AC pouvant émettre plusieurs certificats KRA, chaque certificat KRA sera ajouté à l'attribut utilisateur à plusieurs valeurs de l'objet AC ;
 - e. Sélectionnez un certificat, puis cliquez sur **OK**. Assurez-vous d'avoir sélectionné le certificat voulu ;
 - f. Après avoir ajouté un ou plusieurs certificats KRA, cliquez sur **OK**. Le service AC va redémarrer et seuls les certificats KRA traitent au démarrage du service.
4. Configurer les modèles de certificats nécessaires pour l'archivage des clés :
 - a. Dans la console **Modèles de certificats**, cliquez avec le bouton droit sur le modèle de certificat que vous souhaitez activer pour l'archivage des clés, puis cliquez sur **Propriétés** ;
 - b. Pour l'archivage des clés s'applique en permanence à l'AC, dans la boîte de dialogue **Propriétés**, dans l'onglet **Traitement de la demande**, cochez la case **Archiver la clé privée de chiffrement du sujet**. Dans Windows Server 2008 ou une AC de version ultérieure, sélectionnez **Utiliser un algorithme symétrique avancé pour envoyer la clé à l'autorité de certification**.

Étapes pour configurer l'archivage de clé automatique :

1. Configurer le modèle de certificat KRA
2. Les agents de récupération de clés désignés s'inscrivent à un certificat KRA
3. Activer les agents de récupération de clé sur l'autorité de certification
4. Configurer les modèles de certificats nécessaires pour l'archivage des clés

Démonstration : Configuration d'un AC pour l'archivage principal

Étapes de la démonstration

1. Dans **LON-DC1**, ouvrez la console **Autorité de certification** à partir du **Gestionnaire de serveur**. Cliquez avec le bouton droit sur le dossier **Modèles de certificat**, puis cliquez sur **Gérer**.
2. Dans la console **Modèles de certificats**, ouvrez la boîte de dialogue **Propriétés de l'agent de récupération principal**.
3. Dans l'onglet **Conditions d'émission**, désactivez la case à cocher **Approbation du gestionnaire de certificats de l'AC**.
4. Dans l'onglet **Sécurité**, notez que seuls les admins de domaine et les groupes d'admins entreprise ont l'autorisation de faire les inscriptions.
5. Cliquez droit sur le dossier **Modèles de certificats**, puis émettez le modèle **Agent de récupération principal**.
6. Ouvrez la **Microsoft Management Console** qui comprend le composant logiciel enfichable **Certificats** pour l'utilisateur actuel.
7. Utilisez l'**Assistant d'inscription de certificat** pour demander un nouveau certificat et inscrire le certificat KRA.
8. Actualisez la fenêtre de la console, puis affichez le KRA dans le magasin personnel.
9. Sur **LON-DC1**, dans la console **Autorité de certification**, ouvrez la boîte de dialogue **Propriétés ACAdatum**.
10. Dans l'onglet **Agents de récupération**, cliquez sur **Archiver la clé**, puis ajoutez le certificat **Administrateur** en utilisant la boîte de dialogue **Sélection de l'agent de récupération de clé**.
11. Redémarrer **AD CS** lorsque vous y êtes invité.

Testez vos connaissances

| Question | |
|--|--|
| Lorsque vous révoquez un certificat, où est l'empreinte du certificat publié ? | |
| Sélectionnez la réponse correcte. | |
| | Point de distribution de la liste de révocation de certificats (CDP) |
| | Accès aux informations de l'autorité (AIA) |
| | Liste de révocation des certificats (CRL) |
| | AD DS |
| | Service de répondre en ligne |

Testez vos connaissances

| Question | |
|---|---|
| Lesquelles des mesures suivantes devez vous effectuer pour configurer l'archivage principal sur une AC AD CS ? (Choisissez toutes les réponses applicables.) | |
| Sélectionnez la réponse correcte. | |
| | Configurer le modèle de certificat KRA. |
| | Inscrire un utilisateur désigné pour un certificat KRA. |
| | Publier la clé publique KRA en utilisant la stratégie de groupe. |
| | Configurer un agent de récupération sur l'AC. |
| | Configurer les modèles de certificats voulus pour l'archivage des clés. |

Leçon 3

Utilisation de certificats dans un contexte commercial

Les certificats sont très souvent utilisés dans les communications électroniques d'aujourd'hui. Chaque fois que vous ouvrez une URL HTTPS, le chiffrement est effectué par un certificat. En outre, les certificats sont utilisés pour signer numériquement un contenu et le chiffrer, ainsi que pour authentifier un utilisateur ou un périphérique. Dans cette leçon, vous allez en apprendre davantage sur certaines des façons les plus courantes d'utiliser des certificats dans les environnements professionnels.

Objectifs de la leçon

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

- Décrire comment utiliser des certificats pour SSL (Secure Sockets Layer) ;
- Décrire comment utiliser les certificats pour les signatures numériques ;
- Signer numériquement un document ;
- Décrire comment utiliser les certificats pour le chiffrement de contenu ;
- Chiffrer un fichier avec EFS ;
- Décrire comment utiliser les certificats pour l'authentification.

Utilisation des certificats pour SSL

La plupart des sites qui traitent des données sensibles sont protégés par la technologie de sécurité SSL. SSL établit un lien sécurisé et chiffré entre un serveur et un client. Le plus souvent, la connexion s'effectue entre un serveur Web et un navigateur ou un client de messagerie sur un ordinateur client. SSL est communément perçu comme un protocole de sécurité, car il spécifie les algorithmes de chiffrement et les variables nécessaires pour le chiffrement de la connexion. Sécuriser une connexion avec SSL permet de protéger les données, telles que les numéros de carte de crédit, les identifiants de connexion et d'autres données critiques, lors des transferts de données entre un client et un serveur.

- Sécuriser une connexion avec SSL a pour objectif de protéger les données lors de la communication
- Pour SSL, il est nécessaire d'installer un certificat sur le serveur
- Des problèmes d'approbation peuvent survenir
- SSL fonctionne de la manière suivante :
 1. L'utilisateur saisit une URL en HTTPS
 2. Le serveur Web lui envoie son certificat SSL
 3. Le client effectue une vérification du certificat du serveur
 4. Le client génère une clé de chiffrement symétrique
 5. Le client chiffre cette clé avec la clé publique du serveur
 6. Le serveur utilise sa clé privée pour déchiffrer la clé symétrique cryptée

Pour établir une connexion protégée par SSL, le certificat doit être installé sur le serveur. Votre AC interne ou une AC publique peuvent délivrer un certificat pour SSL. Pour les sites Web disponibles sur Internet, il est courant d'avoir un certificat délivré par une AC publique. Ainsi, votre certificat de serveur est largement approuvé par la plupart des navigateurs. Cependant, vous pouvez également utiliser un certificat émis par votre AC locale. Les deux types de certificats peuvent sécuriser une connexion, mais la plupart des navigateurs qui se connectent sur le site Web où le certificat est installé ne font pas confiance à un certificat délivré en interne. Ce manque de confiance n'empêche pas le certificat de sécuriser la connexion, mais un message d'avertissement est généré lorsque le navigateur se connecte à votre site Web. La plupart des entreprises veulent éviter cette situation, c'est pourquoi la plupart des sites Web sécurisés sur Internet utilisent des certificats publics. Les navigateurs Internet ont avec une liste préinstallée des AC de confiance et ils la stockent dans la boutique d'AC racines de confiance.



Remarque : l'achat d'un certificat SSL public ne garantit pas que tous les clients feront automatiquement confiance au certificat. Assurez-vous que vous choisissez un fournisseur de certificat digne de confiance à l'échelle mondiale et dont les certificats d'AC sont présents dans les magasins d'AC racines de confiance préinstallés dans les clients.

Sécurisation d'une connexion avec un certificat SSL

Après avoir été délivré, chaque certificat a une paire de clés qui lui est associée. La paire de clés se compose d'une clé publique et d'une clé privée. Ces clés fonctionnent ensemble dans un processus de chiffrement. Les données qui sont chiffrées avec une clé publique ne peuvent être déchiffrées qu'avec une clé privée correspondante, et inversement. Chaque paire de clés est unique. En plus d'avoir une paire de clés, chaque certificat a également son nom d'objet qui spécifie l'identité du serveur ou du site Web sur lequel il est installé.

Lorsqu'un navigateur Web se connecte à un site Web sécurisé, le client et le serveur établissent une connexion SSL. La connexion SSL s'établit durant le *protocole de transfert SSL*. Ce processus de protocole de transfert se produit comme décrit ci-dessous :

1. L'utilisateur saisit ou clique sur une adresse URL HTTPS dans le navigateur Web ;
2. Le logiciel du navigateur Web se connecte à un site Web et demande au serveur de s'identifier ;
3. Le serveur Web envoie son certificat SSL. Avec le certificat, le serveur donne également sa clé publique au client ;
4. Le client effectue une vérification du certificat du serveur. Il vérifie le nom du sujet et le compare avec l'URL qui lui permet d'accéder au serveur. En outre, il vérifie si le certificat est délivré par l'une des AC du magasin d'AC racines de confiance. Il vérifie également l'emplacement des points de distribution de liste de révocation de certificats (CDP) pour vérifier si le certificat est révoqué ;
5. Si toutes les vérifications sont concluantes, le client génère une clé de chiffrement symétrique. Le client et le serveur utilisent une clé symétrique pour déchiffrer les données, car les paires de clés publiques et privées ne sont pas très efficaces pour chiffrer et déchiffrer de grandes quantités de données. Le client génère une clé symétrique, puis crypte cette clé avec la clé publique du serveur. Puis, le client envoie la clé symétrique chiffrée au serveur ;
6. Le serveur utilise sa clé privée pour déchiffrer la clé symétrique cryptée. Maintenant, le serveur et le client ont une clé symétrique et le transfert sécurisé des données peut commencer.

Pendant ce processus, le serveur prouve son identité au client en présentant son certificat SSL. Si le nom du serveur dans le certificat correspond à l'URL que le client a demandé et le certificat a été délivré par une CA de confiance, le client croit que le serveur a une identité valide. En outre, le client a vérifié la validité du certificat grâce à sa durée de vie et l'emplacement CDP des CRL. Cela signifie que l'établissement d'une session SSL ne concerne pas seulement le chiffrement, mais aussi une authentification du serveur au client.



Remarque : l'authentification du client ne fait pas partie du protocole de transfert SSL classique. Cela signifie que le client n'a pas à fournir son identité au serveur. Cependant, vous pouvez également configurer votre site Web pour exiger l'authentification du client. Le client peut lui aussi utiliser un certificat pour s'authentifier auprès du serveur.

Configuration d'un certificat SSL sur un serveur

Pour utiliser SSL afin de protéger la communication entre un serveur et un client, vous devez installer le certificat sur le serveur. Vous pouvez l'installer de plusieurs façons différentes. Cependant, avant d'installer le certificat sur le serveur, vous devez définir le ou les noms que le certificat prend en charge. Par exemple, si vous voulez protéger votre site Web sur l'URL www.adatum.com, alors vous avez besoin de délivrer le certificat avec le nom commun www.adatum.com.



Remarque : un certificat n'est délivré que pour un nom de domaine et non pas pour une URL entière. Par exemple, un certificat avec le nom commun www.adatum.com protégera également l'URL www.adatum.com/sales ou une URL similaire.

Dans certains scénarios, vous devez avoir plus d'un nom de domaine sur le même serveur. Microsoft Exchange Server en est un exemple typique. Un certificat installé sur le serveur doit prendre en charge son nom public, par exemple, mail.adatum.com et autodiscover.adatum.com. Comme les deux noms sont associés avec le même site Web et que vous ne pouvez pas affecter plus d'un certificat à un seul site Web, vous devez utiliser un certificat qui prend en charge plusieurs noms, aussi connus sous *autres noms de l'objet*. Cela signifie que vous avez un certificat avec plus d'un nom. Ces certificats peuvent être émis à la fois par une AC interne sur Windows Server 2016 et des AC publiques.



Remarque : au lieu d'avoir un certificat avec plusieurs noms sur le même domaine, vous pouvez également émettre un certificat générique avec un nom commun, par exemple : *.adatum.com. Ce certificat sera valable pour tous les noms avec le suffixe de domaine adatum.com. Si vous choisissez d'utiliser un certificat générique, vous devez prendre des précautions supplémentaires pour sécuriser la clé privée associée. Si la clé privée devait être compromise, elle pourrait être utilisée pour déchiffrer le trafic sensible avec un hôte légitime ou pour usurper l'identité d'un hôte de confiance dans le domaine.

Pour obtenir un certificat SSL auprès d'une AC interne, vous pouvez utiliser les approches suivantes :

- Utiliser la console d'AC sur le serveur pour faire une demande de certificat à l'AC. En utilisant cette approche, vous pouvez spécifier des attributs supplémentaires pour le certificat, tels que le modèle de certificat ou un autre nom de l'objet. Cependant, après l'installation du certificat, vous devez l'attribuer au site Web approprié manuellement ;
- Utiliser la console IIS. Dans la console IIS, vous faites une demande de certificat directement à l'AC. Toutefois, lorsque vous utilisez cette approche, vous n'êtes pas en mesure de choisir un modèle de certificat (l'AC recherche un modèle de serveur Web par défaut) et vous ne pouvez pas spécifier un autre nom de l'objet. Cependant, il s'agit de la façon la plus simple d'installer un certificat sur le site Web ;
- Utiliser l'inscription par le Web de l'AC. Cette approche est appropriée si vous souhaitez délivrer un certificat à un serveur qui ne fait pas partie de votre domaine. Pour ce type d'inscription, vous devez d'abord faire un fichier de demande de certificat (.req), puis soumettre cette demande sur la page d'inscription par le Web de l'AC. Là, vous pouvez également spécifier le modèle de certificat et ajouter d'autres noms de l'objet, si nécessaire.

Si vous achetez un certificat SSL de confiance à une AC publique, la procédure est quelque peu différente. Après avoir choisi un fournisseur de certificats, vous devrez d'abord passer par une procédure administrative pour prouver l'identité de votre entreprise et la propriété du nom de domaine. Puis, vous devez créer une demande de signature de certificat (CSR) sur votre serveur. Cette CSR crée la clé privée et un fichier de données CSR, qui est essentiellement une demande de certificat. Vous envoyez ensuite la CSR à l'émetteur du certificat. L'AC utilise le fichier de données CSR afin de créer une clé publique pour

correspondre à votre clé privée sans compromettre la clé elle-même. L'AC ne reconnaît jamais la clé privée dans ce scénario ou tout scénario précédent pour émettre un certificat, sauf lorsque l'archivage des clés est configuré. Cependant, la clé est tout de même cryptée.

Utilisation de certificats pour les signatures numériques

En plus de protéger les communications, les certificats peuvent également protéger le contenu et vérifier l'identité de l'auteur du contenu.

Lorsque vous recevez un message avec un contenu confidentiel, il est important de savoir que vous pouvez être sûr de deux choses.

Premièrement, vous pouvez être sûr que le message n'a pas été modifié en transit.

Deuxièmement, vous pouvez être sûr que l'identité de l'auteur est vérifiable.

Vous pouvez utiliser des certificats pour protéger et vérifier le contenu ainsi que vérifier l'identité d'un auteur. Il est fréquent qu'un utilisateur signe numériquement un document.

- Les signatures numériques garantissent que :
 - Le contenu n'est pas modifié pendant le transport
 - L'identité de l'auteur est vérifiable
- Les signatures numériques fonctionnent de la manière suivante :
 1. Quand un auteur signe numériquement un document ou un message, le système d'exploitation de son ordinateur crée une synthèse de chiffrement du message
 2. La synthèse de chiffrement est ensuite chiffrée à l'aide de la clé privée de l'auteur et ajoutée à la fin du document ou du message
 3. Le destinataire utilise la clé publique de l'auteur pour déchiffrer la synthèse de chiffrement et la comparer à la synthèse de chiffrement créée sur l'ordinateur du destinataire
- Pour utiliser les signatures numériques, les utilisateurs doivent posséder un certificat basé sur un modèle **Utilisateur**

Les signatures numériques

Quand une personne signe numériquement un document dans une application, comme dans un e-mail, un document Microsoft Word ou similaire, l'utilisateur confirme que le document est *authentique*. Dans ce contexte, authentique signifie que le créateur du document est connu et que le document n'a pas modifié d'une quelconque façon depuis que la personne l'a créé et signé.

Une infrastructure à clé publique (PKI) peut atteindre ce niveau de sécurité. Par rapport au serveur Web de la rubrique précédente, un utilisateur peut également avoir un certificat avec une paire de clés publique et privée. Ce certificat est utilisé dans le processus de signature numérique.

Quand un auteur signe numériquement un document ou un message, le système d'exploitation de son ordinateur crée un algorithme de chiffrement du message qui varie d'un nombre 128 bits à un nombre 256 bits. Ce nombre est généré par l'exécution de l'ensemble du message dans un algorithme de hachage. Ce nombre est ensuite chiffré à l'aide de la clé privée de l'auteur et il est ajouté à la fin du document ou un message.

Lorsque le document ou le message atteint le destinataire, il devra passer par le même algorithme de hachage que lors de la signature numérique. En outre, le destinataire utilise la clé publique de l'auteur pour déchiffrer le condensé qui est ajouté au message. Après avoir été déchiffré, il est comparé à au condensé que le destinataire a généré. S'ils sont identiques, le document ou le message n'a pas été modifié pendant le transport. En outre, si le destinataire est capable de déchiffrer le condensé en utilisant la clé publique de l'auteur, cela signifie que le condensé a été chiffré en utilisant la clé privée de l'auteur, ce qui confirme l'identité de l'auteur. À la fin, le destinataire vérifie également le certificat qui a été utilisé pour prouver l'identité de l'auteur. Au cours de cette vérification, la période de validité, la CRL, le nom du sujet et la confiance de la chaîne de certificats sont également vérifiés.

Mise en œuvre des signatures numériques

Pour mettre en œuvre des signatures numériques dans les communications internes, vous devez délivrer des certificats se basant sur le modèle **Utilisateur**. Vous devez délivrer des certificats à tous les utilisateurs qui utilisent des signatures numériques. Vous pouvez émettre le certificat sans aucune intervention de l'utilisateur si vous utilisez l'inscription automatique. En outre, les utilisateurs doivent utiliser une

application qui prend en charge la signature de contenu. Par exemple, vous pouvez utiliser par défaut des signatures numériques dans Microsoft Word et Microsoft Outlook.

Les signatures numériques sont prêtes à l'utilisation dès que l'application a émis et configuré le certificat. Toutefois, si vous voulez envoyer du contenu signé numériquement en dehors de votre organisation, vous pouvez rencontrer des problèmes de confiance de l'AC. Dans ce scénario, un destinataire n'est pas dans le même domaine AD DS que l'auteur, donc il ne fait pas confiance à l'AC qui a émis le certificat pour la signature numérique. Bien que ce genre de signature numérique sera toujours valide pour protéger du contenu, une application utilisée va probablement générer un avertissement du côté destinataire.

Si vous avez besoin d'envoyer du contenu signé numériquement à des destinataires en dehors de votre organisation, nous vous recommandons d'acheter des certificats d'AC bénéficiant d'une confiance à l'échelle mondiale.

Démonstration : Signature d'un document numérique

Dans cette démonstration, vous verrez comment signer un document numériquement.

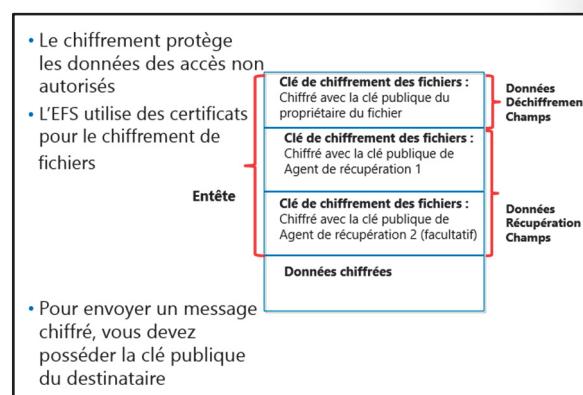
Étapes de la démonstration

- Sur **LON-CL1**, ouvrez l'interface de ligne de commande **Windows PowerShell** et exécutez **mmc.exe**.
- Ajoutez le composant logiciel enfichable **Certificats**, puis choisissez **Mon compte d'utilisateur**.
- Démarrez l'**Assistant Demander un nouveau certificat**, puis inscrivez-vous pour un certificat **Utilisateur**.
- Ouvrez Word 2016. Saisissez du texte dans un document vierge, puis enregistrez le document.
- Cliquez sur **Insérer** dans le ruban, puis insérez la ligne de signature.
- Remplissez les champs de signature avec vos données.
- Cliquez droit sur la ligne de signature, puis choisissez de signer le document.
- Choisissez le certificat.
- Signez le document.
- Assurez-vous que le document ne peut plus être modifié.

Utilisation de certificats pour le chiffrement de contenu

Bien que les signatures numériques peuvent vérifier l'identité d'un auteur et assurer la cohérence du contenu, elles ne peuvent pas protéger le contenu lui-même. Par exemple, si quelqu'un intercepte un message signé numériquement, il peut encore lire son contenu. Cependant, la tentative de modification du contenu sera détectée, car la vérification de la signature numérique échouera.

Si vous souhaitez protéger le contenu du document pour le rendre impossible à lire, vous devez utiliser le chiffrement.



Les systèmes d'exploitation Microsoft Windows prennent en charge un chiffrement basé sur des fichiers appelé système de fichiers (EFS). En outre, Outlook prend en charge le chiffrement des messages électroniques.

EFS.

Pour chiffrer un fichier en utilisant EFS, vous devez avoir un certificat EFS émis. Comme d'autres certificats, ce certificat fournit également une paire de clés privée et publique. Cependant, ces clés ne sont pas utilisées directement pour chiffrer ou déchiffrer le contenu. En effet, les algorithmes utilisant un *chiffrement asymétrique*, où une clé est utilisée pour le chiffrement et une autre pour le déchiffrement, sont inefficaces. Ces algorithmes sont beaucoup plus lents que les algorithmes qui utilisent la même clé pour le chiffrement et le déchiffrement, appelés *chiffrement symétrique*. EFS utilise une approche hybride pour surmonter ce problème.

Lorsque l'utilisateur sélectionne l'option pour chiffrer un fichier, l'ordinateur local génère une clé symétrique, qui est également connue comme la clé de cryptage de fichier, et utilise cette clé pour chiffrer le fichier. Une fois le fichier chiffré, le système utilise la clé publique de l'utilisateur pour crypter la clé symétrique, puis la stocke dans l'en-tête du fichier.

Lorsque l'utilisateur qui a initialement chiffré le fichier veut déchiffrer le fichier et accéder à son contenu, l'ordinateur local accède à la clé privée de l'utilisateur et déchiffre d'abord la clé symétrique de l'en-tête du fichier, qui est aussi appelé champ de déchiffrement des données (DDF). Après cela, la clé symétrique est utilisée pour déchiffrer le contenu.

Cela fonctionne bien si le propriétaire du fichier est la seule personne ayant accès au fichier chiffré. Cependant, il existe des scénarios dans lesquels vous voulez partager des fichiers chiffrés avec d'autres utilisateurs. Il pourrait être difficile ou impossible de déchiffrer le fichier avant de le partager avec d'autres personnes. En outre, si l'utilisateur qui a initialement chiffré le fichier perd sa clé privée, le fichier pourrait être inaccessible à quiconque.

Pour résoudre ce problème, un champ de récupération des données (DRF) est défini pour chaque fichier crypté avec EFS. Lorsque vous configurez EFS pour une utilisation locale ou dans un domaine AD DS, le rôle d'agent de récupération de données (DRA) est défini par défaut et affecté à l'administrateur local ou de domaine. Le DRA est en fait un certificat avec une paire de clés qui peut être utilisée pour décrypter les fichiers dans le cas où la clé privée de l'utilisateur d'origine n'est plus accessible pour une raison quelconque.

Lorsqu'un utilisateur chiffre le fichier avec EFS, sa clé publique est utilisée pour chiffrer la clé symétrique, et la clé cryptée est ensuite stockée dans le DDF, dans l'en-tête du fichier. Au même moment, la clé publique du DRA est utilisée pour chiffrer la clé symétrique une fois de plus. La clé symétrique est chiffrée avec une clé publique du DRA et est ensuite stockée dans le DDF, dans l'en-tête du fichier. S'il y a plus d'un DRA défini, alors la clé symétrique est chiffrée avec les clés publiques de tous les DRA. Ensuite, si l'utilisateur qui a initialement chiffré le fichier n'a pas de clé privée disponible pour une raison quelconque, le DRA peut utiliser sa clé privée pour déchiffrer la clé symétrique du DRF et déchiffrer le fichier.

 **Remarque :** en alternative au DRA, vous pouvez également utiliser l'agent de récupération de clé (KRA) pour récupérer la clé privée d'un utilisateur à partir d'une base de données AC, si l'archivage des clés est activé pour le modèle de certificat EFS sur l'AC.

Lorsqu'un utilisateur souhaite partager un fichier chiffré avec d'autres utilisateurs, une approche similaire à l'utilisation du DRA est réalisée. Lorsque le partage EFS est sélectionné, le propriétaire du fichier doit sélectionner un certificat venant de chacun des utilisateurs qui partagent le fichier. Ces certificats peuvent être publiés sur AD DS et pris à partir de là. Lorsque le certificat est sélectionné, la clé publique de l'utilisateur destinataire est prise, et la clé symétrique est chiffrée et ajoutée à l'en-tête du fichier.

À ce stade, l'autre utilisateur peut également accéder au contenu chiffré de l'EFS, car les utilisateurs peuvent utiliser leurs clés privées pour déchiffrer la clé symétrique.



Remarque : un certificat de récupération de données peut également être défini pour le chiffrement de lecteur BitLocker. Bien qu'un modèle de certificat d'Agent de récupération de données BitLocker ne soit pas prédéfini dans AD CS, vous pouvez copier le modèle KRA puis ajouter de nouvelles stratégies d'application pour le chiffrement BitLocker et la récupération de données en utilisant les identifiants d'objets suivants :

- Chiffrement de lecteur BitLocker = 1.3.6.1.4.1.311.67.1.1 ;
- Agent de récupération de données BitLocker = 1.3.6.1.4.1.311.67.1.2.

Après avoir inscrit un utilisateur pour ce certificat, vous pouvez définir un agent de récupération au niveau de domaine si vous utilisez des paramètres de stratégie de groupe dans le chemin suivant : **Configuration ordinateur\Paramètres Windows\Sécurité\Stratégies clé publique\Chiffrement de lecteur BitLocker**. Nous vous recommandons d'utiliser BitLocker pour le chiffrement complet du lecteur.

Chiffrement des e-mails

En plus d'utiliser EFS pour chiffrer des fichiers et BitLocker pour chiffrer des disques, vous pouvez également utiliser des certificats pour chiffrer les e-mails. Cependant, le chiffrement des e-mails est un peu plus compliqué que celui d'une signature numérique. Même si vous pouvez envoyer des e-mails signés numériquement à tout le monde, vous ne pouvez pas faire la même chose avec un e-mail chiffré. Pour être en mesure d'envoyer un e-mail chiffré à quelqu'un doté d'une PKI, vous devez posséder la clé publique de la paire de clés du destinataire. Dans l'environnement AD DS, où Exchange Server est utilisé comme un système de messagerie, vous pouvez publier les clés publiques de tous les utilisateurs de boîte aux lettres sur une liste d'adresses globale (GAL). Quand vous faites cela, les applications telles qu'Outlook peuvent facilement récupérer la clé publique du destinataire depuis la LAG si vous envoyez des e-mails chiffrés. Lorsque vous envoyez un e-mail crypté à un utilisateur interne, votre application de messagerie récupère la clé publique du destinataire depuis la LAG, chiffre l'e-mail avec elle, puis envoie l'e-mail. Une fois l'e-mail reçu, le destinataire utilise sa clé privée du certificat pour déchiffrer le contenu de l'e-mail.

Cependant, l'envoi d'un e-mail crypté aux utilisateurs externes est plus compliqué. Alors que les clés publiques des utilisateurs internes peuvent être publiées sur AD DS ou la LAG, vous ne pouvez pas faire la même chose avec des utilisateurs externes. Pour envoyer des e-mails chiffrés à un utilisateur externe, vous devez d'abord obtenir sa clé publique. Vous pouvez obtenir la clé si l'utilisateur externe vous l'envoie dans un fichier.cer, que vous pouvez importer dans votre carnet d'adresses local. En outre, si un utilisateur externe vous envoie un e-mail signé numériquement, alors vous obtiendrez sa clé publique, que vous pouvez également importer dans votre carnet d'adresses local. Une fois la clé publique importée dans votre carnet d'adresses, vous pouvez l'utiliser pour envoyer des e-mails chiffrés aux utilisateurs externes.



Remarque : Si vous voulez fournir de l'authenticité, une cohérence du contenu et une protection, alors vous pouvez envoyer un message qui est à la fois chiffré et signé numériquement.

Démonstration : chiffrer un fichier avec EFS (Encrypting File System)

Dans cette démonstration, vous allez apprendre à chiffrer un fichier à l'aide d'EFS.

Étapes de la démonstration

- Ouvrez les propriétés avancées du document Word que vous avez créé dans la démonstration précédente.
- Choisissez Chiffrer le fichier uniquement.**
- Déplacer le document que vous avez chiffré vers le dossier **C:\Users\Public\Documents**.
- Déconnectez-vous de **LON-CLI**.
- Connectez-vous en tant qu'**adatum\Administrateur**.
- Essayez d'accéder au document chiffré dans le dossier **C:\Users\Public\Documents**.

Utilisation de certificats pour l'authentification

Outre l'utilisation de certificats pour la signature numérique et le chiffrement, ils sont souvent utilisés pour l'authentification des utilisateurs et des appareils. Aussi, les certificats sont généralement utilisés pour l'authentification d'accès réseau, car ils fournissent une sécurité élevée pour authentifier les utilisateurs et les ordinateurs et vous évitent d'avoir recours à des méthodes d'authentification basées sur un mot de passe, moins sécurisées.

Par exemple, vous pouvez utiliser des certificats sur les ordinateurs qui sont autorisés à accéder à votre réseau à l'aide d'une connexion par un réseau privé virtuel (VPN). Cela vous permet d'authentifier les périphériques et les utilisateurs. Un utilisateur peut s'authentifier avec un nom d'utilisateur et mot de passe, tandis qu'un appareil s'authentifie avec un certificat. Les appareils qui ne disposent pas du certificat de votre organisation ne seront pas autorisés à se connecter, même si un utilisateur est autorisé. Cette approche améliore la sécurité.

Deux méthodes d'authentification l'accès au réseau utilisent des certificats : le protocole TLS-EAP (Extensible Authentication Protocol-Transport Layer Security) et le protocole PEAP (Protected Extensible Authentication Protocol). Les deux méthodes d'authentification utilisent toujours des certificats pour l'authentification du serveur. En fonction du type d'authentification configuré avec la méthode d'authentification, des certificats peuvent être utilisés pour l'authentification d'utilisateurs et d'ordinateurs clients. Vous devez utiliser l'authentification basée sur les certificats pour les connexions VPN basées sur le protocole L2TP (Layer Two Tunneling Protocol), par-dessus la sécurité du protocole Internet (IPsec).

Les certificats sont également utilisés pour authentifier les clients lorsque la protection d'accès réseau (NAP) est mise en œuvre avec IPsec. Dans ce scénario, l'Autorité HRA (Health Registration Authority) délivre un certificat à un ordinateur qui répond à la stratégie de contrôle d'intégrité pour établir une connexion IPsec.

IIS dans Windows Server 2016 prend également en charge l'authentification par certificat pour les utilisateurs. Par exemple, vous pouvez configurer Microsoft Outlook Web App pour utiliser l'authentification basée sur les certificats.

Vous pouvez utiliser des certificats dans des scénarios pour authentifier l'utilisateur et l'appareil et également pour accéder au réseau et à l'application, tels que :

- VPN L2TP/IPsec
- EAP-TLS
- PEAP
- NAP avec IPsec
- Outlook Web App
- Authentification de périphérique portable

Enfin, vous pouvez également utiliser des certificats pour l'authentification d'un périphérique portable. Certains types d'appareils mobiles peuvent installer les certificats et les utiliser pour authentifier un utilisateur ou un périphérique à la ressource réseau.

Testez vos connaissances

| Question | |
|--|---|
| Lesquelles des affirmations suivantes sont correctes au sujet de l'utilisation de certificats dans un environnement commercial ? (Choisissez toutes les réponses applicables.) | |
| Sélectionnez la réponse correcte. | |
| | Les certificats peuvent être utilisés pour crypter le trafic HTTP entre un serveur Web et le navigateur. |
| | Les certificats peuvent être utilisés pour signer numériquement les documents. |
| | Les documents signés numériquement sont invalidés si les contenus sont modifiés. |
| | Pour envoyer un e-mail crypté à un destinataire externe qui ne fait pas partie de votre PKI interne, vous devez utiliser un certificat de cryptage délivré par une AC publique. |
| | Les fichiers cryptés avec Encrypting File System (EFS) peuvent être lus seulement par la personne qui a crypté le fichier en premier. |

Testez vos connaissances

| Question | |
|---|--|
| Vous êtes l'administrateur AD CS pour A. Datum. Vous voulez permettre à vos utilisateurs AD DS d'effectuer la signature numérique et le cryptage en utilisant des certificats à partir de votre PKI interne. Lesquelles des étapes suivantes sont nécessaires ? | |
| Sélectionnez la réponse correcte. | |
| | Activer un agent de récupération de clés. |
| | Activer un agent de récupération de données. |
| | Publier le modèle de certificat Utilisateur et configurer les groupes des utilisateurs souhaités pour une inscription automatique. |
| | Activer EFS sur les ordinateurs de domaine AD DS en utilisant la stratégie de groupe. |
| | Mettre à niveau tous les ordinateurs de domaine AD DS vers Windows Server 2016 ou Windows 10. |

Leçon 4

Mise en œuvre et gestion des cartes à puce

L'authentification par carte à puce est une approche commune dans les scénarios où vous voulez avoir une authentification multifactorielle pour améliorer la sécurité. En outre, les cartes à puce sont utilisées pour stocker les certificats pour les signatures numériques et le chiffrement. Pour mettre en œuvre une infrastructure de carte à puce, vous devez comprendre comment elles fonctionnent et comment configurer des certificats pour les cartes à puce. Cette leçon décrit la mise en œuvre et la gestion d'une infrastructure de carte à puce.

Objectifs de la leçon

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

- Décrire une carte à puce ;
- Décrire le fonctionnement d'une authentification par carte à puce ;
- Décrire une carte à puce virtuelle ;
- Décrire comment inscrire des certificats pour les cartes à puce ;
- Décrire la gestion des cartes à puce.

Qu'est-ce qu'une carte à puce ?

Le terme *carte à puce* est utilisé pour décrire une classe d'appareils de la taille d'une carte de crédit ou inférieure, dotée des capacités différentes : les cartes à valeur stockée, les cartes sans contact et les cartes à circuit intégré (IC). Toutes ces cartes ont des fonctions différentes, depuis les cartes à bande magnétique communes, utilisées comme cartes de crédit, de débit et pour les ATM (guichet automatique de banque). La carte à puce présente de l'intérêt pour l'ordinateur personnel et les systèmes d'exploitation Windows, car elle peut effectuer des opérations sophistiquées telles que les signatures numériques et les échanges de clés.

- Une carte à puce est un ordinateur miniature, avec des capacités de stockage et de traitement limitées, intégré à une carte en plastique de la taille d'une carte de crédit
- Les cartes à puce :
 - Offrent plusieurs options d'authentification multifactorielle
 - Offrent une sécurité renforcée pour les mots de passe
- Les cartes à puce doivent être utilisées avec un code confidentiel

Une carte à puce est fondamentalement un mini-ordinateur avec des capacités de stockage et de traitement limitées qui est intégré dans une carte en plastique, similaire en taille et en forme à une carte de crédit. Le circuit dans une carte à puce est alimenté par un lecteur de carte à puce après que la carte est insérée dans le lecteur. La communication de données entre une carte à puce et une application s'exécutant sur un ordinateur est réalisée sur une interface série semi-duplex qui est gérée par le lecteur de carte à puce et son pilote de périphérique associé. Les lecteurs de cartes à puce sont disponibles dans une large gamme de facteurs de forme et peuvent se connecter à un ordinateur en utilisant un ordinateur personnel en utilisant une interface PCMCIA (Personal Computer Memory Card International Association) ou de bus USB. Les lecteurs de cartes à puce sont souvent intégrés dans les ordinateurs portables.

Les cartes à puce offrent une sécurité renforcée sur les mots de passe, car il est beaucoup plus difficile pour un utilisateur non autorisé d'acquérir et de maintenir un accès au système. En outre, l'accès à un système protégé par une carte à puce nécessite qu'un utilisateur possède une carte valide et connaisse le code confidentiel (PIN) qui donne accès à cette carte. Par défaut, une seule copie d'une carte à puce

existe, de sorte qu'une seule personne à la fois peut utiliser les identifiants de connexion. En outre, les utilisateurs remarqueront rapidement si leur carte est perdue ou volée, surtout quand leur carte est également utilisée pour l'accès physique aux portes ou d'autres fonctions. Ceci réduit considérablement le risque de vol des identifiants par rapport aux mots de passe.

Comment fonctionne l'authentification par carte à puce ?

L'objectif principal des cartes à puce dans les environnements Windows est d'effectuer une authentification. Vous pouvez utiliser des cartes à puce pour l'authentification à un domaine AD DS. Les cartes à puce ne peuvent pas être utilisées pour se connecter localement aux ordinateurs qui ne sont pas joints au domaine.

Lors de la connexion à AD DS, les cartes à puce peuvent être utilisées des trois façons suivantes :

- Connexion interactive à AD DS en utilisant le protocole Kerberos et un certificat ;
- Authentification client en utilisant un certificat qui correspond à un compte stocké dans AD DS ;
- Connexion à distance qui utilise un certificat avec le protocole EAP-TLS pour authentifier un utilisateur distant à un compte stocké dans AD DS.

- Les cartes à puce peuvent être utilisées pour :
 - La connexion interactive à AD DS
 - L'authentification du client
 - La connexion à distance
 - La connexion hors ligne
- La connexion interactive étape par étape :
 1. La demande de connexion est transmise à la LSA, puis transférée vers le package Kerberos
 2. KDC vérifie le certificat
 3. KDC vérifie la signature numérique sur le service d'authentification
 4. KDC effectue une requête AD DS pour localiser le compte d'utilisateur
 5. KDC génère une clé de chiffrement aléatoire pour chiffrer le TGT
 6. KDC signe la réponse avec sa clé privée et l'envoie à l'utilisateur

Connexion interactive avec des cartes à puce

La connexion interactive est le scénario d'utilisation de la carte à puce le plus courant. Elle est lancée lorsqu'un utilisateur met la carte à puce dans un lecteur de cartes à puce. Le processus généré est similaire à ce qu'il se passe lorsqu'un utilisateur appuie sur Ctrl + Alt + Suppr. Les systèmes d'exploitation Windows inviteront l'utilisateur à indiquer le code PIN de la carte à puce. Le code PIN de la carte à puce est un moyen d'authentifier un utilisateur à la carte à puce et non à un domaine. Après que le code PIN est saisi et accepté, une clé publique d'un certificat stocké sur la carte à puce est utilisée pour authentifier le domaine en utilisant le protocole Kerberos et son la PKINIT (Public Key Cryptography for Initial Authentication) associée dans l'extension Kerberos.

Une fois qu'un utilisateur saisit un code PIN, le système d'exploitation lance une séquence d'actions pour déterminer si l'utilisateur peut être identifié et authentifié sur la base des informations d'identification que l'utilisateur a fournies lors du processus d'authentification à deux facteurs (PIN et carte à puce). Ce procédé est décrit dans les étapes suivantes :

1. La demande d'inscription va en premier à l'autorité de sécurité locale (LSA) qui la transmet au package d'authentification Kerberos s'exécutant sur le client. Le package Kerberos envoie une demande de service d'authentification (AS) au Centre de distribution de clés (KDC) sur un contrôleur de domaine pour demander l'authentification et un ticket TGT (ticket-granting ticket). Dans le cadre de la demande de service d'authentification, le package Kerberos côté client comprend le certificat de l'utilisateur extrait de la carte à puce dans les champs de données de préauthentification de la demande AS. Un authenticateur, qui est inclus dans les champs de données de préauthentification, est signé numériquement par la clé privée de l'utilisateur. Le KDC peut alors vérifier la demande AS qui provient du titulaire du certificat d'accompagnement.
2. Avant la réponse du KDC à la demande de service d'authentification, il vérifie la validité du certificat. Il vérifie si une AC racine de confiance a délivré le certificat sur la carte à puce et il vérifie l'ensemble de la chaîne de certificats. Il vérifie également les emplacements CRL et AIA et que l'AC émettrice est

- autorisée à délivrer des certificats dont l'information de nom peut être utilisée pour l'authentification dans le domaine.
3. Quand un certificat est vérifié, le KDC procède à la vérification de la signature numérique sur la demande de service d'authentification. Cela se fait à l'aide de la clé publique du certificat de l'utilisateur. Parce que la carte à puce stocke les clés privée et publique d'un utilisateur et que l'utilisateur doit entrer un code PIN pour accéder à une clé privée et l'utiliser pour signer les demandes, si la clé publique correspond à la clé privée dans la signature, la demande est légitime. Après cela, l'horodatage est vérifié sur la demande de service d'authentification pour vérifier que la demande ne fait pas partie d'une attaque par relecture.
 4. Lorsque tous ces contrôles sont effectués avec succès, KDC effectue une requête AD DS pour localiser les informations du compte utilisateur. Le compte utilisateur est situé en se basant sur un nom d'utilisateur principal fourni par le nom du sujet du certificat se trouvant sur la carte à puce. Les informations de compte que le KDC extrait d'AD DS sont ensuite utilisées pour concevoir un TGT. Le TGT comprend l'identifiant de sécurité (SID) de l'utilisateur, les SID pour tous les groupes de domaine auxquels l'utilisateur appartient et potentiellement les SID pour tous les groupes universels dont l'utilisateur est membre, dans un environnement simple ou multidomaine.
 5. Après la conception du TGT, le KDC génère une clé de chiffrement aléatoire pour chiffrer le TGT. Quand il chiffre le TGT, le KDC utilise la clé publique de l'utilisateur pour chiffrer cette clé de chiffrement aléatoire. Cette clé chiffrée est incluse dans le champ de données de préauthentification de la réponse du KDC à l'utilisateur.
 6. Le KDC signe la réponse avec sa clé privée et l'envoie à l'utilisateur. L'utilisateur effectue les contrôles nécessaires sur la réponse du KDC, puis utilise sa clé privée pour d'abord déchiffrer la clé aléatoire à partir du champ de données de préauthentification. Une fois que le client obtient la clé, il l'utilise pour déchiffrer le TGT. Une fois en possession du TGT, le protocole Kerberos standard est utilisé pour demander des tickets au service d'accord de tickets pour d'autres domaines de ressources.

Connexion hors ligne avec les cartes à puce

Si un utilisateur utilise un ordinateur portable et une carte à puce pour l'authentification, il aura probablement besoin de se connecter à l'ordinateur même quand il n'est pas connecté à un réseau. Cette situation est semblable à celle d'une connexion hors-ligne avec un nom d'utilisateur et un mot de passe à partir d'un domaine AD DS. Lorsqu'un utilisateur se connecte à un ordinateur hors connexion avec un nom d'utilisateur et un mot de passe à partir d'un domaine AD DS, le système d'exploitation récupère le hachage du mot de passe de domaine qui est stocké dans la LSA et le compare avec le hachage du mot de passe qui a été fourni lors de la connexion.

Cependant, si l'utilisateur se connecte avec une carte à puce, une procédure différente a lieu. Le système d'exploitation utilise alors la clé privée de l'utilisateur venant de la carte à puce pour déchiffrer les informations d'identification supplémentaires qui ont été chiffrées à l'origine en utilisant la clé publique de l'utilisateur.

Qu'est-ce qu'une carte à puce virtuelle ?

Malgré les nombreux avantages des cartes à puce, la mise en œuvre d'une infrastructure de carte à puce est parfois coûteuse. Pour implémenter des cartes à puce, les entreprises doivent acheter du matériel, y compris les cartes à puce et les lecteurs de cartes à puce. Dans certains cas, ce coût empêche le déploiement de l'authentification multifactorielle.

Pour résoudre ces problèmes, Windows Server 2012 AD CS introduit une technologie qui assure la sécurité des cartes à puce, tout en réduisant les coûts matériels et de soutien. Les *cartes à puce virtuelle* (VSC) sont une combinaison de matériel, de logiciels et microprogrammes qui implémentent la même interface, comme une carte à puce physique, mais elles ne sont pas nécessairement limitées à l'intégrité physique du même facteur de forme. Les VSC peuvent être entièrement mises en œuvre dans un logiciel, mais elles utilisent plus souvent les capacités cryptographiques de la puce du module de plate-forme sécurisée (Trusted Platform) qui est présente sur la plupart des cartes mères d'ordinateur produites depuis quelques années.

Comme la puce est déjà dans l'ordinateur, il n'y a pas besoin d'acheter de cartes à puce ni de lecteurs de cartes à puce. Contrairement aux cartes à puce traditionnelles, où un utilisateur possède physiquement la carte, la puce TPM sur la carte mère agit comme une carte à puce qui est toujours insérée. Lorsque vous utilisez cette approche, vous pouvez obtenir un résultat similaire à celui de la méthode d'authentification par carte à puce physique. Les utilisateurs doivent avoir leur ordinateur, qui a été configuré avec la VSC, et connaître un code PIN, qui est nécessaire pour accéder aux certificats stockés sur la puce TPM de l'ordinateur.

Il est important de comprendre comment les VSC protègent les clés privées. Les cartes à puce traditionnelles ont leur propre espace de stockage et mécanismes cryptographiques pour protéger les clés privées. Dans le scénario avec les VSC, les clés privées sont protégées non par l'isolement de la mémoire physique, mais plutôt par les capacités cryptographiques du TPM. Toutes les informations sensibles qui sont stockées sur une carte à puce sont chiffrées en utilisant le TPM, puis elles sont stockées sur le disque dur. Bien que les clés privées sont stockées sur un disque dur en étant chiffrées, toutes les opérations cryptographiques se produisent dans l'environnement isolé et sécurisé du TPM. Les clés privées ne quittent jamais cet environnement sous une forme non chiffrée. Si le disque dur de l'ordinateur est compromis de quelque façon que ce soit, les clés privées ne sont pas accessibles parce qu'elles sont protégées et cryptées par le TPM. Pour plus de sécurité, vous pouvez également chiffrer le lecteur avec BitLocker. Pour déployer les VSC, vous avez besoin d'un Windows Server 2012 ou d'une version ultérieure d'AD CS et de Windows 8 ou d'un ordinateur client plus récent avec une puce TPM embarquée.

- Une infrastructure de carte à puce peut coûter cher
- L'AD CS de Windows Server 2012 met en place les cartes à puce virtuelles
- Les cartes à puce virtuelles tirent profit des performances de la puce TPM
- Aucune dépense pour l'achat de cartes à puce et de lecteurs de cartes à puce
- L'ordinateur agit comme une carte à puce
- Les clés privées sont protégées par les capacités de chiffrement du TPM

Inscription des certificats pour les cartes à puce

Vous devez définir une méthode pour l'inscription des certificats de cartes à puce dans le cadre d'un plan visant à implémenter une infrastructure de carte à puce. Contrairement à d'autres certificats que vous pouvez attribuer aux utilisateurs sans aucune action de leur part, l'inscription aux certificats de cartes à puce nécessite une intervention manuelle d'un administrateur et d'un utilisateur final.

Tout d'abord, vous devez définir un modèle de certificat à utiliser pour les cartes à puce.

Windows Server 2016 AD CS est livré avec deux modèles prédéfinis pour l'utilisation de la carte à puce : **Ouverture de session par carte à puce** et **Utilisateur de carte à puce**. Le modèle **Ouverture de session par carte à puce** sert uniquement à des fins d'authentification, alors que le modèle **Utilisateur de carte à puce** fournit un certificat qui est aussi valable pour la signature numérique et le chiffrement. Ce sont des modèles version 1, ce qui signifie que vous ne pouvez pas modifier leurs options sauf la DACL. En raison de vos options limitées, nous vous recommandons de copier un de ces modèles et de faire des modèles de version 2 ou plus. Ainsi, vous pouvez modifier les options supplémentaires, telles que la période de validité, quel CSP est utilisé sur les cartes à puce, et d'autres informations.

Après avoir configuré un modèle de certificat pour les certificats de cartes à puce, vous devez inscrire un ou plusieurs utilisateurs pour le certificat d'Agent d'inscription. Cela est nécessaire, car les utilisateurs ne sont généralement pas autorisés à inscrire eux-mêmes pour les certificats de cartes à puce. La plupart du temps, les administrateurs émettent des cartes à puce pour les utilisateurs et définissent des codes PIN par défaut. Par la suite, les utilisateurs peuvent changer leur code PIN pour être les seuls à le connaître.

 **Remarque :** nous vous recommandons d'utiliser des fonctionnalités restreintes pour définir les agents d'inscription pour les cartes à puce.

Après avoir défini un Agent d'inscription et délivré un certificat, vous pouvez émettre une carte à puce. Pour délivrer un certificat pour un autre utilisateur, suivez cette procédure :

1. Connectez-vous à la station d'inscription où un lecteur de cartes à puce est installé. Vous devez vous connecter avec le compte utilisateur qui a délivré le certificat d'Agent d'inscription.
2. Ouvrez la console **Certificats**, puis ouvrez le magasin **Mon compte d'utilisateur**.
3. Cliquez avec le bouton droit sur **magasin personnel**, allez à **Toutes les tâches**, cliquez sur **Options avancées**, puis sur **S'inscrire au nom de....**
4. Vous serez invité à sélectionner votre certificat d'Agent d'inscription.
5. Sélectionnez le modèle de certificat voulu pour la carte à puce.
6. Sélectionnez l'utilisateur pour lequel vous émettez une carte à puce. Mettez une carte à puce vide dans l'appareil de lecture.
7. Tapez le code PIN pour la carte à puce que vous souhaitez configurer.
8. Attendez jusqu'à ce qu'un certificat soit généré, puis enregistrez-le sur la carte à puce.
9. Donnez ou envoyez la carte à puce à l'utilisateur final.



Remarque : nous vous recommandons fortement de suggérer aux utilisateurs qu'ils changent leur code PIN de la carte à puce immédiatement après leur première connexion.

Si vous souhaitez gérer l'inscription avec des cartes à puce avec plus d'options avancées, vous devez utiliser un produit dédié tel que le Gestionnaire d'identité Microsoft (MIM).

Gestion de la carte à puce

Vous devez également avoir un plan de gestion de cartes à puce si vous implémentez une infrastructure de cartes à puce en tant que principale méthode pour l'authentification et le stockage d'un certificat utilisateur. La gestion des cartes à puce comprend les tâches et procédures suivantes :

- Publication
- Révocation
- Renouvellement
- Blocage et déblocage
- Duplication
- Suspension

• Tâches de gestion de la carte à puce :

- Publication
 - Révocation
 - Renouvellement
 - Blocage et déblocage
 - Duplication
 - Suspension
- Utilisez MIM pour :
- Émettre des cartes à puce pour les utilisateurs
 - Stocker des informations dans une base de données SQL
 - Gérer les procédures de révocation, de renouvellement, de déblocage, de suspension et de réintégration
 - Fournir aux utilisateurs et aux administrateurs une interface Web en libre-service pour la gestion des cartes à puce
 - Gérer l'impression de cartes à puce avec le matériel approprié
 - Mettre en œuvre des flux de travail pour chaque tâche de gestion

Vous pouvez effectuer certaines de ces procédures et tâches avec les utilitaires Windows intégrés, mais les utilitaires tels que Cardutil ou la console **Certificats** ne proposent pas un grand nombre d'options.

Pour cette raison, nous vous recommandons de mettre en œuvre une solution dédiée pour la gestion des cartes à puce et des certificats. MIM fournit une plate-forme puissante pour une gestion centralisée des cartes à puce.

Avec MIM, vous pouvez déplacer toutes vos tâches de gestion des cartes à puce vers un seul endroit. De plus, vous pouvez mettre en œuvre des flux de travail sur chaque tâche de gestion des cartes à puce.

MIM offre les capacités de gestion des cartes à puce et des certificats suivantes :

- Émettre des cartes à puce pour les utilisateurs ;
- Stocker des informations sur toutes les cartes à puce émises et sur d'autres certificats dans une base de données SQL ;
- Gérer la révocation des cartes à puce, le renouvellement, le déblocage, la suspension, et les Procédures de restauration ;
- Fournir aux utilisateurs et aux administrateurs une interface Web de gestion des cartes à puce en libre-service ;
- Gérer l'impression de cartes à puce avec le matériel approprié ;
- Mettre en œuvre des flux de travail avec une ou plusieurs autorisations pour chaque tâche de gestion.



Remarque : il est important de comprendre que MIM est une solution de gestion des certificats qui ne fournit aucune capacité de PKI. Il propose une fonctionnalité de gestion plus étendue que celle d'une PKI interne existante et il gère les certificats sur les cartes à puce, mais

aussi des certificats d'autres types. Pour mettre en œuvre la solution de gestion des certificats MIM, vous devez avoir conçu une hiérarchie d'AC interne.

Testez vos connaissances

| Question |
|---|
| Lesquels des énoncés suivants sont exacts en ce qui concerne les cartes à puce ? |
| Sélectionnez la réponse correcte. |
| <input type="checkbox"/> Les cartes à puce offrent une option pour l'authentification multifactorielle. |
| <input type="checkbox"/> Les cartes à puce ne peuvent pas être utilisées pour la signature interactive. |
| <input type="checkbox"/> Les cartes à puce contiennent un certificat et une clé privée qui sont accessibles à l'aide d'un code PIN seulement. |
| <input type="checkbox"/> Les cartes à puce offrent une sécurité renforcée au-delà d'un mot de passe. |
| <input type="checkbox"/> Les cartes à puce peuvent être utilisées pour la signature numérique et le chiffrement seulement. |

Testez vos connaissances

| Question |
|---|
| Lors de la mise en œuvre d'une infrastructure de carte à puce, lesquels des processus suivants devraient faire partie de votre cadre de gestion du certificat ? |
| Sélectionnez la réponse correcte. |
| <input type="checkbox"/> Publication |
| <input type="checkbox"/> Révocation |
| <input type="checkbox"/> Renouvellement |
| <input type="checkbox"/> Blocage et déblocage |
| <input type="checkbox"/> Suspension |

Atelier pratique : Déploiement et utilisation de certificats

Scénario

Vous travaillez comme administrateur à A. Datum Corporation. Les exigences de sécurité d'A. Datum augmentent à cause de sa croissance. Le service de sécurité souhaite vraiment permettre un accès sécurisé aux sites essentiels et fournir une sécurité supplémentaire pour des fonctions telles que EFS, les signatures numériques, les cartes à puce et la fonctionnalité DirectAccess dans Windows 8.1 et Windows 10. Le département de sécurité veut notamment évaluer les signatures numériques dans les documents Microsoft Office. Pour répondre à ces exigences et à d'autres en matière de sécurité, A. Datum a décidé d'utiliser des certificats qui sont émis par le rôle AD CS dans Windows Server 2016.

En tant qu'administrateur de réseau principal chez A. Datum, vous êtes responsable de la mise en œuvre l'inscription du certificat. Vous développerez également les procédures et processus de gestion des modèles de certificats et de déploiement et de révocation des certificats.

Objectifs

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

- Configurer des modèles de certificats ;
- Configurer le certificat d'inscription et de l'utilisation ;
- Configurer et implémenter la récupération des clés.

Configuration de l'atelier pratique

Durée approximative : **50 minutes**

Ordinateurs virtuels. **22742A-LON-DC1**, **22742A-LON-SVR1**, **22742A-LON-SVR2** et **22742A-LON-CL1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-LON-DC1**, et dans le volet **Actions**, cliquez sur **Démarrer**.
3. Dans le volet d'**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 : **Pa55w.rd** ;
5. Répéter les étapes 2 et 4 pour **22742A-LON-SVR1**, **22742A-LON-SVR2**, et **22742A-LON-CL1**.

Exercice 1 : Configuration des modèles de certificats

Scénario

Après déploiement de l'infrastructure CA, l'étape suivante consiste à déployer les modèles de certificats nécessaires dans l'organisation. Tout d'abord, A. Datum veut mettre en œuvre un nouveau certificat de serveur Web et des certificats pour les utilisateurs.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un nouveau modèle basé sur le modèle de serveur Web ;
2. Créer un nouveau modèle pour les utilisateurs qui inclut la connexion par carte à puce ;
3. Configurer les modèles de sorte qu'ils puissent être émis ;
4. Incrire le certificat de serveur Web sur **LON-SVR2**.

► **Tâche 1 : Créer un nouveau modèle basé sur le modèle de serveur Web**

1. Sur **LON-DC1**, dans le **Gestionnaire de serveurs**, cliquez sur **Outils**, puis sur **Autorité de certification**.
2. Dans la console **Autorité de certification**, ouvrez la console **Modèles de certificats**.
3. Dupliquez le modèle **Serveur Web**.
4. Créez un nouveau modèle, puis nommez-le **Serveur Web de production**.
5. Configurez la validité sur **3 ans**.
6. Configurez la clé privée comme exportable.
7. Publier la liste de révocation sur **LON-DC1**.

► **Tâche 2 : Créer un nouveau modèle pour les utilisateurs qui inclut la connexion carte à puces**

1. Dans **LON-DC1**, ouvrez la console **Autorité de certification** à partir du **Gestionnaire de serveur**.
2. Ouvrez la console **Modèles de certificats**, puis dupliquez le modèle de certificat **Utilisateur**.
3. Nommez le nouveau modèle **Utilisateur Adatum**.
4. Dans l'onglet **Nom du sujet**, décochez les deux cases **Inclure le nom de compte de messagerie dans le nom du sujet** et **Nom de messagerie électronique**.
5. Ajoutez **Ouverture de session par carte à puce** aux stratégies d'application du nouveau modèle de certificat.
6. Configurez ce nouveau modèle pour remplacer le modèle **Utilisateur**.
7. Permettez aux **Utilisateurs authentifiés** la **Lecture**, l'**Inscription**, et l'**Inscription automatique** pour ce certificat.
8. Fermez la console **Modèles de certificats**.

► **Tâche 3 : Configurer les modèles de sorte qu'ils peuvent être émis**

- Délivrez les certificats basés sur les modèles **Utilisateur Adatum** et **Serveur Web de production**.

► **Tâche 4 : Incrire le certificat de serveur Web sur LON-SVR2**

1. Basculez vers **LON-SVR2**.
2. Ouvrez Windows PowerShell, puis actualisez la stratégie de groupe.
3. Ouvrez le **Gestionnaire de serveur**, puis le **Gestionnaire des services Internet (IIS)**.

4. Inscrivez-vous pour obtenir un certificat de domaine en utilisant les paramètres suivants :
 - Nom commun : **lon-svr2adatum.com**
 - Organisation : **Adatum**
 - Unité d'organisation **Research**
 - Ville/localité : **Seattle**
 - État/Province : **WA**
 - Pays/Région : **USA**
 - Pseudonyme **LON-SVR2**
5. Créez une liaison HTTPS pour le site Web par défaut, puis associez-la au certificat **lon-svr2**.
6. Ouvrez Internet Explorer sur **LON-CL1**, puis <https://lon-svr2.adatum.com>. Veillez à ce que la page **Internet Information Services** s'ouvre et qu'aucune erreur de certificat ne s'affiche.

Résultats : À la fin de cet exercice, vous aurez configuré les modèles de certificats.

Exercice 2 : Inscription et utilisation de certificats

Scénario

La prochaine étape de la mise en œuvre d'une PKI chez A. Datum consiste à configurer l'inscription du certificat. A. Datum souhaite activer différentes options pour la distribution de certificats. Les utilisateurs doivent être en mesure de procéder automatiquement à l'inscription et les utilisateurs de cartes à puce devraient obtenir leur carte à puce par les agents d'inscription. Adatum a délégué les droits d'agent d'inscription pour le groupe du service marketing à l'utilisatrice Annie Conner.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer l'inscription automatique pour les utilisateurs ;
2. Vérifier l'inscription automatique ;
3. Configurer l'agent d'inscription pour les certificats de carte à puce ;
4. Utiliser des certificats pour la signature numérique d'un document Microsoft Office.

► Tâche 1 : Configurer l'inscription automatique pour les utilisateurs

1. Sur **LON-DC1**, ouvrez le **Gestion des stratégies de groupe**.
2. Modifiez la **Stratégie de domaine par défaut**.
3. Aller à **Configuration utilisateur\Stratégies\Paramètres Windows\Sécurité**, puis cliquez sur **Stratégies de clé publique** pour surligner.
4. Activez l'option **Client des services de certificats - Inscription automatique**, puis activez **Renouveler les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués** et **Mettre à jour les certificats qui utilisent les modèles de certificats**.
5. Activez **Client des services de certificats - Stratégie d'inscription des certificats**.
6. Fermez la fenêtre **Éditeur de gestion des stratégies de groupe** et la console **Gestion des stratégies de groupe**.

► **Tâche 2 : Vérifier l'inscription automatique**

1. Sur **LON-CL1**, ouvrez **Windows PowerShell**, puis utilisez **gpupdate /force** pour actualiser la stratégie de groupe.
2. Ouvrez la console **Microsoft Management Console (MMC)** et ajoutez le composant logiciel enfichable **Certificats** pour le compte d'utilisateur.
3. Vérifiez que vous avez reçu un certificat émis sur la base du modèle **Utilisateur Adatum**.
4. Déconnectez-vous de **LON-CL1**.

► **Tâche 3 : Configurer l'agent d'inscription pour les certificats de carte à puce**

1. Sur **LON-DC1**, depuis la console **Autorité de certification**, ouvrez la console **Modèles de certificats**.
2. Permettez à **Annie Conner** de s'inscrire à un certificat d'**Agent d'inscription**.
3. Publier l'**Agent d'inscription** modèle de certificat.
4. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Annie** avec le mot de passe **Pa55w.rd**, puis inscrivez-vous à un certificat d'**Agent d'inscription**.
5. Déconnectez-vous de **LON-CL1**.
6. Sur **LON-DC1**, ouvrez les propriétés d'**AdatumCA**, puis configurez l'**Agent d'inscription limité** de telle sorte qu'Ariane puisse seulement émettre des certificats basés sur **Utilisateur Adatum** pour le groupe de sécurité **Marketing**.

► **Tâche 4 : Utiliser des certificats pour la signature numérique d'un document Microsoft Office**

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Ouvrez Word 2016. Saisissez du texte dans un nouveau document vierge, puis enregistrez le document.
3. Cliquez sur **INSÉRER** dans le ruban, puis insérez une ligne de signature.
4. Remplissez les champs de signature avec vos données.
5. Cliquez droit sur la ligne de signature, puis choisissez de signer le document.
6. Choisissez le certificat auquel vous êtes inscrit par l'inscription automatique.
7. Signez le document.
8. Assurez-vous que le document ne peut plus être modifié.
9. Déconnectez-vous de **LON-CL1**.

Résultats : À la fin de cet exercice, les stagiaires auront implémenté l'inscription de certificats.

Exercice 3 : Configuration et mise en œuvre de récupération de clés

Scénario

Dans le cadre de l'établissement d'une infrastructure à clé publique (PKI), vous souhaitez configurer et tester des procédures de récupération de clé privée. Vous souhaitez attribuer un certificat KRA pour un administrateur et configurer un CA et des modèles de certificats spécifiques pour permettre l'archivage de clés. En outre, vous souhaitez tester une procédure de récupération de clé.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer l'autorité de certification (AC) pour délivrer des certificats KRA ;
2. Acquérir le certificat KRA ;
3. Configurer l'AC pour autoriser la récupération des clés ;
4. Configurer un modèle personnalisé pour l'archivage des clés ;
5. Vérifier la fonctionnalité d'archivage des clés ;
6. Préparez le module suivant.

► Tâche 1 : Configurer l'autorité de certification (AC) pour délivrer des certificats KRA

1. Sur **LON-DC1**, dans la console **Autorité de certification**, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
2. Dans la console **Modèles de certificats**, ouvrez la boîte de dialogue **Propriétés de l'agent de récupération principal**.
3. Dans l'onglet **Conditions d'émission**, désactivez la case à cocher **Approbation du gestionnaire de certificats de l'AC**.
4. Dans l'onglet **Sécurité**, notez que seuls les Admins de domaine et les groupes d'Admins entreprise ont l'autorisation de faire les inscriptions.
5. Cliquez droit sur le dossier **Modèles de certificats**, puis émettez le modèle **Agent de récupération principal**.

► Tâche 2 : Acquérir le certificat KRA

1. Créez la Microsoft Management Console qui inclut le composant logiciel enfichable **Certificats** pour l'utilisateur actuel.
2. Utilisez l'**Assistant d'inscription de certificat** pour demander un nouveau certificat et inscrire le certificat KRA.
3. Actualisez la fenêtre de la console, puis affichez le KRA dans le magasin personnel.

► Tâche 3 : Configurer l'AC pour autoriser la récupération de clé

1. Dans **LON-DC1**, ouvrez la console **Autorité de certification** à partir du **Gestionnaire de serveur**. Ouvrez ensuite la boîte de dialogue **Propriétés AdatumCA**.
2. Dans l'onglet **Agents de recouvrement**, cliquez sur **Archiver la clé**, puis ajoutez le certificat en utilisant la boîte de dialogue **Sélection de l'agent de récupération de clé**.
3. Redémarrez **Services de certificats** lorsque vous y êtes invité.

► Tâche 4 : Configurer un modèle personnalisé pour l'archivage de clés

1. Sur **LON-DC1**, ouvrez la console **Modèles de certificats**.
2. Dupliquez le modèle **Utilisateur** et nommez-le **Utilisateur archivé**.

3. Dans l'onglet **Traitement de la demande**, sélectionnez l'option pour **Archiver la clé privée de chiffrement du sujet**. En utilisant l'option d'archivage de la clé, le KRA peut obtenir la clé privée du magasin de certificats.

4. Cliquez sur l'onglet **Nom du sujet**, puis décochez les cases **Nom de messagerie électronique** et **Inclure le nom de compte de messagerie dans le nom du sujet**.

5. Émettez le modèle **Utilisateur archivé**.

► Tâche 5 : Vérifier la fonctionnalité d'archivage de clé

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Mary** avec le mot de passe **Pa55w.rd**.

2. Créez la Microsoft Management Console qui inclut le composant logiciel enfichable **Certificats**.

3. Demandez et inscrivez un nouveau certificat basé sur le modèle **Utilisateur archivé**.

4. Depuis la boutique personnelle, recherchez le certificat **Utilisateur archivé**.

5. Supprimer le certificat pour Mary afin de simuler une clé perdue.

6. Basculez vers **LON-DC1**.

7. Ouvrez la console **Autorité de certification**, développez **AdatumCA**, puis cliquez sur le magasin **Certificats délivrés**.

8. Dans la console **Autorité de certification**, notez le numéro de série du certificat qui a été délivré à Mary.

9. Sur **LON-DC1**, dans l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
Certutil -getkey <numéro de série> outputblob
```



Remarque : Remplacer le numéro de série dans la commande ci-dessus par le numéro de série que vous avez noté. Si vous copiez et collez le numéro de série, supprimer les espaces entre les numéros.

10. Vérifiez que le fichier **Outputblob** s'affiche maintenant dans le dossier **C:\Users\Administrateur**.

11. Pour convertir le fichier **outputblob**, en un fichier.pfx importable, à l'invite de commandes, saisissez la commande suivante, puis appuyez sur Entrée :

```
Certutil-recoverkey outputblob Mary.pfx
```

12. Entrez et confirmez le mot de passe **Pa55w.rd** pour le certificat.

13. Vérifier la création de la clé récupérée dans le dossier **C:\Users\Administrateur**.

14. Basculez vers **LON-CL1**.

15. Ouvrez **Explorateur de fichiers**, puis connectez-vous à **\LON-DC1.adatum.com\c\$**. Lorsque vos données d'identifications sont demandées, utilisez **Adatum\Administrateur** avec le mot de passe **Pa55w.rd**. Copiez et collez le fichier **Mary.pfx** à partir de **\LON-DC1.adatum.com\c\$\utilisateurs\administrateur** à **C:\Users\Mary** sur **LON-CL1**.

16. Sur **LON-CL1**, importez le certificat **Mary.pfx**.

17. Vérifiez que le certificat s'affiche dans le magasin personnel.

Résultats : À la fin de cet exercice, les stagiaires auront configuré la récupération de clé.

► **Tâche 6 : Préparer le module suivant**

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-CL1**, **22742A-LON-SVR1**, et **22742A-LON-SVR2**.

Question : Que devez-vous faire pour récupérer les clés privées ?

Question : Quel est l'avantage d'utiliser un agent d'inscription restreint ?

Révision du module et Takeaways

Questions de contrôle des acquis

Question : Listez les conditions requises pour utiliser l'inscription automatique pour les certificats.

Question : Comment les cartes à puce virtuelles fonctionnent-elles ?

Enjeux et scénarios du monde réel

Contoso Ltd. souhaite déployer une infrastructure PKI pour soutenir et sécuriser plusieurs services. L'entreprise a décidé d'utiliser Windows Server 2016 AD CS en tant que plateforme pour la PKI. Les certificats seront utilisés principalement pour EFS, pour la signature numérique et pour les serveurs Web. Étant donné que les documents qui seront chiffrés sont importants, il est essentiel de disposer d'une stratégie de récupération d'urgence en cas de perte de clés. En outre, les clients qui auront accès à des parties sécurisées du site de l'entreprise ne doivent pas recevoir d'avertissement dans leurs navigateurs.

- Quel type de déploiement Contoso devrait-il choisir ?
- Quel type de certificats Contoso devrait-il utiliser pour EFS et la signature numérique ?
- Quel type de certificats Contoso devrait-il utiliser pour un site Web ?
- Comment Contoso peut-il faire en sorte que les données EFS chiffrées ne soient pas perdues si un utilisateur perd un certificat ?

Outils

- La console **Autorité de certification**
- La console **Modèles de certificats**
- La console **Certificats**
- **Certutil.exe**

Recommandations

- Lors du remplacement de vieux modèles de certificats, utiliser des modèles de remplacement.
- Toujours archiver les certificats qui sont utilisés à des fins de chiffrement.
- Utilisez l'inscription automatique pour le déploiement de masse des certificats.
- Si vous utilisez des cartes à puce, assurez-vous que les utilisateurs changent leur PIN régulièrement.
- Si vous utilisez des cartes à puce, mettez en œuvre une solution de gestion de carte à puce.

Problèmes courants et conseils de dépannage

| Problème courant | Conseil pour la résolution du problème |
|---|--|
| Le modèle de certificat n'est pas visible durant l'inscription. | |
| L'inscription automatique ne fonctionne pas. | |
| L'utilisateur qui a chiffré un fichier ne peut pas le déchiffrer. | |

Module 10

Implémentation et administration de AD FS

Sommaire :

| | |
|---|-------|
| Présentation du module | 10-1 |
| Leçon 1 : Présentation de AD FS | 10-2 |
| Leçon 2 : Exigences et planification AD FS | 10-11 |
| Leçon 3 : Déploiement et configuration AD FS | 10-25 |
| Leçon 4 : Présentation du proxy d'application Web | 10-42 |
| Atelier pratique : Implémentation de AD FS | 10-53 |
| Révision du module et Takeaways | 10-64 |

Présentation du module

Grâce à Services de fédération Active Directory (AD FS) (AD FS) du système d'exploitation Windows Server 2016, les organisations offrent à leurs utilisateurs la souplesse pour se connecter, et s'authentifier sur les applications disponibles sur un réseau local, dans une entreprise partenaire, ou sur un service en ligne. Avec AD FS, votre organisation peut gérer ses propres comptes utilisateur et les utilisateurs n'ont à retenir qu'une série d'identifiants. Ceux-ci permettent l'accès à de nombreuses applications, même celles dispersées sur différents emplacements.

Objectifs

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

- Décrire AD DS.
- Expliquer comment déployer AD FS.
- Expliquer comment implémenter AD FS pour une seule organisation.
- Expliquer comment étendre AD FS à des clients externes.
- Mettre en œuvre l'authentification unique (SSO) pour soutenir les services en ligne.

Leçon 1

Présentation de AD FS

AD FS est l'implémentation Microsoft d'un cadre de la fédération d'identité qui permet aux organisations d'établir les approbations de fédération et de partager les ressources au-delà des services de l'organisation et de Active Directory Domain Services (AD DS). AD FS respecte les normes des Web services communes, permettant ainsi l'interopérabilité avec les solutions de fédération d'identité fournies par les autres fournisseurs. AD FS étudie les différents scénarios de gestion pour lesquels les mécanismes d'authentification classiques utilisés dans une organisation ne fonctionnent pas.

Cette leçon présente des concepts et des normes que l'AD FS met en œuvre et les scénarios de gestion qu'elle peut étudier.

Objectifs des leçons

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

- Décrire la fédération d'identité.
- Décrire l'identité basée sur les revendications.
- Décrire les Web services.
- Décrire AD DS.
- Décrire les nouvelles fonctionnalités de l'AD FS.
- Expliquer comment l'AD FS permet l'authentification unique dans une seule organisation
- Expliquer comment AD FS permet l'authentification unique dans une fédération business-to-business

Qu'est-ce que la fédération d'identité ?

La fédération d'identité vous permet de fournir l'identification, l'authentification et l'autorisation au-delà des limites de l'organisation et de la plate-forme. Vous pouvez l'instaurer au sein d'une seule organisation pour permettre l'accès aux diverses applications Web, ou entre des entreprises qui entretiennent un lien de confiance.

Pour établir un partenariat de fédération d'identité, les deux partenaires s'accordent pour créer un rapport de confiance fédérée. Cette confiance fédérée repose sur une relation d'affaires permanente, et elle permet aux organisations de mettre en œuvre des processus opérationnels que la relation d'affaires détermine.

- Permet l'identification, l'authentification et l'autorisation à travers les limites organisationnelles et celles liées à la plateforme
- Nécessite une relation d'approbation fédérée entre deux organisations ou entités
- Permet aux organisations de conserver le contrôle sur les personnes pouvant accéder aux ressources
- Permet aux organisations de conserver le contrôle de leurs comptes d'utilisateurs et de groupes

 **Remarque :** Une approbation fédérée n'est pas la même chose qu'une approbation de forêt que les organisations peuvent configurer entre les forêts AD DS. Dans une approbation fédérée, les serveurs AD FS dans deux organisations ne doivent jamais communiquer directement les uns avec les autres. En outre, toutes les communications dans un déploiement de la fédération se produisent via HTTPS, de sorte que vous n'avez pas besoin d'ouvrir plusieurs ports sur les pare-feux pour permettre la fédération.

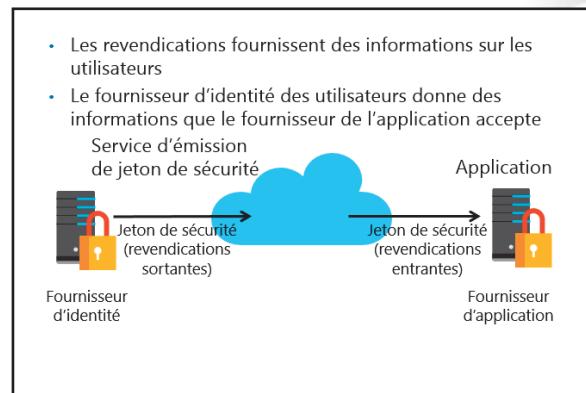
Dans le cadre de la confiance fédérée, chaque partenaire définit les ressources accessibles à l'autre organisation et les modalités d'accès. Par exemple, pour la mise à jour d'une prévision de ventes, un commercial peut avoir besoin de collecter les informations de la base de données d'un fournisseur, hébergée sur son réseau. L'administrateur du domaine pour le représentant des ventes s'assure que les représentants des ventes appropriés appartiennent au groupe qui demande l'accès à la base de données du fournisseur. L'administrateur de l'organisation qui détient la base de données, s'assure que les employés des partenaires ont accès uniquement aux données nécessaires.

Dans une solution de fédération d'identités, les identités des utilisateurs et les informations d'identification les concernant sont stockées, détenues et gérées par l'organisation où se trouvent les utilisateurs. Dans le cadre de la confiance de la fédération d'identité, chaque organisation définit également les modalités de partage en toute sécurité des identités utilisateur pour limiter l'accès aux ressources. Chaque partenaire définit les services qu'il met à la disposition des partenaires de confiance et des clients, ainsi que les autres organisations et utilisateurs sur lesquels il peut compter. Chaque partenaire détermine également les types d'informations, d'identification et de demandes qu'il accepte, et ses politiques de confidentialité pour empêcher l'accès à l'information privée.

Vous pouvez également utiliser la fédération d'identités au sein d'une seule organisation. Par exemple, une organisation peut prévoir plusieurs applications en ligne nécessitant une authentification. En utilisant AD FS, l'organisation peut mettre en œuvre une solution d'authentification pour toutes les applications, facilitant l'accès à l'application pour les utilisateurs dans de nombreux domaines internes ou forêts. La solution peut également s'étendre aux partenaires extérieurs à l'avenir, sans demander aux développeurs de modifier l'application.

Qu'est-ce que l'identité basée sur les revendications et l'authentification basée sur les revendications ?

Dans la plupart des organisations, les utilisateurs se connectent au réseau et sont authentifiés par un contrôleur de domaine AD DS. Un utilisateur qui donne les bonnes informations d'identification au contrôleur de domaine reçoit un jeton de sécurité. Les applications en cours d'exécution sur les serveurs dans le même environnement AD DS font confiance aux jetons de sécurité fournis par les contrôleurs de domaine AD DS, car les serveurs sont en liaison avec les mêmes contrôleurs de domaine où les utilisateurs sont authentifiés.



Ce type d'authentification ne s'étend pas facilement au-delà des limites des forêts AD DS. Même si la confiance selon le protocole d'authentification Kerberos V5 ou l'authentification Windows intégrée (IWA) peut être instaurée entre deux forêts AD DS, les ordinateurs clients et les contrôleurs de domaine, de chaque côté, doivent communiquer avec les contrôleurs de domaine de l'autre forêt pour prendre des décisions concernant l'authentification et l'autorisation. Cette communication nécessite le trafic réseau qui est envoyé sur plusieurs ports, ceux-ci doivent donc être ouverts sur tous les pare-feux entre les contrôleurs de domaine et les autres ordinateurs. Le problème se complique davantage lorsque les utilisateurs doivent accéder aux ressources hébergées sur des systèmes du cloud comme Microsoft Azure ou Microsoft Office 365.

L'authentification basée sur les revendications fournit un mécanisme pour séparer l'authentification de l'utilisateur et l'autorisation des applications individuelles. Avec l'authentification basée sur les revendications, les utilisateurs peuvent s'authentifier auprès d'un service d'annuaire au sein de leur organisation, et la demande est acceptée d'après cette authentification. La demande est ensuite soumise à

une application utilisée dans une organisation différente. L'application permet l'accès des utilisateurs aux informations ou fonctionnalités d'après les revendications présentées. Toutes les communications se font via HTTPS.

La *revendication* utilisée dans l'authentification basée sur les revendications est une déclaration sur un utilisateur, définie dans une organisation ou une technologie, et approuvée dans une autre. La demande peut comprendre diverses informations. Par exemple, elle peut indiquer l'adresse e-mail de l'utilisateur, le nom principal de l'utilisateur (UPN), et les informations sur les groupes spécifiques auxquels appartient l'utilisateur. Cette information est collectée à partir du stockage d'identités lorsque l'utilisateur est correctement authentifié.

L'organisation qui gère l'application définit les types de revendications que l'application acceptera. Par exemple, l'application peut demander l'adresse email de l'utilisateur pour vérifier l'identité, et ensuite utiliser l'appartenance au groupe qui est communiquée dans la revendication pour déterminer le niveau d'accès de l'utilisateur dans l'application.

Présentation des services Web

Pour l'authentification basée sur les revendications, pour fonctionner, les organisations doivent s'accorder sur le format d'échange de revendications. À la place d'un format défini par chaque entreprise, un cahier des charges déterminé de façon générale comme *Web services* a été créé. Toute organisation qui veut mettre en œuvre une solution d'identité fédérée peut utiliser ce cahier des charges.

Les Web services comprennent un cahier des charges utilisé pour des applications et des services reliés à la structure dont les fonctionnalités et les interfaces sont exposées à des utilisateurs potentiels grâce aux standards technologiques du web, tels que XML, le protocole Simple Object Access (SOAP), Web Services Description Language (WSDL), HTTP et HTTPS. L'objectif de la création d'applications Web, en utilisant les Web services, est de simplifier l'interopérabilité des applications sur les multiples plates-formes de développement, les technologies et les réseaux.

Un ensemble de normes de l'industrie définissent les Web services pour renforcer l'interopérabilité :

- La plupart des Web services utilisent XML pour transmettre les données par le biais de HTTP et HTTPS. Avec XML, les développeurs peuvent créer leurs propres étiquettes personnalisées, facilitant ainsi la définition, la transmission, la validation et l'interprétation des données entre les applications et les organisations.
- Les Web services exposent des fonctionnalités utiles aux utilisateurs Web par le biais d'un protocole Web normalisé. Dans la plupart des cas, les Web services utilisent SOAP, le protocole de communication pour les services Web XML. SOAP est une spécification qui définit le format XML pour les messages, et il donne principalement la description d'un document XML valide.
- Les Web services donnent suffisamment d'informations sur leurs interfaces pour permettre à un utilisateur de créer une application client pour communiquer avec un service. Cette description est généralement fournie dans un document XML appelé un document WSDL. Autrement dit, un fichier WSDL est un document XML qui décrit un ensemble de messages SOAP et la façon dont ces derniers sont échangés.

- Les services Web comprennent un ensemble normalisé de spécifications utilisées pour construire des applications et services
- Généralement, les services Web :
 - Transmettent des données au format XML ;
 - Utilisent SOAP pour définir le format de message en XML ;
 - Utilisent WSDL pour définir les messages SOAP valides ;
 - Utilisent UDDI pour décrire les services Web disponibles.
- SAML est une norme d'échange de réclamations d'identité

- Les Web services sont enregistrés pour que les utilisateurs potentiels puissent les trouver facilement. Cela se fait avec Universal Description, Discovery, and Integration (UDDI). Une entrée de répertoire UDDI est un fichier XML qui décrit une entreprise et ses services.

Les spécifications des Services Web en matière de sécurité

Les spécifications des services Web comprennent plusieurs composants qui sont généralement connus comme les WS-* spécifications. Cependant, les spécifications les plus importantes pour un environnement AD FS sont les spécifications des services Web en matière de sécurité (WS-Security). WS-Security comprend les spécifications suivantes :

- WS-Security : Message de sécurité SOAP et le profil du certificat X 509 Token. La WS-Security décrit les améliorations apportées à la messagerie SOAP qui assurent la qualité de la protection par un message d'intégrité, un message de confidentialité et un simple message d'authentification. La WS-Security fournit également un mécanisme général, néanmoins évolutif, pour associer les jetons de sécurité aux messages. Par ailleurs, il propose un mécanisme de codage des jetons de sécurité binaires, en particulier, les certificats X 509 et les tickets Kerberos, dans les messages SOAP.
- ConWeb Services Trust (WS-Trust). WS-Trust définit des extensions qui se fondent sur WS-Security pour demander et émettre des jetons de sécurité, et pour gérer les relations de confiance.
- Fédération de Web services (WS-Federation). WS-Federation détermine les mécanismes que WS-Security peut utiliser pour permettre l'identité en fonction des attributs, l'authentification et l'autorisation de fédération dans les différents domaines de confiance.
- Profil WS-Federation Passive Requestor (WS-F PRP). Cette extension WS-Security décrit la façon dont les clients passifs, tels que les navigateurs Web, obtiennent des jetons à partir d'un serveur de fédération, et comment les clients envoient les jetons à un serveur de fédération. Les demandeurs passifs de ce profil sont limités au protocole HTTP ou HTTPS.
- Profil actif du demandeur WS-Federation. Cette extension WS-Security décrit la façon dont les clients actifs, telles que les applications périphériques mobiles basés sur SOAP, peuvent être authentifiés et autorisés, et comment les clients peuvent soumettre les demandes dans un scénario de fédération.

Security Assertion Markup Language

Security Assertion Markup Language (SAML) est un standard XML pour l'échange de revendications entre un fournisseur d'identité et un fournisseur de service ou d'application. SAML suppose que l'utilisateur a été authentifié par un fournisseur d'identité et que le fournisseur d'identité a rempli les informations de réclamation appropriées dans le jeton de sécurité. Lorsque le fournisseur d'identité authentifie l'utilisateur, il transmet une assertion SAML au fournisseur de services. Selon cette affirmation, le fournisseur de services peut prendre les décisions d'autorisation et de personnalisation sur une application. La communication entre les serveurs de fédération repose sur un document XML qui enregistre le certificat X 509 pour la signature de jeton et le jeton SAML 1.1 ou SAML 2.0.

Qu'est-ce que le AD FS ?

Le AD FS est l'implémentation Microsoft d'une solution de fédération d'identité qui utilise l'authentification des revendications. Le AD FS instaure les mécanismes servant au fournisseur d'identité et au fournisseur de services dans un déploiement de fédération d'identité.

Le AD FS présente les fonctionnalités suivantes :

- Un fournisseur de revendications en entreprise pour les applications basées sur les revendications. Vous pouvez configurer un serveur AD FS en tant que fournisseur de revendications, cela signifie que le serveur AD FS peut émettre des réclamations sur les utilisateurs authentifiés. Cela permet à une organisation d'offrir à ses utilisateurs l'accès aux applications concernant les revendications d'une autre organisation, en utilisant l'inscription unique SSO.
- Un fournisseur de service de fédération pour la fédération d'identité entre les domaines. Ce service permet une SSO de Web fédéré entre les domaines, en renforçant ainsi la sécurité et en réduisant les traitements pour les administrateurs IT.

• AD FS est le produit de la fédération d'identité Microsoft qui peut utiliser une authentification basée sur les revendications

• AD FS offre les fonctionnalités suivantes :

- Une authentification unique pour les applications basées sur le Web ;
- L'interopérabilité avec les services Web sur plusieurs plateformes ;
- Une prise en charge pour de nombreux clients, tels que les navigateurs Web, les appareils mobiles et les applications ;
- Une extensibilité pour soutenir les revendications personnalisées à partir des applications tierces ;
- La délégation de la gestion des comptes à l'organisation de l'utilisateur.

Fonctionnalités d'AD FS

Voici quelques-unes des principales fonctionnalités de AD FS :

- Web SSO. De nombreuses organisations déploient AD DS. Après l'authentification à l'AD DS par IWA, les utilisateurs peuvent accéder à toutes les autres ressources accessibles dans les limites de la forêt de AD DS. L'AD FS étend cette fonctionnalité aux applications Intranet ou Internet permettant aux clients, partenaires et fournisseurs d'avoir une expérience utilisateur similaire, simplifiée quand ils ont accès aux applications en ligne d'une organisation.
- Interopérabilité de Web services. L'AD FS est compatible avec les spécifications de Web services. L'AD FS emploie la spécification de fédération de WS-* appelée WS-Federation. La WS-Federation permet à des environnements qui n'utilisent pas le modèle d'identité Windows Identity Foundation (WIF), de fédérer avec les environnements qui utilisent le système d'exploitation Windows.
- Support client passif et intelligent. L'AD FS étant basé sur le WS-* architecture, il prend en charge les messages fédérés entre tous les points de terminaison WS-activés, y compris les messages entre les serveurs et les clients passifs, tels que les navigateurs. L'AD FS dans Windows Server 2016 permet l'accès pour les clients intelligents SOAP, tels que les téléphones portables, les assistants numériques personnels et les applications de bureau. L'AD FS met en œuvre la WS-FPRP et certaines des normes de la WS-Federation concernant le profil du demandeur actif pour le support client.
- Une architecture évolutive. L'AD FS présente une architecture évolutive qui prend en charge différents types de jeton de sécurité, y compris les jetons SAML et l'authentification Kerberos grâce à l'authentification Windows, et permet d'effectuer des transformations des revendications personnalisées. Par exemple, l'AD FS peut convertir un type de jeton dans un autre, ou elle peut ajouter une logique commerciale personnalisée comme variable dans une demande d'accès. Les organisations peuvent utiliser cette extensibilité pour modifier l'AD FS pour coexister avec leur infrastructure de sécurité existante et leurs politiques commerciales.
- Sécurité améliorée. L'AD FS augmente également la sécurité des solutions fédérées en déléguant la responsabilité de la gestion des comptes à l'organisation la plus proche de l'utilisateur. Chaque organisation individuelle dans une fédération poursuit la gestion de ses propres identités, et chacune peut partager en toute sécurité et accepter les informations d'identification provenant des autres membres.

Nouveautés de AD DS dans Windows Server 2016

Nouvelles fonctionnalités AD FS introduites dans Windows Server 2012

La version AD FS livrée avec Windows Server 2012 comprend plusieurs nouvelles fonctionnalités :

- L'intégration avec le système d'exploitation du Windows Server 2012. Dans Windows Server 2012, l'AD FS figure comme rôle du serveur que vous pouvez installer à l'aide du gestionnaire de serveur. Lorsque vous installez le rôle de serveur, tous les composants du système d'exploitation nécessaires s'installent automatiquement.
- Intégration avec le contrôle d'accès dynamique. Lorsque vous déployez le contrôle d'accès dynamique, vous pouvez configurer les revendications des utilisateurs et du périphérique émises par les contrôleurs de domaine AD DS. L'AD FS peuvent utiliser les revendications de l'AD DS émises par les contrôleurs de domaine. Cela signifie que l'AD FS peut prendre des décisions d'autorisation d'après les comptes utilisateur et les comptes de l'ordinateur.
- Les commandes Applet, de l'interface de ligne de commande Windows PowerShell pour administrer l'AD FS. Windows Server 2012 fournit de nombreuses nouvelles commandes Applet que vous pouvez utiliser pour installer et configurer le rôle de serveur AD FS.

- Nouvelles fonctionnalités AD FS introduites dans Windows Server 2012 :
 - L'intégration avec le système d'exploitation Windows Server 2012 ;
 - L'intégration avec le Contrôle d'accès dynamique ;
 - Les applets de commande Windows PowerShell pour administrer AD FS.

- Nouvelles fonctionnalités AD FS introduites dans Windows Server 2016 :
 - Un support pour tout répertoire qui est compatible LDAP v3 ;
 - De nouveaux facteurs d'authentification ;
 - Une amélioration de la gestion d'AD FS ;
 - Un accès conditionnel.

Nouvelles fonctionnalités AD FS introduites dans Windows Server 2016

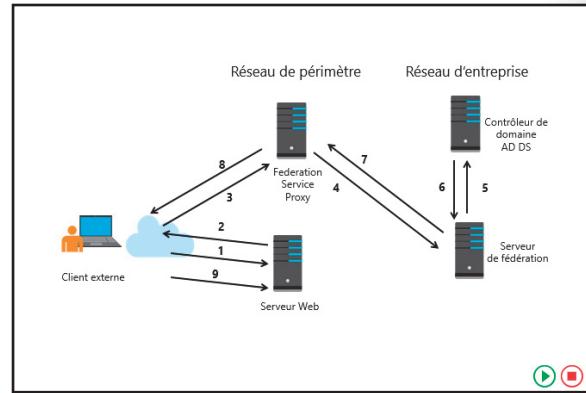
La version AD FS livrée avec Windows Server 2016 comprend les nouvelles fonctionnalités suivantes :

- Support pour tout répertoire compatible avec Lightweight Directory Access Protocol (LDAP) v3. Cela permet à vos utilisateurs de :
 - Se connecter à l'AD FS à partir de n'importe quel répertoire tiers compatible avec LDAP v3.
 - Se connecter à partir de domaines et de forêts AD DS non approuvés, ou partiellement.
- De nouveaux facteurs d'authentification. L'AD FS fournit d'autres moyens pour authentifier les utilisateurs et les périphériques. En plus de l'utilisation de l'AD DS et des répertoires LDAP, vous pouvez également configurer « Azure multi-factor authentication » comme moyen d'authentification.
- Améliorations de la gestion AD FS, comprenant :
 - Les stratégies d'applications. Dans l'AD FS pour Windows Server 2012 R2, vous devez utiliser un langage de règles de revendications pour créer les politiques AD FS personnalisées. L'AD FS dans Windows Server 2016 assure la gestion avec assistant, ce qui facilite la création de politiques personnalisées.
 - La gestion des services délégués. L'AD FS dans Windows Server 2016 distingue les administrateurs de serveur AD FS des administrateurs des services de AD FS. Cela signifie que l'administrateur AD FS n'a plus besoin d'être un administrateur de serveur local.
- Accès conditionnel L'AD FS dans Windows Server 2016 améliore l'enregistrement du périphérique en fonctionnant avec « Azure Active Directory » (Azure AD), pour limiter les périphériques, ou demander plusieurs facteurs d'authentification, en fonction de la gestion ou de l'état de conformité. Par exemple, avec l'accès conditionnel, vous pouvez :

- Autoriser l'accès à partir des périphériques de vos utilisateurs uniquement qui sont gérés selon les normes de l'entreprise ou qui s'y conforment.
- Limiter l'accès à des ordinateurs connectés au domaine de l'entreprise, y compris les périphériques administrés et les ordinateurs connectés au domaine.
- Exiger Multi-Factor Authentication (AMF) pour les ordinateurs qui ne sont pas connectés au domaine et les périphériques non conformes.

Comment AD FS permet l'authentification unique dans une même organisation

Pour de nombreuses organisations, la configuration de l'accès aux applications et services ne devrait pas demander un déploiement AD FS. Si tous les utilisateurs appartiennent à la même forêt AD DS, et si toutes les applications fonctionnent sur des serveurs faisant partie de la même forêt, vous pouvez généralement utiliser l'authentification AD DS pour accéder à l'application. Mais, il existe plusieurs situations pour lesquelles vous pouvez utiliser l'AD FS pour optimiser l'expérience utilisateur, en permettant l'authentification unique. Dans une organisation unique, vous pouvez utiliser l'AD FS pour activer la SSO lorsque :



- Vos applications ne sont pas supportées par les serveurs Windows ou tout autre serveur qui prend en charge l'authentification AD DS, ou elles sont supportées par les serveurs qui utilisent le serveur Windows, et qui ne sont pas connectés au domaine. Les applications peuvent nécessiter les services SAML ou Web pour l'authentification et l'autorisation.
- Vous avez plusieurs domaines et forêts. Cela peut être dû à des fusions et des acquisitions, ou à des impératifs de sécurité. Les utilisateurs dans plusieurs forêts peuvent avoir besoin d'accéder aux mêmes applications.
- Les utilisateurs externes peuvent avoir besoin d'accéder aux applications déployées sur les serveurs internes. Les utilisateurs externes peuvent se connecter à des applications à partir d'ordinateurs qui n'appartiennent pas au domaine interne.

Vous pouvez utiliser l'AD FS pour activer l'inscription unique SSO dans ces situations. Si votre organisation dispose d'une forêt AD DS unique, vous devez déployer uniquement un serveur de fédération unique. Ce serveur peut fonctionner comme fournisseur de revendications pour authentifier les demandes des utilisateurs et fournir les revendications. Le même serveur est également la partie se fiant à l'autorisation pour l'accès aux applications.

Les étapes suivantes décrivent le flux de communication dans ce cas :

1. L'ordinateur client, situé en dehors du réseau, accède à une application en ligne sur le serveur Web. L'ordinateur client envoie une demande HTTPS au serveur Web.
2. Le serveur Web reçoit la demande, et constate que l'ordinateur client n'a pas de réclamation.
3. Le serveur Web redirige l'ordinateur client sur l'application Web Proxy. L'ordinateur client envoie une demande HTTPS à l'application Web Proxy. En fonction de la situation, l'application Web Proxy peut demander à l'utilisateur de s'authentifier ou d'utiliser l'authentification Windows pour récupérer les informations d'identification de l'utilisateur.

4. L'application Web Proxy transmet la demande et les informations d'identification au serveur de fédération.
5. Le serveur de fédération utilise l'AD DS pour authentifier l'utilisateur.
6. Si l'authentification réussit, le serveur de fédération recueille les informations AD DS de l'utilisateur. Cette information est ensuite utilisée pour générer les demandes de l'utilisateur.



Remarque : Une partie se fiant sur la confiance pour l'application Web doit exister dans l'AD FS. Si le même utilisateur tente d'accéder à une application Web différente, les différentes demandes des utilisateurs peuvent être incluses dans le jeton de sécurité, qui est transmis à l'utilisateur, puis à l'application Web.

7. Si l'authentification réussit, les informations d'authentification et les autres informations sont collectées dans un jeton de sécurité et communiquées à l'application Web Proxy.



Remarque : Ce jeton de sécurité est signé pour l'application Web spécifique. Par conséquent, une partie se fiant sur la confiance avec cette application web doit exister dans l'AD FS.

8. L'application Web Proxy délivre le jeton au client.
9. Le client présente le jeton au serveur Web. La ressource Web :
 - a. Reçoit la demande et valide les jetons signés.
 - b. Utilise les revendications du jeton de l'utilisateur pour donner l'accès à l'application.

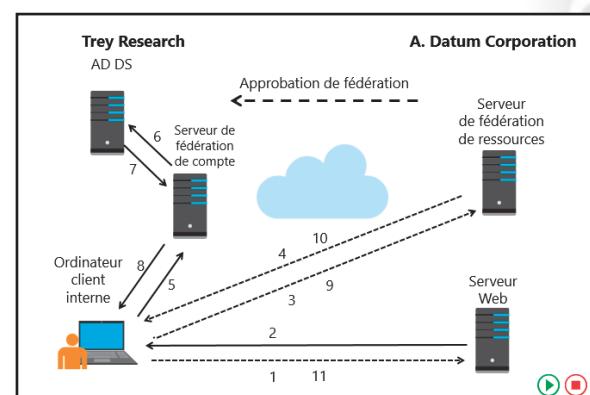


Remarque : La diapositive et la description précédente emploient les termes *service de fédération Proxy* et *application Web Proxy* pour décrire les services de rôle AD FS. Le serveur de fédération délivre les revendications et absorbe les revendications dans cette situation.

L'application Web Proxy est un composant Proxy recommandé pour les déploiements quand les utilisateurs externes au réseau ont besoin d'accéder à l'environnement AD FS. Ces composants sont détaillés dans la leçon suivante.

Comment AD FS permet l'authentification unique dans une fédération business-to-business

L'un des scénarios les plus courants pour le déploiement AD FS, est de fournir une inscription unique SSO dans une fédération business-to-business. Dans ce cas, l'organisation qui demande l'accès à une autre application ou un autre service de l'organisation peut gérer ses propres comptes utilisateur et définir ses propres mécanismes d'authentification. L'autre organisation peut déterminer les applications et les services accessibles aux utilisateurs externes, et quelles revendications seront acceptées pour l'accès à l'application. Pour permettre le partage des applications ou services dans ce scénario, les organisations doivent établir une approbation de fédération, puis définir les règles communes en matière de demandes d'échange.



La diapositive de cette section est une diapositive animée qui montre le volume de trafic dans un scénario fédéré business-to-business au moyen d'une application Web en charge des revendications. Dans ce cas, les utilisateurs de « Trey Research » doivent accéder à une application en ligne de « A. Datum Corporation ». Le processus d'authentification AD FS est le suivant :

1. Un utilisateur de « Trey Research » utilise un navigateur pour établir une connexion HTTPS au serveur Web de « A. Datum Corporation ».
2. L'application Web reçoit la demande, et vérifie que l'utilisateur ne dispose pas d'un jeton valide enregistré dans un cookie par le navigateur Web. Comme l'utilisateur n'est pas authentifié, l'application Web redirige le client vers le serveur de fédération de « A. Datum Corporation » par un message de redirection HTTP 302.
3. L'ordinateur client envoie une demande HTTPS au serveur de fédération de « A. Datum Corporation ». Le serveur de fédération détermine le « home realm » pour l'utilisateur. Dans ce cas, il s'agit de « Trey Research ».
4. Le serveur Web redirige l'ordinateur client vers le serveur de fédération dans le « home realm » de l'utilisateur, qui est « Trey Research ».
5. L'ordinateur client envoie une demande HTTPS au serveur de fédération de « Trey Research ».
6. Si l'utilisateur est déjà enregistré dans ce domaine, le serveur de fédération peut prendre son ticket Kerberos et la demande d'authentification à partir de l'AD DS pour le compte de l'utilisateur en utilisant IWA. Si l'utilisateur n'est pas enregistré dans ce domaine, il est invité à s'identifier.
7. Le contrôleur de domaine AD DS authentifie l'utilisateur et envoie le message de confirmation sur le serveur de fédération avec les autres informations concernant l'utilisateur que le serveur de fédération peut utiliser pour générer les demandes de l'utilisateur.
8. Le serveur de fédération crée la demande de l'utilisateur d'après les règles définies pour le partenaire de fédération. Le serveur de fédération met les données sur les réclamations dans un jeton de sécurité signé numériquement, puis le transmet à l'ordinateur client qui le renvoie au serveur de fédération de « A. Datum Corporation ».
9. Le serveur de fédération de « A. Datum Corporation » confirme la fiabilité du jeton de sécurité.
10. Le serveur de fédération de « A. Datum Corporation » crée et signe un nouveau jeton, qu'il envoie à l'ordinateur client. L'ordinateur client envoie ensuite le jeton vers l'URL originale qui a été demandée.
11. L'application sur le serveur Web reçoit la demande et valide les jetons signés. Le serveur web délivre au client un cookie de session confirmant l'authentification. Le serveur de fédération émet un cookie persistant basé sur les fichiers, d'une validité de 30 jours par défaut. Il supprime l'étape de découverte du « home realm » pendant la durée de vie du cookie. Le serveur donne alors l'accès à l'application en se fondant sur les revendications de l'utilisateur.

Question : Vérifiez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|--|---------|
| Une approbation fédérée est la même chose qu'une approbation de forêt que les organisations peuvent configurer entre les forêts AD DS. | |

Leçon 2

Exigences et planification AD FS

Quand vous comprenez le fonctionnement AD FS, vous pouvez déployer le service. Avant de déployer AD FS, vous devez comprendre les composants que vous devez déployer et les conditions que vous devez respecter, notamment en ce qui concerne les certificats. Cette leçon donne un aperçu du déploiement du rôle de serveur du AD FS dans Windows Server 2016.

Objectifs des leçons

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

- Décrire les composants AD RMS.
- Configuration des prérequis AD FS
- Décrire l'infrastructure principale publique (PKI) et les exigences de certification pour l'AD FS.
- Décrire les rôles du serveur de fédération AD FS.
- Décrire comment fournir une haute disponibilité pour AD FS.
- Décrire comment planifier la capacité pour AD FS.
- Décrire comment planifier un déploiement AD FS pour les services en ligne de Microsoft.

Composants AD FS

Pour comprendre le processus de configuration pour AD FS, vous devez d'abord comprendre tous les éléments qui font partie de AD FS. Ces composants fonctionnent ensemble pour fournir une solution complète pour l'authentification basée sur les revendications dans une organisation ou entre les organisations.

| | |
|--------------------------------------|--|
| Serveur de fédération | Parties de confiance |
| Proxy FSP et Proxy d'application Web | Approbation de fournisseur de revendications |
| Revendications | Approbation d'une partie de confiance |
| Règles de revendication | Certificats |
| Magasin d'attributs | Points de terminaison |
| Fournisseurs de revendications | |

Le tableau suivant répertorie les composants AD FS.

| Composant | Les tâches qu'il exécute |
|---|--|
| Serveur de fédération | Le serveur de fédération émet, gère et valide les demandes portant sur des revendications d'identité. Toutes les implémentations de AD FS nécessitent au moins un service de fédération pour chaque partie. |
| Proxy de serveur de fédération et proxy d'application Web | Le proxy du serveur de fédération est un composant facultatif que vous déployez habituellement dans un réseau de périmètre. Il n'ajoute aucune fonctionnalité au déploiement AD FS, mais il est déployé pour fournir une couche de renforcement de la sécurité pour les connexions à partir de l'Internet pour le serveur de fédération. Dans Windows Server 2016, la fonctionnalité du proxy du serveur de fédération fait partie du Proxy d'application Web. |
| Revendications | Une revendication est une déclaration qui est faite par une entité de confiance sur un objet comme un utilisateur. La revendication peut inclure le nom de l'utilisateur, le titre du poste ou tout autre facteur pouvant être utilisé dans un scénario d'authentification. |
| Règles de revendication | Les règles de réclamation déterminent la façon dont les serveurs de fédération traitent les revendications. Par exemple, une règle de revendication peut indiquer qu'une adresse e-mail est acceptée comme une réclamation valide ou qu'un nom de groupe d'une organisation se traduit par un rôle spécifique à l'application dans l'autre organisation. Les règles sont habituellement traitées en temps réel, dès que les réclamations sont faites. |
| Magasin d'attributs | AD FS utilise un magasin d'attributs pour rechercher les valeurs des réclamations. AD DS est un magasin d'attribut courant qui est disponible par défaut, car le rôle du serveur de fédération doit être installé sur un serveur relié au domaine. |
| Fournisseurs de revendications | Le fournisseur de revendications est le serveur qui émet les réclamations et authentifie les utilisateurs. Un fournisseur de revendications fonctionne comme un côté du processus d'authentification et d'autorisation AD FS. Le fournisseur de revendications gère l'authentification des utilisateurs et émet ensuite les revendications que l'utilisateur présente à une partie de confiance. |
| Parties de confiance | La partie de confiance est la partie où se trouve l'application, et elle fonctionne comme l'autre côté du processus d'authentification et d'autorisation AD FS. La partie de confiance est un service Web qui consomme les réclamations du fournisseur de revendications. Le serveur de la partie utilisatrice doit avoir WIF installé ou utiliser l'agent en charge des revendications AD FS 1.0. |

| Composant | Les tâches qu'il exécute |
|--|---|
| Approbation de fournisseur de revendications | L'approbation du fournisseur de revendications contient les données de configuration qui définissent les règles selon lesquelles un client peut demander les revendications d'un fournisseur de revendications puis les soumettre à une partie de confiance. La confiance se compose de différents identifiants tels que les noms, les groupes et les règles. |
| Approbation d'une partie de confiance | L'approbation d'une partie de confiance contient les données de configuration AD FS utilisées pour fournir des revendications concernant un utilisateur ou un client à une partie de confiance. Elle se compose de différents identifiants, tels que les noms, les groupes et les règles. |
| Certificats | AD FS utilise des certificats numériques lors de la communication sur Secure Sockets Layer (SSL) ou dans le cadre du processus d'émission de jetons, du processus de réception de jetons et le processus de publication de métadonnées. Les certificats numériques sont également utilisés pour la signature des jetons. |
| Points de terminaison | Les points de terminaison sont des mécanismes de Windows Communication Foundation qui permettent l'accès aux technologies AD FS, y compris l'émission de jetons et la publication de métadonnées. AD FS est livré avec les points de terminaison intégrés qui sont responsables des fonctionnalités spécifiques. |

Exigences AD FS

Avant de déployer AD FS, vous devez vous assurer que votre réseau interne réponde aux conditions préalables de base. La configuration des services réseau suivants est essentielle pour un déploiement AD FS réussi :

- Connectivité réseau. La connectivité réseau suivante est nécessaire :
 - L'ordinateur client doit être en mesure de communiquer avec l'application Web, le serveur de fédération de ressources ou le proxy de serveur de fédération et le serveur de fédération de comptes ou le proxy de serveur de fédération en utilisant le protocole HTTPS.
 - Les proxys de serveurs de fédération doivent être en mesure de communiquer avec les serveurs de fédération dans la même organisation en utilisant le protocole HTTPS.
 - Les serveurs de fédération et les ordinateurs clients internes doivent être en mesure de communiquer avec les contrôleurs de domaine pour l'authentification.
- AD DS AD DS est un élément essentiel de l'AD FS. Le serveur de fédération doit être relié à un domaine AD DS. Cependant, le proxy d'application Web n'a pas besoin d'être relié au domaine.

Un déploiement AD FS réussi comprend l'infrastructure critique suivante :

- Connectivité du réseau TCP/IP
- AD DS
- Magasin d'attributs
- DNS

- Magasin d'attributs. AD FS utilise un magasin d'attributs pour générer des informations sur les revendications. Le magasin d'attributs contient des informations sur les utilisateurs, qui sont extraites du magasin par le serveur AD FS une que l'utilisateur été authentifié.
- DNS (Domain Name System). La résolution de noms permet aux clients de trouver les serveurs de fédération. Les ordinateurs clients doivent résoudre les noms DNS pour tous les serveurs de fédération ou batteries AD FS auxquelles ils se connectent et pour les applications Web que l'ordinateur client tente d'utiliser. Si un ordinateur client est externe au réseau, l'ordinateur client doit résoudre le nom DNS pour le proxy d'application Web, et non pour le serveur de fédération interne ou la batterie AD FS. Le proxy d'application Web doit résoudre le nom du serveur de fédération interne ou de la batterie. Si les utilisateurs internes doivent accéder directement au serveur de fédération interne et si les utilisateurs externes doivent se connecter via le proxy du serveur de fédération, vous devez configurer plusieurs enregistrements DNS dans les zones DNS internes et externes.

Exigences certificat et PKI

AD FS permet aux ordinateurs de communiquer de façon sécurisée et améliorée, même si elles peuvent être dans des endroits différents. Dans ce scénario, la plupart des communications entre les ordinateurs passent par l'Internet. Pour aider à assurer la sécurité du trafic réseau, toutes les communications sont cryptées à l'aide d'un chiffrement SSL. Ce facteur signifie qu'il est important de choisir et d'attribuer correctement des certificats SSL aux serveurs AD FS. Pour fournir un chiffrement SSL, les serveurs AD FS utilisent des certificats comme les certificats de services de communication, les certificats de signature de jetons et les certificats de déchiffrement de jetons.

- Les certificats utilisés par AD FS :
 - Certificats de communication de service ;
 - Certificats de signature de jetons ;
 - Certificats de déchiffrement de jeton ;
- Lors du choix des certificats, veillez à ce que le certificat de communication de service soit approuvé par tous les partenaires et clients de la fédération.

Certificats de communication de service

AD FS permet de sécuriser toutes les communications à l'aide d'un chiffrement SSL, ce qui nécessite un certificat. Tous les ordinateurs qui communiquent avec le serveur AD FS doivent approuver le certificat utilisé pour la communication de service. Si tous les ordinateurs et les périphériques qui entrent en contact avec votre serveur AD FS sont reliés au domaine, vous pouvez envisager d'utiliser un certificat généré en interne pour AD FS. Cependant, dans la plupart des cas, un minimum de communication existe entre le serveur AD FS et les ordinateurs externes ou les entreprises partenaires. Dans ce cas, vous devez utiliser un certificat d'une autorité de certification (CA) tierce. Vous pouvez utiliser un composant logiciel du certificat et de la console de **Gestion AD FS** console pour gérer tous les certificats.

 **Remarque :** Si vous modifiez le certificat de communication de service après la configuration initiale, vous devez le modifier pour tous les nœuds de la batterie de serveurs et vous assurer que le service AD FS est autorisé à lire la clé privée sur le certificat de chaque nœud.

Certificats de signature de jetons

AD FS utilise un certificat de signature de jetons pour signer chaque jeton ayant des problèmes de serveur de fédération. Ce certificat est essentiel dans un déploiement AD FS, car la signature de jeton indique le serveur fédération qui a émis le jeton. Le fournisseur de revendications utilise ce certificat pour s'identifier et la partie de confiance l'utilise pour vérifier que le jeton provient d'un partenaire de fédération de confiance.

La partie de confiance nécessite également un certificat de signature de jetons pour signer les jetons qu'elle prépare pour applications compatibles avec AD FS. Pour que les applications de destination valident ces jetons, le certificat de signature de jeton de la partie de confiance doit valider ces jetons.

Lorsque vous configurez un serveur de fédération, le serveur attribue un certificat auto-signé comme certificat de signature de jetons. Dans la plupart des cas, vous n'avez pas besoin de mettre à jour ce certificat avec un certificat d'une autorité de certification tierce. Lorsque AD FS crée une approbation de fédération, il configure l'approbation de ce certificat en même temps. Vous pouvez configurer plusieurs certificats de signature de jetons sur le serveur de fédération, mais AD FS utilise uniquement le certificat principal.

Certificats de déchiffrement de jeton

AD FS utilise des certificats de déchiffrement de jetons pour chiffrer le jeton d'utilisateur tout entier avant de transmettre le jeton à travers le réseau du serveur de fédération du fournisseur de revendications au serveur de fédération de la partie de confiance. Pour offrir cette fonctionnalité, AD FS fournit la clé publique du certificat de serveur de fédération de la partie de confiance au serveur de fédération du fournisseur de revendications. Le certificat est envoyé sans la clé privée. Le serveur du fournisseur de revendications utilise la clé publique du certificat pour chiffrer le jeton d'utilisateur. Lorsque le serveur du fournisseur de revendications renvoie le jeton au serveur de fédération de la partie de confiance, il utilise la clé privée du certificat pour déchiffrer le jeton. Cela fournit une couche supplémentaire de renforcement de la sécurité lors de la transmission des certificats à travers un réseau non sécurisé, comme l'Internet.

Lorsque vous configurez un serveur de fédération, le serveur attribue un certificat auto-signé comme le certificat de décryptage de jeton. Dans la plupart des cas, vous n'êtes pas tenu de mettre à jour ce certificat avec un certificat provenant d'une autorité de certification tierce. Lorsque AD FS crée une approbation de fédération, il configure l'approbation de ce certificat en même temps.

 **Remarque :** les proxys de serveurs de fédération exigent seulement un certificat SSL. Le serveur de fédération utilise ce certificat pour permettre la communication SSL pour toutes les connexions clientes.

Choisir une autorité de certification

Les serveurs de fédération AD FS peuvent utiliser des certificats auto-signés ; des certificats provenant d'une autorité de certification interne et privée ; ou des certificats qui ont été achetés auprès d'une autorité de certification externe et publique. Dans la plupart des déploiements AD FS, le facteur le plus important lors du choix des certificats est qu'ils soient approuvés par toutes les parties concernées. Cela signifie que si vous configurez un déploiement AD FS qui interagit avec d'autres organisations, vous utiliserez presque certainement une autorité de certification publique pour le certificat SSL sur un proxy de serveur de fédération, car les certificats délivrés par l'autorité de certification publique sont automatiquement approuvés par tous les partenaires.

Si vous déployez AD FS uniquement pour votre organisation et que tous les serveurs et les ordinateurs clients sont sous votre contrôle, vous pouvez envisager d'utiliser un certificat provenant d'une autorité de certification interne et privée. Si vous déployez une autorité de certification interne et en entreprise dans Windows Server 2016, vous pouvez utiliser la stratégie de groupe pour aider à faire en sorte que tous les ordinateurs de l'organisation approuvent automatiquement les certificats émis par l'autorité de certification interne. Le recours à une autorité de certification interne peut diminuer de façon significative le coût des certificats.

 **Remarque :** le déploiement d'une autorité de certification interne à l'aide des services de certificats Active Directory (AD CS) est un processus simple, mais il est essentiel de planifier et de mettre en œuvre le déploiement avec attention.

Rôles du serveur de fédération

Dans Windows Server 2016, les rôles du serveur pour AD FS sont :

- Fournisseurs de revendications Un fournisseur de revendications est un serveur de fédération qui fournit aux utilisateurs des jetons signés contenant des revendications. Les serveurs de fédération du fournisseur de revendications sont déployés dans les entreprises où se trouvent les comptes d'utilisateurs. Lorsqu'un utilisateur demande un jeton, le serveur de fédération du fournisseur de revendications vérifie l'authentification des utilisateurs en utilisant AD DS, puis recueille des informations à partir d'un magasin d'attributs comme AD DS ou Active Directory Lightweight Directory Services (AD LDS) pour remplir la demande de l'utilisateur avec les attributs requis par l'organisation partenaire. Le serveur émet des jetons au format SAML. Le serveur de fédération du fournisseur de revendications contribue également à protéger le contenu des jetons de sécurité en transit en les signant et éventuellement en les chiffrant.
- Partie de confiance. Une partie de confiance est un serveur de fédération qui reçoit des jetons de sécurité d'un fournisseur de revendications approuvé. Les serveurs de fédération de partie de confiance sont déployés dans les organisations qui fournissent l'accès aux applications aux organisations de fournisseur de revendications. La partie de confiance accepte et valide la revendication, puis émet de nouveaux jetons de sécurité que le serveur Web peut utiliser pour fournir un accès approprié à l'application.

- Un serveur de fédération fournisseur de réclamations :
 - Authentifie les utilisateurs internes ;
 - Gère les jetons signés contenant des revendications de l'utilisateur.
- Un serveur de fédération qui est une partie de confiance :
 - Consomme les jetons du fournisseur de revendications ;
 - Gère les jetons d'accès aux applications.
- Un proxy FSP :
 - Est situé dans un réseau de périmètre ;
 - Fournit une couche d'amélioration de la sécurité pour les serveurs de fédération internes.



Remarque : Un serveur AD FS unique peut fonctionner à la fois comme fournisseur de revendications et comme partie de confiance, même avec les mêmes organisations partenaires. Le serveur AD FS fonctionne comme un fournisseur de revendications lorsqu'il authentifie les utilisateurs et fournit des jetons pour une autre organisation, mais il peut également accepter des jetons de la même organisation ou d'organisations différentes dans un rôle de partie de confiance.

- Proxy d'application Web. Un proxy d'application Web fournit un niveau supplémentaire de renforcement de la sécurité pour le trafic AD FS qui vient de l'Internet aux serveurs de fédération AD FS internes. Un proxy de service de fédération peut être déployé à la fois dans les organisations de fournisseurs de revendications et de parties de confiance. Du côté du fournisseur de revendications, le proxy recueille les informations d'authentification des ordinateurs clients et passe au serveur de fédération du fournisseur de revendications pour le traitement. Le serveur de fédération émet un jeton de sécurité au proxy, qui l'envoie au proxy de la partie de confiance. Le proxy de fédération de la partie de confiance accepte ces jetons, puis les transmet au serveur de fédération interne. Le serveur de fédération de la partie de confiance émet un jeton de sécurité pour l'application Web puis envoie le jeton au proxy de serveur de fédération, qui transmet le jeton au client. Le proxy d'application Web ne fournit pas de jetons et ne crée pas de revendications. Il transmet uniquement les demandes des clients aux serveurs AD FS internes. Toutes les communications entre le proxy d'application Web et le serveur de fédération utilisent le protocole HTTPS.



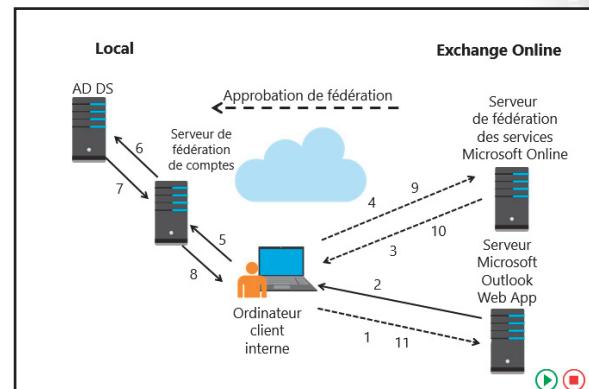
Remarque : vous ne pouvez pas configurer un proxy d'application Web comme fournisseur de revendications ou comme partie de confiance. Le fournisseur de revendications et la partie de confiance doivent être membres d'un domaine AD DS. Vous pouvez configurer le proxy d'application Web comme un membre d'un groupe de travail ou comme un membre d'une forêt extranet et vous pouvez le déployer dans un réseau de périmètre.

Planification d'un déploiement AD FS pour les services en ligne

Vous pouvez utiliser AD FS pour fournir une expérience SSO aux utilisateurs à travers plusieurs plates-formes du cloud. Par exemple, une fois que les utilisateurs se sont authentifiés avec leurs identifiants AD DS, ils peuvent utiliser ces informations d'identification de domaine pour accéder à des services de Microsoft online services, comme Azure, Microsoft Intune ou Office 365.



Remarque : AD FS peut également fournir une SSO à d'autres fournisseurs basés sur le cloud. Parce que les services AD FS sont basés sur des standards ouverts, ils peuvent interagir avec tout système fondé sur des revendications conformes.



Un déploiement Microsoft Exchange hybride est un exemple de service basé sur le cloud qui utilise AD FS pour l'authentification. Dans ce type de déploiement, une organisation déploie une partie ou la totalité de ses boîtes de réception dans un environnement 365 Office. Toutefois, l'organisation gère l'ensemble de ses comptes d'utilisateur dans son environnement AD DS local. Le déploiement utilise un outil de synchronisation d'annuaire pour synchroniser les informations de compte utilisateur de l'environnement local au déploiement d'Office 365.

Quand les utilisateurs tentent de se connecter à leurs boîtes de réception Office 365, ils doivent s'authentifier avec leurs identifiants AD DS internes. Si les utilisateurs tentent de se connecter directement à l'environnement Office 365, ils sont redirigés vers le déploiement AD FS interne pour s'authentifier avant d'avoir l'accès.

Les étapes suivantes décrivent ce qui se passe lorsqu'un utilisateur tente d'accéder à sa boîte de réception en ligne en utilisant un navigateur Web :

1. L'utilisateur ouvre un navigateur Web et envoie une demande HTTPS au serveur Office 365 Outlook Web App.
2. Le serveur Outlook Web App reçoit la demande et vérifie si l'utilisateur fait partie d'un déploiement hybride Exchange Server. Si tel est le cas, le serveur redirige l'ordinateur client vers le serveur de fédération Microsoft online services.
3. L'ordinateur client envoie une demande HTTPS au serveur de fédération Microsoft online services.
4. L'ordinateur client est de nouveau redirigé vers le serveur local de fédération. La redirection vers le domaine d'accueil de l'utilisateur est basée sur le suffixe UPN de l'utilisateur.
5. L'ordinateur client envoie une demande HTTPS au serveur local de fédération.

6. Si l'utilisateur est déjà connecté au domaine, le serveur local de fédération peut prendre ticket Kerberos de l'utilisateur et demander une authentification de l'AD DS pour le compte de l'utilisateur en utilisant l'authentification Windows. Si les signes de l'utilisateur provenant de l'extérieur du réseau ou d'un ordinateur qui n'est pas membre du domaine interne, l'utilisateur est invité à entrer les informations d'identification.
7. Le contrôleur de domaine AD DS authentifie l'utilisateur puis renvoie le message de réussite au serveur de fédération avec d'autres informations relatives à l'utilisateur et que le serveur de fédération peut utiliser pour générer les revendications de l'utilisateur.
8. Le serveur de fédération crée la revendication pour l'utilisateur selon les règles définies lors de la configuration du serveur AD FS. Les données des revendications sont placées dans un jeton de sécurité signé numériquement et transmis au navigateur de l'utilisateur. Ensuite, les données sont envoyées à l'ordinateur client, qui les publie de nouveau sur les serveurs de fédération Microsoft online services.
9. Le serveur de fédération de Microsoft online services vérifie que le jeton de sécurité provient d'un partenaire de fédération de confiance. Cette approbation est configurée lorsque vous configurez l'environnement du serveur Exchange hybride.
10. Le serveur de fédération Microsoft online services crée et signe un nouveau jeton qu'il envoie à l'ordinateur client, qui le renvoie à son tour au serveur Outlook Web App.
11. Le serveur Outlook Web App reçoit la demande et valide les jetons signés. Le serveur délivre au client un cookie de session indiquant qu'il s'est authentifié avec succès. L'utilisateur est alors autorisé à accéder à sa boîte de réception Exchange Server.

Préparation de l'intégration SSO avec Microsoft online services

Une SSO, également appelée *fédération d'identité*, permet de simplifier le processus de connexion à vos utilisateurs lorsqu'ils accèdent à des services en ligne comme Office 365 ou Microsoft Intune. Grâce aux SSO, les utilisateurs peuvent utiliser leurs identifiants AD DS internes pour accéder à ces services en ligne. Lorsque vous configurez AD FS pour fournir une authentification unique pour Microsoft online services, vous créez une approbation fédérée entre l'annuaire local de votre organisation et le domaine fédéré que vous indiquez dans votre Azure AD client.



Remarque : Pour plus d'informations sur Azure AD, voir la Leçon 1, « Présentation des déploiements AD DS avancés » dans le module 3, « Gestion de l'infrastructure AD DS avancée ».

Pour déployer l'intégration SSO avec Microsoft online services, utilisez les étapes principales suivantes :

1. Préparer votre environnement pour la SSO :
 - a. Déployer AD DS dans votre environnement local.
 - b. Installer le rôle AD FS.
 - c. Préparer AD DS. En fonction de vos domaines, vous pourriez avoir besoin d'accomplir ces tâches :
 - i. Vérifier que les UPN sont fixés et connus par les utilisateurs.
 - ii. Vérifier que le suffixe de domaine UPN est sous le domaine que vous choisissez de mettre en place pour l'authentification unique.



Remarque : rappelez-vous que les UPN que vous utilisez pour la SSO ne peuvent contenir que des lettres, des chiffres, des points, des tirets et des tirets du bas.

- iii. Assurez-vous que le nom de domaine que vous choisissez de fédérer est enregistré en tant que domaine public auprès d'un bureau d'enregistrement ou dans vos propres serveurs publics DNS.



Remarque : si votre nom de domaine AD DS n'est pas un domaine Internet public, vous devez définir un UPN pour avoir un suffixe de domaine pouvant être enregistré publiquement. Dans cette situation, nous vous recommandons d'utiliser quelque chose de familier à vos utilisateurs, comme leur domaine de messagerie.

Pour préparer votre environnement Active Directory pour l'authentification unique, vous pouvez exécuter l'outil Microsoft Deployment Readiness Tool. Cet outil inspecte votre environnement Active Directory et fournit un rapport contenant des informations pour savoir si vous êtes prêt à configurer SSO. Sinon, il énumère les changements à effectuer pour préparer la SSO.



Remarque : pour télécharger l'outil, rendez-vous sur la page « Microsoft Office 365 Deployment Readiness Tool » à l'adresse suivante : <http://aka.ms/D9vmqf>

2. Déployez des services de fédération :
 - a. Déployer votre batterie de serveurs AD FS.
 - b. Configurer l'accès extranet :
 - i. Installer le rôle du Proxy d'applications Web.
 - ii. Configurez le Proxy d'application Web.
 - c. Établissez une synchronisation entre AD DS et Azure AD :
 - i. En utilisant Windows PowerShell et le module Azure AD pour Windows PowerShell, ajoutez les domaines nécessaires avec l'applet de commande **New-MsolFederatedDomain**.



Remarque : pour des conseils supplémentaires sur ces étapes, consultez la Liste de vérification : « Utiliser AD FS pour mettre en œuvre et gérer les authentifications uniques » à l'adresse suivante : <http://aka.ms/U193rk>

3. Déploiement de la synchronisation des annuaires :
 - a. Téléchargez et installez Azure AD Connect pour permettre la synchronisation du domaine dans Azure.
4. Vérifier l'authentification unique :
 - a. Sur un ordinateur relié au domaine, connectez-vous à votre service cloud de Microsoft en utilisant le même nom de connexion que vous utilisez pour vos informations d'identification d'entreprise.
 - b. Cliquez sur le champ **Mot de passe**. Si l'authentification unique est mise en place, le champ **Mot de passe** sera grisé et vous verrez le message suivant : **Vous devez à présent vous connecter à votre entreprise**.
 - c. Cliquez sur le lien **Connectez-vous à votre entreprise**. Si vous êtes en mesure de vous connecter, une SSO a été mise en place.

Planification d'un déploiement AD FS à haute disponibilité

La disponibilité de votre environnement AD FS est essentielle lorsque les services dans Office 365 sont activés pour l'authentification fédérée. Par exemple, si votre serveur de fédération est indisponible, toutes les demandes d'authentification des utilisateurs échoueront et les utilisateurs ne pourront pas accéder aux services d'Office 365. De même, si votre proxy de fédération est indisponible, les demandes d'authentification des utilisateurs externes ne seront pas transmises à votre serveur de fédération et ces utilisateurs ne pourront pas accéder aux services d'Office 365. Par conséquent, il est essentiel que la préparation pour le déploiement AD FS comprenne la planification de la haute disponibilité de vos serveurs de fédération AD FS et les serveurs proxy de fédération AD FS.

Lorsque vous planifiez la disponibilité de votre environnement AD FS pour authentification fédérée, il vous faut prendre en compte les catégories suivantes :

- La batterie de serveurs de fédération ;
- Équilibrage de la charge réseau (NLB) ;
- La base de données de configuration.

 **Remarque :** la disponibilité AD FS affecte uniquement l'authentification des utilisateurs et n'a aucune incidence sur les services d'Office 365. Par exemple, si les utilisateurs ne peuvent pas accéder à leur messagerie dans Office 365, leurs boîtes de réception dans Exchange Online continueront de recevoir des e-mails.

Batterie de serveurs de fédération

Avec Windows Server 2012 ou une version antérieure, vous pouvez déployer le serveur de fédération AD FS en tant que serveur autonome ou dans une batterie de serveurs de fédération. Cependant, nous vous recommandons de toujours déployer plus d'un serveur dans une batterie de serveurs de fédération. Même si la batterie se compose initialement que d'un seul serveur de fédération, cette méthode de déploiement vous offre la possibilité d'ajouter d'autres serveurs de fédération ultérieurement pour l'équilibrage de la charge ou la tolérance aux pannes. Toutefois, si le serveur de fédération AD FS est déployé en tant que serveur autonome, vous ne pourrez pas ajouter des serveurs ultérieurement.

Avec Windows Server 2012 R2 ou une version ultérieure, vous pouvez déployer le serveur de fédération AD FS que dans une batterie de serveurs de fédération. Bien que cette méthode de déploiement vous offre la possibilité d'ajouter d'autres serveurs de fédération ultérieurement, nous vous recommandons de déployer plus d'un serveur de fédération dans une batterie pour vos environnements de production.

L'équilibrage de la charge réseau

Vous devez utiliser l'équilibrage de la charge réseau (NLB) ou d'autres formes de regroupement pour allouer une adresse IP unique pour plusieurs serveurs de fédération AD FS. Avec cette option de déploiement, la défaillance d'un serveur de fédération unique ne devrait pas affecter les services de fédération pour les utilisateurs. De même, vous devez également utiliser l'équilibrage de la charge réseau pour fournir un réseau de proximité AD FS dans le réseau de périmètre pour veiller à ce que les clients externes ne soient pas touchés par la défaillance d'un ordinateur proxy AD FS.

 **Remarque :** Bien que ce cours n'entre pas dans les détails, vous pouvez également déployer un équilibrage de charge matérielle à la place d'un équilibrage de la charge réseau pour fournir une haute disponibilité à vos serveurs de fédération et serveurs proxy de fédération.

Base de données de configuration

Si vous avez choisi la base de données interne Windows comme stockage de données AD FS, une copie de la base de données de configuration existe sur chaque serveur. Toutefois, si vous avez choisi Microsoft SQL Server comme stockage de données AD FS, vous devez planifier un déploiement SQL Server à haute disponibilité. Par opposition à la base de données interne Windows, le déploiement d'une batterie de serveurs de fédération AD FS avec SQL Server ne permet pas une haute disponibilité de la base de données de configuration, par défaut. Par exemple, si le serveur exécutant SQL Server est indisponible, le serveur de fédération AD FS ne pourra pas se connecter à la base de données de configuration et le service AD FS ne démarra pas. Par conséquent, vous devriez envisager de déployer AD FS avec un cluster SQL Server ou un partenaire de basculement SQL Server. Même si vous pouvez activer le cluster SQL Server à tout moment, le partenaire de basculement du cluster SQL Server peut être activé uniquement pendant le déploiement AD FS ou après. La raison est que vous utilisez AD FS pour configurer le partenaire de basculement.

 **Remarque :** pour plus d'informations sur les solutions à haute disponibilité de SQL Server, reportez-vous à la page : « Solutions haute disponibilité (SQL Server) » à l'adresse suivante : <http://aka.ms/lSr6m4>

Planification de capacité

La planification de capacité pour les serveurs de fédération vous aide à évaluer les besoins en matériel pour chaque serveur de fédération et pour le nombre de serveurs de fédération à déployer. La planification de capacité contribue également à estimer et à préparer l'augmentation de la taille de la base de données de configuration AD FS.

Feuille de calcul de planification des capacités

La feuille de calcul de planification des capacités AD FS inclut des fonctionnalités semblables à celles d'une calculatrice, comme prendre des données d'utilisation attendues sur les utilisateurs de votre organisation, et renvoie un nombre optimal recommandé de serveurs de fédération pour un environnement de production AD FS.

La feuille de calcul de planification des capacités AD FS nécessite les entrées suivantes :

- Une valeur (40, 60, ou 80 pour cent) qui représente au mieux le pourcentage du nombre total d'utilisateurs prévu pour envoyer des demandes d'authentification à AD FS pendant les périodes de pic d'utilisation.
- Une valeur (1 minute, 15 minutes ou 1 heure) qui représente au mieux la durée de la période de pic d'utilisation attendue
- Le nombre total d'utilisateurs qui nécessitent un accès SSO à l'application en charge des revendications, selon que les utilisateurs :
 - Se connectent à AD DS depuis un ordinateur sur le réseau d'entreprise
 - Se connectent à AD DS à distance depuis un ordinateur
 - Se connectent depuis une autre organisation ou depuis un fournisseur d'identité SAML 2.0

• Utilisez les éléments suivants lors de la planification de la capacité de vos serveurs de fédération :

- Exigences relatives à la feuille de calcul pour la planification de la capacité :
 - Le pourcentage du nombre total d'utilisateurs prévu pour envoyer des demandes d'authentification à AD FS pendant les périodes d'utilisation maximale ;
 - La durée prévue de la période d'utilisation maximale ;
 - Le nombre total d'utilisateurs qui nécessitent un accès à authentification unique (SSO).

• Tableau des estimations :

| Nombre d'utilisateurs | Nombre minimal de serveurs |
|-----------------------|--------------------------------------|
| Moins de 1 000 | 2 serveurs de fédération, 2 proxys |
| 1 000 - 15 000 | 2 serveurs de fédération, 2 proxys |
| 15 000 - 60 000 | 3-5 serveurs de fédération, 2 proxys |
| Plus de 60 000 | 5+ serveurs de fédération, 3+ proxys |



Remarque : pour plus d'informations sur la feuille de calcul de planification des capacités AD FS ou pour la télécharger, consultez la page : « Planification des capacités du serveur AD FS » à l'adresse suivante : <http://aka.ms/M9f7aw>

Tableau d'estimation

FS AD peut évoluer pour supporter des dizaines de milliers d'utilisateurs, et il vous permet d'ajouter d'autres serveurs de fédération à une batterie de serveurs pendant que votre entreprise évolue. Vous pouvez utiliser le tableau suivant pour vous aider à estimer le nombre minimum de serveurs de fédération AD FS et de serveurs proxy d'application Web ou serveurs proxy de fédération que vous aurez besoin de déployer. Ces estimations sont basées sur le nombre d'utilisateurs qui auront besoin d'un accès SSO au service cloud, y compris l'accès à distance.



Remarque : sauf indication contraire, tous les serveurs de fédération doivent être déployés dans une batterie de serveurs de fédération avec un magasin de base de données interne Windows pour la base de données de configuration. Bien que le nombre de serveurs de fédération peut être diminué dans certains scénarios du tableau suivant, un serveur de fédération supplémentaire est inclus pour assurer la redondance.

| Nombre d'utilisateurs ayant accès aux services Office 365 | Nombre minimum de serveurs AD FS à déployer | Recommandation et étapes |
|---|---|--|
| Moins de 1 000 utilisateurs | 2 serveurs de fédération 2 proxys | Avec moins d'utilisateurs, envisagez de déployer les serveurs de fédération sur deux contrôleurs de domaine existants puis de mettre en œuvre l'équilibrage de la charge en utilisant l'équilibrage de la charge réseau. Pour les proxys, envisagez d'utiliser deux serveurs Web existants ou serveurs proxy, puis configurez les deux serveurs pour le rôle de serveur proxy de fédération ou de proxy d'application Web. |
| 1 000 - 15 000 utilisateurs | 2 serveurs de fédération 2 proxys | Pour les organisations de moyenne à grande taille, envisagez de déployer les serveurs de fédération sur deux ordinateurs dédiés avec l'équilibrage de la charge réseau. Envisagez le déploiement des proxys sur deux ordinateurs dédiés avec l'équilibrage de la charge réseau. |
| 15 000 - 15 000 utilisateurs | 3 - 5 serveurs de fédération 2 proxys | Pour chaque incrément de 15 000 utilisateurs au-delà de 15 000, vous devez déployer un serveur de fédération supplémentaire à la batterie à charge équilibrée, jusqu'à un maximum de cinq serveurs pris en charge par la base de données interne Windows, ou plus avec une base de données SQL Server. Pour les proxys, envisagez de déployer des nœuds supplémentaires pour améliorer les performances. |

| Nombre d'utilisateurs ayant accès aux services Office 365 | Nombre minimum de serveurs AD FS à déployer | Recommandation et étapes |
|---|--|--|
| Plus de 60 000 utilisateurs | 5 serveurs de fédération ou plus 3 proxys ou plus | Pour les entreprises de plus de 60 000 utilisateurs, vous devez mettre en œuvre cinq serveurs de fédération (ou plus) qui utilisent SQL Server comme base de données de configuration. Vous devez également déployer trois proxys ou plus qui utilisent du matériel d'équilibrage de charge et non d'équilibrage de charge réseau (NLB). |

Démonstration : Installation du rôle serveur AD FS

Dans cette démonstration, vous allez apprendre à :

- Installer AD FS ;
- Ajouter un enregistrement DNS pour l'AD FS ;
- Configurer AD FS.

Procédure de démonstration

Installer AD FS

1. Sur **LON-DC1**, ouvrez Windows Powershell et utilisez l'applet de commande **Add-KdsRootKey** pour créer la clé racine du Service de distribution de clés de groupe Microsoft.
2. Utilisez le **Gestionnaire de serveur** pour installer le rôle **Services AD FS**.

Ajouter un enregistrement DNS pour AD FS

- Sur **LON-DC1**, utilisez le **Gestionnaire DNS** pour ajouter un nouvel enregistrement d'hôte au AD FS dans la zone de recherche directe **Adatum.com**, puis utilisez les paramètres suivants :
 - Nom : **adfs**
 - Adresse IP : **172.16.0.10**

Configurer AD FS

1. Sur **LON-DC1**, dans les notifications du **Gestionnaire de serveur**, cliquez sur **Configurer les Services AD FS sur ce serveur**.
2. Utilisez les options suivantes pour configurer le serveur AD FS :
 - **Créer le premier serveur de fédération dans une batterie de serveurs de fédération**
 - Compte à utiliser pour la configuration : **Adatum\Administrateur**
 - Certificat SSL **adfs.adatum.com**
 - Nom d'affichage du service de fédération : **A. Datum Corporation**
 - Créer un compte de service géré de groupe : **Adatum\Service ADFS**
 - **Créez une base de données sur ce serveur à l'aide de la base de données interne Windows**

Question : Vérifiez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|---|---------|
| Dans Windows Server 2016, la fonctionnalité du serveur proxy de fédération fait partie du rôle Proxy d'application Web. | |

Leçon 3

Déploiement et configuration AD FS

Le scénario de déploiement AD FS le plus simple est celui effectué au sein d'une seule organisation. Dans ce scénario, un serveur AD FS peut fonctionner à la fois comme fournisseur de revendications et comme partie de confiance. Tous les utilisateurs de ce scénario sont internes, tout comme l'application à laquelle ils accèdent.

Cette leçon apporte des détails sur les composants requis pour configurer l'AD FS dans le cadre d'un déploiement en interne. Ces composants comprennent les revendications, les règles de revendication, les approbations des fournisseurs de revendications et celles des parties de confiance.

Objectifs des leçons

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

- Décrire les revendications AD FS et les règles de revendication ;
- Décrire une approbation de fournisseur de revendications ;
- Décrire une approbation de partie de confiance ;
- Expliquer comment configurer les approbations des fournisseurs de revendications et des parties de confiance ;
- Expliquer comment installer et configurer AD FS ;
- Expliquer comment configurer un compte partenaire et un partenaire de ressource ;
- Expliquer comment configurer les règles de revendications ;
- Décrire comment fonctionne la découverte du domaine d'accueil ;
- Expliquer comment gérer un déploiement AD FS.

Quelles sont les revendications AD FS et les règles de revendications ?

Les revendications AD FS fournissent le lien entre le fournisseur de revendications et les rôles des parties de confiance dans le cadre d'un déploiement AD FS. Une *revendication AD FS* est une déclaration effectuée par une entité de confiance, comme un fournisseur de revendications, sur un sujet particulier, comme un utilisateur. Le fournisseur de revendications crée les revendications et la partie de confiance les consomme. Les revendications AD FS offrent aux fournisseurs de revendications un moyen flexible et normalisé leur permettant de communiquer des informations spécifiques sur les utilisateurs au sein de leur organisation. Les revendications AD FS fournissent également aux parties de confiance un moyen permettant de définir exactement les informations dont ils ont besoin, afin de permettre l'accès aux applications. Les informations relatives aux revendications fournissent les détails requis pour permettre l'accès aux applications qui prennent en charge les revendications.

- Les revendications fournissent des informations sur les utilisateurs du fournisseur à la partie de confiance
- AD FS :
 - Fournit un ensemble de revendications intégrées par défaut ;
 - Permet la création de revendications personnalisées ;
 - Demande que chaque revendication ait un URI unique.
- Les revendications peuvent être :
 - Récupérées à partir d'un magasin d'attributs ;
 - Calculées sur la base des valeurs récupérées ;
 - Transformées en d'autres valeurs.



Types de revendications

Chaque revendication AD FS correspond à un type spécifique de revendication : adresse e-mail, nom d'utilisateur principal, nom de famille et autres. Les utilisateurs reçoivent des revendications en fonction du type de revendication défini. Ainsi, un utilisateur peut recevoir par exemple une revendication du type **Nom de famille** affichant **Weber** comme valeur. L'AD FS propose de nombreux types de revendications intégrés. Vous pouvez également en créer de nouveaux en fonction de vos besoins organisationnels.

Un URI (Uniform Resource Identifier) identifie de manière unique chaque type de revendication AD FS. Ces informations font partie des métadonnées du serveur AD FS. Si par exemple l'organisation du fournisseur de revendications et l'organisation de la partie de confiance décident d'utiliser un type de revendication **Numéro de compte**, toutes deux doivent configurer un type de revendication sous ce nom. Le type de revendication est alors publié. Son URI doit être identique sur les deux serveurs AD FS.

Comment les valeurs des revendications sont-elles peuplées ?

Les revendications émises par un fournisseur de revendications contiennent les informations requises par la partie de confiance pour permettre l'accès approprié à l'application. Dans le cadre de la planification d'un déploiement AD FS, une des premières étapes est de définir exactement quelles sont les informations que les applications doivent posséder sur chaque utilisateur afin de pouvoir lui fournir l'accès requis. Une fois réunies ces informations, les revendications sont alors définies sur le serveur de fédération du fournisseur de revendications. Le serveur AD FS peut obtenir les informations nécessaires pour émettre une revendication de plusieurs façons :

- Il peut récupérer la revendication à partir d'un magasin d'attributs. En effet, les informations nécessaires à l'émission d'une revendication sont très souvent déjà stockées dans un magasin d'attributs disponible sur le serveur de fédération. Ainsi, une organisation peut décider que la revendication doit inclure l'UPN de l'utilisateur, son adresse e-mail et son appartenance à des groupes spécifiques. Si ces informations sont déjà stockées dans l'AD DS, le serveur de fédération peut les récupérer à partir de l'AD DS lors de la création de la revendication. Étant donné que l'AD FS peut utiliser plusieurs types de sources pour émettre des revendications (AD DS, AD LDS, SQL Server, annuaire LDAP non Microsoft ou magasin d'attributs personnalisé), vous pouvez définir presque n'importe quelle valeur dans la revendication.
- L'AD FS peut calculer la revendication à partir des informations recueillies. Les serveurs de fédération de fournisseur de revendications peuvent également calculer les informations à partir des données recueillies auprès d'un magasin d'attributs. Par exemple, vous voulez inclure des informations sur le salaire d'une personne dans une revendication. Ces informations sont sans doute stockées dans une base de données des ressources humaines, mais leur valeur réelle peut être considérée comme étant confidentielle. Dans ce cas, vous pouvez définir une réclamation catégorisant les salaires au sein d'une organisation, puis demander au serveur AD FS de calculer dans quelle catégorie appartient un utilisateur spécifique. De cette façon, la revendication ne comprend que les informations de catégorie de salaire et pas le salaire réel de l'utilisateur.
- L'AD FS peut transformer la revendication d'une valeur à une autre. Parfois, les informations stockées dans un magasin d'attributs ne correspondent pas exactement à celles requises par l'application pour traiter les informations d'autorisation. L'application peut définir des rôles utilisateur qui ne correspondent pas exactement aux attributs stockés dans un magasin d'attributs. Cependant, le rôle d'application peut être mis en corrélation avec les membres du groupe AD DS. Ainsi, les utilisateurs du groupe des ventes peuvent être mis en corrélation avec un rôle d'application spécifique, alors que les utilisateurs du groupe de gestion des ventes peuvent être corrélés avec un rôle d'application différent. Pour établir la corrélation dans l'AD FS, vous pouvez configurer une transformation des revendications qui obtient la valeur indiquée par le fournisseur de revendications et la traduit en une revendication utilisable par l'application de la partie de confiance.

- Si vous avez déployé le Contrôle d'accès dynamique, l'AD FS peut transformer une revendication de périphérique de Contrôle d'accès dynamique en une revendication AD FS. Cela permet de s'assurer que les utilisateurs peuvent accéder à un site Web AD FS uniquement à partir de postes de travail de confiance ayant reçu une revendication de périphérique valide.

Règles de revendication

Les *règles de revendication* définissent la façon dont les demandes sont envoyées et consommées par les serveurs AD FS. Elles définissent la logique métier à appliquer aux revendications fournies par les fournisseurs de revendications et acceptées par les parties de confiance. Vous pouvez utiliser les règles de revendication pour :

- Définir quelles revendications entrantes sont acceptées par un ou plusieurs fournisseurs de revendications.
- Définir quelles revendications sortantes sont fournies à une ou plusieurs parties de confiance.
- Appliquer les règles d'autorisation pour permettre l'accès à une partie de confiance spécifique pour un ou plusieurs utilisateurs ou groupes d'utilisateurs.

Vous pouvez configurer deux types de règles de revendication :

- Les règles de revendication pour une approbation de fournisseur de revendications. L'approbation de fournisseur de revendications est la relation d'approbation AD FS établie entre un serveur AD FS et un fournisseur de revendications. Vous pouvez configurer les règles de revendications pour définir comment le fournisseur traite et émet les revendications.
- Les règles de revendication pour une approbation de partie de confiance. L'approbation de partie de confiance est la relation d'approbation AD FS établie entre un serveur AD FS et une partie de confiance. Vous pouvez configurer des règles de revendication qui définissent la façon dont la partie de confiance accepte les revendications provenant du fournisseur de revendications.

Les règles de revendication configurées pour un fournisseur de revendications AD FS sont toutes considérées comme *règles de transformation d'acceptation*. Ces règles déterminent les types de revendications traitées par le fournisseur de revendications, puis envoyées à une partie de confiance. Quand vous configurez l'AD FS en interne au sein d'une seule organisation, une approbation de fournisseur de revendications est configurée par défaut au niveau du domaine AD DS local. Cet ensemble de règles définit les revendications qui sont acceptées par l'AD DS.

Il existe trois types de règles de revendication pour une partie de confiance :

- Les règles de transformation d'émission. Ces règles définissent les revendications envoyées à la partie de confiance définie dans l'approbation de partie de confiance.
- Les règles d'autorisation d'émission. Ces règles définissent les utilisateurs dont l'accès à la partie de confiance est autorisé ou refusé selon l'approbation de partie de confiance. Cet ensemble de règles peut inclure des règles qui permettent ou refusent explicitement l'accès à une partie de confiance.
- Les règles d'autorisation de délégation. Ces règles définissent les revendications qui précisent quels utilisateurs peuvent agir au nom d'autres utilisateurs pendant l'accès à la partie de confiance. Cet ensemble de règles peut inclure des règles qui autorisent ou refusent explicitement des délégués à une partie de confiance.

 **Remarque :** Une règle de revendication peut être associée à une seule relation d'approbation fédérée. Cela signifie que vous ne pouvez pas créer un ensemble de règles pour une approbation, puis les réutiliser pour d'autres approbations configurées sur votre serveur de fédération.

Les serveurs AD FS sont préconfigurés avec un ensemble de règles et plusieurs modèles par défaut, que vous pouvez utiliser pour créer des règles de revendication communes. Vous pouvez créer des règles de revendication personnalisées en utilisant le langage de règles de revendication AD FS.

Qu'est-ce qu'une approbation de fournisseur de revendications ?

Une approbation de fournisseur de revendications est configurée sur le serveur de fédération de la partie de confiance. *L'approbation de fournisseur de revendications* identifie le fournisseur de revendications et décrit comment la partie de confiance consomme les revendications émises par le fournisseur. Vous devez configurer une approbation de fournisseur de revendications pour chaque fournisseur. Une approbation de fournisseur de revendications est configurée par défaut pour le domaine AD DS local. Par contre, vous devez configurer tout fournisseur de revendications supplémentaire.

- Les approbations du fournisseur de réclamations :
 - Sont configurées sur le serveur de fédération de la partie de confiance ;
 - Identifient le fournisseur de revendications ;
 - Configurent les règles de revendication pour le fournisseur de revendications.
- Dans un scénario d'organisation unique, une approbation du fournisseur de revendication appelé Active Directory définit la manière dont les informations d'identification d'un utilisateur AD DS sont traitées
- Les approbations du fournisseur de revendications peuvent être configurées par :
 - Importation des métadonnées de fédération ;
 - Importation d'un fichier de configuration ;
 - Configuration manuelle de l'approbation.

Par défaut, un serveur AD FS est configuré avec une approbation de fournisseur de revendications nommée Active Directory. Cette approbation définit les règles de revendication, qui sont toutes des règles de transformation d'acceptation définissant la façon dont le serveur AD FS accepte les identifiants AD DS. Ainsi, les règles de revendication par défaut concernant l'approbation de fournisseur de revendications comprennent des règles qui transmettent les noms d'utilisateur, les identificateurs de sécurité (SID) et les SID de groupe à la partie de confiance. Dans un déploiement AD FS d'organisation unique où l'AD DS authentifie tous les utilisateurs, l'approbation de fournisseur de revendications par défaut peut suffire.

Quand vous développez le déploiement AD FS pour inclure d'autres organisations, vous devez créer des approbations de fournisseur de revendications supplémentaires pour chaque organisation fédérée agissant comme fournisseur d'identité. Vous avez trois options pour configurer l'approbation de fournisseur de revendications :

- Importer les données du fournisseur de revendications par le biais des métadonnées de fédération. Si le serveur de fédération AD FS ou le serveur proxy de fédération est accessible sur le réseau à partir du serveur de fédération AD FS, vous pouvez saisir le nom d'hôte ou l'URL du serveur de fédération partenaire. Dans ce cas, votre serveur de fédération AD FS se connecte au serveur partenaire et télécharge les métadonnées de fédération à partir du serveur. Les métadonnées de fédération contiennent toutes les informations nécessaires pour configurer l'approbation de fournisseur de revendications. Dans le cadre du téléchargement de métadonnées de fédération, votre serveur de fédération télécharge également le certificat SSL utilisé par le serveur de fédération partenaire.
- Importer les données du fournisseur de revendications à partir d'un fichier. Utilisez cette option si le serveur de fédération partenaire n'est pas directement accessible à partir de votre serveur de fédération, mais que l'organisation partenaire a exporté sa configuration et vous l'a fournie dans un fichier. Le fichier de configuration doit inclure les informations de configuration de l'organisation partenaire et le certificat SSL que le serveur de fédération partenaire utilise.
- Configurer manuellement une approbation de fournisseur de revendications. Utilisez cette option si vous souhaitez configurer tous les paramètres qui concernent l'approbation de fournisseur de revendications. Quand vous choisissez cette option, vous devez indiquer les caractéristiques prises en charge par le fournisseur de revendications et l'URL utilisée pour accéder aux serveurs AD FS du fournisseur. Vous devez également ajouter le certificat SSL que l'organisation partenaire utilise.

Qu'est-ce qu'une approbation de partie de confiance ?

Vous définissez une approbation de partie de confiance sur le serveur de fédération du fournisseur de revendications. *L'approbation de partie de confiance* identifie la partie de confiance et définit les règles de revendication qui déterminent la façon dont elle traite et accepte les demandes du fournisseur de revendications.

Dans un scénario d'organisation unique, la partie de confiance définit comment le serveur AD FS interagit avec les applications déployées au sein de l'organisation. Quand vous configurez la partie de confiance pour une organisation unique, vous devez indiquer l'URL de l'application interne. Vous pouvez également configurer des paramètres tels que l'URL utilisée par le serveur Web, les règles d'autorisation d'émission pour l'application et si l'application prend en charge SAML 2.0 ou si elle nécessite des jetons AD FS 1.0.

- Les approbations d'une partie de confiance :
 - Sont configurées sur le serveur de fédération du fournisseur de revendications ;
 - Identifient la partie de confiance ;
 - Configurent les règles de revendication pour la partie de confiance.
- Dans un scénario d'organisation unique, une approbation de partie de confiance définit la connexion aux applications internes
- Vous pouvez configurer les approbations d'une partie de confiance grâce à :
 - L'importation des métadonnées de fédération
 - L'importation d'un fichier de configuration
 - La configuration manuelle de l'approbation

La configuration d'une approbation de partie de confiance est similaire à celle de l'approbation de fournisseur de revendications. Quand vous développez le déploiement AD FS pour inclure d'autres organisations, vous devez créer des approbations de partie de confiance supplémentaires pour chaque organisation fédérée. Vous avez trois options pour configurer une approbation de partie de confiance :

- Importer les données de la partie de confiance à partir des métadonnées de fédération ; Si le serveur de fédération AD FS ou le serveur proxy de fédération est accessible sur le réseau à partir du serveur de fédération AD FS, vous pouvez saisir le nom d'hôte ou l'URL du serveur de fédération partenaire. Dans ce cas, votre serveur de fédération AD FS se connecte au serveur partenaire, puis télécharge les métadonnées de fédération à partir du serveur. Les métadonnées de fédération contiennent toutes les informations nécessaires pour configurer l'approbation de partie de confiance. Dans le cadre du téléchargement de métadonnées de fédération, votre serveur de fédération télécharge également le certificat SSL que le serveur de fédération du partenaire utilise.
- Importer les données de la partie de confiance à partir d'un fichier ; Utilisez cette option si le serveur de fédération partenaire n'est pas directement accessible à partir de votre serveur de fédération. Dans ce cas, l'organisation partenaire peut exporter ses informations de configuration dans un fichier, puis vous le fournir. Le fichier de configuration doit inclure les informations de configuration de l'organisation partenaire et le certificat SSL que le serveur de fédération partenaire utilise.
- Configurer manuellement une approbation de partie de confiance ; Utilisez cette option si vous souhaitez configurer tous les paramètres qui concernent l'approbation de partie de confiance.

Démonstration : Configuration d'approbations de fournisseur de revendications et de partie de confiance

Dans cette démonstration, vous allez apprendre à :

- Configurer une approbation de fournisseur de revendications ;
- Configurer une application WIF pour AD FS ;
- Configurer une approbation de partie de confiance.

Procédure de démonstration

Configurer une approbation de fournisseur de revendications

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, ouvrez **Gestion AD FS**.
2. Allez sur **Approbations de fournisseur de revendications**, puis modifiez les règles de revendication pour **Active Directory**.
3. Ajoutez une règle de transformation d'acceptation avec les paramètres suivants :
 - Modèle de règle de revendication : **Envoyer des attributs LDAP en tant que revendications**
 - Nom de la règle de revendication : **Règle des attributs LDAP sortants**
 - Magasin d'attributs : **Active Directory (AD)**
 - Mappage des attributs LDAP :
 - Adresses électroniques : **Adresse électronique**
 - Nom d'utilisateur principal : **Nom d'utilisateur principal**

Configurer une application WIF pour AD FS

1. Sur **LON-SVR1**, ouvrez le **Gestionnaire de serveur**, puis ouvrez l'utilitaire de fédération Windows Identity Foundation.
2. Dans l'**Assistant Utilitaire de fédération**, saisissez les informations suivantes :
 - Emplacement de la configuration d'application :
C:\inetpub\wwwroot\AdatumTestApp\web.config
 - URI de l'application : **https://lon-svr1.adatum.com/AdatumTestApp/**
 - **Utilisez un STS existant**
 - Emplacement du document de métadonnées de la fédération STS WS :
https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml
 - **Désactivez la validation de la chaîne de certificats**
 - **Pas de chiffrement**

Configurer une approbation de partie de confiance

1. Sur **LON-DC1**, dans la console **AD FS**, ajoutez une approbation de partie de confiance avec les paramètres suivants :
 - **Importez des données concernant la partie de confiance publiées en ligne ou sur un réseau local**
 - Adresse des métadonnées de fédération : **https://lon-svr1.adatum.com/adatumtestapp/**
 - Nom d'affichage : **Application de test A. Datum Corporation**
 - **Autoriser tout le monde**
2. Laissez ouverte la fenêtre **Modifier la stratégie d'émission de revendications pour l'application de test A. Datum Corporation** pour la tâche suivante. (Cette fenêtre peut être cachée derrière le Gestionnaire de serveur.)
3. Sur **LON-DC1**, dans la fenêtre **Modifier la stratégie d'émission de revendications pour l'application de test A. Datum Corporation**, ajoutez une règle dans l'onglet **Règles de transformation d'émission**.
4. Procédez à l'**Assistant Ajout de règle de revendication de transformation** avec les paramètres suivants :

- Modèle de règle de revendication : **Transférer ou filtrer une revendication entrante**
 - Nom de la règle de revendication : **Transférer le nom de compte Windows**
 - Type de revendication entrante : **Nom du compte Windows**
 - **Transférer toutes les valeurs de revendication**
5. Créer trois autres règles pour transférer les types de revendications **Adresse e-mail, UPN et Nom**.

Question : Que sont les règles de revendication ? Dans quel but pouvez-vous utiliser des règles de revendication ?

Installation et configuration de AD FS

Avant de déployer votre service de fédération, vous devez préparer l'environnement pour l'installation de AD FS. Cela peut comprendre la préparation de la base de données de configuration et de tous les comptes et certificats de service requis, ainsi que la préparation des enregistrements d'hôte DNS pour un accès interne ou externe au réseau d'entreprise.

SQL Server

Si vous envisagez d'héberger la base de données de configuration pour la batterie de serveurs de fédération AD FS sur SQL Server, vous devez déployer l'instance de SQL Server avant d'installer le premier serveur de fédération. Dans Windows Server 2016, AD FS prend en charge multiples options pour assurer la haute disponibilité de votre batterie de serveurs de fédération si SQL Server est utilisé. Vous devriez envisager une de ces options en préparant la base de données de configuration.

- Vous pourriez avoir besoin de préparer les éléments suivants avant d'installer AD FS :
 - Serveur SQL ;
 - Compte de service ;
 - Certificats ;
 - DNS ;
- Pendant le déploiement d'AD FS, vous :
 1. Installez AD FS ;
 2. Configurez AD FS ;
 3. Créez le premier serveur de fédération dans une batterie ;
 4. Ajoutez un serveur de fédération à une batterie ;
 5. Mettez à jour AD FS.



Remarque : Pour plus d'informations, consultez :

« Federation Server Farm Using SQL Server » à l'adresse : <http://aka.ms/mok3lw>

Compte de service

Si possible, vous devriez envisager d'utiliser un compte de service administré du groupe (gMSA) pour AD FS. Pendant l'étape de déploiement, l'**Assistant d'installation AD FS** crée et configure automatiquement un gMSA si vous disposez des autorisations requises pour AD DS. Autrement, vous devez créer un gMSA avant le déploiement du serveur de fédération AD FS.

Si vous n'êtes pas en mesure d'utiliser un gMSA, vous devez créer un compte de service standard dans AD DS avant de déployer le serveur de fédération AD FS et définir que le mot de passe n'expire jamais. Ce compte de service exige les droits d'accès suivants sur le serveur de fédération AD FS :

- Ouvrir une session en tant que service ;
- Ouvrir une session en tant que tâche.

Certificat

Vous pouvez importer le certificat pendant l'installation AD FS, mais devez demander le certificat SSL approprié à une autorité de certification approuvée publiquement avant le déploiement. Quand vous recevez le certificat de l'autorité de certification, installez-le dans le magasin de certificats personnels sur le serveur de fédération AD FS. Si vous déployez une batterie de serveurs de fédération, le nom du sujet ou le nom commun du certificat (CN) indiqué sur le certificat SSL doit correspondre au nom du service de fédération ou être un nom de certificat SSL avec caractères génériques. Ce certificat doit être installé dans le magasin de certificats personnels sur chacun des serveurs de fédération dans la batterie de serveurs.

DNS

Outre AD DS, DNS est l'un des principaux services de réseau et son rôle est essentiel au fonctionnement de AD FS. Grâce aux jeux d'enregistrements DNS, les utilisateurs et autres fournisseurs de services peuvent localiser votre service de fédération sur Internet et sur votre réseau d'entreprise.

Quand vous configurez le DNS pour assurer une prise en charge de AD FS, vous devriez considérer les points suivants :

- Si vous déployez une batterie de serveurs de fédération, vous devez créer un enregistrement d'hôte DNS sur vos serveurs DNS internes incluant le nom DNS du cluster NLB qui correspond à votre batterie de serveurs de fédération.
- Si vous déployez un serveur de fédération autonome, vous devez créer un enregistrement d'hôte DNS sur vos serveurs DNS internes incluant le nom DNS qui correspond à votre serveur de fédération.
- Si vous déployez un serveur proxy de fédération, vous devez créer un enregistrement d'hôte DNS sur les serveurs DNS du réseau de périmètre incluant le nom DNS utilisé pour l'équilibrage de charge qui correspond au serveur proxy AD FS ou au groupe de serveurs Proxy d'application Web.
- Si vous déployez un serveur proxy de fédération autonome, vous devez créer un enregistrement d'hôte DNS sur les serveurs DNS du réseau de périmètre incluant le nom DNS qui correspond à votre serveur proxy AD FS ou à votre serveur Proxy d'application Web.
- Si vous ne déployez pas de proxy de fédération, vous devez créer un enregistrement d'hôte DNS sur vos serveurs DNS du réseau de périmètre incluant le nom DNS du cluster NLB qui correspond à votre batterie de serveurs de fédération ou à votre serveur de fédération.



Remarque : Vous ne devriez pas utiliser des enregistrements CNAME en tant que nom du service de fédération.

Installer AD FS

Dans Windows Server 2016, AD FS 3.0 est installé en tant que rôle dans le Gestionnaire de serveur.

L'**Assistant Configuration du Gestionnaire de serveur** effectue les vérifications de validation et installe automatiquement tous les services requis par AD FS. Le rôle de serveur AD FS comprend des applets de commande Windows Powershell que vous pouvez utiliser pour effectuer un déploiement basé sur le Windows Powershell des serveurs et proxys AD FS.

Pour installer le rôle de serveur AD FS, utilisez le Gestionnaire de serveur **Assistant Ajout de rôles et de fonctionnalités** et choisissez le rôle de serveur AD FS. L'**Assistant Ajout de rôles et de fonctionnalités** sélectionne automatiquement les fonctionnalités Microsoft.NET Framework et AD FS Management Tools. Aucune autre fonctionnalité n'est requise.

Configurer AD FS

Quand le rôle AD FS est installé, l'**Assistant Ajout de rôles et de fonctionnalités** vous permet de démarrer l'**Assistant de configuration AD FS** pour configurer le serveur AD FS. Les étapes à effectuer dans l'**Assistant de configuration AD FS** varient selon que vous créez le premier serveur de fédération dans une batterie de serveurs de fédération ou que vous ajoutez un serveur de fédération à une batterie de serveurs de fédération existante. Vous pouvez également démarrer l'**Assistant de configuration AD FS** à partir du menu **Outils** du Gestionnaire de serveur ou à partir de l'écran de démarrage.

Créer le premier serveur de fédération dans une batterie de serveurs de fédération

Pour créer le premier serveur de fédération dans une batterie de serveurs de fédération, procédez comme suit :

1. Dans l'**Assistant de configuration AD FS**, sélectionnez l'option **Créer le premier serveur de fédération dans une batterie de serveurs de fédération**.
2. Sur la page **Se connecter à AD DS**, sélectionnez le compte qui dispose des autorisations d'administrateur de domaine AD DS. Si le compte que vous utilisez pour installer AD FS dispose des autorisations appropriées, laissez l'option par défaut, puis procédez à la suite. Sinon, modifiez-le en conséquence. Le compte que vous sélectionnez ne doit pas correspondre aux informations d'identification de votre compte de service.
3. Sur la page **Spécifier les propriétés de service**, sélectionnez le certificat correspondant à partir de la liste **Certificat SSL** (ou importez le certificat SSL s'il n'était pas déjà installé avant l'installation), puis spécifiez le **Nom du service de fédération** de la batterie de serveurs de fédération.
4. Sur la page **Spécifier un compte de service**, indiquez les informations d'identification du compte de service approprié pour AD FS.
5. Sur la page **Spécifier une base de données de configuration**, sélectionnez l'option pour créer une base de données en utilisant la base de données interne Windows (WID) ou l'option pour spécifier l'emplacement, le nom d'hôte et l'instance d'une base de données SQL Server existante.
6. Sur la page **Examiner les options**, notez que l'assistant affiche le résumé de vos choix, y compris vos actions de service de compte :
 - Si vous choisissez d'utiliser une base de données WID, l'assistant indique qu'il s'agit du serveur principal de la batterie de serveurs de fédération et que la base de données WID est installée.
 - Si vous choisissez d'utiliser une base de données SQL Server existante, l'assistant indique que qu'il s'agit du premier serveur de la batterie de serveurs et fournit les informations de la chaîne de connexion pour se connecter à SQL Server et récupérer la configuration.
7. Sur la page **Vérifications des conditions préalables**, notez que l'assistant affiche les résultats de la vérification préalable avant de procéder à l'installation de AD FS.



Remarque : Vous pouvez également utiliser l'applet de commande Windows Powershell **Install-AdfsFarm** pour déployer le premier serveur de fédération dans une batterie de serveurs de fédération.

Ajouter un serveur de fédération à une batterie de serveurs de fédération

Pour ajouter un serveur supplémentaire à une batterie de serveurs AD FS, procédez comme suit :

1. Dans l'**Assistant de configuration AD FS**, sélectionnez l'option **Ajouter un serveur de fédération à une batterie de serveurs de fédération**.
2. Sur la page **Se connecter à AD DS**, sélectionnez le compte qui dispose des autorisations d'administrateur de domaine AD DS. Si le compte que vous utilisez pour installer AD FS dispose des autorisations appropriées, laissez l'option par défaut, puis procédez à la suite. Sinon, modifiez-le en conséquence. Le compte que vous sélectionnez ne doit pas correspondre aux informations d'identification de votre compte de service.
3. Sur la page **Spécifier une batterie de serveurs**, indiquez le nom du serveur de fédération principal d'une batterie de serveurs qui utilise WID ou indiquez le nom d'hôte de la base de données et le nom d'instance d'une batterie de serveurs de fédération existante qui utilise SQL Server.
4. Sur la page **Spécifier le certificat SSL**, sélectionnez le certificat correspondant à partir de la liste **certificat SSL** ou importez le certificat SSL, si vous ne l'avez pas installé avant l'installation. Contrairement à l'autre option d'installation, vous n'êtes pas obligé de spécifier le nom du service de fédération de la batterie de serveurs de fédération. En effet, l'assistant connaît déjà le nom du service de fédération, s'appuyant sur les informations de base de données que vous avez fournies plus tôt.
5. Sur la page **Spécifier un compte de service**, indiquez les informations d'identification du compte de service approprié pour AD FS. Le compte que vous spécifiez doit être le même que celui utilisé sur le serveur de fédération principal dans la batterie de serveurs.
6. Sur la page **Examiner les options**, notez que l'assistant affiche le résumé de vos choix :
 - Si vous choisissez d'utiliser une base de données WID, l'assistant indique qu'il s'agit du serveur secondaire dans la batterie de serveurs et que la base de données WID est installée et répliquée à partir du serveur principal.
 - Si vous choisissez d'utiliser une base de données SQL Server existante, l'assistant indique les informations de la chaîne de connexion pour se connecter à SQL Server et récupérer la configuration.
7. Sur la page **Vérifications des conditions préalables**, notez que l'assistant affiche les résultats de la vérification préalable avant de procéder à l'installation de AD FS.



Remarque : Vous pouvez également utiliser l'applet de commande Windows Powershell **Add-AdfsFarmNode** pour ajouter un serveur de fédération à une batterie de serveurs de fédération.

Mettre à jour AD FS

Afin de vous assurer que votre environnement AD FS est fiable et stable, vous devez installer les mises à jour recommandées pour AD FS. Après l'installation et la configuration de vos serveurs de fédération AD FS, vous pouvez utiliser Microsoft Update pour vérifier les mises à jour disponibles.



Remarque : Pour plus d'informations sur toutes les mises à jour disponibles pour AD FS, reportez-vous à : « Updates for Services de fédération Active Directory (AD FS) (AD FS) » sur : <http://aka.ms/r8x4zf>

Configuration d'un partenaire de compte et d'un partenaire de ressource

Dans un scénario AD FS interentreprises, la terminologie utilisée pour décrire les deux partenaires impliqués dans un déploiement AD FS varie légèrement. Dans un tel scénario, l'organisation fournisseur de revendications peut également être appelée *partenaire de compte*. Une organisation partenaire de compte est une organisation dans laquelle les comptes utilisateurs sont stockés dans un magasin d'attributs. Un partenaire de compte prend en charge les tâches suivantes :

- Rassembler les informations d'identification des utilisateurs d'un service Web, puis les authentifier.
- Créer des revendications pour les utilisateurs, puis les intégrer dans des jetons de sécurité. Les jetons peuvent ensuite être présentés par une approbation de fédération pour obtenir l'accès aux ressources de fédération situées dans l'organisation d'un partenaire de ressource.

- Un partenaire de compte est un fournisseur de revendications dans un scénario de fédération interentreprise. Pour configurer un partenaire de compte :
 - Mettez en œuvre la topologie physique ;
 - Ajoutez un magasin d'attributs ;
 - Configurez une approbation de partie de confiance ;
 - Ajoutez une description de la revendication ;
 - préparez les ordinateurs clients pour la fédération.
- Un partenaire de ressource est une partie de confiance dans un scénario de fédération interentreprise. Pour configurer un partenaire de confiance :
 - Mettez en œuvre la topologie physique ;
 - Ajoutez un magasin d'attributs ;
 - Configurez une approbation de fournisseur de revendications ;
 - Créez un ensemble de règles de revendication pour l'approbation du fournisseur de revendications.

Utilisez les étapes suivantes pour configurer l'organisation partenaire de compte et la préparer pour la fédération :

1. Mettre en œuvre la topologie physique pour le déploiement du partenaire de compte. Cette étape peut comprendre le choix du nombre de serveurs de fédération et de serveurs proxy de fédération à déployer, ainsi que la configuration des enregistrements et certificats DNS requis.
2. Ajouter un magasin d'attributs. Utilisez la console **Gestion AD FS** pour ajouter le magasin d'attributs. Dans la plupart des cas, vous utilisez le magasin d'attributs Active Directory par défaut qui doit être employé pour l'authentification. Si besoin, vous pouvez toutefois ajouter d'autres magasins d'attributs pour construire les revendications d'utilisateur. Pour vous connecter à une organisation partenaire de ressource, vous créez une approbation de partie de confiance. La façon la plus simple est d'utiliser l'URL des métadonnées de fédération qui est fournie par l'organisation partenaire de ressource. Avec cette option, votre serveur AD FS recueille automatiquement les informations nécessaires pour l'approbation de partie de confiance.
3. Ajouter une description de revendication. La description de revendication énumère les revendications que votre organisation fournit au partenaire de ressource. Ces informations peuvent inclure les noms d'utilisateurs, adresses e-mail, informations d'appartenance au groupe ou autres informations permettant d'identifier les utilisateurs.
4. Préparer les ordinateurs clients pour la fédération. Cela peut impliquer deux étapes :
 - Ajouter le serveur de fédération partenaire de compte. Dans les navigateurs des ordinateurs clients, ajoutez le serveur de fédération de partenaires de compte à la liste de sites de l'Intranet local. En ajoutant le serveur de fédération de partenaires de compte à la liste Intranet local des ordinateurs clients, vous activez l'IWA, ce qui évite aux utilisateurs d'être invités à s'authentifier s'ils sont déjà connectés au domaine. Vous pouvez utiliser des objets de stratégie de groupe (GPO) pour associer l'URL à la liste de sites de l'Intranet local.
 - Configurer les certificats de confiance. Il s'agit d'une étape facultative, nécessaire uniquement si un ou plusieurs serveurs auxquels accèdent les clients ne disposent pas de certificats de confiance. L'ordinateur client peut devoir se connecter aux serveurs de fédération de comptes, aux serveurs de fédération de ressources ou encore aux serveurs proxy de fédération ainsi qu'aux serveurs Web de destination. Si l'un de ces certificats ne provient pas d'une autorité de certification approuvée

publiquement, vous pouvez devoir ajouter le certificat ou certificat racine requis au magasin de certificats des clients. Pour cela, vous pouvez utiliser des objets de stratégie de groupe.

Partenaire de ressource

Le *partenaire de ressource* correspond à la partie de confiance dans un scénario de fédération interentreprises. L'organisation partenaire de ressource correspond à l'endroit où se trouvent les ressources et où celles-ci sont rendues accessibles aux organisations partenaires de compte. Le partenaire de ressource prend en charge les tâches suivantes :

- Accepter les jetons de sécurité que le serveur partenaire de compte de la fédération produit et valide
- Consommer les réclamations des jetons de sécurité et fournir de nouvelles demandes à ses serveurs Web après avoir pris une décision d'autorisation

Les serveurs Web doivent avoir des agents web WIF ou AD FS 1.x informés des réclamations installés pour externaliser la logique d'identité et accepter les réclamations. WIF fournit un ensemble d'outils de développement qui permettent aux développeurs d'intégrer dans leurs applications l'authentification et l'autorisation basée sur les réclamations. WIF comprend également un kit de développement de logiciels et des exemples d'applications.

 **Remarque :** Vous pouvez utiliser des jetons SAML pour intégrer des applications sur les serveurs web non-Microsoft avec AD FS. Un logiciel open-source supplémentaire ou tiers est généralement nécessaire pour soutenir l'utilisation de jetons SAML sur un serveur Web non-Microsoft.

La configuration d'une organisation partenaire de ressource est similaire à la configuration d'une organisation du partenaire de compte et comporte les étapes suivantes :

1. Mettre en œuvre la topologie physique pour le déploiement du partenaire de ressource. Les étapes de planification et de mise en œuvre sont les mêmes que celles pour le partenaire de compte, avec l'ajout de la planification de l'emplacement et la configuration du serveur web.
2. Ajouter un magasin d'attributs. Le fournisseur de réclamations utilise le magasin d'attributs pour recueillir des données qui sont nécessaires pour émettre les réclamations. Les données des magasins d'attributs sont ensuite projetés en tant que réclamations à l'endroit du client.
3. Connectez-vous à une organisation partenaire de compte en créant une approbation de fournisseur de réclamations.
4. Créer un ensemble de règles de réclamation pour l'approbation du fournisseur de réclamation.

Configuration des règles de réclamation

Dans un déploiement AD FS d'organisation unique, il pourrait être simple de concevoir et mettre en œuvre des règles de réclamation. Dans de nombreux cas, vous pourriez avoir besoin de fournir uniquement le nom d'utilisateur ou du groupe que AD FS recueille de la réclamation et présente sur le serveur Web. Dans un scénario business-to-business, il est plus probable que vous devrez configurer des règles de réclamation plus compliquées pour définir l'accès des utilisateurs entre des systèmes très différents.

- Les scénarios interentreprises peuvent nécessiter des règles de revendication plus complexes
- Vous pouvez créer des règles de revendication en utilisant les modèles suivants :
 - Envoyer des attributs LDAP en tant que revendications ;
 - Envoyer une appartenance à un groupe comme revendication ;
 - Laisser passer ou filtrer une revendication entrante ;
 - Transformer une revendication entrante ;
 - Autoriser ou refuser les utilisateurs en se basant sur une réclamation entrante.
- Vous pouvez également créer des règles personnalisées en utilisant le langage des règles de réclamation AD FS

Les règles de réclamation définissent comment les partenaires de compte (fournisseurs de réclamations) créent des réclamations et comment les partenaires de ressources (parties utilisatrices) consomment les réclamations. AD FS fournit plusieurs modèles de règles que vous pouvez utiliser lorsque vous configurez des règles de réclamation :

- Envoyer des attributs LDAP en tant que Réclamations. Utilisez ce modèle lorsque vous sélectionnez des attributs spécifiques dans un magasin d'attributs LDAP pour remplir les réclamations. Vous pouvez configurer plusieurs attributs LDAP en tant que réclamations individuelles en une seule règle de réclamation que vous créez à partir de ce modèle. Par exemple, vous pouvez créer une règle qui extrait les attributs AD DS **sn** (Nom de famille) et **givenName** de tous les utilisateurs authentifiés et envoie ensuite ces valeurs comme des réclamations sortantes à envoyer à une partie utilisatrice.
- Envoyez une appartenance à un groupe en tant que Réclamation. Utilisez ce modèle pour envoyer un type de réclamation particulière et une valeur de réclamation associée qui est basée sur AD DS appartenance au groupe de sécurité de l'utilisateur. Par exemple, vous pouvez utiliser ce modèle pour créer une règle qui envoie un type de réclamation de groupe avec une valeur d'**Administration des ventes** si l'utilisateur est un membre du groupe de sécurité Sales Manager au sein du domaine AD DS. Cette règle émet une seule de réclamation sur la base du groupe AD DS que vous avez sélectionné en tant que partie du modèle.
- Laisser passer ou filtrer une réclamation entrante. Utilisez ce modèle pour définir des restrictions supplémentaires sur la base desquelles les réclamations sont soumises à des parties utilisatrices. Par exemple, vous voudrez peut-être utiliser une adresse de messagerie d'utilisateur en tant que réclamation, mais transmettre l'adresse e-mail uniquement si le suffixe de domaine sur l'adresse e-mail est *adatum.com*. Lorsque vous utilisez ce modèle, vous pouvez passer à travers n'importe quelle réclamation que vous avez extrait des règles de configuration des magasins d'attribut qui détermine si la demande est transmise en fonction de divers critères.
- Transformer une réclamation entrante. Utilisez ce modèle pour cartographier la valeur d'un attribut dans le magasin d'attribut de fournisseur de réclamations à une valeur différente dans le magasin d'attributs de la partie utilisatrice. Par exemple, vous voudrez peut-être fournir à tous les membres du département marketing d'A. Datum Corporation un accès limité à une application d'achat à Trey Research. À Trey Research, l'attribut utilisé pour définir le niveau d'accès limité pourrait avoir un attribut de **LimitedPurchaser**. Pour faire face à ce scénario, vous pouvez configurer une règle de réclamation qui transforme une réclamation sortante avec une valeur Département de marketing à une réclamation entrant en une valeur d'attribut **ApplicationAccess** de **LimitedPurchaser**. Les règles créées à partir de ce modèle doivent présenter une relation directe entre la demande au fournisseur de réclamation et la demande au partenaire de confiance.
- Autoriser ou Refuser des utilisateurs sur la base d'une réclamation entrante. Ce modèle est disponible uniquement lorsque vous configurez des règles d'autorisation d'émission ou des règles d'autorisation de délégation sur un groupe de partie utilisatrice. Utilisez ce modèle pour créer des règles qui autorisent ou refusent l'accès par les utilisateurs à une partie utilisatrice, en fonction du type et de la valeur d'une demande entrante. Ce modèle de règle de réclamation vous permet d'effectuer un contrôle d'autorisation du fournisseur de réclamations avant que les demandes soient envoyées à une partie utilisatrice. Par exemple, vous pouvez utiliser ce modèle de règle pour créer une règle qui autorise uniquement les utilisateurs du groupe de vente à accéder à une partie de confiance, alors que les demandes d'authentification des membres d'autres groupes ne seront pas envoyés à la partie utilisatrice.

Si aucun des modèles de règles de réclamation intégrés ne fournit les fonctionnalités dont vous avez besoin, vous pouvez créer des règles plus complexes en utilisant la langue des règles de réclamation AD FS. En créant une règle personnalisée, vous pouvez extraire des informations sur les réclamations à partir de plusieurs magasins d'attributs et combiner des types de réclamations dans une seule règle de réclamation.

Comment fonctionne la découverte du domaine de base

Certaines organisations partenaires de ressources qui abrite les applications en charge des réclamations pourraient vouloir permettre à plusieurs partenaires de compte pour accéder à leurs applications. Dans ce scénario, lorsque les utilisateurs se connectent à l'application Web, il doit y avoir un mécanisme pour diriger les utilisateurs vers le serveur de fédération AD FS dans leur domaine d'accueil, plutôt que sur le serveur de fédération d'une autre organisation. Le processus pour diriger les clients vers le compte partenaire approprié est *home realm discovery* (découverte du domaine d'accueil).

- La découverte de domaine d'accueil identifie le serveur AD FS chargé de fournir des revendications concernant un utilisateur
- Deux méthodes pour la découverte de domaine d'accueil existent :
 - Inviter les utilisateurs lors de leur première authentification ;
 - Inclure une chaîne *whr* dans l'application URL.
- Les applications SAML peuvent utiliser un profil préconfiguré pour la découverte de domaine d'accueil

La découverte du domaine d'accueil se produit après que le client se soit connecté sur le site de la partie utilisatrice et est redirigé vers le serveur de fédération de la partie utilisatrice. À ce stade, le serveur de fédération de la partie utilisatrice doit rediriger le client vers le serveur de fédération dans le domaine d'accueil du client afin que l'utilisateur puisse s'authentifier. Si plusieurs fournisseurs de réclamations sont configurés sur le serveur de fédération de la partie utilisatrice, il doit savoir vers quel serveur fédération rediriger le client.

En général, il existe deux façons de mettre en œuvre la maison royaume découverte :

- Demandez aux utilisateurs de choisir leur domaine d'accueil. Avec cette option, lorsque les utilisateurs sont redirigés vers le serveur de fédération de la partie utilisatrice, le serveur de fédération peut afficher une page Web qui leur demande d'identifier leur entreprise. Une fois que les utilisateurs ont sélectionné l'entreprise appropriée, le serveur de fédération peut utiliser cette information pour rediriger les ordinateurs clients vers le serveur d'accueil de la fédération appropriée pour l'authentification.
- Modifier le lien afin que l'application Web passe le paramètre *whr* qui contient le domaine d'accueil de l'utilisateur. Le serveur de fédération de la partie utilisatrice utilise ce paramètre pour rediriger automatiquement l'utilisateur vers le domaine d'accueil approprié. Cela signifie que l'utilisateur n'a pas à être invité à sélectionner le domaine d'accueil, parce que le paramètre *WHR* dans l'URL sur lequel l'utilisateur clique contient les informations nécessaires pour le serveur de fédération de la partie utilisatrice. Le lien modifié pourrait ressembler à ce qui suit :
<https://www.adatum.com/OrderApp/?whr=urn:federation:TreyResearch>.



Remarque : L'une des options disponibles pour la découverte du domaine d'accueil avec des applications compatibles SAML 2.0 est un profil SAML appelé IdPInitiated SSO. Ce profil SAML permet aux utilisateurs d'accéder en premier lieu, à leur fournisseur local de réclamation qui peut préparer un jeton utilisateur avec les réclamations nécessaires pour accéder à l'application web du partenaire. L'AD FS dans Windows Server 2012 ne met pas pleinement en œuvre le profil IdPInitiated SSO, mais il fournit une partie de la même fonctionnalité en mettant en œuvre un paramètre nommé *RelayState*.



Lectures supplémentaires : Pour plus d'informations sur *RelayState*, consultez : «Fournisseur d'identité de Soutien a initié RelayState» à : <http://aka.ms/Df8hq5>



Remarque : Le processus de découverte du domaine d'accueil se produit la première fois qu'un utilisateur tente d'accéder à une application Web. Une fois l'utilisateur authentifié, un

cookie de découverte du domaine d'accueil est délivré au client. Cela permet de garantir que l'utilisateur n'a pas besoin de passer par ce processus la prochaine fois. Cependant, ce cookie expire après un mois, à moins que l'utilisateur efface le cache des cookies avant expiration.

Démonstration : Configuration des règles de réclamation

Dans cette démonstration, vous apprendrez comment configurer des règles de réclamation sur un groupe de partie utilisatrice qui transmet un nom de groupe dans le cadre de la réclamation. Vous verrez également comment configurer une règle de réclamation qui limite l'accès des membres d'un groupe particulier à l'application.

Procédure de démonstration

- Sur **LON-DC1**, dans le Gestionnaire AD FS, dans la fenêtre **Edit Claim Rules for A. Datum Corporation Test App**, ajouter une **Issuance Transform Rule** règle de transformation d'émission avec les paramètres suivants :
 - Modèle de règle de revendication : **Transférer ou filtrer une revendication entrante**
 - Nom de la règle de revendication : **Envoyer la règle du nom de groupe**
 - Type de revendication entrante : **Groupe**
 - Transférer toutes les valeurs de revendication**
- Ajouter une nouvelle règle de contrôle d'accès en utilisant les paramètres suivants
 - Stratégie de contrôle d'accès **Groupe spécifique autorisé**
 - Nom du groupe : **Research**
- Modifier la politique d'émission de réclamation avec les paramètres suivants :
 - Nom de la règle de revendication : **Passer par UPN**
 - Type de revendication entrante : **Nom d'utilisateur principal**
 - Valeur de réclamation entrante : **@adatum.com**
- Voir la langue de règle pour la règle **Passez par UPN**.

Gérer un déploiement AD FS

Bien que AD FS soit déployé pour soutenir SSO sans beaucoup de traitements administratifs, vous pourriez avoir besoin d'effectuer périodiquement plusieurs tâches de gestion après avoir déployé AD FS. Cette rubrique décrit deux des tâches les plus courantes.

Gérer le cycle de vie des certificats

Pour éviter les problèmes qui sont causés par l'expiration des certificats, les certificats auto-générés et auto-signés générés par AD FS supportent un transfert automatique, qui renouvelle les certificats AD FS une fois par an sans intervention manuelle. Ce processus AD FS, appelé *automatic certificate rollover*, génère deux

- Après l'installation, vous devrez peut-être parfois effectuer des tâches de gestion AD FS, y compris :
 - Gérer le cycle de vie des certificats ;
 - Utiliser la substitution automatique de certificat, qui renouvelle les certificats AD FS une fois par an ;
 - Utiliser l'applet de commande **Get-AdfsCertificate** pour afficher les dates d'expiration des certificats ;
 - Utiliser l'applet de commande **Update-MsolFederatedDomain** pour gérer la substitution de certificat lorsque le certificat de signature de jetons AD FS se renouvelle sur une base annuelle ;
 - Utiliser l'applet de commande **Set-AdfsSyncProperties** pour changer les serveurs de fédération AD FS primaires et secondaires.

nouveaux certificats de signature de jetons chaque année. Si Office 365 n'est pas mis à jour avec le nouveau certificat de signature de jetons, aucun utilisateur ne peut se connecter et utiliser Office 365, parce que ce certificat signe toutes les assertions du serveur de fédération. Si une PKI interne est utilisée pour délivrer le certificat de signature de jetons, AD FS ne fournit pas le transfert automatique de certificat, et vous devez donc renouveler manuellement les certificats et les mettre à jour dans votre Office 365 locataire.

Vous pouvez utiliser la console **AD FS Management** pour afficher les dates d'expiration du certificat pour les communications de service, le décryptage de jeton et les certificats de signature de jetons. Dans l'arborescence de la console, développez **Service**, puis cliquez sur **Certificates**. Vous pouvez également utiliser le module Azure AD afin que Windows PowerShell affiche les détails du certificat lorsque vous utilisez l'applet de commande Windows PowerShell **Get ADFSCertificate**.

Si vous préférez utiliser le transfert automatique de certificat pour la gestion des cycles de vie de vos certificats, vous devez activer la fonctionnalité dans AD FS et installer l'outil d'installation automatique de mise à jour des métadonnées Office 365. Cette fonction est activée dans AD FS avec l'applet Windows PowerShell **Set-ADFSProperties**. Après avoir installé l'outil, vous pouvez utiliser l'applet Windows PowerShell **Update-MsolFederatedDomain** pour mettre à jour automatiquement le service Office 365 lorsque le certificat de signature de jetons AD FS se renouvelle sur une base annuelle. Cet outil devrait être exécuté en tant que tâche quotidienne planifiée sur le serveur AD FS ; sinon, le renouvellement du certificat de signature de jetons sur le serveur AD FS doit être contrôlé manuellement. La tâche planifiée mise à jour de l'outil doit être exécutée sur un seul serveur AD FS dans une grappe de serveurs de fédération.

 **Remarque :** Pour en savoir plus et télécharger l'outil d'installation automatique des métadonnées de mise à jour Office 365, reportez-vous à : «Microsoft Office 365 Federation Metadata Update Automation Installation Tool» sur : <http://aka.ms/i1hw8d>

Modification des serveurs de fédération AD FS primaires et secondaires

Si vous utilisez WID en tant que magasin de données AD FS, vous pouvez modifier les serveurs de fédération primaire et secondaire si vous utilisez le module Azure AD pour Windows PowerShell. Cette méthode vous permet de modifier le paramètre de rôle de base de données du serveur AD FS, puis de modifier le rôle.

Par exemple, si vous voulez passer du serveur de fédération primaire AdfsServer1 au serveur de fédération secondaire AdfsServer2, utilisez la procédure suivante :

1. Identifier le serveur de fédération secondaire (AdfsServer2) qui deviendra le serveur de fédération primaire.
2. Sur le serveur de fédération secondaire (AdfsServer2), à l'invite **Microsoft Azure AD Module for Windows PowerShell**, saisissez la commande ci-après, puis appuyez sur Entrée.

```
Set-AdfsSyncProperties -Rôle PrimaryComputer
```

3. Sur le serveur de fédération primaire (AdfsServer1), à l'invite **Microsoft Azure AD Module for Windows PowerShell**, saisissez la commande ci-après, puis appuyez sur Entrée.

```
Set-AdfsSyncProperties -Role SecondaryComputer -PrimaryComputerName AdfsServer2
```

Le serveur de fédération primaire devient un serveur de fédération secondaire avec une base de données IFD en lecture seule et le serveur de fédération secondaire devient le serveur de fédération primaire avec une base de données IFD en lecture / écriture à partir de laquelle les autres serveurs de fédération secondaire récupèrent leurs copies de bases de données.

 **Remarque :** La commutation des rôles de serveur de fédération AD FS ne s'applique pas si SQL Server est utilisé en tant que magasin de base de données de configuration AD FS. En effet, tous les serveurs AD FS de la fédération ont un accès en lecture / écriture à la base de données SQL Server.

Leçon 4

Présentation du proxy d'application Web

De nombreuses organisations ont besoin d'étendre l'infrastructure AD FS au-delà des réseaux privés et sur Internet. Pour améliorer la sécurité pour AD FS et les applications AD FS, vous utilisez le proxy d'application Web. Il est également important de prendre en compte la disponibilité importante pour AD FS, car il s'agit d'un service critique après sa mise en œuvre.

Objectifs des leçons

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

- Décrire les nouvelles fonctionnalités de l'application Web Proxy dans Windows Server 2016 ;
- Décrire la configuration d'une application pour le proxy d'application Web ;
- Décrire le proxy d'application Web et AD FS ;
- Expliquer l'installation et la configuration du Proxy d'application Web.

Qu'est-ce que le proxy d'application Web ?

Le proxy d'application Web dans Windows Server 2016 est un service de rôle d'accès à distance que vous pouvez utiliser pour garantir l'accès à distance sécurisé aux applications Web sur votre réseau interne. Les fonctions proxy d'application Web à la fois en tant que proxy inversé pour les applications Web et en tant que proxy AD FS.

Vous devez placer le proxy d'application Web dans un réseau de périmètre, parce que les clients externes qui accèdent à des applications Web ou AD FS établissent des connexions avec le proxy d'application Web. Le proxy d'application Web se connecte ensuite à l'application Web ou AD FS sur le réseau interne. Vous ne avez pas besoin de configuration spécifique au client pour utiliser le proxy d'application Web.

Lorsque vous mettez en œuvre le proxy d'application Web, vous améliorez la sécurité pour les applications Web ou AD FS en les isolant du contact direct avec Internet. Cela peut aider à protéger l'application Web ou AD FS interne de tous les paquets ou requêtes mal-formées qui pourraient entraîner une violation de la sécurité. Par exemple, le proxy d'application Web peut aider à protéger contre une attaque Zero-day qui utilise des requêtes mal-formées, ce qui peut entraîner une attaque par déni de service sur un serveur qui héberge une application Web. Le proxy d'application Web abandonne les demandes non valides avant qu'elles atteignent l'application Web sur un réseau interne.

Parce que le proxy d'application Web est complètement indépendant du logiciel de serveur Web utilisé, il est peu probable que le proxy d'application Web soit aussi vulnérable à la même attaque par déni de service qu'une application Web.

Windows Server 2016 comprend plusieurs améliorations au rôle Proxy d'application Web, y compris :

- La pré-authentification pour la publication de l'application Basic HTTP ;
- La publication de domaine avec un caractère générique des applications ;
- La redirection HTTP vers HTTPS ;
- La publication HTTP.



Remarque : Le proxy d'application Web utilise AD FS pour Pré-authentifier les utilisateurs d'Internet et il agit en tant que proxy FS AD pour la publication d'applications en charge des réclamations.

AD FS fournit aux utilisateurs une capacité SSO, qui permet aux utilisateurs d'entrer leurs informations d'identification pour accéder à une application Web de l'organisation sans être invité à entrer leurs informations d'identification à nouveau. Avec le proxy d'application Web, vous pouvez publier des applications en charge des réclamations qui utilisent la pré-authentification AD FS et des applications web qui utilisent la pré-authentification pass-through.

Habituellement, vous placez le proxy d'application Web dans votre réseau de périmètre entre deux dispositifs pare-feu.

 **Remarque :** Le serveur AD FS et les applications qui sont publiées sont situées dans le réseau d'organisation avec les contrôleurs de domaine et d'autres serveurs internes et le second pare-feu permet de les protéger. Ce scénario permet de fournir un accès sécurisé aux applications organisationnelles pour les utilisateurs sur Internet. Dans le même temps, ce scénario permet de protéger l'infrastructure TI de l'organisation contre les menaces de sécurité issues d'Internet.

Améliorations dans le proxy d'application Web dans Windows Server 2016

Windows Server 2016 comprend plusieurs améliorations du rôle Proxy d'application Web, y compris :

- La pré-authentification pour la publication d'applications HTTP Basic. HTTP Basic est le protocole d'autorisation qui est utilisé par de nombreux protocoles, y compris Exchange ActiveSync, pour connecter des périphériques, y compris des smartphones, avec des boîtes de réception Exchange Server.

 **Remarque :** Le proxy d'application Web interagit avec AD FS en utilisant la redirection qui n'est pas prise en charge sur les clients Exchange ActiveSync.

Le proxy d'application Web dans Windows Server 2016 vous permet de publier une application qui utilise le protocole HTTP Basic en activant l'application HTTP pour recevoir une partie de confiance non liée aux réclamations pour l'appli du service de fédération.

- L'édition de domaine Wildcard pour les applications afin de simplifier la publication d'applications Microsoft SharePoint. Pour soutenir des scénarios tels que ceux qui utilisent SharePoint 2013, l'URL externe pour l'application peut maintenant comporter une wildcard qui vous permet de publier des applications multiples à partir d'un domaine spécifique. https://*.sp-apps.adatum.com est un exemple d'URL.
- HTTP vers redirection HTTPS. Pour permettre de garantir que vos utilisateurs peuvent accéder à votre application, même s'ils ont omis de saisir **HTTPS** dans l'URL, le proxy d'application Web dans Windows Server 2016 prend désormais en charge la redirection HTTP vers HTTPS.
- Publication HTTP. Vous pouvez maintenant publier des applications HTTP en utilisant la pré-authentification pass-through.

Proxy d'application Web et proxy AD FS

De nombreuses organisations ont besoin pour fournir une authentification que les utilisateurs et les périphériques soient situés sur un réseau qui est externe à l'organisation. Dans la plupart des cas, le fait de permettre aux clients d'accéder à un serveur AD FS situé sur un réseau interne directement à partir d'Internet est un risque de sécurité inacceptable. Nous recommandons un proxy AD FS pour permettre aux clients sur Internet d'accéder à AD FS.

Un proxy AD FS est un proxy inversé situé dans un réseau de périmètre spécifiquement dédié à AD FS. Les clients se connectant à partir d'Internet communiquent avec le proxy AD FS dans le réseau de périmètre et non directement avec le serveur AD FS. Le proxy AD FS atténue les risques liés à la connectivité Internet pour AD FS.

- Le Proxy d'application Web Proxy est un proxy AD FS
- Le même certificat est utilisé sur le serveur AD FS et le Proxy d'application Web
- Un DNS fractionné autorise le même nom pour remédier aux adresses IP différentes



Remarque : Le terme *AD FS proxy* référencé ici est un terme générique désignant un serveur qui fournit des connexions de réseau indirectes au service de fédération et ne constitue pas une référence directe au serveur proxy AD FS dans Windows Server 2012.

Processus d'authentification

Un serveur interne AD FS utilise l'authentification Windows pour demander l'authentification. Cela fonctionne bien pour les ordinateurs internes qui sont reliés au domaine et peuvent automatiquement passer les informations d'identification du poste de travail à AD FS pour automatiser l'authentification. Cela empêche les utilisateurs de voir une demande d'informations d'authentification.

Lorsque les ordinateurs qui ne sont pas joints au domaine communiquent avec AD FS, le navigateur Web présente aux utilisateurs une invite de connexion. Cette invite d'ouverture de session demande un nom d'utilisateur et mot de passe, mais ne fournit aucun contexte.

Lorsque vous utilisez un proxy AD FS, une page d'authentification est fournie pour les ordinateurs qui ne sont pas joints au domaine. Ceci permet d'obtenir une meilleure compatibilité que celle de l'authentification Windows basé sur un navigateur pour clients AD FS qui utilisent des systèmes d'exploitation non Microsoft. Vous pouvez également personnaliser la page Web pour fournir plus de contexte pour les utilisateurs en ajoutant un logo de l'entreprise, par exemple.

Résolution DNS

Pour garantir un mouvement continu entre les réseaux internes et externes, le proxy d'application Web utilise le même nom d'hôte lors des accès AD FS interne et externe. Sur le réseau interne, le nom d'hôte AD FS décide de l'adresse IP du serveur interne AD FS. Sur le réseau externe, le nom d'hôte AD FS décide de l'adresse IP du proxy AD FS. Dans les deux cas, le nom d'hôte AD FS est différent de ceux des ordinateurs qui hébergent les rôles AD FS.

Certificats

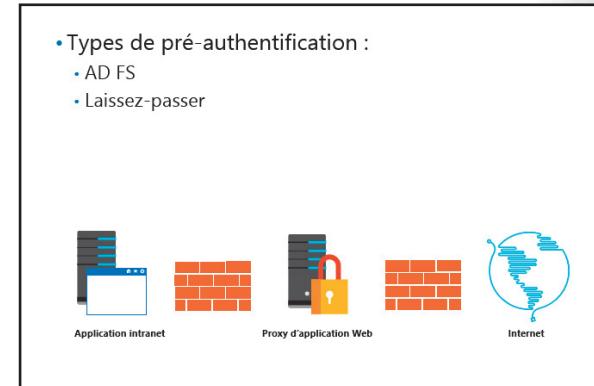
Le certificat utilisé sur un serveur interne AD FS a un nom d'objet qui est le même que le nom d'hôte de AD FS — par exemple, adfs.adatum.com. Parce que le même nom d'hôte est utilisé pour accéder à AD FS en interne et en externe via le proxy AD FS, vous devez configurer le proxy AD FS avec le même certificat que le serveur AD FS. Si le sujet du certificat ne correspond pas au nom d'hôte, l'authentification AD FS échouera.

 **Remarque :** Pour aider à garantir que vous avez un certificat avec le même nom de sujet, exporter le certificat du serveur AD FS et l'importer sur le serveur proxy d'application Web
Rappelez-vous d'inclure la clé privée lorsque vous exportez le certificat.

Modes d'authentification du Proxy d'application Web

Le Proxy d'application Web est utilisé pour aider à protéger les applications Web et AD FS quand elles sont accessibles à partir de l'Internet. Vous devez placer le serveur proxy d'application Web dans un réseau de périmètre. Pour installer le Proxy d'application Web, vous devez avoir mis en œuvre AD FS dans votre organisation. Toutes les informations de configuration pour le proxy d'application Web sont stocké dans AD FS.

Lorsque vous utilisez le proxy d'application Web comme proxy inversé pour les applications Web, vous devez configurer chaque application. Pour chaque application, vous devez configurer le type de pré-authentification pour l'application et les URL.



Pré-authentification de passage

Lorsque vous utilisez la pré-authentification pass-through, aucune pré-authentification n'est effectuée et les demandes valides sont transmises aux applications Web sur un réseau interne sans effectuer l'authentification sur un utilisateur. L'application effectue toutes les authentification pour une application seulement après qu'un utilisateur soit connecté. Vous pouvez utiliser la pré-authentification pass-through pour toute application web.

La pré-authentification aide à protéger une application Web des paquets mal-formés qui peuvent provoquer une attaque par déni de service. Cependant, l'application Web n'est pas protégée contre les menaces au niveau de l'application lorsque l'application traite incorrectement des données valides. Par exemple, une demande HTTPS avec des commandes HTTP valides est transmise à l'application, même si les mesures requises par les commandes HTTP peuvent entraîner l'échec de l'application Web.

Pré-authentification AD FS

Vous pouvez configurer le proxy d'application Web pour utiliser la pré-authentification AD FS ou l'authentification pass-through. Lorsque vous utilisez AD FS pour la pré-authentification, AD FS authentifie une demande de l'utilisateur avant de la transmettre à une application web interne. Ceci permet de garantir que seuls les utilisateurs autorisés peuvent envoyer des données à une application Web. La pré-authentification AD FS offre un plus grand niveau de protection que l'authentification pass-through, parce que les utilisateurs non authentifiés ne peuvent pas soumettre des demandes à l'application.

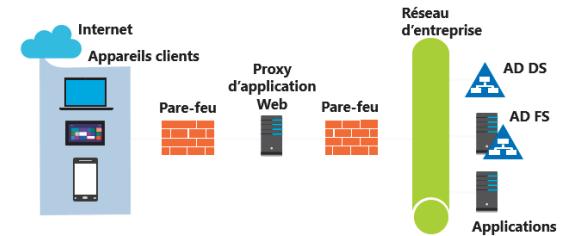
Seule une application compatible avec les réclamations qui utilise AD FS pour l'authentification peut utiliser la pré-authentification AD FS. Vous devez configurer l'application en charge des réclamations dans AD FS en tant que partie de confiance et la sélectionner dans une liste lorsque le proxy d'application Web est configuré. Le proxy d'application Web est conscient des parties de confiance configurées dans AD FS en raison de l'intégration entre AD FS et le proxy d'application Web.

Scénarios pour l'utilisation du Proxy d'application Web

Avec le proxy d'application Web, les organisations peuvent fournir un accès sélectif aux applications exécutées sur des serveurs à l'intérieur de l'organisation pour les utilisateurs situés à l'extérieur de l'organisation. Le processus permettant de rendre l'application externe disponible est connu sous le nom de *publishing*. Contrairement aux solutions traditionnelles de réseau privé virtuel (VPN), les utilisateurs peuvent accéder uniquement aux applications que vous publiez via un serveur proxy d'application Web. En fonction du soutien de l'application, l'accès à ces applications peut provenir essentiellement de tout appareil, y compris les appareils mobiles.

Le Proxy d'application Web peut être utilisé pour publier :

- Les services SharePoint ;
- Les services Exchange ;
- Les services Passerelle Bureau à distance ;
- Et d'autres applications personnalisées métier (LOB).



En plus des services de fédération d'édition, le serveur proxy d'application Web est largement utilisé pour publier des applications de navigateur, telles que celles de Remote Desktop Gateway (RD Gateway) et d'autres, applications (LOB) ligne d'activité personnalisée. En fait, il est également possible de publier des services HTTP back-end qui sont consommés par des applications non-navigateur.

Configuration des URL et certificats

Pour chaque application que vous publiez, vous devez configurer une URL externe et une URL du serveur interne. Les utilisateurs externes accèdent à l'application en utilisant l'URL externe. Le serveur proxy d'application Web utilise l'URL interne du serveur pour accéder à l'application au nom des utilisateurs externes.

Si vous utilisez le DNS fractionné, il est fréquent d'avoir la même valeur pour l'URL des serveur externe et interne. Certaines applications enregistrent des erreurs lorsque les URL externe et interne du serveur diffèrent. Lorsque l'URL externe et l'URL du serveur back-end diffèrent, seul le nom d'hôte dans l'URL change. Le chemin d'accès de l'application reste le même. Par exemple, si l'URL interne pour une application est <https://server1.adatum.com/app1>, vous ne pouvez pas avoir une URL externe de <https://extranet.adatum.com/Application1>.

Lorsque vous définissez l'URL externe, vous devez également sélectionner un certificat qui contient le nom d'hôte dans l'URL externe. Ce certificat doit être installé sur le serveur local. Cependant, il n'a pas besoin de faire correspondre le certificat utilisé sur le serveur back-end hébergeant l'application. Vous pouvez avoir un certificat pour chaque nom d'hôte utilisé sur le serveur proxy d'application Web ou un certificat unique avec plusieurs noms.

Publication des services SharePoint

Vous pouvez publier un site SharePoint via un serveur proxy d'application Web lorsque le site SharePoint est configuré pour l'authentification ou IWA basée sur les réclamations ou IWA. Si vous préférez utiliser AD FS pour la pré-authentification, vous devez configurer une partie de confiance en utilisant une des méthodes suivantes :

- Si le site SharePoint utilise l'authentification basée sur les réclamations, utilisez le **Add Relying Party Trust Wizard** pour configurer la partie de confiance compter pour l'application ;
- Si le site SharePoint utilise IWA, utilisez le **Add Non-Claims-Based Relying Party Trust Wizard** pour configurer la partie de confiance pour l'application ; Si vous souhaitez utiliser IWA avec une application Web basée sur les réclamations, vous devez déployer le Kerberos Key Distribution Center vers les contrôleurs du domaine.



Remarque : Pour authentifier les utilisateurs en utilisant IWA, le serveur proxy d'application Web doit être joint au domaine.

Pour fournir un accès IWA, le serveur proxy d'application Web doit être en mesure de fournir l'usurpation d'identité des utilisateurs à l'application publiée. Cette usurpation d'identité est appelé *Kerberos constrained delegation* et l'application doit être configurée pour supporter l'usurpation d'identité. Vous devez configurer le serveur proxy d'application Web pour la délégation aux principaux noms de service (SPN) des serveurs back-end.



Lectures supplémentaires : Pour plus d'informations sur la configuration d'un site Web à l'utilisation d'IWA et à la délégation Kerberos contrainte, reportez-vous à : « Configure a site to use Integrated Windows authentication » sur : <http://aka.ms/Nbsbll>

Si votre site SharePoint est configuré en utilisant des mappages d'accès alternatifs ou des collections de sites nommées par l'hôte, vous pouvez publier votre application avec différentes URL de serveur externe et back-end. Toutefois, si votre site SharePoint n'est pas configuré en utilisant des mappages d'accès ou des collections de sites nommées par l'hôte, les URL de serveur externe et back-end doivent être identiques.

Publication de services d'échange

Exchange Server fournit de multiples services pour les administrateurs et les utilisateurs, y compris l'appli Outlook Web App, Exchange Control Panel, Outlook Anywhere et Exchange ActiveSync. Ces services sont indépendants avec des URL différentes et de configurations d'authentification différentes. Le tableau suivant décrit les services d'échange que vous pouvez publier sur le proxy d'application Web et les types de pré-authentification pris en charge pour ces services.

| Service d'échange | Types de pré-authentification pris en charge |
|---------------------------------------|--|
| Outlook Web App | <ul style="list-style-type: none"> AD FS utilisant une authentification non basée sur les réclamations Pass-through AD FS utilisant une authentification basée sur les réclamations pour Exchange Server 2013 |
| Échanger le Panneau de configuration. | <ul style="list-style-type: none"> Pass-through |
| Outlook Anywhere | <ul style="list-style-type: none"> Pass-through |
| Exchange ActiveSync | <ul style="list-style-type: none"> Pass-through |

Afin que le service Outlook Anywhere fonctionne correctement, vous devez publier trois URL :

- L'URL Autodiscover
- Le nom d'hôte externe du serveur d'échange (qui est, l'URL auquel les clients Outlook accéderont)
- Le FQDN interne de l'instance du serveur d'échange

Pour publier l'appli Web Outlook en utilisant IWA, vous devez utiliser **Add Non-Claims-Based Relying Party Trust Wizard** pour configurer le groupe du parti de confiance pour l'application.



Remarque : Pour permettre aux utilisateurs de s'authentifier en utilisant IWA, le serveur proxy d'application Web doit être joint au domaine.

Pour fournir un accès IWA, l'application sur le serveur proxy d'application Web doit être configurée pour supporter la délégation Kerberos contrainte. Vous devez également enregistrer un SPN pour le compte de service du service Web et configurer le serveur proxy d'application Web pour la délégation à la SPN des serveurs back-end. Dans un environnement Exchange hautement disponible, vous devez utiliser un compte de service de remplacement.

 **Lectures supplémentaires :** Pour plus d'informations sur la configuration de l'authentification Kerberos pour les serveurs Exchange équilibrage de charge, reportez-vous à : « Configuring Kerberos authentication for load-balanced Client Access servers » sur : <http://aka.ms/Nd2avi>

Publier les services Remote Desktop Gateway

Certaines organisations offrent un accès aux services RD Gateway à partir d'Internet directement sur le serveur RD Gateway. Cependant, vous pourriez envisager de publier des services RD Gateway via le proxy d'application Web si vous souhaitez restreindre l'accès à votre passerelle RD et ajouter la pré-authentification pour les utilisateurs distants. Lors de la planification de votre déploiement, vous avez deux options pour la publication des services RD Gateway via le proxy d'application Web :

- Publication de l'application en utilisant l'authentification pass-through.

La publication de la demande avec l'authentification pass-through fournit un point d'entrée unique dans votre environnement de bureau à distance. Cependant, la méthode de déploiement varie selon que le rôle de votre accès à distance au bureau Web (RD Web Access) (**/rdweb** répertoire virtuel) et Passerelle RD (**/rpc** répertoire virtuel) sont sur le même serveur ou sur des serveurs différents :

- Si la RD Web Access et les rôles RD Gateway sont hébergés sur le même serveur passerelle RD, il vous suffit de publier la racine de la passerelle RD FQDN via le proxy d'application Web (par exemple, <https://rdg.contoso.com/>).
- Si la RD Web Access et les rôles RD Gateway sont hébergés sur des serveurs de passerelle RD distincts, vous devez publier individuellement les deux répertoires virtuels. Dans ce scénario, les applications publiées peuvent utiliser des FQDN externes identiques ou différents. Par exemple :
 - En utilisant le même FQDN, les URL peuvent être <https://rdg.contoso.com/rdweb/> et <https://rdg.contoso.com/rpc/>.
 - En utilisant des FQDN différents, les URL peuvent être <https://rdweb.contoso.com/rdweb/> et <https://gateway.contoso.com/rpc/>.

- Publication de l'application en utilisant la préauthentification.

De même, en ce qui concerne la façon dont vous publiez une application basée sur les réclamations, vous utilisez **Add Relying Party Trust Wizard** pour créer une *approbation manuelle d'une partie de confiance* pour la passerelle RD FQDN. L'utilisation de ce processus signifie que vous devez créer un partie de confiance factice pour faire respecter la pré-authentification afin que les clients puissent utiliser la pré-authentification sans délégation Kerberos contrainte au serveur publié.

Lorsqu'un utilisateur s'authentifie sur l'application pour le serveur de passerelle RD publié en utilisant le client Remote Desktop Connection (mstsc.exe), le serveur back-end répond au client qu'une pré-authentification est nécessaire. À son tour, le client reçoit un cookie de proxy d'application Web qui est obtenu par l'intermédiaire du navigateur. Ce cookie est ensuite utilisé par le client Remote Desktop Connection en guise de preuve d'authentification.

 **Remarque :** Vous devez désactiver l'attribut **HttpOnly** sur l'application publiée pour permettre au client de Remote Desktop Connection d'utiliser le cookie de proxy d'application Web obtenu par l'intermédiaire du navigateur.

Les utilisateurs s'authentifiant sur le serveur RD Web Access utilisent encore la forme d'inscription Web Access. Ceci permet d'obtenir le plus petit nombre d'invites d'authentification des utilisateurs parce que la forme d'inscription RD Web Access crée un magasin d'informations d'identification côté client, qui peut ensuite être utilisé par le client Remote Desktop Connection pour tout lancement à distance de l'application par la suite.

 **Lectures supplémentaires :** Pour plus d'informations sur la publication RD Gateway via le proxy d'application Web, reportez-vous à : « Publication d'applications avec SharePoint, Exchange et RDG » sur : <http://aka.ms/C7f0wn>

Installation et configuration du Proxy d'application Web

Lors de la préparation pour le déploiement de votre service de fédération, vous pourriez avoir besoin de préparer quelques articles avant d'installer le proxy d'application Web. Cependant, vous ne devriez pas commencer à mettre en œuvre le proxy d'application Web jusqu'à ce que vous ayez déployé la grappe de serveurs de fédération AD FS.

 **Remarque :** Vous pouvez déployer le proxy d'application Web uniquement sur Windows Server 2012 R2 ou sur une version ultérieure. Alternativement, vous déployez le proxy AD FS pour utiliser un proxy pour le service de fédération sur Windows Server 2012 R2 ou sur une version antérieure.

- Vous pourriez avoir besoin de préparer les éléments suivants avant d'installer le Proxy d'application Web :
 - Certificats
 - Équilibrage de charge
 - DNS
- Lors du déploiement du Proxy d'application Web, vous :
 - Installez le Proxy d'application Web ;
 - Configurez le Proxy d'application Web ;
 - Mettez à jour le Proxy d'application Web.

Certificat

Parce que vous n'êtes pas en mesure d'importer le certificat pendant l'installation du proxy d'application Web, vous devez demander le certificat SSL approprié requis pour le proxy d'application Web à partir d'un CA publiquement approuvé avant le déploiement. Après avoir reçu le certificat du CA, vous devez l'installer dans le magasin de certificats personnel sur le serveur du proxy d'application Web.

Dans la plupart des scénarios, vous utilisez le certificat SSL de la grappe de serveurs de fédération AD FS pour le proxy d'application Web. Toutefois, si la grappe de serveurs de fédération AD FS prend en charge l'IWA via le proxy d'application Web, avec la protection avancée pour l'authentification activée, vous devez utiliser le même certificat SSL. Si ce scénario s'applique à votre environnement AD FS, vous devez exporter le certificat SSL de l'un des serveurs de fédération dans la grappe, puis l'importer dans le magasin de certificats personnel sur le serveur du proxy d'application Web.

Dans les deux cas, si vous déployez plus d'un serveur proxy d'application Web pour soutenir votre environnement AD FS, vous devez importer le certificat SSL approprié à chacun des serveurs proxy d'applications Web supplémentaires avant d'installer le proxy d'application Web. Cela vaut aussi pour les certificats génériques.

Équilibrage de charge

Lorsque vous déployez deux ou plusieurs serveurs proxy d'application Web dans un tableau, vous devez les configurer pour NLB. Vous pouvez accomplir cela avec le matériel, ce qui est recommandé pour les grands déploiements ou avec le logiciel, ce qui est recommandé pour les petits et moyens déploiements. Pour les équilibriseurs de charge du logiciel, vous pouvez activer NLB pour le réseau proxy d'application Web.

DNS

Vous devez configurer un enregistrement d'hôte DNS sur les serveurs de périmètre DNS avant d'installer le serveur proxy d'application Web. Parce que le serveur proxy d'application Web est généralement placé dans le réseau de périmètre, nous vous recommandons :

- De configurer le serveur proxy d'application Web pour utiliser des serveurs DNS externes pour la résolution de nom externe ;
- D'ajouter un nom d'hôte interne que le serveur proxy d'application Web doit résoudre, comme celui de la grappe AD FS interne aux fichiers **Hosts** sur le serveur du proxy d'application Web.

 **Remarque :** Vous ne devriez pas utiliser des enregistrements CNAME pour le nom du serveur proxy d'application Web.

Installer le Proxy d'application Web

Sur Windows Server 2012 R2 et sur les versions ultérieures, le proxy d'application Web est installé à partir du Gestionnaire Server en tant qu'un rôle. L'**Assistant de configuration du Gestionnaire de serveur** effectue des contrôles de validation et installe automatiquement le service requis par le proxy d'application Web. Le service de rôle du serveur proxy d'application Web comprend des applets de commande Windows PowerShell que vous pouvez utiliser pour effectuer un déploiement basé sur Windows PowerShell.

Pour installer le service de rôle du serveur proxy d'application Web, utilisez **Gestionnaire de serveur Add Roles and Features Wizard** et sélectionnez le rôle de serveur Accès à distance. Sur la page **Role services**, sélectionnez la **Web Application Proxy role service**. L'**Assistant Ajouter Rôles et fonctionnalités** installe automatiquement les caractéristiques requises, y compris la console **Remote Access Management**.

 **Remarque :** Sinon, vous pouvez utiliser l'applet de commande Windows PowerShell **Install-WindowsFeature Web-Application-Proxy** pour installer le service de rôle du serveur proxy d'application web.

Configurer le Proxy d'application Web

Après l'installation du service de rôle du serveur proxy d'application web, vous devez lancer la console **Remote Access Management** pour configurer le proxy d'application Web à la publication AD FS. Vous pouvez lancer la console **Remote Access Management** à partir du menu **Tools** dans Gestionnaire de serveur ou à partir de l'écran de démarrage. Les étapes de la configuration de chaque serveur proxy d'application Web dans votre environnement AD FS sont les mêmes:

1. Dans la console **Remote Access Management**, sélectionnez d'exécution **Web Application Proxy Configuration Wizard**.
2. Sur la page **Federation Server**, indiquez le nom de la grappe du service de fédération, et d'utiliser les informations d'identification d'un compte avec des autorisations d'administrateur local sur les serveurs de fédération AD FS.
3. Sur la page **AD FS Proxy Certificate**, sélectionnez le certificat SSL approprié pour terminer la configuration.

 **Remarque :** sinon, vous pouvez utiliser l'applet de commande Windows PowerShell **Install-WebApplicationProxy** pour configurer le proxy d'**Install-WebApplicationProxy** pour configurer le proxy d'application Web à la publication AD FS.

Mettre à jour le Proxy d'application Web

Pour vous assurer que votre environnement AD FS est fiable et stable, vous devez installer les mises à jour recommandées pour le proxy d'application Web. Après l'installation et la configuration de vos serveurs proxy d'application Web, vous pouvez utiliser Microsoft Update pour vérifier les mises à jour disponibles.

 **Remarque :** Pour plus d'informations sur toutes les mises à jour disponibles pour AD FS, reportez-vous à : « Updates for Services de fédération Active Directory (AD FS) (AD FS) » sur : <http://aka.ms/PI09m2>

Démonstration : Installation et configuration du Proxy d'application Web

Dans cette démonstration, vous apprendrez à :

- Installer le Proxy d'application Web ;
- Exporter le certificat à partir du serveur AD FS ;
- Importer le certificat vers le serveur proxy d'applications web ;
- Configurer le Proxy d'application Web.

Procédure de démonstration

Installer le Proxy d'application Web

- Sur **LON-SVR2**, Ouvrez **Gestionnaire de serveur**, ajouter le rôle de serveur **Remot Access** et le service de rôle **Web Application Proxy**.

Exporter le certificat adfs.adatum.com à partir de LON-DC1

1. Sur **LON-DC1**, ouvrez la console de gestion **Microsoft Management Console (MMC)**, et ajoutez le composant logiciel enfichable **Certificats** pour l'**ordinateur local**.
2. À partir du dossier **Personnal**, exportez le certificat **adfs.adatum.com** en utilisant les paramètres suivants :
 - **Oui, exporter la clé privée**
 - Format de fichier : **Échange d'informations personnelles - PKCS # 12 (.PFX)**
 - Mot de passe : **Pa55w.rd**
 - Nom du fichier **C:\adfs.pfx**

Importez le certificat adfs.adatum.com sur LON-SVR2

1. Sur **LON-SVR2**, ouvrez la console de gestion **Microsoft Management Console (MMC)**, et ajoutez le composant logiciel enfichable **Certificats** pour l'**ordinateur local**.
2. À partir du dossier **Personnal**, importez le certificat **adfs.adatum.com** en utilisant les paramètres suivants :
 - Nom du fichier **\LON-DC1\c\$\adfs.pfx**
 - Mot de passe : **Pa55w.rd**
 - **Marquer cette clé comme exportable. Cela vous permettra de sauvegarder ou transporter vos clés à une date ultérieure**
 - Magasin de certificats : **Personnel**

Configurez le Proxy d'application Web

1. Sur **LON-SVR2**, dans **Gestionnaire de serveur**, cliquez sur l'icône **Notifications**, puis cliquez sur **Open the Web Application Proxy Wizard**.
2. Dans le **Web Application Proxy Wizard**, fournir les paramètres de configuration suivants :
 - Nom du service de fédération : **adfs.adatum.com**
 - Nom d'utilisateur : **Adatum\Administrateur**
 - Mot de passe : **Pa55w.rd**
 - Certificat à utiliser par le proxy AD FS : **adfs.adatum.com**

Testez vos connaissances

| Question | |
|--|---|
| Lequel des énoncés suivants concernant la configuration du Proxy d'application Web est correct ? (Choisissez toutes les réponses applicables.) | |
| Sélectionnez la réponse correcte. | |
| | Pour installer le proxy d'application Web, vous devez avoir implémenté AD FS dans votre organisation. |
| | Pour installer le proxy d'application Web, vous devez avoir implémenté AD FS dans votre organisation. |
| | Pour chaque application que vous publiez, vous devez configurer une URL externe et une URL du serveur interne. |
| | Lorsque vous définissez l'URL externe, vous devez également sélectionner un certificat qui contient le nom d'hôte dans l'URL interne. |
| | Lorsque vous définissez l'URL externe, vous devez également sélectionner un certificat qui contient le nom d'hôte dans l'URL externe. |

Atelier pratique : Implémentation de AD FS

Scénario

A. Datum Corporation a mis en place une variété de relations d'affaires avec d'autres entreprises et les clients. Certaines de ces entreprises partenaires et les clients ont besoin d'accéder à des applications métier qui sont en cours d'exécution sur le réseau A. Datum Corporation. Les groupes d'affaires à A. Datum Corporation veulent fournir un maximum de fonctionnalité et l'accès à ces entreprises. Les services de sécurité et des opérations veulent faire en sorte que les partenaires et les clients puissent accéder uniquement aux ressources pour lesquelles ils bénéficient d'autorisations et que la mise en œuvre de la solution n'augmente pas de manière significative la charge de travail de l'équipe opérationnelle. A. Datum Corporation travaille également sur la migration de certaines parties de son infrastructure réseau vers les services en ligne, y compris Azure et Office 365.

Pour répondre à ces besoins de l'entreprise, A. Datum Corporation envisage d'implémenter AD FS. Dans le déploiement initial, l'entreprise envisage d'utiliser AD FS pour implémenter SSO pour les utilisateurs internes ayant un accès à une application sur un serveur Web. A. Datum Corporation a également conclu un partenariat avec une autre entreprise, Trey Research. Les utilisateurs de Trey Research devraient être en mesure d'accéder à la même application.

Comme l'un des principaux administrateurs de réseau à A. Datum Corporation, il est de votre responsabilité d'implémenter la solution AD FS. Comme une preuve de concept, vous déployez un échantillon d'application prenant en charge les revendications et configuez AD FS pour permettre à la fois aux utilisateurs internes et à ceux de Trey Research d'accéder à la même application.

Objectifs

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

- Configurer des pré-requis AD FS ;
- Installer et configurer AD FS ;
- Configurer et valider l'authentification unique pour une seule organisation ;
- Configurer et valider l'authentification unique pour un scénario de fédération d'entreprises.

Configuration de l'atelier pratique

Durée approximative : 90 minutes

Ordinateurs virtuels. **22742A-LON-DC1**, **22742A-LON-DC2**, **22742A-LON-SVR1** et **22742A-LON-CL1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**

Ordinateur virtuel : **22742A-TREY-DC1**.

Nom d'utilisateur : **TreyResearch\Administrateur**

Mot de passe : **Pa55w.rd**

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-LON-DC1**, et dans le volet **Actions**, cliquez sur **Démarrer**.
3. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-LON-DC2**, et dans le volet **Actions**, cliquez sur **Démarrer**.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

4. Pour les deux contrôleurs de domaine, dans le volet **Actions**, cliquez sur **Connect**. Attendez que l'ordinateur virtuel démarre.
5. Connectez-vous en utilisant les informations d'identification suivantes :
 - Nom d'utilisateur : **Adatum\Administrateur**
 - Mot de passe : **Pa55w.rd**
6. Répétez les étapes 3 à 5 pour **22742A-LON-SVR1** et **22742A-LON-CL1**.
7. Répétez les étapes 3 à 4 pour **22742A-TREY-DC1**. Connectez-vous en tant que **TreyResearch\Administrateur** avec le mot de passe **Pa55w.rd**.

Exercice 1 : Configuration des pré-requis AD FS

Scénario

Pour déployer AD FS à A. Datum Corporation, vous devez vérifier que tous les composants requis sont configurés. Vous prévoyez de vérifier qu'AD CS est déployé dans l'organisation, puis configurez les certificats requis pour AD FS sur le serveur AD FS et sur les serveurs Web. Vous prévoyez également de configurer les redirecteurs DNS pour permettre la communication entre Adatum.com et TreyResearch.net.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer les redirecteurs DNS ;
2. Configurer les approbations de certificats ;
3. Demander et installer un certificat pour le serveur Web.

► Tâche 1 : Configurer les redirecteurs DNS

1. Sur **LON-DC1**, utilisez le Gestionnaire DNS pour créer un redirecteur conditionnel avec les paramètres suivants :
 - Domaine DNS : **TreyResearch.net**
 - Adresse IP du serveur maître : **172.16.10.10**
 - **Conservez ce redirecteur conditionnel dans Active Directory et reproduisez-le comme suit : Tous les serveurs DNS dans cette forêt**
2. Sur **TREY-DC1**, utilisez le Gestionnaire DNS pour créer un redirecteur conditionnel avec les paramètres suivants :
 - Domaine DNS : **Adatum.com**
 - Adresse IP du serveur maître : **172.16.0.10**
 - **Conservez ce redirecteur conditionnel dans Active Directory et reproduisez-le comme suit : Tous les serveurs DNS dans cette forêt**



Remarque : Dans un environnement de production, il est probable que vous allez utiliser le DNS internet au lieu de redirecteurs conditionnels.

► Tâche 2 : Configurer les approbations de certificats

1. Sur **LON-DC1**, Utilisez l'Explorateur de fichiers pour copier **TREY-DC1.TreyResearch.net_TreyResearchCA.crt** à partir de **\TREY-DC1\CertEnroll** sur **C:**.

2. Ouvrez **Group Policy Management**, puis modifiez la **Default Domain Policy** (stratégie par défaut du domaine).
3. Dans **Group Policy Management Editor**, allez à **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Trusted Root Certification Authorities**.
4. Importer **C:\TREY-DC1.TreyResearch.net_TreyResearchCA.crt** en tant qu'autorité de certification racine approuvée.
5. Sur **TREY-DC1**, Utilisez l'Explorateur de fichiers pour aller à **\LON-DC1\CertEnroll**.
6. Faites un clic-droit sur **LON-DC1.Adatum.com_AdatumCA.crt**, puis installer le certificat dans le magasin **Trusted Root Certification Authorities**.
7. Sur **LON-SVR1**, exécutez **Gpupdate**.

 **Remarque :** Si vous obtenez des certificats d'une autorité digne de confiance, vous n'avez pas besoin de configurer une approbation de certificat entre les organisations.

► Tâche 3 : Demander et installer un certificat pour le serveur Web

1. Sur **LON-SVR1**, à partir de **Gestionnaire de serveur**, ouvrez **Microsoft Internet Information Services (IIS)** et voir ensuite les certificats de serveur.
2. Créez un certificat de domaine avec les paramètres suivants :
 - o Nom commun : **lon-svr1.adatum.com**
 - o Organisation : **A. Datum Corporation**
 - o Unité d'organisation **Research**
 - o Ville / localité : **Londres**
 - o Région : **Angleterre**
 - o Pays / Région : **GB**
 - o Autorité de certification : **AdatumCA**
 - o Pseudonyme : **certificat AdatumTestApp**
3. Ajouter une liaison HTTPS pour le site par défaut en utilisant le paramètre suivant :
 - o Certificat SSL : **certificat AdatumTestApp**

Résultats : Après avoir terminé cet exercice, vous devez avoir activé avec succès la résolution DNS et les approbations de certificat entre les domaines. En outre, vous avez activé un certificat SSL pour le site Web et validé son accès.

Exercice 2 : Installation et configuration AD FS

Scénario

Le premier scénario d'implémentation de l'application AD FS preuve de concept est de veiller à ce que les utilisateurs internes puissent utiliser SSO pour accéder à l'application Web. Vous envisagez de configurer le serveur AD FS et une application Web pour permettre ce scénario. Vous voulez également vérifier que les utilisateurs internes peuvent accéder à l'application. Pour démarrer l'implémentation de AD FS, installez AD FS sur le contrôleur de domaine A. Datum Corporation et configurez le serveur en tant que serveur de fédération autonome. Vous pourrez également configurer le serveur pour utiliser un certificat de signature de jetons signé CA.

Les tâches principales de cet exercice sont les suivantes :

1. Créez un enregistrement DNS pour AD FS.
2. Installer AD FS ;
3. Configurer AD FS ;
4. Vérifier la fonctionnalité AD FS.

► Tâche 1 : Créer un enregistrement DNS pour AD FS

- Sur **LON-DC1**, Utilisez le Gestionnaire DNS pour ajouter un nouvel enregistrement d'hôte pour AD FS :
 - Zone de recherche directe : **Adatum.com**
 - Nom : **adfs**
 - Adresse IP : **172.16.0.10**

► Tâche 2 : Installer AD FS

1. Sur **LON-DC1**, cliquez sur **Démarrer**, cliquez avec le bouton droit sur **Windows PowerShell**, puis sur **Exécuter comme administrateur**.
2. Exécutez la commande suivante pour créer la clé racine du Service de distribution de clés de groupe Microsoft afin de générer le mot de passe du compte de service géré de groupe pour le compte qui sera utilisé plus tard dans cet atelier pratique.

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

3. Ouvrez **Gestionnaire de serveur**, puis ajoutez le rôle **Services de fédération Active Directory (AD FS)**.

► Tâche 3 : Configurer AD FS

1. Sur **LON-DC1**, dans **Gestionnaire de serveur**, cliquez sur l'icône **Notifications**, puis cliquez sur **Configurer les services de fédération sur ce serveur**.
2. Utilisez les options suivantes pour configurer le serveur AD FS :
 - **Créer le premier serveur de fédération dans une batterie de serveurs de fédération**
 - Compte à utiliser pour la configuration : **Adatum\Administrateur**
 - Certificat SSL **adfs.adatum.com**
 - Nom d'affichage du service de fédération : **A. Datum Corporation**
 - Créer un compte de service géré de groupe : **Adatum\Service ADFS**
 - **Créez une base de données sur ce serveur à l'aide de la base de données interne Windows**



Remarque : Le certificat adfs.adatum.com a été préconfiguré pour cette tâche. Dans votre propre environnement, vous devez obtenir ce certificat.

► Tâche 4 : Vérifier la fonctionnalité AD FS

1. Sur **LON-CL1**, Ouvrez Internet Explorer, puis aller à <https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml>.
2. Vérifiez que le fichier charge, puis fermez Internet Explorer.

Résultats : À la fin de cet exercice, vous devez avoir installé et configuré AD FS avec succès. Vous devez également avoir vérifié le bon fonctionnement en affichant le contenu du fichier **FederationMetadata.xml**.

Exercice 3 : Configuration d'une application interne pour AD FS

Scénario

Le premier scénario d'implémentation de l'application AD FS preuve de concept est de veiller à ce que les utilisateurs internes puissent utiliser SSO pour accéder à l'application Web. Vous envisagez de configurer le serveur AD FS et une application Web pour permettre ce scénario. Vous voulez également vérifier que les utilisateurs internes peuvent accéder à l'application.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer l'approbation de fournisseur de revendications Active Directory ;
2. Configurer l'application pour qu'elle se fie aux revendications entrantes ;
3. Configurer une approbation de partie de confiance pour l'application en charge des revendications ;
4. Configurer des règles de réclamation pour l'approbation de partie de confiance ;
5. Tester l'accès de l'application en charge des revendications ;
6. Configurer Internet Explorer pour passer automatiquement des informations d'identification locales à l'application.

► Tâche 1 : Configurer l'approbation de fournisseur de revendications Active Directory

1. Sur **LON-DC1**, dans **Gestionnaire de serveur**, ouvrez AD FS Management.
2. Allez sur **Approbations de fournisseur de revendications**, puis modifiez les règles de revendication pour **Active Directory**.
3. Ajoutez une règle de transformation d'acceptation avec les paramètres suivants :
 - Modèle de règle de revendication : **Envoyer des attributs LDAP en tant que réclamations**
 - Nom : **Règle des attributs LDAP sortants**
 - Magasin d'attributs : **Active Directory (AD)**
 - Cartographie des attributs LDAP des types de réclamations sortantes :
 - Adresses électroniques : **Adresse électronique**
 - Nom d'utilisateur principal : **Nom d'utilisateur principal**
 - Nom d'affichage : **Nom**

► Tâche 2 : Configurer l'application pour qu'elle se fie aux revendications entrantes

1. Sur **LON-SVR1**, ouvrez le **Gestionnaire de serveur**, puis ouvrez l'utilitaire de fédération Windows Identity Foundation.
2. Dans **Federation Utility Wizard**, utilisez les informations suivantes :
 - Emplacement de la configuration d'application :
C:\inetpub\wwwroot\AdatumTestApp\web.config
 - URI de l'application : **https://lon-svr1.adatum.com/AdatumTestApp/**
 - **Utilisez un STS existant**
 - Emplacement du document de métadonnées de la fédération STS WS : **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**
 - **Désactiver la validation de la chaîne de certificat**
 - **Pas de chiffrement**

► Tâche 3 : Configurer une approbation de partie de confiance pour l'application en charge des revendications

1. Sur **LON-DC1**, dans la console **AD FS**, ajoutez une approbation de partie de confiance avec les paramètres suivants :
 - **Importez des données concernant la partie de confiance publiées en ligne ou sur un réseau local**
 - Adresse des métadonnées de fédération : **https://lon-svr1.adatum.com/adatumtestapp/**
 - Nom d'affichage : **Application de test A. Datum Corporation**
 - **Autoriser tout le monde**
2. Laissez ouverte la fenêtre **Modifier la stratégie d'émission de revendications pour l'application de test A. Datum Corporation** pour la tâche suivante. (Cette fenêtre peut être cachée derrière le Gestionnaire de serveur.)

► Tâche 4 : Configurer des règles de réclamation pour l'approbation de partie de confiance

1. Sur **LON-DC1**, dans la fenêtre **Edit Claim Issuance Policy for A. Datum Corporation Test App**, sur l'onglet **Issuance Transform Rules**, ajoutez une règle.
2. Procédez à l'**Assistant Ajout de règle de revendication de transformation** avec les paramètres suivants :
 - Modèle de règle de revendication : **Transférer ou filtrer une revendication entrante**
 - Nom de la règle de revendication : **Transférer le nom de compte Windows**
 - Type de revendication entrante : **Nom du compte Windows**
 - **Transférer toutes les valeurs de revendication**
3. Créer trois autres règles pour transférer les types de revendications **Adresse e-mail**, **UPN** et **Nom**.

► Tâche 5 : Tester l'accès de l'application en charge des revendications

1. Sur **LON-CL1**, utilisez Internet Explorer pour accéder à **https://lon-svr1.adatum.com/AdatumTestApp/**.



Remarque : Il est essentiel d'utiliser la barre oblique de fin (/) dans l'URL pour l'étape 1.

2. Lorsque vous y êtes invité, enregistrez-vous en tant que **Adatum\Adam** avec le mot de passe **Pa55w.rd**.
3. Vérifiez les informations de réclamation affichées par l'application, puis fermez Internet Explorer.

► **Tâche 6 : Configurer Internet Explorer pour passer automatiquement des informations d'identification locales à l'application**

1. Sur **LON-CL1**, dans Internet Explorer, ouvrez **Internet Options**.
2. Sur l'onglet **Security**, ajouter les sites suivants à la zone **intranet local** :
 - **https://adfs.adatum.com**
 - **https://lon-svr1.adatum.com**
3. Utilisez Internet Explorer pour accéder à **https://lon-svr1.adatum.com/AdatumTestApp/**.



Remarque : Il est essentiel d'utiliser la barre oblique de fin (/) dans l'URL pour l'étape 3.

4. Notez que vous n'êtes pas invité pour informations d'identification.
5. Vérifiez les informations de réclamation affichées par l'application, puis fermez Internet Explorer.

Résultats : Après avoir terminé cet exercice, vous devriez avoir réussi à configurer AD FS pour prendre en charge l'authentification pour une application.

Exercice 4 : Configuration AD FS pour partenaires commerciaux fédérés

Scénario

Le deuxième scénario de déploiement est de permettre aux utilisateurs de Trey Research d'accéder à l'application Web. Vous envisagez de configurer l'intégration de AD FS à Trey Research avec AD FS à A. Datum Corporation, puis de vérifier que les utilisateurs de Trey Research peuvent accéder à l'application. Vous voulez également confirmer que vous pouvez configurer l'accès qui est basé sur des groupes d'utilisateurs. Vous devez vous assurer que tous les utilisateurs de A. Datum Corporation, et que seuls les utilisateurs qui sont dans le groupe de production chez Trey Research peuvent accéder à l'application.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un enregistrement DNS pour AD FS à Trey Research ;
2. Créer un certificat à Trey Research ;
3. Installer AD FS pour Trey Research ;
4. Configurer AD FS pour Trey Research ;
5. Configurer une approbation de fournisseur de revendications pour le serveur Trey Research AD FS ;
6. Configurer d'une approbation de partie de confiance pour l'application A. Datum Corporation ;
7. Vérifier l'accès au site Web ;

8. Configurer les règles de revendication d'autorisation d'émission pour permettre l'accès uniquement à des groupes spécifiques ;
9. Vérifier l'accès au site Web avec les restrictions de groupe ;
10. Préparer le module suivant.

► **Tâche 1 : Créer un enregistrement DNS pour AD FS à Trey Research**

- Sur **TREY-DC1**, utiliser le Gestionnaire DNS pour ajouter un nouvel enregistrement d'hôte avec les informations suivantes :
 - Zone de recherche directe : **TreyResearch.net**
 - Nom : **adfs**
 - Adresse IP : **172.16.10.10**

► **Tâche 2 : Créer un certificat à Trey Research**

1. Sur **TREY-DC1**, ouvrez IIS Manager, puis afficher les certificats de serveur.
2. Créez un certificat de domaine avec les paramètres suivants :
 - Nom commun : **adfs.TreyResearch.net**
 - Organisation : **Trey Research**
 - Unité d'organisation **Research**
 - Ville / localité : **Londres**
 - Région : **Angleterre**
 - Pays / Région : **GB**
 - Autorité de certification : **TreyResearchCA**
 - Pseudonyme : **adfs.TreyResearch.net**

► **Tâche 3 : Installer AD FS pour Trey Research**

1. Sur **TREY-DC1**, cliquez sur **Démarrer**, cliquez avec le bouton droit sur **Windows PowerShell**, puis sur **Exécuter comme administrateur**.
2. Exécutez la commande suivante pour créer une clé racine du service de distribution des clés afin de générer les mots de passe gMSA du compte qui sera utilisé plus tard dans cet atelier pratique.

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

3. Ouvrez **Gestionnaire de serveur**, puis ajoutez le rôle **Services de fédération Active Directory (AD FS)**.

► **Tâche 4 : Configurer AD FS pour Trey Research**

1. Sur **TREY-DC1**, dans **Gestionnaire de serveur**, cliquez sur l'icône **Notifications**, puis cliquez sur **Configurer les services de fédération sur ce serveur**.
2. Utilisez les options suivantes pour configurer le serveur AD FS :
 - **Créer le premier serveur de fédération dans une batterie de serveurs de fédération**
 - Compte à utiliser pour la configuration : **TreyResearch\Administrateur**
 - Certificat SSL **adfs.treyresearch.net**
 - Nom d'affichage du service de fédération : **Trey Research**

- Créer un compte de service géré de groupe : **TreyResearch\ADFSService**
 - **Créez une base de données sur ce serveur à l'aide de la base de données interne Windows**
- **Tâche 5 : Configurer une approbation de fournisseur de revendications pour le serveur Trey Research AD FS**
1. Sur **LON-DC1**, utilisez la console **AD FS Management** pour ajouter une nouvelle approbation de fournisseur de réclamations avec les paramètres suivants :
 - **Importer des données concernant le fournisseur de réclamations publiées en ligne ou sur un réseau local**
 - Adresse des métadonnées de fédération : **<https://adfs.treyresearch.net>**
 - Nom d'affichage : **Trey Research**
 - **Ouvrez la boîte de dialogue Modifier les règles de réclamation pour ce fournisseur de réclamations à la fermeture de l'assistant**
 2. Créer une règle de réclamation pour Trey Research en utilisant les paramètres suivants
 - Le modèle de règle de revendication : **Transférer ou filtrer une revendication entrante**
 - Nom de la règle de revendication : **Transférer le nom de compte Windows**
 - Type de revendication entrante : **Nom du compte Windows**
 - **Transférer toutes les valeurs de revendication**
- **Tâche 6 : Configurer une approbation de partie de confiance pour l'application A. Datum Corporation.**
1. Sur **TREY-DC1**, utilisez la console **AD FS Management** pour créer une nouvelle approbation d'une partie de confiance avec les paramètres suivants :
 - **Importez des données concernant la partie de confiance publiées en ligne ou sur un réseau local**
 - Adresse des métadonnées de fédération : **adfs.adatum.com**
 - Nom d'affichage : **A. Datum Corporation**
 - **Permettre à tous l'accès à cette partie de confiance**
 - **Configurer la stratégie d'émission des réclamations pour l'application sélectionnée**
 2. Créez une nouvelle règle de réclamation de transformation avec les paramètres suivants
 - Le modèle de règle de revendication : **Transférer ou filtrer une revendication entrante**
 - Nom de la règle de revendication : **Transférer le nom de compte Windows**
 - Type de revendication entrante : **Nom du compte Windows**
 - **Transférer toutes les valeurs de revendication**
- **Tâche 7 : Vérifier l'accès au site Web**
1. Sur **TREY-DC1**, Ajoutez le domaine **adatum.com** à la liste de permission **Per Site Privacy Actions**.
 2. Utilisez Internet Explorer pour accéder à **<https://lon-svr1.adatum.com/adatumtestapp/>**.
 3. Sélectionnez le domaine d'accueil **Trey Research** puis enregistrez-vous en tant que **TreyResearch\April** avec le mot de passe **Pa55w.rd**.
 4. Vérifiez que vous pouvez accéder à l'application

5. Fermez Internet Explorer, puis connectez-vous au même site. Vérifiez que vous n'êtes pas invité à entrer un domaine d'accueil cette fois.



Remarque : Vous n'êtes pas invité à un domaine d'accueil lors du deuxième accès.

Après qu'un utilisateur sélectionne un domaine d'accueil et qu'une autorité de domaine authentifie l'utilisateur, le serveur de fédération de la partie utilisatrice émet un cookie **_LSRealm**. La durée de vie par défaut de ce cookie est de 30 jours. Par conséquent, pour vous connecter à plusieurs reprises, vous devez supprimer ce cookie après chaque tentative de connexion pour revenir à un état de bon fonctionnement.

► **Tâche 8 : Configurer les règles de revendication d'autorisation d'émission pour permettre l'accès uniquement à des groupes spécifiques**

1. Sur **TREY-DC1**, dans la console **AD FS Management**, supprimez la règle de politique d'émission nommée **Pass through Windows account name** de l'approbation de partie de confiance A. Datum Corporation.
2. Utilisez les paramètres suivants pour ajouter une règle de transformation d'émission à l'approbation de partie de confiance A. Datum Corporation qui autorise tous les utilisateurs qui sont membres du groupe de production :
 - Le modèle de règle de revendication : **Transférer ou filtrer une revendication entrante**
 - Nom de la règle de revendication : **Autoriser les membres de production**
 - Type de revendication entrante : **Groupe**
 - Valeur de réclamation entrante : **Treyresearch-Production**
3. Utilisez les paramètres suivants pour ajouter une transformation règle de réclamation à l'approbation du fournisseur de réclamations du répertoire actif afin qu'il envoie l'affiliation au groupe en tant que réclamation :
 - Le modèle de règle de revendication : **Envoyez une appartenance à un groupe comme une revendication**
 - Nom de la règle de revendication : **Réclamation du groupe de production**
 - Groupes d'utilisateurs : **Production**
 - Type de revendication sortante : **Groupe**
 - Valeur de réclamation sortante : **Treyresearch-Production**

► **Tâche 9 : Vérifier l'accès au site Web avec les restrictions de groupe**

1. Sur **TREY-DC1**, Ajoutez le domaine **adatum.com** à la liste de permissions **Per Site Privacy actes**.
2. Utilisez Internet Explorer pour vérifier l'accès à <https://lon-svr1.adatum.com/adatumtestapp/>.
3. Connectez-vous en tant qu'**TreyResearch\Ben** avec le mot de passe **Pa55w.rd**.
4. Vérifiez que vous pouvez accéder à l'application parce que Ben est un membre du groupe **TreyResearch\Production**.

Résultats : Après avoir terminé cet exercice, vous devez avoir configuré avec succès un accès à une application prenant en charge les réclamations dans une organisation partenaire.

► **Tâche 10 : Préparer le module suivant**

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-DC2**, **22742A-LON-SVR1**, **22742A-TREY-DC1**, et **22742A-LON-CL1**.

Question : Pourquoi est-il important de configurer adfs.adatum.com pour l'utiliser comme un nom d'hôte pour le service AD FS ?

Question : Comment pouvez-vous vérifier si AD FS fonctionne correctement ?

Révision du module et Takeaways

Méthode conseillée

Dans les versions antérieures de AD FS, il était courant d'utiliser l'Assistant Configuration de la sécurité (SCW) pour appliquer les meilleures pratiques de sécurité spécifiques à AD FS aux serveurs de fédération et aux ordinateurs proxy de serveur de fédération. Dans Windows Server 2016, SCW a été supprimé parce que la sécurité des fonctionnalités est renforcée par défaut. Par conséquent, si vous avez besoin de contrôler des paramètres de sécurité spécifiques, vous pouvez soit utiliser la stratégie de groupe soit Microsoft Security Compliance Manager (voir <http://aka.ms/Ncq8jm>).

Questions de contrôle des acquis

Question : Votre organisation envisage d'implémenter AD FS. À court terme, seuls les clients internes utiliseront AD FS pour accéder aux applications internes. Cependant, plus tard, vous devez fournir un accès aux applications basées sur le Web dont la sécurité est renforcée par AD FS pour les utilisateurs à domicile. Combien de certificats obtiendrez-vous d'une certification tierce ?

Question : Votre organisation a implémenté avec succès un seul serveur AD FS et un seul Proxy d'application Web. Initialement, AD FS n'était utilisé que pour une seule application, mais maintenant il est utilisé pour plusieurs applications critiques de l'entreprise. AD FS doivent être configurés pour être hautement disponible.

Pendant l'installation de AD FS, vous avez choisi d'utiliser WID. Pouvez-vous utiliser cette base de données dans une configuration à haute disponibilité ?

Module 11

Implémentation et administration des Services de gestion des droits Active Directory (AD RMS)

Sommaire :

| | |
|---|-------|
| Présentation du module | 11-1 |
| Leçon 1 : Présentation de AD RMS | 11-2 |
| Leçon 2 : Déploiement et gestion d'une infrastructure AD RMS | 11-12 |
| Leçon 3 : Configurer la protection de contenu AD RMS | 11-22 |
| Atelier pratique : Implémentation d'une infrastructure AD RMS | 11-28 |
| Contrôle des acquis et éléments à retenir | 11-34 |

Présentation du module

Les Services de gestion des droits Active Directory (AD RMS) permettent de protéger le contenu en allant au-delà du chiffrement des périphériques de stockage soit au moyen du Chiffrement de lecteur BitLocker soit par le chiffrement de fichiers individuels à l'aide du Système de chiffrement des fichiers (EFS). Les Services de gestion des droits Active Directory (AD RMS) permettent de protéger les données à la fois en transit et au repos sur presque tous les appareils ou plate-formes. Les Services de gestion des droits Active Directory (AD RMS) permettent également de rendre les données accessibles uniquement aux utilisateurs autorisés pour une durée déterminée et dans un but précis.

Ce module vous présente les Services de gestion des droits Active Directory (AD RMS). Il décrit comment déployer les Services de gestion des droits Active Directory (AD RMS) et comment configurer la protection du contenu.

Objectifs

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

- Décrire les Services de gestion des droits Active Directory (AD RMS) ;
- Déployer et gérer une infrastructure de Services de gestion des droits Active Directory (AD RMS) ;
- Configurer la protection de contenu des Services de gestion des droits Active Directory (AD RMS).

Leçon 1

Présentation de AD RMS

Avant de déployer les Services de gestion des droits Active Directory (AD RMS), vous devez savoir comment ils fonctionnent, comment les déployer et quels sont les éléments compris dans un déploiement de Services de gestion des droits Active Directory (AD RMS). Vous devez aussi comprendre les concepts qui se cachent derrière les différents certificats et licences AD RMS.

Cette leçon donne un aperçu des Services de gestion des droits Active Directory (AD RMS) et décrit les scénarios dans lesquels vous pouvez les utiliser pour protéger les données confidentielles de votre entreprise.

Objectifs des leçons

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

- Décrire les Services de gestion des droits Active Directory (AD RMS) ;
- Décrire les cas où les Services de gestion des droits Active Directory (AD RMS) sont utilisés ;
- Décrire les composants des Services de gestion des droits Active Directory (AD RMS) ;
- Décrire les certificats et licences des Services de gestion des droits Active Directory (AD RMS) ;
- Expliquer comment fonctionne les Services de gestion des droits Active Directory (AD RMS) ;
- Décrire les Services de gestion des droits Microsoft Azure (Azure RMS).

Expliquer les différences entre les Services de gestion des droits Microsoft Azure (Azure RMS), les Services de gestion des droits Active Directory (AD RMS) et les Services de gestion des droits Azure pour Office 365.

Qu'est-ce que les Services de gestion des droits Active Directory (AD RMS) ?

AD RMS est une technologie de protection de l'information qui minimise les risques de fuites de données. La *fuite de données* est la transmission non autorisée d'informations à des personnes internes ou externes à l'organisation qui ne devraient pas avoir accès à l'information. Les Services de gestion des droits Active Directory (AD RMS) s'intègrent à certains produits Microsoft existants, y compris Windows Server, Microsoft Exchange Server, Microsoft SharePoint Server et Microsoft Office et à des services en ligne tels que Office 365.

Une technologie de protection de l'information qui :

- Réduit les fuites de données par sa conception
- Peut être intégrée à certains produits Microsoft et aux systèmes d'exploitation Windows Server
- Aide à protéger les données en transit, au repos et essentiellement à tout emplacement

Les Services de gestion des droits Active Directory (AD RMS) permettent de protéger les données à la fois en transit et au repos. Par exemple, les Services de gestion des droits Active Directory (AD RMS) permettent de protéger les documents dans le courrier électronique en empêchant les messages accidentellement adressés aux mauvais destinataires de s'ouvrir. Vous pouvez également utiliser les Services de gestion des droits Active Directory (AD RMS) pour aider à protéger les données stockées sur des périphériques tels que les lecteurs USB amovibles. L'inconvénient de ces autorisations d'accès aux fichiers et dossiers est que, après qu'un fichier ait été copié vers un autre emplacement, les autorisations d'origine ne sont plus valables. Un fichier copié sur un lecteur USB hérite des autorisations de l'appareil de

destination. Toutefois, après avoir copié un fichier avec un attribut de lecture seule, celui-ci peut être modifié en changeant les autorisations des fichiers et des dossiers. Si vous décidez d'utiliser le Système de chiffrement des fichiers (EFS), vous permettez de protéger le fichier de façon permanente. Toutefois, il n'est pas facile de partager ce fichier avec d'autres utilisateurs, et vous ne pouvez pas configurer des autorisations spécifiques.

Avec les Services de gestion des droits Active Directory (AD RMS), vous pouvez aider à protéger un fichier dans presque tous les emplacements, quelles que soient les autorisations d'accès des fichiers et des dossiers. Avec les Services de gestion des droits Active Directory (AD RMS), seuls les utilisateurs qui sont autorisés à ouvrir un fichier peuvent visionner le contenu de ce fichier. En outre, vous pouvez contrôler les actions des fichiers, telles que la copie, l'impression, le transfert et bien d'autres.

Scénarios d'utilisation pour les Services de gestion des droits Active Directory (AD RMS)

Les Services de gestion des droits

Active Directory (AD RMS) sont principalement utilisés pour le contrôle de la distribution des informations sensibles. Vous pouvez utiliser les Services de gestion des droits Active Directory (AD RMS) en les associant à des techniques de chiffrement pour permettre la sécurisation des données stockées ou en transit. Il existe plusieurs raisons de contrôler la diffusion d'informations sensibles, comme par exemple pour s'assurer que seuls les membres du personnel autorisés ont accès à un fichier, que les messages électroniques sensibles ne peuvent pas être transmis ou que les détails d'un projet qui n'est pas encore sorti ne sont pas rendus publics. Prenez les scénarios suivants :

L'utilisation principale de AD RMS est de contrôler la distribution des informations sensibles, et les scénarios d'utilisation typiques comprennent :

- Une aide pour empêcher l'accès à des documents confidentiels, indépendamment de leur emplacement
- Une utilisation des autorisations selon l'action basées sur des comptes AD DS
- Une aide pour empêcher que des courriers électroniques confidentiels sortent d'une organisation

- Scénario 1. Le Directeur général (CEO) copie une feuille de calcul qui contient les enveloppes de rémunération des cadres de l'organisation provenant d'un dossier protégé sur un serveur de fichiers sur son lecteur USB personnel. Sur le trajet du retour chez lui, le PDG laisse le lecteur USB dans le train, où une personne sans lien avec l'organisation le trouve. Sans les Services de gestion des droits Active Directory (AD RMS), celui qui trouve le lecteur USB peut ouvrir le fichier. Avec les Services de gestion des droits Active Directory (AD RMS), vous pouvez aider à faire en sorte que les utilisateurs non autorisés ne peuvent pas ouvrir le fichier.
- Scénario 2. Un document interne est visible par un certain groupe de personnes autorisées au sein d'une organisation. Ces personnes ne devraient pas être en mesure de modifier ou d'imprimer le document. Vous pouvez utiliser la fonctionnalité native de Microsoft Word 2003 ou une version ultérieure pour limiter ces fonctionnalités. Pour ce faire, chaque personne doit disposer d'un compte Microsoft ou d'un compte de Services de domaine Active Directory (AD DS). Avec les Services de gestion des droits Active Directory (AD RMS), vous pouvez configurer ces autorisations sur base des comptes existants dans les Services de domaine Active Directory (AD DS) ou pour les utilisateurs externes à l'organisation, vous pouvez les identifier en utilisant des comptes Microsoft.
- Scénario 3. Les gens au sein d'une organisation ne devraient pas avoir accès à la transmission des messages électroniques sensibles auxquels une classification particulière a été attribuée. Avec les Services de gestion des droits Active Directory (AD RMS), vous pouvez activer un expéditeur pour attribuer une classification particulière à un nouveau message électronique et cette classification permet de s'assurer que le destinataire ne sera pas en mesure de transmettre le message.

Présentation des composants des Services de gestion des droits Active Directory (AD RMS)

Une infrastructure de Services de gestion des droits Active Directory (AD RMS) se compose de plusieurs éléments et l'élément principal est le cluster de Services de gestion des droits Active Directory (AD RMS). Le cluster de certification racine des Services de gestion des droits Active Directory (AD RMS) est créé lorsque vous déployez le premier serveur des Services de gestion des droits Active Directory (AD RMS) dans une forêt. Le cluster de certification racine des Services de gestion des droits

- Le cluster AD RMS :
 - Il est créé quand vous déployez le premier serveur AD RMS
- Le serveur AD RMS :
 - Le contenu est protégé par licences AD RMS ;
 - Il certifie l'identité des utilisateurs et des périphériques de confiance.
- Le client AD RMS :
 - Il s'intègre dans Windows Vista, Windows 7 et versions ultérieures ;
 - Il interagit avec les applications activées pour AD RMS.
- Les applications activées pour AD RMS :
 - Elles permettent la publication et la consommation de contenu protégé par AD RMS
 - Elles comprennent Office, Serveur Exchange et SharePoint Server
 - Elles peuvent être créées par le kit de développement logiciel (SDK) AD RMS.

Active Directory (AD RMS) gère l'ensemble du trafic de licences et de certifications pour le domaine dans lequel il est installé. Les Services de gestion des droits Active Directory (AD RMS) stockent les informations de configuration dans une base de données Microsoft SQL Server ou dans une base de données interne Windows (WID). Dans les environnements vastes, la base de données SQL Server est hébergée sur un serveur distinct du serveur qui héberge le rôle des Services de gestion des droits Active Directory (AD RMS).

Les *clusters de licences seules* des Services de gestion des droits Active Directory (AD RMS) sont utilisés dans des environnements distribués. Les clusters de licences seules ne fournissent pas la certification, mais ils permettent la répartition des licences pour la consommation et la publication de contenu. Les clusters de licences seules se déploient souvent en de grandes succursales dans les organisations qui utilisent les Services de gestion des droits Active Directory (AD RMS).

Serveur AD RMS

Le serveur AD RMS doit faire partie du domaine AD DS. Lorsque vous installez les Services de gestion des droits Active Directory (AD RMS), les informations sur l'emplacement du cluster sont publiées sur AD DS dans un endroit connu sous le nom de *point de connexion de service*. Les ordinateurs qui sont membres du domaine interrogent le point de connexion de service pour déterminer l'emplacement des services AD RMS. AD RMS est un rôle de serveur que vous pouvez installer à l'aide du Gestionnaire de serveur sur Windows Server 2016, Windows Server 2012 et les systèmes d'exploitation Windows Server 2008.

Client des Services de gestion des droits Active Directory (AD RMS)

Le client AD RMS est intégré aux systèmes d'exploitation Windows 10, Windows 8.1, Windows 8, Windows 7 et Windows Vista. Le client AD RMS permet aux applications AD RMS activées d'appliquer la fonctionnalité dictée par un modèle de Services de gestion des droits Active Directory (AD RMS). Sans le client AD RMS, les applications AD RMS activées ne peuvent pas interagir avec le contenu protégé des Services de gestion des droits Active Directory (AD RMS).

Applications AD RMS activées

Les applications AD RMS activées permettent aux utilisateurs de créer et de consommer le contenu protégé des Services de gestion des droits Active Directory (AD RMS). Par exemple, Microsoft Outlook 2010 ou une version ultérieure permet aux utilisateurs de voir et de créer des messages électroniques protégés. Word 2007 ou une version ultérieure permet de voir et de créer des documents protégés de traitement de texte. Microsoft fournit un kit de développement logiciel (SDK) des Services de gestion des droits Active Directory (AD RMS) pour permettre aux développeurs d'applications de prendre en charge la protection du contenu des Services de gestion des droits Active Directory (AD RMS).

Certificats et licences des Services de gestion des droits Active Directory (AD RMS)

Pour comprendre comment fonctionne les Services de gestion des droits Active Directory (AD RMS), vous devez connaître ses différents types de certificats et de licences. Chacun de ces certificats et chacune de ces licences fonctionne différemment. Certains certificats, tels que les certificats de licence serveur, sont très importants et vous devez les sauvegarder régulièrement.

- Les certificats et licences AD RMS comprennent :
- Certificats de licence serveur
 - Certificats des ordinateurs AD RMS
 - Certificats de compte de droits (RAC)
 - Certificats de licence client
 - PL
 - Licences utilisateur final

Certificat de licence serveur

Le certificat de licence serveur est généré lorsque vous créez le cluster de Services de gestion des droits Active Directory (AD RMS). Sa durée de validité est de 250 ans. Un certificat de licence serveur permet à un cluster de Services de gestion des droits Active Directory (AD RMS) d'émettre :

- Des certificats de licence serveur sur d'autres serveurs du cluster ;
- Des certificats de compte de droits (RAC) aux clients ;
- Des certificats de licence client ;
- Des licences de publication (PL) ;
- Des licences d'utilisation ;
- Modèles de politique de droits.

La clé publique du certificat de licence serveur crypte la clé de contenu dans une licence de publication. Cela permet à un serveur AD RMS d'extraire la clé de contenu et de délivrer des licences d'utilisateur final à l'encontre de la clé de publication.

Certificat d'ordinateur AD RMS

Le certificat d'ordinateur AD RMS est utilisé pour identifier un ordinateur ou un périphérique de confiance. Ce certificat identifie le référentiel sécurisé d'un ordinateur client. La clé publique du certificat de l'ordinateur crypte la clé privée de certificats de compte de droits (RAC). La clé privée du certificat de l'ordinateur déchiffre les certificats de compte de droits (RAC).

Certificat de compte de droits (RAC)

Le certificat de compte de droits (RAC) identifie un utilisateur spécifique. La période de validité par défaut de ce RAC est de 365 jours. Les certificats de compte de droits (RAC) ne peuvent être délivrés que pour les utilisateurs des Services de domaine Active Directory (AD DS) qui ont des adresses e-mail associées à leurs comptes. Un RAC est délivré la première fois qu'un utilisateur tente d'accéder au contenu protégé des Services de gestion des droits Active Directory (AD RMS) ou d'effectuer une tâche des Services de gestion des droits Active Directory (AD RMS), comme la création d'un document protégé. Vous pouvez ajuster la période de validité par défaut en utilisant le nœud **Stratégie de certificat RAC** de la console des Services de gestion des droits Active Directory (AD RMS).

Un RAC temporaire a une durée de validité de 15 minutes. Un RAC temporaire est délivré lorsqu'un utilisateur accède au contenu protégé des Services de gestion des droits Active Directory (AD RMS) à partir d'un ordinateur qui ne fait pas partie de la même forêt que le cluster AD RMS ou forêt approuvée. Vous pouvez ajuster la période de validité par défaut en utilisant le nœud **Stratégie de certificat RAC** de la console des Services de gestion des droits Active Directory (AD RMS).

Les Services de gestion des droits Active Directory (AD RMS) prennent en charge les certificats de compte de droits (RAC) supplémentaires suivants :

- Certificats de compte de droits (RAC) des Services de fédération Active Directory (AD FS) Ces RAC sont délivrés aux utilisateurs fédérés et ont une durée de validité de sept jours.
- Deux types de RAC Windows Live ID. Les RAC Windows Live ID utilisés sur les ordinateurs privés ont une période de validité de six mois. Les RAC Windows Live ID utilisés sur les ordinateurs publics sont valides jusqu'à ce que l'utilisateur se déconnecte.

Certificat de licence client

Un certificat de licence client permet à un utilisateur de publier du contenu protégé AD RMS lorsque l'ordinateur client n'est pas connecté au même réseau que le cluster AD RMS. La clé publique du certificat de licence client crypte la clé de contenu symétrique et l'inclut dans la licence de publication qu'elle émet. La clé privée du certificat de licence client signe les licences de publication qui sont émises lorsque le client n'est pas connecté au cluster AD RMS.

Les certificats de licence client sont liées au RAC d'un utilisateur spécifique. Si un autre utilisateur pour qui un RAC n'a pas été délivré tente de publier du contenu protégé AD RMS du même client, il ou elle sera incapable de le faire tant que le client est connecté au cluster AD RMS et peut émettre un RAC pour cet utilisateur.

Licence de publication (PL)

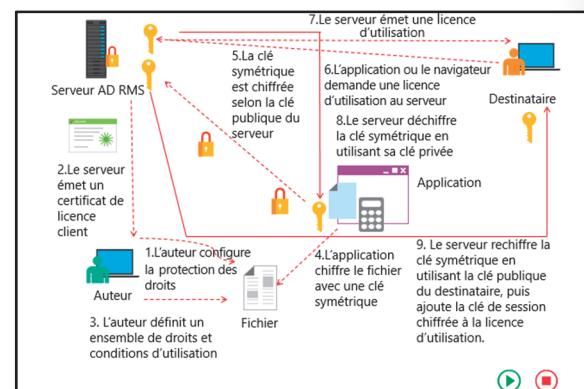
Une licence de publication (PL) détermine les droits applicables au contenu protégé AD RMS. Par exemple, la licence de publication détermine si un utilisateur peut modifier, imprimer ou enregistrer un document. La licence de publication (PL) contient la clé de contenu, qui est chiffrée au moyen de la clé publique du service de licence. Elle contient également l'URL et la signature numérique du serveur AD RMS.

Licence utilisateur final

Une licence utilisateur final est nécessaire pour consommer du contenu protégé AD RMS. Le serveur AD RMS délivre une licence utilisateur final pour chaque utilisateur et pour chaque document. Les licences utilisateur final sont mises en cache par défaut.

Comment fonctionne les Services de gestion des droits Active Directory (AD RMS) :

Lorsqu'un utilisateur aide soit à protéger le contenu à l'aide des Services de gestion des droits Active Directory (AD RMS) soit tente d'accéder au contenu protégé des Services de gestion des droits Active Directory (AD RMS), plusieurs tâches et procédures sont effectuées en arrière-plan. Pour le diagnostic et le dépannage, il est important de comprendre comment fonctionne AD RMS. Même s'ils ne sont pas liés aux services de certificats Active Directory, les Services de gestion des droits Active Directory (AD RMS) utilisent des certificats et le cryptage de manière intensive.



Les Services de gestion des droits Active Directory (AD RMS) fonctionnent de la manière suivante :

1. la première fois qu'un auteur configure la protection des droits pour un document - comme, par exemple, une application - un certificat de licence client est demandé au serveur AD RMS. Un client localise le serveur AD RMS en utilisant le point de connexion de service dans AD DS.
2. Le serveur délivre alors un certificat de licence client au client, à moins que le client se trouve sur la liste d'exclusion dans AD RMS.
3. Lorsque l'auteur reçoit le certificat de licence client en provenance du serveur AD RMS, il ou elle peut configurer les droits d'utilisation sur le document. L'auteur peut effectuer la configuration manuellement ou en appliquant des modèles pré-établis.
4. Lorsque l'auteur configure les droits d'utilisation, l'application AD RMS activée crypte le fichier à l'aide d'une clé symétrique. Une clé symétrique est générée sur le périphérique client. Lorsque la AD RMS est appliquée au document, le document est en fait chiffré.
5. Cette clé symétrique est ensuite chiffrée au moyen de la clé publique du serveur AD RMS que l'auteur utilise. Cette clé symétrique cryptée est distribuée au serveur AD RMS et stockée sur celui-ci. Parce qu'elle est chiffrée avec la clé publique du serveur, elle ne peut être déchiffrée qu'à l'aide de la clé privée du serveur.
6. L'auteur du contenu protégé des Services de gestion des droits Active Directory (AD RMS) distribue le fichier au destinataire. Le destinataire du fichier ouvre ce dernier à l'aide d'une application ou d'un navigateur AD RMS. Il est impossible d'ouvrir le contenu protégé des Services de gestion des droits Active Directory (AD RMS) à moins que l'application ou le navigateur ne prenne en charge AD RMS. Si le destinataire ne dispose pas d'un certificat de compte sur l'appareil actuel, l'utilisateur en reçoit un à ce stade. L'application ou le navigateur transmet une demande de licence d'utilisation au serveur des Services de gestion des droits Active Directory (AD RMS) de l'auteur.
7. Le serveur des Services de gestion des droits Active Directory (AD RMS) détermine si le destinataire est autorisé. Si le destinataire est autorisé, le serveur des Services de gestion des droits Active Directory (AD RMS) délivre une licence d'utilisation.
8. Le serveur AD RMS déchiffre la clé symétrique qui a été chiffrée à l'étape 5 en utilisant sa clé privée.
9. Le serveur des Services de gestion des droits Active Directory (AD RMS) rechiffre la clé symétrique en utilisant la clé publique du destinataire, puis ajoute la clé de session chiffrée à la licence d'utilisation. La licence d'utilisation et la clé symétrique chiffrée sont ensuite distribuées au destinataire. Le destinataire utilise sa clé privée pour déchiffrer la clé symétrique. Après cela, la clé symétrique est utilisée pour déchiffrer le contenu protégé des Services de gestion des droits Active Directory (AD RMS).

Qu'est-ce que les Services de gestion des droits Azure ?

L'implémentation de Services de gestion des droits Active Directory (AD RMS) dans une infrastructure de réseau local et dans une forêt AD DS permet de protéger les informations. Cependant, elle peut être inefficace dans les cas où le contenu protégé des Services de gestion des droits Active Directory (AD RMS) doit être partagé avec les organisations sélectionnées ou des personnes externes à une organisation. En plus de créer des approbations ou d'utiliser un compte Microsoft, vous pouvez maintenant utiliser les capacités de gestion des droits du

- Azure RMS est la protection RMS du cloud
- Azure RMS est disponible dans Office 365 Entreprise E3, Office 365 ProPlus et comme service distinct
- Azure RMS fournit :
 - Intégration d'IRM avec Office
 - Intégration d'IRM dans Exchange Online
 - Intégration d'IRM dans SharePoint Online
 - Intégration de Windows Server ICF
- L'application de partage RMS s'intègre à l'Explorateur de fichiers

service de cloud public Azure. En outre, dans certains cas, une organisation pourrait ne pas avoir suffisamment de ressources pour mettre en place une infrastructure AD RMS locale.

Azure RMS vous offre la possibilité d'utiliser une protection RMS à partir du cloud sans mettre en œuvre une infrastructure de Services de gestion des droits Active Directory (AD RMS) locale. En utilisant les Services de gestion des droits Azure, vous pouvez attribuer aux documents des stratégies et des restrictions d'utilisation et ensuite partager ces documents avec d'autres organisations qui souscrivent au service Azure. Étant donné que les Services de gestion des droits Azure s'intègrent à tous les services et à toutes les applications Office 365, vous pouvez utiliser toutes les capacités des Services de gestion des droits à la fois du cloud et de l'environnement sur site.

Les Services de gestion des droits Azure sont disponibles dans les abonnements Office 365 Entreprise E3 et Office 365 ProPlus. Vous pouvez également l'acheter comme un service distinct et l'utiliser avec votre cloud ou des ressources sur site. Les Services de gestion des droits Azure fournissent les fonctionnalités suivantes :

- Intégration de la Gestion des droits relatifs à l'information (IRM) dans Office. Toutes les applications Office déployées localement peuvent utiliser les Services de gestion des droits Azure pour aider à protéger le contenu.
- Intégration de la Gestion des droits relatifs à l'information (IRM) dans Exchange Online. Les Services de gestion des droits Azure vous permettent d'aider à protéger et à consommer des messages électroniques soit dans Outlook sur le Web ou dans Outlook. Vous pouvez également consommer des messages protégés de la Gestion des droits relatifs à l'information (IRM)- à l'aide d'Exchange ActiveSync sur les appareils qui prennent en charge l'IRM, tels que les appareils Windows 10 Mobile ou les appareils basés sur iOS. En outre, les administrateurs peuvent utiliser les règles de protection Outlook et les règles de transport Exchange pour la protection et le décryptage pour s'assurer que le contenu ne soit pas divulgué par inadvertance en dehors d'une organisation.
- Intégration de la Gestion des droits relatifs à l'information (IRM) dans SharePoint Online. Lorsque les Services de gestion des droits Azure sont utilisés, les administrateurs peuvent configurer la protection automatique de la Gestion des droits relatifs à l'information (IRM) des documents dans une bibliothèque SharePoint.
- Infrastructure de classification des fichiers de Windows Server (FCI). Si votre ordinateur fonctionne sous Windows Server et possède la fonctionnalité de Gestionnaire de ressources du serveur de fichiers(FSRM), vous avez une infrastructure de classification de fichiers (FCI). La fonctionnalité FSRM permet d'analyser les fichiers sur le serveur et de saisir une action configurée. Par exemple, vous pouvez marquer des fichiers sensibles comme **Sensible**. Après la classification d'un fichier ou d'un dossier, vous pouvez exécuter une autre tâche du Gestionnaire de ressources du serveur de fichiers(FSRM) pour appliquer un modèle de Services de gestion des droits Azure pour le fichier ou le dossier, sur base de la classification Ainsi, si le FSRM trouve un dossier nommé **Paie** et le classe comme **Sensible**, votre FSRM peut appliquer un modèle de Services de gestion des droits Azure correspondant au type de données. Dans ce cas, vous pouvez utiliser un modèle qui limite l'accès au département Paie.

Avantages pour l'organisation

Ces fonctionnalités de Services de gestion des droits Azure offrent plusieurs avantages aux organisations en :

- Aidant les organisations à atteindre les objectifs de conformité. Les Services de gestion des droits Azure sont certifiés pour plusieurs programmes de l'industrie, y compris la Loi sur la transférabilité et la responsabilité de l'assurance maladie (HIPAA) des États-Unis et les normes de sécurité des données de l'industrie des cartes de paiement de niveau 1. De nombreuses organisations sont nécessaires pour stocker des données sensibles chiffrées et celles-ci peuvent utiliser les Services de gestion des droits Azure pour le faire.

- Aidant les organisations à réduire les fuites de données. Dans de nombreuses organisations, les utilisateurs peuvent diffuser des données d'entreprise sans autorisation. Par exemple, une organisation peut être sur le point d'annoncer un nouveau produit, mais une mention du produit a déjà été faite avant que l'organisation ne soit prête à faire l'annonce. Cela se produit souvent parce que les employés transfèrent des messages électroniques internes à des adresses électroniques à l'extérieur de l'organisation, ou copient des fichiers sur des appareils et les emportent à l'extérieur. Les Services de gestion des droits Azure permettent de minimiser les fuites de données en rendant difficile le transfert d'informations pour les employés en dehors de l'organisation sans qu'ils ne soient suivis. Contrairement aux Services de gestion des droits Active Directory (AD RMS), qui sont déployés localement, les Services de gestion des droits Azure vous offrent la possibilité de suivre géographiquement l'emplacement où un fichier est utilisé.
- Aidant les organisations à partager des données confidentielles avec les partenaires et autres organismes extérieurs. Étant donné que les Services de gestion des droits Azure autorisent une collaboration presque virtuelle avec les utilisateurs en dehors de votre organisation, les organisations peuvent améliorer la sécurité en matière de collaboration et de partage des données.
- Minimisant les risques de verrouillage d'accès d'une organisation à ses propres données. Imaginez un scénario dans lequel un manager se prépare à quitter l'entreprise et décide de chiffrer tous les fichiers sur son ordinateur en utilisant la protection de Services de gestion des droits Azure pour que seul son compte utilisateur puisse y avoir accès. Normalement, cela peut poser un problème, surtout si le département Informatique supprime le compte de l'utilisateur avant que tout le monde ne se rende compte que le gestionnaire a chiffré les fichiers. Les Services de gestion des droits Azure offrent une fonctionnalité optionnelle, nommée la fonctionnalité de Super Utilisateur, pour permettre l'accès aux documents chiffrés, même si le chiffrement d'origine spécifiait uniquement un utilisateur particulier qui aurait quitté l'organisation. Un groupe spécial, nommé le groupe de Supers Utilisateurs des Services de gestion des droits Azure, peut permettre d'avoir accès aux documents chiffrés.

Application de partage de Services de gestion de droits

L'application de partage de Services de gestion de droits peut être téléchargée gratuitement auprès de Microsoft. Cette application améliore la façon dont vous pouvez protéger et partager des documents. Après avoir été installée, l'application ajoute un menu de protection des Services de gestion des droits Azure dans le menu contextuel de l'Explorateur de fichiers. Lorsque vous faites un clic droit sur un fichier ou un dossier, vous voyez un nouveau élément du menu **Protéger avec les Services de gestion de droits**. Cet élément vous permet de protéger un fichier sur votre ordinateur, de partager un fichier protégé, de suivre l'utilisation d'un fichier partagé et de supprimer la protection d'un fichier. La fonctionnalité se rattache également aux modèles de Services de gestion des droits Azure. Alternativement, vous pouvez utiliser des autorisations personnalisées.

 **Liens de référence :** Pour télécharger les RMS libres partageant l'application de Microsoft, rendez-vous sur : <http://aka.ms/v1s1xd>

Comparaison AD RMS, Azure RMS et Azure RMS pour Office 365

Les fonctionnalités de base des Services de gestion des droits Active Directory (AD RMS), des Services de gestion des droits Azure et des Services de gestion des droits Azure pour Office 365 sont similaires. Ils utilisent tous le chiffrement pour aider à protéger les données et s'intègrent aux mêmes applications basées sur les serveurs Exchange Server et SharePoint Server.

Les Services de gestion des droits Active Directory (AD RMS) et les Services de gestion des droits Azure s'intègrent également à l'infrastructure de classification de fichiers (FCI)

de Windows Server, mais pas les Services de gestion des droits Azure pour Office 365. Microsoft a commencé à ajouter en premier lieu de nouvelles fonctionnalités aux versions d'applications basées sur le cloud. Par conséquent, les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365 possèdent des fonctionnalités que les Services de gestion des droits Active Directory (AD RMS) ne possèdent pas. Microsoft est susceptible de continuer avec cette approche tandis qu'un nouveau développement progresse. Quelques unes des principales différences entre les Services de gestion des droits Active Directory (AD RMS), les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365 comprennent :

- L'intégration d'applications basées sur le serveur. Les Services de gestion des droits Active Directory (AD RMS) et les Services de gestion des droits Azure s'intègrent aux versions sur- site d'Exchange Server, de SharePoint Server et de l'infrastructure de classification de fichiers (FCI) de Windows Server. Cependant, les Services de gestion des droits Azure s'intègrent également à Office 365, Exchange Online, SharePoint Online et Microsoft OneDrive for Business, alors que ce n'est pas le cas pour les Services de gestion des droits Active Directory (AD RMS). Les Services de gestion des droits Azure pour Office 365 s'intègrent aux versions sur site d'Exchange Server et SharePoint Server en plus d'Exchange Online, de SharePoint Online et de OneDrive for Business. Pour les organisations qui explorent actuellement le cloud, l'utilisent ou prévoient un déplacement futur vers ce dernier, nous recommandons les Services de gestion des droits Azure comme meilleur choix.
- Le partage entre les différentes organisations. Avec les Services de gestion des droits Active Directory (AD RMS), vous pouvez créer des approbations entre les différentes organisations pour partager le contenu protégé des Services de gestion de droits - parmi ces organisations. Cependant, ce partage nécessite beaucoup de planification et de travail. L'un des facteurs les plus limitant des Services de gestion des droits Active Directory (AD RMS) est la complexité du partage de documents protégés des Services de gestion de droits à de multiples organisations. Les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365 suppriment cette barrière. Avec les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365, les approbations sont en place par défaut. Si les organisations possèdent Office 365, les Services de gestion des droits Azure ou des Services de gestion de droits pour les particuliers, vous pouvez partager le contenu protégé des Services de gestion de droits RMS avec eux sans créer des approbations ou effectuer d'autres configurations.
- Partage au moyen de l'application de partage des Services de gestion de droits. Avec les Services de gestion des droits Active Directory (AD RMS), vous pouvez utiliser l'application de partage des Services de gestion de droits (RMS) pour partager des documents RMS protégés avec d'autres personnes de votre organisation. Cependant, vous ne pouvez pas les partager avec les gens à l'extérieur de votre organisation. Avec les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365, vous pouvez partager ces documents avec des personnes à l'intérieur et à l'extérieur de votre organisation. Vous pouvez également utiliser les notifications par courriel pour savoir quand

| Fonctionnalité | AD RMS | Azure RMS | Azure RMS pour Office 365 |
|---|--------|-----------|---------------------------|
| IRM pour serveur Exchange sur site et serveur SharePoint interne | Oui | Oui | Oui |
| IRM pour Exchange Online et SharePoint Online | Non | Oui | Oui |
| La possibilité de partager avec n'importe quelle organisation sans configuration supplémentaire | Non | Oui | Oui |
| Modèles par défaut | Non | Oui | Oui |
| La capacité de protéger tout type de fichier | Oui | Oui | Oui |
| Suivi de document protégé par RMS | Non | Oui | Non |
| Assistance appareil mobile | Oui | Oui | Oui |

quelqu'un tente d'accéder à votre document RMS protégé. En outre, vous bénéficiez d'un accès à un site de suivi de document-pour suivre l'utilisation des documents et les révoquer.

- Prise en charge de Azure Multi-Factor Authentication (Azure MFA). Les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365 prennent en charge Azure MFA, alors que les Services de gestion des droits Active Directory (AD RMS) prennent en charge Azure MFA uniquement avec un serveur local MFA. Cela vous permet d'améliorer la sécurité de votre contenu RMS protégé en demandant deux facteurs d'authentification.

 **Lectures supplémentaires :** Pour plus d'informations, consultez : « Comparaison de la gestion des droits Azure et des Services de gestion des droits Active Directory (AD RMS) » sur : <http://aka.ms/sndlw0>

Du point de vue d'un administrateur, d'autres différences existent entre les Services de gestion des droits Active Directory (AD RMS), les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365 :

- Infrastructure. Pour prendre en charge les Services de gestion des droits Active Directory (AD RMS)- sur site, vous devez déployer au moins un serveur des Services de gestion des droits Active Directory (AD RMS). Pour les installations à haute disponibilité, vous avez besoin d'au moins deux serveurs des Services de gestion des droits Active Directory (AD RMS). En outre, vous devez avoir au moins un serveur qui exécute SQL Server pour héberger les bases de données. Vous devez également configurer un compte AD DS à utiliser comme compte de service AD RMS. Si vous voulez utiliser des identités fédérées pour permettre l'utilisation de votre infrastructure de Services de gestion des droits Active Directory (AD RMS) sur plusieurs organisations, vous avez besoin des Services de fédération Active Directory (AD FS) et d'un serveur d'application Web Proxy dans le réseau de périmètre. Enfin, vous devez obtenir un certificat SSL (Secure Sockets Layer) pour les Services de gestion des droits Active Directory (AD RMS). Pour les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365, Azure fournit tous ces composants d'infrastructure.
- Administration et maintenance. Les Services de gestion des droits Active Directory (AD RMS) exigent des composants d'infrastructure qui nécessitent une administration et une maintenance occasionnelle. Par exemple, vous pourriez avoir besoin d'installer un ensemble de services pour SQL Server ou résoudre les problèmes de performances sur le serveur de Services de gestion des droits Active Directory (AD RMS). D'autres tâches, telles que l'installation des dernières mises à jour de sécurité sur les serveurs, sont des tâches mensuelles de routine. Pour les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365, Azure gère ces activités.
- Prise en charge. Lorsque les Services de gestion des droits Active Directory (AD RMS) cessent de répondre ou rencontrent un autre problème majeur que vous ne pouvez pas résoudre, vous devez appeler le support technique Microsoft et travailler avec eux pour résoudre le problème. Microsoft résout des problèmes semblables rencontrés avec les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365. Les Services de gestion des droits Azure et les Services de gestion des droits Azure pour Office 365, comme tous les autres services Azure, possèdent des accords de niveau de service et des accords de haute disponibilité dans l'ensemble des principaux composants.

Question : Quand un utilisateur reçoit-il un certificat RAC ?

Vérifiez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|--|---------|
| Azure RMS est déployé localement sur un serveur. | |

Leçon 2

Déploiement et gestion d'une infrastructure AD RMS

Avant de déployer les Services de gestion des droits Active Directory (AD RMS), il est important d'avoir un plan qui convient à l'environnement de votre organisation. Le déploiement de Services de gestion des droits Active Directory (AD RMS) dans une forêt de domaine unique est différent des scénarios dans lesquels vous avez besoin de prendre en charge la publication et la consommation de contenu sur plusieurs forêts, organisations partenaires de confiance ou sur Internet. Avant de déployer les Services de gestion des droits Active Directory (AD RMS), vous devez comprendre les exigences des clients et avoir une stratégie appropriée de sauvegarde et de récupération des Services de gestion des droits Active Directory (AD RMS). Cette leçon donne un aperçu du déploiement des Services de gestion des droits Active Directory (AD RMS) et des étapes que vous devez suivre pour sauvegarder, récupérer et désaffecter une infrastructure de Services de gestion des droits Active Directory (AD RMS).

Objectifs des leçons

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

- Décrire des cas de déploiement des Services de gestion des droits Active Directory (AD RMS) ;
- Expliquer comment configurer le cluster des Services de gestion des droits Active Directory (AD RMS) ;
- Installer le premier serveur d'un cluster de Services de gestion des droits Active Directory (AD RMS) ;
- Décrire les exigences des clients des Services de gestion des droits Active Directory (AD RMS) ;
- Expliquer comment mettre en place une stratégie de sauvegarde et de récupération des Services de gestion des droits Active Directory (AD RMS) ;
- Expliquer comment désactiver et supprimer les Services de gestion des droits Active Directory (AD RMS) ;
- Expliquer comment surveiller les Services de gestion des droits Active Directory (AD RMS) ;
- Expliquer comment implémenter le partage externe pour les Services de gestion des droits Active Directory (AD RMS).

Scénarios de déploiement AD RMS

Un déploiement des Services de gestion des droits Active Directory (AD RMS) se compose d'un ou plusieurs serveurs, appelé *cluster*. Un cluster de Services de gestion des droits Active Directory (AD RMS) n'est pas un cluster de basculement à haute disponibilité. Lorsque vous déployez des Services de gestion des droits Active Directory (AD RMS), vous devez les implémenter sur un serveur qui est hautement disponible. Les Services de gestion des droits Active Directory (AD RMS) se déplacent généralement comme un ordinateur virtuel hautement disponible (VM).

Scénarios de déploiement pour AD RMS :

- Déployé dans une forêt unique ;
- Déployé dans des forêts multiples ;
- Utilisé sur un extranet ;
- Intégré à AD FS ;
- Déployé dans Azure comme service Azure RMS.

Lorsque vous déployez des Services de gestion des droits Active Directory (AD RMS) dans une seule forêt, vous disposez d'un cluster de Services de gestion des droits Active Directory (AD RMS) unique. Ceci est la forme la plus commune de déploiement de Services de gestion des droits Active Directory (AD RMS). Vous pouvez ajouter des serveurs au cluster de Services de gestion des droits Active Directory (AD RMS) pour fournir davantage de capacité.

Lorsque vous déployez des Services de gestion des droits Active Directory (AD RMS) dans plusieurs forêts, chaque forêt doit avoir son propre cluster racine de Services de gestion des droits Active Directory (AD RMS), sauf lorsque vous déployez des Services de fédération Active Directory (AD FS) pour utiliser un cluster de Services de gestion des droits Active Directory (AD RMS) unique pour plusieurs forêts. Il est nécessaire de configurer les domaines de publication approuvés des Services de gestion des droits Active Directory (AD RMS) ou des domaines d'utilisateurs de confiance pour aider à faire en sorte que le contenu des Services de gestion des droits Active Directory (AD RMS) peut être protégé et consommé sur les différentes forêts.

Vous pouvez également déployer les Services de gestion des droits Active Directory (AD RMS) pour les emplacements extranet. Dans ce déploiement, le serveur de licences des Services de gestion des droits Active Directory (AD RMS) est accessible par les hôtes de l'Internet. Vous utilisez ce type de déploiement pour prendre en charge la collaboration avec des utilisateurs externes.

Vous pouvez déployer des Services de gestion des droits Active Directory (AD RMS) avec AD FS ou le système d'authentification Azure Active Directory (Azure AD) (anciennement connu sous le nom Microsoft Federation Gateway). Dans ce scénario, les utilisateurs profitent de l'identité fédérée pour publier et consommer du contenu protégé par des droits.

La meilleure chose à faire est de ne pas déployer les Services de gestion des droits Active Directory (AD RMS) sur un contrôleur de domaine. Si vous déployez des Services de gestion des droits Active Directory (AD RMS) sur un contrôleur de domaine, vous devez ajouter le compte de service des Services de gestion des droits Active Directory (AD RMS) au groupe d'administrateurs du domaine. Cependant, l'ajout de comptes de services aux groupes très privilégiés n'est pas une bonne chose.

Comme alternative au déploiement de Services de gestion des droits Active Directory (AD RMS) sur site, vous pouvez choisir d'utiliser les Services de gestion des droits Azure comme décrits précédemment.

Configuration du cluster AD RMS

Après avoir installé le rôle de serveur des Services de gestion des droits Active Directory (AD RMS), vous devez configurer le cluster de Services de gestion des droits Active Directory (AD RMS) avant de pouvoir utiliser ces derniers. La configuration du cluster de Services de gestion des droits Active Directory (AD RMS) implique la configuration des composants suivants:

- Appartenance du Cluster aux Services de gestion des droits Active Directory (AD RMS). Choisissez si vous souhaitez créer un nouveau cluster racine de Services de gestion des droits Active Directory (AD RMS) ou joindre un cluster existant.
- Base de données de configuration. Sélectionnez si vous souhaitez utiliser une instance SQL Server existante dans laquelle stocker la base de données de configuration des Services de gestion des droits Active Directory (AD RMS) ou si vous souhaitez configurer et installer localement une base de données interne Windows (WID). Vous pouvez utiliser SQL Server 2008 ou une version plus récente

La configuration AD RMS comprend la configuration des composants suivants :

- Nouveau cluster ou cluster existant
- Base de données de configuration
- Compte de service
- Mode de chiffrement
- Stockage de clé de cluster
- Mot de passe de clé de cluster
- Site web du cluster
- Adresse du cluster
- Certificat de licence
- Inscription du point de connexion de service

pour prendre en charge un déploiement de Services de gestion des droits Active Directory (AD RMS) dans Windows Server 2016. Le mieux est d'utiliser une base de données SQL Server qui est hébergée sur un serveur distinct.

- Compte de service. Nous vous recommandons d'utiliser un compte d'utilisateur de domaine standard avec des autorisations supplémentaires. Vous pouvez utiliser un compte de service géré comme le compte de service AD RMS.
- Mode de chiffrement. Choisissez la force du chiffrement utilisé avec les Services de gestion des droits Active Directory (AD RMS) :
 - Cryptographic Mode 2 utilise des clés RSA 2048 bits et des hachages Secure Hash Algorithm 256 (SHA-256).
 - Cryptographic Mode 1 utilise des clés RSA 1045 bits et des hachages Secure Hash Algorithm 1 (SHA-1).
- Stockage de la clé de cluster : Choisissez l'emplacement de stockage de la clé de cluster. Vous pouvez la stocker dans les Services de gestion des droits Active Directory (AD RMS), ou vous pouvez utiliser un fournisseur de services de chiffrement (CSP). Si vous utilisez un fournisseur de services de chiffrement (CSP) et que vous voulez ajouter d'autres serveurs, vous aurez besoin de distribuer la clé manuellement.
- Mot de passe de la clé de cluster : Ce mot de passe crypte la clé de cluster et est nécessaire si vous souhaitez soit joindre d'autres serveurs des Services de gestion des droits Active Directory (AD RMS) au cluster soit restaurer le cluster à partir d'une sauvegarde.
- Site web du Cluster. Choisissez quel site sur le serveur local hébergera le site du cluster de Services de gestion des droits Active Directory (AD RMS).
- Adresse du cluster. Indiquez le nom de domaine complet à utiliser avec le cluster. Vous avez la possibilité de choisir un site Web qui est ou non chiffré avec SSL. Si vous ne choisissez pas le chiffrement SSL, vous ne pourrez pas ajouter la prise en charge de la fédération d'identité. Après avoir défini l'adresse du cluster et le port, vous ne pouvez pas en changer sans supprimer complètement les Services de gestion des droits Active Directory (AD RMS).
- Certificat de licence. Choisissez le nom amical que le certificat de licence du serveur utilisera. Il doit représenter la fonction du certificat.
- Enregistrement de point de connexion de service. Choisissez d'enregistrer le point de connexion de service dans AD DS lorsque le cluster de Services de gestion des droits Active Directory (AD RMS) est créé. Le point de connexion de service permet aux ordinateurs qui sont membres du domaine de localiser automatiquement le cluster de Services de gestion des droits Active Directory (AD RMS). Seuls les utilisateurs qui sont membres du groupe Administrateurs de l'entreprise peuvent enregistrer le point de connexion de service. Vous pouvez effectuer cette étape après que le cluster de Services de gestion des droits Active Directory (AD RMS) ait été créé. Vous ne devez pas effectuer cette étape au cours du processus de configuration.

Démonstration : Installation du premier serveur d'un cluster AD RMS

Dans cette démonstration, vous verrez comment déployer les Services de gestion des droits Active Directory (AD RMS) sur un ordinateur exécutant Windows Server 2016.

Procédure de démonstration

Configurer un compte de service

1. Connectez-vous à **LON-DC1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.

2. Utilisez le centre administratif Active Directory pour créer une unité d'organisation (UO) nommée **Comptes de service** dans le domaine **adatum.com**.
3. Créez un nouveau compte d'utilisateur dans le comptes de service UO avec les propriétés suivantes :
 - o Prénom: **ADRMSSVC**
 - o Ouverture de la session UPN de l'utilisateur : **ADRMSSVC**
 - o **User SamAccountName Logon : Adatum\ADRMSSVC**
 - o Mot de passe : **Pa55w.rd.**
 - o Confirmer le mot de passe : **Pa55w.rd.**
 - o Le mot de passe n'expire jamais : **Activé**
 - o L'utilisateur ne peut pas modifier le mot de passe : **Activé**

Préparation du système DNS (Domain Name System)

- Utilisez la console **Gestionnaire DNS** pour créer un enregistrement d'une ressource hôte (A) dans la zone **adatum.com** avec les propriétés suivantes :
 - o Nom : **adrms**
 - o Adresse IP : **172.16.0.21**

Installation du rôle AD RMS

1. Connectez-vous à **LON-SVR1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd.**
2. Utilisez l'**Assistant Ajouter rôles et fonctionnalités** pour ajouter le rôle **Services de gestion des droits Active Directory** sur **LON-SVR1** en utilisant l'option suivante :
 - o Services de rôle : **Services Active Server Directory Rights Management**

Configuration des Services de gestion des droits Active Directory (AD RMS)

1. Dans le **Gestionnaire de serveurs**, à partir du nœud **AD RMS**, cliquez sur **Plus** pour démarrer la configuration post-déploiement de AD RMS.
2. Dans l'**Assistant de configuration d'AD RMS**, complétez les informations suivantes :
 - o **Créer un nouveau cluster racine AD RMS**
 - o **Utiliser la base de données interne Windows sur ce serveur**
 - o **Utiliser Adatum\ADRMSSVC comme compte de service**
 - o Mode de chiffrement : **Cryptographic Mode 2**
 - o Stockage de clé du cluster : **Utiliser un stockage de clés AD RMS géré de manière centralisée**
 - o Mot de passe de la clé du cluster : **Pa55w.rd.**
 - o Site Web du cluster : **Site Web par défaut**
 - o Type de connexion : **Utilisation d'une connexion non chiffrée**
 - o Nom de domaine complet : **http://adrms.adatum.com**
 - o Port : **80**
 - o Certificat du concédant : **AdatumADRMS**
 - o Enregistrer le point de connexion de service AD RMS : **Enregistrez le point de connexion de service maintenant**
3. Déconnectez-vous de **LON-SVR1**.



Remarque : Vous devez vous déconnecter avant de pouvoir gérer AD RMS.

Exigences client AD RMS

Le contenu AD RMS est publié et consommé uniquement par des ordinateurs qui exécutent le client de Services de gestion des droits Active Directory (AD RMS). Windows 10, Windows 8.1, Windows 8, Windows 7 et Windows Vista comprennent le logiciel client de Services de gestion des droits Active Directory (AD RMS). Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 et Windows Server 2008 incluent également le client de Services de gestion des droits Active Directory (AD RMS). Ces systèmes d'exploitation ne nécessitent pas de configuration supplémentaire pour consommer et publier du contenu protégé de Services de gestion des droits Active Directory (AD RMS).

- Le client est inclus dans Windows Vista ou les versions plus récentes
- Le client est inclus dans Windows Server 2008 et les versions plus récentes
- Le client est disponible en téléchargement pour les Systèmes d'exploitation Windows XP et Mac OS X
- Les applications activées pour AD RMS comprennent Office 2007 et les versions plus récentes
- Serveur Exchange 2007 et les versions plus récentes prennent en charge AD RMS
- Le client AD RMS a besoin d'une Licence d'accès client (CAL) RMS

Le logiciel client AD RMS est disponible pour le téléchargement sur les ordinateurs qui exécutent le système d'exploitation Windows XP ou Mac OS X. Ce logiciel client doit être installé avant que les utilisateurs de ces systèmes d'exploitation ne puissent consommer et publier du contenu protégé des Services de gestion des droits Active Directory (AD RMS).

Les Services de gestion des droits Active Directory (AD RMS) nécessitent des applications compatibles. Les applications de serveur qui prennent en charge les Services de gestion des droits Active Directory (AD RMS) comprennent Exchange Server 2007 et versions plus récentes et Office SharePoint Server 2007 et versions plus récentes.

Les applications clients, tels que celles incluses dans Office 2003 et versions plus récentes, peuvent publier et consommer du contenu protégé des Services de gestion des droits Active Directory (AD RMS). Vous pouvez utiliser le kit de développement logiciel (SDK) des Services de gestion des droits Active Directory (AD RMS) pour créer des applications qui permettent de publier et de consommer le contenu protégé des Services de gestion des droits Active Directory (AD RMS). XML Paper Specification Viewer et Internet Explorer peuvent également visionner le contenu protégé des Services de gestion des droits Active Directory (AD RMS).

Vous pouvez également utiliser une application de partage de RMS sur les appareils mobiles qui exécutent Windows 10 Mobile, iOS et Android pour aider à protéger certains types de contenu.



Remarque : Microsoft a publié la nouvelle version du logiciel client de Services de gestion des droits Active Directory (AD RMS) - le client de Services de gestion des droits Active Directory (AD RMS) 2.1. Vous pouvez le télécharger à partir du Centre de téléchargement Microsoft. Entre autres, la nouvelle version offre un nouveau kit de développement logiciel (SDK) que vous pouvez également télécharger à partir du Centre de téléchargement Microsoft. Le nouveau kit de développement logiciel (SDK) des Services de gestion des droits Active Directory (AD RMS) offre un moyen simple pour les développeurs de créer des applications et des solutions qui protègent et consomment le contenu critique. Avec le nouveau SDK, vous pouvez créer des applications et des solutions activées sur les droits beaucoup plus rapidement et facilement que auparavant.

Licence du client de Services de gestion des droits Active Directory (AD RMS)

Pour utiliser les Services de gestion des droits Active Directory (AD RMS) dans votre environnement AD DS, vous devez disposer de licences d'accès client (CAL) à la gestion des droits de Windows. Ces licences d'accès client sont différentes des licences d'accès client (CAL) Windows Server classiques dont vous avez besoin pour connecter un client à un serveur. Chaque utilisateur qui permet de créer ou d'utiliser des fichiers protégés par des droits doit posséder une licence d'accès client utilisateur de Services de gestion de droits (RMS). Alternativement, vous pouvez utiliser des licences d'accès client d'appareils RMS pour les ordinateurs qui créent et visionnent le contenu RMS protégé.

Si vous avez besoin de partager votre contenu RMS protégé à l'extérieur de votre organisation, vous pouvez obtenir une licence de connecteur externe RMS. Cette licence donne à une organisation le droit d'autoriser un nombre illimité d'utilisateurs externes à accéder ou à utiliser une seule licence sans qu'il soit nécessaire d'acquérir une CAL pour chaque utilisateur externe.

Mise en œuvre d'une stratégie de sauvegarde et de récupération AD RMS

Pour aider à prévenir la perte de données, vous devez sauvegarder un serveur de Services de gestion des droits Active Directory (AD RMS) de sorte que vous pouvez le récupérer en cas de corruption de fichier ou d'échec du serveur. Si le serveur de Services de gestion des droits Active Directory (AD RMS) devient inaccessible, tout le contenu protégé des Services de gestion des droits Active Directory (AD RMS) devient aussi inaccessible.

Une simple stratégie de sauvegarde et de récupération des Services de gestion des droits

- Sauvegarder la clé privée et les certificats
- Veiller à sauvegarder régulièrement la base de données AD RMS
- Exporter les modèles pour les sauvegarder
- Exécuter le serveur AD RMS comme Machine virtuelle, et faire une sauvegarde complète du serveur

Active Directory (AD RMS) consiste à exécuter le serveur de Services de gestion des droits Active Directory (AD RMS) en tant que VM, puis à utiliser le produit de sauvegarde d'une entreprise, tel que Microsoft System Center Data Protection Manager, pour effectuer des sauvegardes régulières de l'ordinateur virtuel. Certains des éléments importants qui nécessitent des sauvegardes sont la clé privée, les certificats, la base de données des Services de gestion des droits Active Directory (AD RMS) et des modèles. Vous pouvez également effectuer une sauvegarde complète du serveur en exécutant le serveur de Services de gestion des droits Active Directory (AD RMS) sur un ordinateur virtuel.

Le mieux est que vous sauvegardiez la clé privée des Services de gestion des droits Active Directory (AD RMS) et tous les certificats qui les utilisent. La méthode la plus simple de le faire est d'exporter les certificats vers un endroit plus sûr. Vous devez également sauvegarder de manière régulière la base de données des Services de gestion des droits Active Directory (AD RMS). La méthode que vous utilisez pour faire cela dépend de si les Services de gestion des droits Active Directory (AD RMS) utilisent SQL Server ou une base de données interne Windows (WDI). Pour sauvegarder les modèles, configurez les modèles à exporter vers un dossier partagé, puis sauvegardez-les.

Lorsque vous effectuez une récupération du rôle de Services de gestion des droits Active Directory (AD RMS), il peut être nécessaire de supprimer l'objet **Point de connexion de service** de AD DS. Vous avez besoin de faire cela si vous récupérez un serveur de configuration racine des Services de gestion des droits Active Directory (AD RMS) et que les tentatives du serveur à s'approvisionner lui-même en tant que serveur de licence uniquement.

Mise hors service et retrait de AD RMS

Avant de supprimer un serveur de Services de gestion des droits Active Directory (AD RMS), vous devez désaffecter ce serveur. La désaffectation des Services de gestion des droits Active Directory (AD RMS) met le cluster dans un état où les consommateurs de contenu protégé des Services de gestion des droits Active Directory (AD RMS) peuvent obtenir des clés spéciales qui déchiffrent ce contenu, quelles que soient les restrictions existantes qui ont été imposées concernant l'utilisation de ce contenu. Si vous ne disposez pas d'une période de désaffectation, et si vous supprimez simplement le serveur de Services de gestion des droits Active Directory (AD RMS), le contenu protégé des Services de gestion des droits Active Directory (AD RMS) deviendra inaccessible.

- Déclassement d'un cluster AD RMS avant de le retirer :
 - Désactiver le besoin de fournir une clé qui déchiffre du contenu AD RMS publié auparavant ;
 - Laisser le serveur en mode désactivé jusqu'à ce que tout le contenu protégé par AD RMS ait migré ;
 - Exporter le certificat de licence serveur avant de désinstaller le rôle AD RMS.

Pour ce faire, procédez comme suit :

1. Connectez-vous au serveur qui héberge les Services de gestion des droits Active Directory (AD RMS) et que vous voulez désaffecter.
2. Modifiez la liste de contrôle d'accès du fichier **Désaffectation.asmx**. Accordez au groupe **Tout le monde** l'autorisation **Lire et exécuter** sur le fichier. Ce fichier est stocké dans le dossier **%SystemDrive%\Inetpub\wwwroot_wmcs\désaffectation**.
3. Dans la console **AD RMS**, développez le nœud **Politiques de sécurité**, puis cliquez sur le noeud **Désaffectation**.
4. Dans le volet **Actions**, cliquez sur **Activer désaffectation**, puis cliquez sur **Désaffectation**.
5. Lorsque vous êtes invité à confirmer que vous voulez désaffecter le serveur, cliquez sur **Oui**.

Après avoir terminé le processus de désaffectation des Services de gestion des droits Active Directory (AD RMS) et avant de désinstaller le rôle de Services de gestion des droits Active Directory (AD RMS), vous devez exporter le certificat de licence de serveur de Services de gestion des droits Active Directory (AD RMS).

Contrôle d'AD RMS

La Surveillance de la fonctionnalité AD RMS est essentielle dans chaque scénario de déploiement. Vous pouvez surveiller les Services de gestion des droits Active Directory (AD RMS) en utilisant des outils qui sont intégrés à Windows Server et aux Services de gestion des droits Active Directory (AD RMS) ou en utilisant les services de surveillance externes, tels que le Gestionnaire d'opérations System Center. Les Services de gestion des droits Active Directory (AD RMS) fournissent trois types de rapports au sein de la console de Services de gestion des droits Active Directory (AD RMS) :

- AD RMS intègre une fonctionnalité de surveillance et de création de rapports
- Il faut avoir Microsoft Report Viewer pour créer des rapports
- Les rapports disponibles sont les suivants :
 - Statistiques
 - Health (état de santé)
 - Résolution des problèmes
- Operations Manager peut surveiller AD RMS avec un pack d'administration existant

- Rapports statistiques. Ces rapports vous donnent des informations sur le nombre de comptes d'utilisateurs qui ont reçu les certificats de compte de droits (RAC) du cluster de Services de gestion des droits Active Directory (AD RMS). Étant donné qu'une licence d'accès client (CAL) distincte est requise pour chaque RAC, vous pouvez utiliser ce rapport pour estimer le nombre de licences d'accès client des Services de gestion des droits Active Directory (AD RMS) que vous avez besoin d'acheter. Les rapports statistiques vous donnent le nombre de comptes d'utilisateurs qui sont certifiés pour les Services de gestion des droits Active Directory (AD RMS), le nombre de comptes d'utilisateurs de domaine certifiés et le nombre d'identités fédérées certifiées.
- Rapports d'intégrité. Les rapports d'intégrité du système vous donnent des informations sur les demandes que le serveur de Services de gestion des droits Active Directory (AD RMS) reçoit dans un certain laps de temps. En utilisant Microsoft Report Viewer, ce rapport génère des graphiques et des données numériques sur le nombre total de demandes reçues par les Services de gestion des droits Active Directory (AD RMS). Cela inclut la durée moyenne de traitement de chaque demande, le nombre de demandes qui ont été traitées avec succès et le nombre de demandes qui ont échoué. Vous pouvez également voir le pourcentage de demandes traitées avec succès. Si vous voyez un grand nombre de demandes ayant échoué, cela peut indiquer une configuration du client incorrecte.
- Rapports de dépannage. Ces rapports fournissent une liste de numéros pour le nombre total de demandes d'utilisateurs ayant abouti et échoué pour chaque type de demande. Par exemple, vous pouvez voir le nombre total de demandes de certification, le nombre total de demandes pour trouver l'emplacement de service et le nombre total de demandes de certificat de licence serveur.

 **Remarque :** Les rapports statistiques sont disponibles par défaut. Toutefois, pour utiliser les rapports d'intégrité et de dépannage, vous devez avoir installé Microsoft.NET Framework 3.5 et Microsoft Report Viewer 2008 Service Pack 1 (SP1) ou une version ultérieure. Ceux-ci sont disponibles gratuitement sur le Centre de téléchargement Microsoft.

 **Remarque :** vous pouvez également surveiller les Services de gestion des droits Active Directory (AD RMS) en utilisant le Gestionnaire d'opérations. Vous pouvez télécharger le pack de gestion System Center pour les Services de gestion des droits Active Directory (AD RMS), qui avertit les administrateurs à l'avance au sujet des questions qui pourraient avoir une incidence sur les services pour qu'ils puissent enquêter et prendre des mesures correctives, le cas échéant.

 **Lectures supplémentaires :** Pour plus d'informations, consultez : « Scénarios de surveillance » sur : <http://aka.ms/Pyumq7>

Mise en œuvre du partage externe

Dans certains cas, vous devez activer le partage de contenu protégé des Services de gestion des droits Active Directory (AD RMS) avec les utilisateurs d'autres organisations. La technologie AD RMS donne plusieurs méthodes pour y parvenir.

Les stratégies d'approbations permettent aux utilisateurs qui sont externes à votre organisation de consommer le contenu protégé des Services de gestion des droits Active Directory (AD RMS). Par exemple, une stratégie d'approbations peut permettre aux utilisateurs des environnements BYOD (Bring Your Own Device) de consommer leur propre contenu protégé de Services de gestion des droits Active Directory (AD RMS), même si ces appareils ne font pas partie du domaine AD DS de l'organisation. Les approbations AD RMS sont désactivées par défaut et vous devez les activer avant de pouvoir les utiliser. Les Services de gestion des droits Active Directory (AD RMS) soutiennent les stratégies d'approbations suivantes:

- Domaines d'utilisateurs approuvés. Cette stratégie d'approbations permet à un cluster de Services de gestion des droits Active Directory (AD RMS) de traiter les demandes de certificats de licence du client ou d'utiliser des licences des utilisateurs qui disposent de certificats de compte de droits (RAC) émis par un cluster de Services de gestion des droits Active Directory (AD RMS) différent. Par exemple, supposons que A. Datum Corporation et Trey Research sont des organisations distinctes qui ont chacune déployé des Services de gestion des droits Active Directory (AD RMS). Les domaines d'utilisateurs approuvés permettent à chaque organisation de publier et de consommer le contenu protégé de Services de gestion des droits Active Directory (AD RMS) vers et depuis l'organisation partenaire sans avoir à implémenter des approbations AD DS ou AD FS.
- Domaines de publication approuvés. Cette stratégie d'approbations permet à un cluster de Services de gestion des droits Active Directory (AD RMS) d'émettre des licences d'utilisateur final pour le contenu qui utilise des licences de publication (PL) émises par un cluster de Services de gestion des droits Active Directory (AD RMS) différent. Les domaines de publication approuvés renforcent l'infrastructure des Services de gestion des droits Active Directory (AD RMS) existante.
- Approbation de fédération. Cette stratégie d'approbations fournit l'authentification unique pour les technologies partenaires. Les partenaires fédérés peuvent consommer du contenu protégé des Services de gestion des droits Active Directory (AD RMS) sans déployer leurs propres infrastructures de Services de gestion des droits Active Directory (AD RMS). Une approbation de fédération exige un déploiement AD FS.
- Un compte Microsoft Vous pouvez utiliser cette stratégie d'approbations pour permettre aux utilisateurs autonomes possédant des comptes Microsoft de consommer le contenu protégé des Services de gestion des droits Active Directory (AD RMS) qui est généré par les utilisateurs de votre organisation. Toutefois, les utilisateurs de compte Microsoft sont incapables de créer du contenu qui sera protégé par le cluster de Services de gestion des droits Active Directory (AD RMS).
- Un système d'authentification Azure AD. Cette stratégie d'approbations permet à un cluster de Services de gestion des droits Active Directory (AD RMS) de traiter les demandes de publication et de consommation du contenu protégé des Services de gestion des droits Active Directory (AD RMS) à partir d'organisations externes en acceptant les jetons d'authentification basés sur les revendications du système d'authentification Azure. Plutôt que de configurer une approbation de fédération, chaque organisation est en relation avec le système d'authentification Azure. Le système d'authentification Azure agit comme un courtier approuvé.

- Les domaines d'utilisateurs approuvés échangent du contenu protégé entre deux organisations
- Les domaines de publication approuvés consolident l'architecture AD RMS
- Les approbations fédérées permettent aux utilisateurs d'organisations partenaires d'accéder et d'utiliser une infrastructure AD RMS locale
- Les comptes Microsoft permettent à des utilisateurs autonomes d'avoir accès à du contenu AD RMS
- Le système d'authentification Azure permet à un cluster AD RMS de travailler avec des organisations partenaires sans qu'une approbation fédérée directe soit nécessaire

Implémentation d'un accès externe aux Services de gestion des droits Active Directory (AD RMS)

Le type d'accès externe que vous configurez dépend des types d'utilisateurs externes qui ont besoin d'accéder au contenu de votre organisation.

Lorsque vous devez déterminer la méthode à utiliser, examinez les questions suivantes :

- Est-ce que l'utilisateur externe appartient à une organisation qui possède déjà un déploiement des Services de gestion des droits Active Directory (AD RMS) ?
- Est-ce que l'organisation de l'utilisateur externe dispose déjà d'une approbation de fédération avec votre organisation ?
- Est-ce que l'organisation de l'utilisateur externe a établi une relation avec un système d'authentification Azure ?
- Est-ce que l'utilisateur externe doit publier du contenu protégé des Services de gestion des droits Active Directory (AD RMS) accessible à vos détenteurs de certificats de compte de droits (RAC) ?

Il est possible que les organisations utilisent une solution avant d'en fixer une autre. Par exemple, aux stades initiaux, seul un petit nombre d'utilisateurs externes pourrait exiger l'accès au contenu protégé des Services de gestion des droits Active Directory (AD RMS). Dans ce cas, l'utilisation de comptes Microsoft pour les certificats de compte de droits (RAC) pourrait être appropriée. Lorsque plus d'utilisateurs externes d'une seule organisation demandent un accès, une solution différente pourrait être appropriée. L'avantage financier d'une solution pour une organisation doit dépasser le coût de la mise en place de cette solution.

Testez vos connaissances

| Question |
|---|
| Pour mettre en œuvre un cluster AD RMS, quels composants sont nécessaires ? |
| Sélectionnez la bonne réponse. |
| Office |
| Un compte de service |
| Une base de données |
| AD FS |
| Un certificat Secure Sockets Layer (SSL) |

Question : Lorsque vous décidez de supprimer votre cluster AD RMS de AD DS, que devez-vous faire en premier ?

Leçon 3

Configurer la protection de contenu AD RMS

Les Services de gestion des droits Active Directory (AD RMS) utilisent des modèles de stratégie de droits pour appliquer un ensemble cohérent de stratégies pour aider à protéger le contenu. Lors de la configuration des Services de gestion des droits Active Directory (AD RMS), vous devez élaborer des stratégies pour aider à faire en sorte que les utilisateurs soient toujours en mesure d'accéder au contenu protégé des Services de gestion des droits Active Directory (AD RMS) à partir d'un ordinateur qui n'est pas connecté à un cluster de Services de gestion des droits Active Directory (AD RMS). Vous devez également élaborer des stratégies pour empêcher à certains utilisateurs d'accéder au contenu protégé des Services de gestion des droits Active Directory (AD RMS). En outre, vous devez élaborer des stratégies pour aider à faire en sorte que le contenu protégé des Services de gestion des droits Active Directory (AD RMS) soit récupérable s'il a expiré, que le modèle a été supprimé ou que l'auteur du contenu n'est plus disponible.

Objectifs des leçons

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

- Décrire les modèles de stratégie de droits ;
- Créer un modèle de stratégie de droits ;
- Fournir des modèles de stratégie de droits pour une utilisation hors ligne ;
- Décrire les politiques d'exclusion ;
- Créer une politique d'exclusion pour une application ;
- Décrire le groupe de Super Utilisateurs des Services de gestion des droits Active Directory (AD RMS).

Quels sont les modèles de stratégie de droits ?

Les modèles de stratégie de droits vous permettent de configurer les stratégies standards des Services de gestion des droits Active Directory (AD RMS) pour une organisation. Par exemple, vous pouvez configurer des modèles standards qui accordent des droits de visionnage uniquement, qui empêchent toute modification, tout enregistrement ou toute impression ou qui empêchent le transfert de messages ou la réponse à ceux-ci en cas d'utilisation avec Exchange Server.

Vous créez des modèles de stratégie de droits en utilisant la console des Services de gestion des droits Active Directory (AD RMS). Ils sont stockés dans la base de données des Services de gestion des droits Active Directory (AD RMS) et peuvent être stockés au format XML. Lorsque le contenu est consommé, le client vérifie à l'aide des Services de gestion des droits Active Directory (AD RMS) qu'il dispose de la version la plus récente du modèle.

L'auteur d'un document peut choisir d'aider à protéger le contenu en appliquant un modèle existant. Pour ce faire, l'auteur doit utiliser une application des Services de gestion des droits Active Directory (AD RMS). Par exemple, dans Word 2003 ou une version ultérieure, un auteur applique un modèle en utilisant la fonction **Protéger le document**. Word interroge ensuite le système de domaine Active Directory (AD DS) pour déterminer l'emplacement du serveur des Services de gestion des droits

Les modèles de stratégie des droits :

- Autorisent des auteurs à appliquer des formulaires standards de protection dans toute une organisation ;
- Existent dans différentes applications, ce qui permet différents formulaires de droits ;
- Vous permettent de configurer les droits liés à la consultation, la modification et l'impression de documents ;
- Vous permettent de configurer les droits d'expiration de contenu ;
- Vous permettent de configurer la révocation de contenu.

Active Directory (AD RMS). Après avoir déterminé un emplacement pour le serveur des Services de gestion des droits Active Directory (AD RMS), l'auteur peut utiliser les modèles disponibles.

Les modèles de Services de gestion des droits Active Directory (AD RMS) prennent en charge les droits suivants :

- Le contrôle total ; Donne à l'utilisateur un contrôle complet sur un document protégé des Services de gestion des droits Active Directory (AD RMS) ;
- Afficher. Donne à l'utilisateur la possibilité de visualiser un document protégé des Services de gestion des droits Active Directory (AD RMS) ;
- Modifier. Permet à l'utilisateur de modifier un document protégé des Services de gestion des droits Active Directory (AD RMS) ;
- Enregistrer. Permet à l'utilisateur d'utiliser la fonction **Enregistrer** sur un document protégé des Services de gestion des droits Active Directory (AD RMS).
- Exporter (Enregistrer sous) ; Permet à l'utilisateur d'utiliser la fonction **Enregistrer sous** sur un document protégé des Services de gestion des droits Active Directory (AD RMS).
- Imprimer ; Permet l'impression d'un document protégé des Services de gestion des droits Active Directory (AD RMS) ;
- Transférer. Permet au destinataire d'un message protégé des Services de gestion des droits Active Directory (AD RMS) de transmettre ce message ; Ceci est utilisé avec Exchange Server.
- Répondre. Permet au destinataire d'un message protégé des Services de gestion des droits Active Directory (AD RMS) de répondre à ce message ; Ceci est utilisé avec Exchange Server.
- Répondre à tous. Permet au destinataire d'un message protégé des Services de gestion des droits Active Directory (AD RMS) d'utiliser la fonction **Répondre à tous** pour répondre à ce message ; Ceci est utilisé avec Exchange Server.
- Extraire. Permet à l'utilisateur de copier des données à partir du fichier ; Si ce droit n'est pas accordé, l'utilisateur ne peut pas copier de données à partir du fichier.
- Autoriser les macros. Permet à l'utilisateur d'utiliser des macros ;
- Voir les droits. Permet à l'utilisateur de voir les droits attribués ;
- Modifier des droits. Permet à l'utilisateur de modifier des droits attribués ;

Les droits peuvent uniquement être accordés et ne peuvent pas être explicitement refusés. Par exemple, pour faire en sorte qu'un utilisateur ne puisse pas imprimer un document, le modèle associé au document ne doit pas inclure le droit d'impression.

Les administrateurs peuvent également créer des droits personnalisés qui peuvent être utilisés avec les applications compatibles avec les Services de gestion des droits Active Directory (AD RMS).

Les modèles de Services de gestion des droits Active Directory (AD RMS) peuvent également configurer des documents avec les propriétés suivantes :

- **Expiration du contenu.** Cela détermine le moment où le contenu expire. Les options sont les suivantes :
 - Jamais. Le contenu n'expire jamais ;
 - Il expire à une date donnée. Le contenu expire à une date et une heure bien précises ;
 - Il expire ultérieurement. Le contenu expire dans un certain nombre de jours après sa création.
- **Expiration de la licence d'utilisation.** Ceci détermine à quelle période la licence d'utilisation prendra fin et à quel moment une nouvelle licence devra être obtenue.

- **Utilisation d'un navigateur complémentaire pour permettre aux utilisateurs de visualiser le contenu protégé.** Cela permet aux utilisateurs de visualiser le contenu en utilisant un navigateur complémentaire et ne les oblige pas à posséder une application compatible avec les Services de gestion des droits Active Directory (AD RMS).
- **Demande d'une nouvelle licence d'utilisation à chaque fois que le contenu est consommé.** Lorsque vous activez cette option, la mise en cache côté client est désactivée. Cela signifie que le document ne peut pas être consommé lorsque l'ordinateur est hors ligne.
- **Politiques de révocation.** Ceci permet l'utilisation d'une liste de révocation. Cette fonction permet à un auteur de révoquer l'autorisation de consommation de contenu. Vous pouvez spécifier à quelle fréquence la liste de révocation est cochée, la valeur par défaut étant une fois toutes les 24 heures.

Après avoir appliqué un modèle de stratégie des Services de gestion des droits Active Directory (AD RMS) à un document, toutes les mises à jour de ce modèle seront également appliquées à ce document. Par exemple, si vous avez un modèle sans politique d'expiration de contenu qui est utilisé pour aider à protéger les documents et que vous modifiez ce modèle pour inclure une politique d'expiration de contenu, les documents protégés auront alors une politique d'expiration. Les modifications du modèle sont visibles après l'obtention de la licence d'utilisateur final. Si les licences d'utilisateur final sont configurées pour ne pas expirer et qu'un utilisateur qui a accès au document possède déjà une licence, cet utilisateur pourrait ne pas recevoir le modèle mis à jour.



Remarque : Vous devriez éviter de supprimer des modèles, parce que les documents qui utilisent ces modèles deviennent inaccessibles pour tout le monde, sauf pour les membres du groupe de Super Utilisateurs. Mieux vaut archiver ces modèles plutôt que de les supprimer.

Vous pouvez visionner les droits associés à un modèle en sélectionnant le modèle dans la console des Services de gestion des droits Active Directory (AD RMS), puis en cliquant sur **Voir le résumé des droits** dans le menu **Actions**.

Démonstration : Création d'un modèle de stratégie de droits

Dans cette démonstration, vous voyez comment créer un modèle de stratégie de droits qui permet aux utilisateurs de visualiser un document, mais de ne pas effectuer d'autres actions.

Procédure de démonstration

- Sur **LON-SVR1**, dans la console **AD RMS**, utilisez le noeud **Modèle de stratégie de droits** pour créer un modèle de stratégie de droits distribué avec les propriétés suivantes :
 - Langue : **Anglais (États-Unis)**
 - Nom : **LectureSeule**
 - Description : **Accès en lecture seule. Pas de copie ni d'impression.**
 - Utilisateurs et droits : **executives@adatum.com**
 - Droits pour quiconque : **Afficher**
 - **Accordez au propriétaire (auteur) un droit de contrôle total sans expiration**
 - Expiration du contenu : **Expire après 7 jours**
 - Expiration de la licence d'utilisation : **Expire après 7 jours**

- Exigez une nouvelle licence d'utilisation à chaque fois que le contenu est consommé (désactiver la mise en cache côté client) : **Activé**

Fournir des modèles de stratégie pour une utilisation hors ligne

Si les utilisateurs publient des modèles reliés aux Services de gestion des droits Active Directory (AD RMS) quand ils ne sont pas connectés au réseau, vous devez veiller à ce qu'ils aient accès à une copie locale des modèles de stratégie de droits disponibles.

Vous pouvez configurer les ordinateurs pour obtenir et stocker automatiquement des modèles de stratégie de droits publiés des pour qu'ils soient disponibles hors connexion. Pour pouvoir activer cette fonctionnalité, les ordinateurs doivent exécuter Windows Vista SP1 ou une version ultérieure pour les clients et Windows Server 2008 ou une version ultérieure pour les serveurs.

1. Activer la tâche planifiée Gestion des modèles de stratégie de droits d'accès AD RMS Droits (Automatisé)
- 2.Modifier la clé de registre pour spécifier l'emplacement du dossier partagé des modèles
3. Publier des modèles dans un dossier partagé

Pour activer cette fonctionnalité, dans le **Planificateur de tâches**, activez la tâche planifiée **Gestion (automatisée) du modèle de stratégie de droits des Services de gestion des droits Active Directory (AD RMS)**, puis modifiez la clé de registre suivante :

```
HKEY_CURRENT_USER \ Software \ Microsoft \ Office \ 12.0 \ Common \ DRM
```

Indiquez l'emplacement suivant pour stocker les modèles :

```
%LocalAppData%\ Microsoft\DRM\Modèles
```

Lorsque les ordinateurs qui exécutent ces systèmes d'exploitation sont reliés au domaine, le client des Services de gestion des droits Active Directory (AD RMS) interroge le cluster des Services de gestion des droits Active Directory (AD RMS) au sujet des nouveaux modèles ou met à jour les modèles existants.

Comme alternative à la distribution des modèles, vous pouvez utiliser des dossiers partagés pour stocker les modèles. Vous pouvez configurer un dossier partagé pour les modèles en effectuant la procédure suivante :

1. Dans la console **AD RMS**, faites un clic droit sur le nœud **Modèles de stratégie de droits**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés des modèles de stratégie de droits**, spécifiez l'emplacement du dossier partagé sur lequel les modèles seront publiés.

Quelles sont les stratégies d'exclusion ?

Les politiques d'exclusion vous aident à empêcher les comptes spécifiques de l'utilisateur, le logiciel client ou les applications d'utiliser les Services de gestion des droits Active Directory (AD RMS).

Exclusion de l'utilisateur

La politique d'exclusion de l'utilisateur vous permet de configurer des Services de gestion des droits Active Directory (AD RMS) de sorte que les comptes d'utilisateurs spécifiques, qui sont identifiés par un attribut Email Active Directory de ces comptes d'utilisateurs, ne puissent pas obtenir des licences d'utilisation. Pour ce faire, vous devez ajouter le RAC de chaque utilisateur sur une liste d'exclusion. L'exclusion de l'utilisateur est désactivée par défaut. Après avoir activé l'exclusion de l'utilisateur, vous pouvez exclure les certificats de compte de droits (RAC) spécifiques.

Vous pouvez utiliser l'exclusion de l'utilisateur lorsque vous avez besoin d'empêcher un utilisateur spécifique d'accéder au contenu protégé des Services de gestion des droits Active Directory (AD RMS). Par exemple, lorsqu'un utilisateur quitte l'organisation, vous pouvez exclure les RAC de cette personne pour vous assurer qu'il ou elle ne puisse pas accéder au contenu protégé. Vous pouvez bloquer les RAC qui sont attribuées à des utilisateurs internes et externes.

Exclusion d'applications

La politique d'exclusion des applications vous permet d'empêcher des applications spécifiques, telles que Microsoft PowerPoint, de créer ou de consommer du contenu protégé des Services de gestion des droits Active Directory (AD RMS). Vous pouvez spécifier des applications par les noms de leurs fichiers exécutables. Vous pouvez également spécifier une version minimale et maximale de l'application. L'exclusion d'applications est désactivée par défaut



Remarque : il est possible de contourner l'exclusion de l'application en renommant un fichier exécutable.

Exclusion de la version du référentiel

La politique d'exclusion de la version du référentiel vous permet d'exclure des clients des Services de gestion des droits Active Directory (AD RMS) tels que ceux possédant des systèmes d'exploitation spécifiques, comme Windows XP et Windows Vista. L'exclusion de la version du référentiel est désactivée par défaut. Après avoir activé l'exclusion de la version du référentiel, vous devez spécifier la version minimale du référentiel à utiliser avec un cluster de Services de gestion des droits Active Directory (AD RMS).



Lectures supplémentaires : Pour plus d'informations, consultez : « Activation des politiques d'exclusion » sur : <http://aka.ms/Lnwbcr>

Démonstration : Création d'une stratégie d'exclusion pour une application

Dans cette démonstration, vous voyez comment exclure l'application PowerPoint des Services de gestion des droits Active Directory (AD RMS).

Procédure de démonstration

- Sur **LON-SVR1**, dans la console **AD RMS**, activez l'Exclusion de l'application.
- Dans la boîte de dialogue **Exclude application**, saisissez les informations suivantes :
 - Nom de fichier d'application : **Powerpnt.exe**
 - Version minimale : **14.0.0.0**
 - Version maximale : **16.0.0.0**

Groupe de super utilisateurs AD RMS

Le groupe de Super Utilisateurs des Services de gestion des droits Active Directory (AD RMS) est un rôle particulier et les membres de ce groupe disposent d'un contrôle total sur l'ensemble du contenu protégé par des-droits géré par le cluster. Les membres du groupe de Super Utilisateurs disposent tous de droits de propriétaires dans toutes les licences d'utilisation qui sont émises par le cluster des Services de gestion des droits Active Directory (AD RMS) sur lequel le groupe de Super Utilisateurs est configuré. Cela signifie que les membres de ce groupe peuvent déchiffrer n'importe quel fichier de contenu protégé par des droits et supprimer les droits de protection de ces fichiers.

- Les membres du groupe de super utilisateurs reçoivent tous les droits du propriétaire complets dans toutes les licences d'utilisation émises par le cluster AD RMS sur lequel est configuré le groupe de super utilisateurs.
- Le Groupe de super utilisateurs :
 - Est non configuré par défaut ;
 - Peut être utilisé comme mécanisme de récupération de données pour le contenu protégé par AD RMS :
 - Peut récupérer du contenu qui a expiré ;
 - Peut récupérer du contenu si le modèle est supprimé ;
 - Peut récupérer du contenu sans requérir les informations d'identification de l'auteur ;
 - Doit être un groupe Active Directory avec une adresse e-mail assignée.

Le groupe de Super Utilisateurs des Services de gestion des droits Active Directory (AD RMS) fournit une méthode de récupération des données pour le contenu protégé des Services de gestion des droits Active Directory (AD RMS). Cette méthode est utile lorsque vous avez besoin de récupérer des données protégées des Services de gestion des droits Active Directory (AD RMS), par exemple lorsque le contenu a expiré, qu'un modèle a été supprimé ou lorsque vous n'avez pas accès.

Les membres du groupe de Super Utilisateurs reçoivent des licences de propriétaires pour l'utilisation de l'ensemble du contenu qui est protégé par le cluster des Services de gestion des droits Active Directory (AD RMS) sur lequel ce groupe de Super Utilisateurs particulier est activé. Les membres du groupe de Super Utilisateurs peuvent réinitialiser le mot de passe de la clé privée du serveur des Services de gestion des droits Active Directory (AD RMS).

En tant que membre du groupe de Super Utilisateurs, vous pouvez accéder à l'ensemble du contenu protégé des Services de gestion des droits Active Directory (AD RMS), même si vous devez être particulièrement prudent lorsque vous gérez les membres de ce groupe. Si vous choisissez d'utiliser le groupe de Super Utilisateurs des Services de gestion des droits Active Directory (AD RMS), envisagez d'implémenter une stratégie de groupe restreinte et d'audit pour limiter le nombre de membres du groupe et de vérifier toutes les modifications qui sont apportées. L'activité des Super Utilisateurs est décrite dans le journal des événements de l'application.

Le groupe de Super Utilisateurs est désactivé par défaut. Vous pouvez activer le groupe de Super Utilisateurs en effectuant la procédure suivante :

1. Dans la console **AD RMS**, développez le nœud du serveur, puis cliquez sur **Politiques de sécurité**.
2. Dans la zone **Politiques de sécurité**, sous **Super Utilisateurs**, cliquez sur **Modifier les paramètres Super Utilisateurs**.
3. Dans le volet **Actions**, cliquez sur **Activer les super utilisateurs**.

Pour définir un groupe particulier en tant que groupe de Super Utilisateurs :

1. Dans la zone **Politiques de sécurité\Super utilisateurs**, cliquez sur **Modifier le groupe de Super Utilisateurs**.
2. Indiquez l'adresse e-mail associée avec le groupe de Super Utilisateurs.

Question : Quels types d'autorisations un groupe de super utilisateurs possède-t-il ?

Atelier pratique : Implémentation d'une infrastructure AD RMS

Scénario

A. Datum Corporation effectue des recherches hautement confidentielles, de sorte que leur équipe de sécurité veut mettre en place une sécurité supplémentaire pour certains des documents générés par le service de recherche. L'équipe de sécurité est soucieuse car toute personne ayant accès en lecture aux documents peut les modifier et les distribuer comme bon lui semble. L'équipe de sécurité veut fournir un niveau de protection supplémentaire qui suit le document même si celui-ci se déplace dans le réseau ou en dehors du réseau.

En tant que responsable administrateur réseau chez A. Datum Corporation, vous devez planifier et mettre en place une solution des Services de gestion des droits Active Directory (AD RMS) qui vous aidera à fournir le niveau de protection exigé par l'équipe de sécurité. La solution AD RMS doit fournir de nombreuses options pouvant être adaptées à une large palette d'exigences professionnelles et de sécurité.

Objectifs

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

- Installer et configurer les Services de gestion des droits Active Directory (AD RMS) ;
- Configurer des modèles de Services de gestion des droits Active Directory (AD RMS) ;
- Utiliser les Services de gestion des droits Active Directory (AD RMS) sur les clients.

Configuration de l'atelier pratique

Durée approximative : 60 minutes

Ordinateurs virtuels. **22742A-LON-DC1**, **22742A-LON-DC2**, **22742A-LON-SVR1** et **22742A-LON-CL1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**.

Pour cet atelier pratique, vous devez utiliser l'environnement d'ordinateur virtuel disponible. Avant de commencer cet atelier pratique, vous devez effectuer la procédure suivante :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-LON-DC1**, et dans le volet **Actions**, cliquez sur **Démarrer**.
3. Dans le volet d'**Actions**, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.

4. Ouvrez une session en utilisant les informations d'authentification suivantes :
 - o Nom d'utilisateur : **Administrateur**
 - o Mot de passe : **Pa55w.rd.**
 - o Domaine : **Adatum**
5. Répétez les étapes 2 et 3 pour **22742A-LON-DC2**, **22742A LON-SVR1** et **22742A-LON-CL1**.

Exercice 1 : Installation et configuration de AD RMS

Scénario

La première étape du déploiement d'AD RMS chez A. Datum Corporation est de déployer un serveur unique dans un cluster AD RMS. Vous allez commencer par configurer les enregistrements DNS appropriés et le compte de service AD RMS, puis vous allez installer et configurer le premier serveur AD RMS. Vous activerez également le groupe des super utilisateurs AD RMS.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer le nom de domaine du système (DNS) et le compte de service des Services de gestion des droits Active Directory (AD RMS) et DNS ;
2. Installer et configurer le rôle du serveur des Services de gestion des droits Active Directory (AD RMS) ;
3. Configurer le groupe de Super Utilisateurs des Services de gestion des droits Active Directory (AD RMS).

► Tâche 1 : Configurer le compte de service AD RMS et DNS

1. Connectez-vous à **LON-DC1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd.**
2. À partir du **Gestionnaire de serveur**, ouvrez le **Centre administratif Active Directory** et créez une unité d'organisation (UO) nommée **Comptes de service** dans le domaine **Adatum.com**.
3. Créez un nouveau compte d'utilisateur dans les **Comptes de service** UO avec les propriétés suivantes :
 - o Prénom : **ADRMSSVC**
 - o Ouverture de la session UPN de l'utilisateur : **ADRMSSVC**
 - o **UserSamAccountName Logon** : **Adatum\ADRMSSVC**
 - o Mot de passe : **Pa55w.rd.**
 - o Confirmer le mot de passe : **Pa55w.rd.**
 - o Le mot de passe n'expire jamais : **Activé**
 - o L'utilisateur ne peut pas modifier le mot de passe : **Activé**
4. Créez un nouveau groupe de sécurité global dans le conteneur **Utilisateurs** nommé **ADRMS_SuperUtilisateurs**. Définissez l'adresse e-mail de ce groupe comme **ADRMS_SuperUtilisateurs@adatum.com**.
5. Créez un nouveau groupe de sécurité global dans le conteneur **Utilisateurs** nommé **Cadres**. Définissez l'adresse e-mail de ce groupe comme **executives@adatum.com**.
6. Ajoutez les comptes d'utilisateurs **Aidan Norman** et **Holly Spencer** au groupe **Cadres**.
7. Utilisez la console **Gestionnaire DNS** pour créer un enregistrement d'une ressource hôte (A) dans la zone **Adatum.com** avec les propriétés suivantes :
 - o Nom : **adrms**

- Adresse IP : **172.16.0.21**

► **Tâche 2 : Installer et configurer le rôle serveur AD RMS**

1. Connectez-vous à **LON-SVR1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd.**
2. À partir du **Gestionnaire de serveur**, utilisez l'**Assistant Ajouter rôles et fonctionnalités** pour ajouter le rôle **Service de gestion des droits Active Directory (AD RMS)** sur **LON-SVR1** en utilisant l'option suivante :
 - Services de rôle : **Service de gestion des droits Active Directory**
3. À partir du noeud **AD RMS** dans le **Gestionnaire de serveur**, cliquez sur **Plus** pour démarrer la configuration post-déploiement des Service de gestion des droits Active Directory (AD RMS).
4. Dans l'**Assistant de configuration d'AD RMS**, complétez les informations suivantes :
 - **Créer un nouveau cluster racine AD RMS**
 - **Utiliser la base de données interne Windows sur ce serveur**
 - Compte de service : **Adatum\ADRMSSVC**
 - Mode de chiffrement : **Cryptographic Mode 2**
 - Stockage de clé du cluster : **Utiliser un stockage de clés AD RMS géré de manière centralisée**
 - Mot de passe de la clé du cluster : **Pa55w.rd.**
 - Site Web du cluster : **Site Web par défaut**
 - Type de connexion : **Utilisation d'une connexion non chiffrée**
 - Nom de domaine complet : **http://adrms.adatum.com**
 - Port : **80**
 - Certificat du concédant : **AdatumAD RMS**
 - Enregistrer le point de connexion de service AD RMS : **Enregistrez le point de connexion de service maintenant**
5. Utilisez la console **Gestionnaire des services internet (IIS)** pour activer l'**authentification anonyme** sur les répertoires virtuels **Site Web par défaut _wmcs** et **Site Web par défaut _wmcs \ licencing**.
6. Déconnectez-vous de **LON-SVR1**.



Remarque : Vous devez vous déconnecter avant de pouvoir gérer AD RMS. Cet atelier pratique utilise le port 80 pour plus de commodité. Dans les environnements de production, vous aider à protéger les Services de gestion des droits Active Directory (AD RMS) en utilisant une connexion cryptée.

► **Tâche 3 : Configurer le groupe de super utilisateurs AD RMS.**

1. Connectez-vous à **LON-SVR1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd.**
2. À partir du **Gestionnaire de serveur**, ouvrez la console **AD RMS**, puis activez **Super Utilisateurs**.
3. Définissez le groupe **ADRMS_SuperUtilisateurs@adatum.com** en tant que groupe **Super Utilisateurs**.

Résultats : À la fin de cet exercice, vous devez avoir installé et configuré AD RMS.

Exercice 2 : Configuration des modèles AD RMS

Scénario

Après avoir déployé le serveur AD RMS, vous devez à présent configurer les modèles de stratégie de droits et les stratégies d'exclusion pour l'organisation. Vous déployerez alors les deux composants.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer un nouveau modèle de stratégie de droits ;
2. Configurer la distribution de modèle de stratégie de droits ;
3. Configurer une politique d'exclusion.

► Tâche 1 : Configurer un nouveau modèle de stratégie de droits

- Sur **LON-SVR1**, utilisez le noeud **Modèle de stratégie de droits** de la console **AD RMS** pour créer un modèle de stratégie de droits distribué avec les propriétés suivantes :
 - Langue : **Anglais (États-Unis)**
 - Nom : **LectureSeule**
 - Description : **Accès en lecture seule. Pas de copie ni d'impression.**
 - Utilisateurs et droits : **executives@adatum.com**
 - Droits pour executives@adatum.com : **Afficher**
 - **Accorder au propriétaire (auteur) un droit de contrôle total sans expiration**
 - Expiration du contenu : **7 jours**
 - Expiration de la licence d'utilisation : **7 jours**
 - **Exiger une nouvelle licence d'utilisation à chaque fois que le contenu est consommé (désactiver la mise en cache côté client)**

► Tâche 2 : Configurer la distribution de modèle relative à la stratégie des droits

1. Sur **LON-SVR1**, ouvrez une invite de commandes Windows PowerShell, saisissez les commandes suivantes puis appuyez sur Saisir après chacune :

```
New-Item c:\rmstemplates -ItemType Directory
New-SmbShare -Name RMSTEMPLATES -Path c:\rmstemplates -FullAccess ADATUM\ADRMSSVC
New-Item c:\docshare -ItemType Directory
New-SmbShare -Name docshare -Path c:\docshare -FullAccess "Tout le monde"
```

2. Dans la console **AD RMS**, définissez l'emplacement du fichier de modèles de stratégie de droits sur **\\\\LON-SVR1\\RMSTEMPLATES**.
3. Ouvrez **Explorateur de fichiers** et consultez le dossier **C:\\rmstemplates**. Vérifiez que le dossier **LectureSeule.xml (ReadOnly.xml)** est présent.

► Tâche 3 : Configurer une stratégie d'exclusion

1. Sur **LON-SVR1**, dans la console **AD RMS**, activez l'**Exclusion d'applications**.
2. Dans la boîte de dialogue **Exclure application**, saisissez les informations suivantes :
 - Nom de fichier d'application : **Powerpnt.exe**
 - Version minimale : **14.0.0.0**
 - Version maximale : **16.0.0.0**

Résultats : À la fin de cet exercice, vous devez avoir configuré les modèles AD RMS.

Exercice 3 : Utilisation de AD RMS sur les clients

Scénario

Dernière étape du déploiement : vérifier que la configuration fonctionne correctement.

Les tâches principales de cet exercice sont les suivantes :

1. Créez un document protégé par des droits
2. Vérifiez l'accès interne au contenu protégé des Services de gestion des droits Active Directory (AD RMS) en tant qu'utilisateur autorisé.
3. Ouvrez un document protégé par des droits en tant qu'utilisateur non autorisé.
4. Préparez le module suivant.

► Tâche 1 : Créer un document protégé par des droits

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Aidan** avec le mot de passe **Pa55w.rd**.
2. Depuis le menu **Démarrer**, ouvrir **Internet Explorer**, puis ajouter **http://adrms.adatum.com** aux sites intranet locaux.
3. Ouvrez **Word 2016**, puis créez un document nommé **Cadres uniquement**. Dans le document, saisissez le texte suivant : **Ce document est seulement pour les cadres et il ne devrait pas être modifié.**
4. À partir de la section **Autorisations**, choisissez de restreindre l'accès. Appliquez le modèle d'autorisation **Lectureseule** au document.
5. Enregistrez le document dans le partage **\\\lon-svr1\docpartage**. Nommez-le **Cadres uniquement.docx**.
6. Déconnectez-vous de **LON-CL1**.

► Tâche 2 : Vérifier l'accès interne au contenu AD RMS protégé en tant qu'utilisateur autorisé

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Holly** avec le mot de passe **Pa55w.rd**.
2. Depuis le menu **Démarrer**, ouvrir **Internet Explorer**, puis ajouter **http://adrms.adatum.com** aux sites intranet locaux.
3. Dans le dossier **\\\lon-svr1\docpartage**, ouvrez le document **Cadres uniquement**.
4. Vérifiez que vous ne pouvez pas modifier ou enregistrer le document.
5. Sélectionnez une ligne de texte dans le document, puis faites un clic droit dessus. Vérifiez que vous ne pouvez pas modifier ce texte.
6. Consultez les autorisations du document.
7. Déconnectez-vous de **LON-CL1**.

► Tâche 3 : Ouvrir un document protégé par des droits comme un utilisateur non autorisé

1. Connectez-vous à **LON-CL1** en tant que **Adatum\Harry** avec le mot de passe **Pa55w.rd**.
2. Depuis le menu **Démarrer**, ouvrir **Internet Explorer**, puis ajouter **http://adrms.adatum.com** aux sites intranet locaux.
3. Dans le dossier **\\\lon-svr1\docpartage**, tentez d'ouvrir le document **Cadres uniquement**.
4. Vérifiez qu'**Harry Lawrence** n'a pas l'autorisation d'ouvrir le document.

5. Déconnectez-vous de **LON-CL1**.

► **Tâche 4 : Préparer le module suivant**

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-SVR1**, **22742A-LON-DC2**, et **22742A-LON-CL1**.

Résultats : Après avoir terminé cet exercice, vous devriez avoir vérifié que le déploiement AD RMS est réussi.

Question : Quelles mesures pouvez-vous prendre pour vous assurer que vous pouvez utiliser les services IRM avec le rôle AD RMS ?

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Quels sont les avantages d'avoir un certificat SSL installé sur le serveur AD RMS lorsque vous effectuez une configuration AD RMS ?

Question : Vous devez fournir un accès au contenu protégé par AD RMS à cinq utilisateurs qui sont des entrepreneurs non affiliés et qui ne sont pas membres de votre organisation. Quelle méthode faut-il utiliser pour fournir cet accès ?

Question : Vous voulez empêcher les utilisateurs de protéger des contenus PowerPoint à l'aide de modèles AD RMS. Que devez-vous faire pour accomplir cet objectif ?

Méthode conseillée

- Avant de déployer AD RMS, vous devez analyser les besoins professionnels de votre organisation et créer les modèles nécessaires. Vous devriez vous réunir avec les utilisateurs pour les informer de la fonctionnalité AD RMS et leur demander des commentaires sur les types de modèles dont ils veulent disposer.
- Contrôler strictement la composition du groupe de super utilisateurs. Les utilisateurs de ce groupe ont un accès complet à tous les contenus protégés par AD RMS.

Module 12

Mise en œuvre de la synchronisation AD DS avec Microsoft Azure AD

Sommaire :

| | |
|--|-------|
| Vue d'ensemble du module | 12-1 |
| Leçon 1 : Planification et préparation pour la synchronisation de répertoires | 12-2 |
| Leçon 2 : Mise en œuvre de synchronisation de répertoires en utilisant Azure AD Connect | 12-13 |
| Leçon 3 : Gestion des identités avec la synchronisation de répertoires | 12-23 |
| Atelier pratique : Configuration de la synchronisation des annuaires | 12-38 |
| Contrôle des acquis et éléments à retenir | 12-44 |

Vue d'ensemble du module

Microsoft Azure Active Directory (Azure AD) est une instance en ligne des services de domaine Active Directory (AD DS). Azure AD fournit une authentification et une autorisation pour la plupart des offres de Cloud Microsoft, y compris Microsoft Azure, Microsoft Office 365 et Microsoft Intune. L'authentification par Azure AD peut se faire sur une base de cloud uniquement, ou via la synchronisation d'annuaire AD DS sur site. Vous avez également la possibilité d'activer la synchronisation des mots de passe ou d'activer l'authentification de l'utilisateur avec des comptes d'utilisateur sur site via Active Directory Federation Services (AD FS) ou d'autres fournisseurs d'authentification unique (SSO).

Dans ce module, vous allez apprendre à planifier, préparer et mettre en œuvre la synchronisation d'annuaire entre AD DS local et Azure AD. Ce module porte sur la façon de préparer un environnement local pour la synchronisation d'annuaire, de préparer et de configurer la synchronisation d'annuaire ainsi que gérer des identités après l'activation de la synchronisation d'annuaire.

Objectifs

À la fin de ce module, vous allez pouvoir d'effectuer les tâches suivantes :

- Planifier et préparer la synchronisation de répertoires ;
- Mettre en œuvre la synchronisation de répertoires en utilisant Microsoft Azure Active Directory Connect (Azure AD Connect) ;
- Gérer les identités avec la synchronisation de répertoires.

Leçon 1

Planification et préparation pour la synchronisation de répertoires

Avant d'implémenter la synchronisation d'annuaire, vous devez d'abord comprendre son fonctionnement et ses exigences. Vous devez également savoir comment préparer votre AD DS local pour la synchronisation et la configuration d'un client Azure AD pour le processus de synchronisation.

Objectifs de la leçon

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

- Décrire comment étendre le champ d'application de l'AD DS ;
- Décrire comment Azure AD fonctionne en tant que système d'authentification ;
- Décrire la synchronisation de l'annuaire ;
- Décrire comment utiliser AD FS avec Azure AD ;
- Expliquer comment planifier la virtualisation d'annuaire ;
- Décrire les conditions requises pour la synchronisation d'annuaire et expliquer comment la préparer ;
- Configurer un client pour la synchronisation d'annuaire.

Extension du champ d'application d'AD DS

AD DS présente de nombreux avantages technologiques mais également pour l'entreprise. AD DS est toutefois conçu pour des déploiements sur site, gérés de manière indépendante, des éléments qui se reflètent dans la plupart de ses caractéristiques. Ses mécanismes d'authentification et d'autorisation reposent en grande partie sur les ordinateurs ayant des membres de domaine reliés en permanence au domaine. La communication avec les contrôleurs de domaine implique des protocoles tels que le protocole LDAP pour les services de recherche dans le répertoire, le protocole Kerberos pour l'authentification et le protocole SMB pour le téléchargement de données de stratégie de groupe. Aucun de ces protocoles n'est adapté aux environnements Internet.

- La limitation d'AD DS est qu'il a à l'origine été conçu pour des déploiements sur site :
 - Client unique de par sa conception ;
 - Il emploie des protocoles qui ne sont pas adaptés à la communication Internet ;
 - Il nécessite des ordinateurs appartenant à un domaine pour offrir une fonctionnalité complète ;
- Vous pouvez installer des contrôleurs de domaine AD DS sur les machines virtuelles Azure.



Le fait de servir plusieurs organisations clientes à partir d'une seule installation est très difficile à mettre en œuvre dans un domaine unique dans l'AD DS. Même s'il est possible de fournir un niveau plus élevé d'autonomie en déployant des domaines supplémentaires au sein de la même forêt ou en déployant plusieurs forêts avec des relations d'approbation entre-elles, ces arrangements sont complexes à mettre en place et à gérer. AD DS vous permet de mettre en œuvre la combinaison souhaitée d'efficacité, de contrôle, de sécurité et de flexibilité au sein des réseaux d'entreprise. Il ne convient toutefois pas vraiment pour le monde d'aujourd'hui ouvert à internet, dominé par les services de cloud et les périphériques portables. En outre, AD DS n'est pas conçu pour fonctionner avec les applications ou les services Internet.

Extension de l'authentification AD DS

Une façon de pallier cette lacune est d'étendre les capacités d'AD DS en utilisant un système intermédiaire qui gère la traduction des constructions et des protocoles AD DS sur site (tels que les jetons et le protocole Kerberos) vers leurs équivalents pour Internet. Le rôle de serveur AD FS et la fonctionnalité serveur proxy d'application Web de Windows Server offrent cette possibilité. Par conséquent, les utilisateurs, les périphériques et les applications peuvent bénéficier des fonctionnalités d'authentification et d'autorisation AD DS sans avoir à faire partie du même domaine ou d'un domaine approuvé.

Azure AD Device Registration (précédemment connue sous le nom de Workplace Join) est un exemple d'une fonctionnalité qui est liée à l'authentification des périphériques. Celle-ci a été introduite dans le système d'exploitation Windows Server 2012 R2 et utilise AD DS, AD FS et un proxy d'application Web. Device Registration facilite l'enregistrement des périphériques qui ne sont pas associés à un domaine dans une base de données AD DS. Elle offre des avantages d'authentification et d'autorisation supplémentaires, y compris de SSO aux applications web sur site et prend en charge les stratégies de contrôle d'accès conditionnel qui détectent si une demande d'accès provient d'un périphérique enregistré.

Prise en charge de la fédération

La principale caractéristique d'AD FS et du proxy d'application Web est de prendre en charge la fédération. Une fédération ressemble à une relation d'approbation traditionnelle, mais elle repose sur des revendications (contenues dans les jetons) pour représenter les utilisateurs ou périphériques authentifiés. Elle se base sur des certificats pour établir des approbations et faciliter une communication sécurisée avec un fournisseur d'identité. En outre, elle repose sur des protocoles compatibles avec Internet tels que HTTPS, Web Services Trust Language (WS-Trust), la Fédération des services Web (WS-Federation), ou OAuth pour gérer le transport et le traitement des données d'authentification et d'autorisation. En effet, AD DS, en association avec AD FS et un proxy d'application Web, peut fonctionner comme un fournisseur de revendications capable d'authentifier les demandes de services basées sur le Web et les applications qui ne peuvent pas, ou qui ne sont pas non-autorisées à accéder directement aux contrôleurs de domaine AD DS.

Microsoft Azure

Vous pouvez également étendre AD DS dans le cloud d'une manière différente par le déploiement de contrôleurs de domaine AD DS dans des ordinateurs virtuels basés sur l'infrastructure Azure en tant que service (IaaS). Cependant, il est important de vous assurer que vous protégez ces contrôleurs de domaine contre un accès externe non autorisé. Vous pouvez utiliser ces déploiements pour construire une solution de récupération après une récupération d'urgence pour un environnement AD DS sur site existant, pour mettre en œuvre un environnement de test ou pour fournir l'authentification et l'autorisation locale aux services cloud hébergés par Azure qui font partie du même réseau virtuel.

Azure AD en tant que système d'authentification

Malgré les nombreuses similitudes entre Azure AD et AD DS, il existe également de nombreuses différences. Il est important de comprendre qu'utiliser Azure AD ne revient pas à déployer un contrôleur de domaine Active Directory sur un ordinateur virtuel Azure et à l'ajouter à votre domaine sur site. Il est important de connaître les caractéristiques suivantes de Azure AD :

- Azure AD est principalement une solution d'identité et est conçu pour les applications Internet en utilisant les communications HTTP (port 80) et HTTPS (port 443) ;

Principales différences entre Azure AD et AD DS :

- Azure AD est conçu pour les applications basées sur Internet ;
- Dans Azure AD, il n'y a pas d'unités d'organisation, ni d'objets de stratégie de groupe ;
- Il est impossible d'interroger Azure AD via LDAP ;
- Azure AD n'utilise pas l'authentification Kerberos ;
- Azure AD comprend des services de fédération.

- Les utilisateurs et les groupes Azure AD sont créés dans une structure plane et il n'y a pas d'unités d'organisation (UO) ou d'objets de stratégie de groupe (GPO) ;
- Azure AD ne peut être interrogé via LDAP mais utilise API REST sur HTTP et HTTPS ;
- Azure AD n'utilise pas l'authentification Kerberos mais les protocoles HTTP et HTTPS, tels que Security Assertion Markup Language (SAML), WS-Federation et OpenID Connect pour l'authentification (et OAuth pour l'autorisation) ;
- Azure AD comprend des services de fédération et de nombreux services tiers (tels que Facebook) qui sont fédérés avec Azure AD et l'approuvent.

Options d'authentification Azure AD

Les options d'authentification lors de l'utilisation de Azure AD se trouvent dans l'une des trois catégories principales :

- Cloud uniquement. Les identités uniquement dans Cloud sont exactement comme le nom l'indique : l'identité de l'utilisateur existe seulement dans le cloud, de sorte que toutes les gestions de mot de passe et les contrôles stratégiques se font via Azure AD. Chaque utilisateur aura deux identités totalement distinctes.
- Synchronisation d'annuaire avec synchronisation de mot de passe optionnelle Avec la synchronisation d'annuaire, vous configurez un serveur de synchronisation d'annuaire ou un système qui fournit la synchronisation uni- ou bidirectionnelle d'utilisateurs, de groupes et d'attributs d'AD DS sur site à Azure AD. Dans le cas des environnements hybrides Microsoft Exchange, certains attributs en ligne sont également synchronisés sur site. Cependant, il est important de se rappeler que même avec la synchronisation des mots de passe, il y a encore deux ensembles d'informations d'identification de sécurité. Les synchronisation d'annuaire et de mot de passe restent alignées. Les utilisateurs s'authentifient encore à Azure AD pour accéder à Microsoft Exchange Online et d'autres services en ligne.
- SSO avec AD FS. L'option SSO donne le contrôle d'authentification à votre service d'annuaire. Par conséquent, les utilisateurs ne s'authentifient plus auprès de Azure AD mais bien auprès d'AD FS. Ainsi, lorsqu'un utilisateur tape user@adatum.com dans la page de connexion d'un service de cloud tel qu'Office 365, il reçoit un message lui disant qu'il a été redirigé vers la page de connexion de son organisation. Il entre maintenant son identité sur site et s'authentifie pour les services en ligne en utilisant un jeton délégué qui vérifie que l'utilisateur a été authentifié avec succès par leur service d'annuaire sur site.

Dans la phase pilote d'un déploiement, vous utilisez des identités de cloud uniquement parce que cette option ne nécessite pas d'infrastructure sur site. Dans cette phase, vous préparez la synchronisation d'annuaire avec la synchronisation des mots de passe.

Les utilisateurs synchronisés par mot de passe peuvent se connecter aux services de Cloud Microsoft, comme Office 365, Microsoft Dynamics CRM et Intune, en utilisant le même mot de passe qu'ils utilisent lors de la connexion à leur réseau local. Le mot de passe de l'utilisateur se synchronise à Azure AD via un hachage de mot de passe et l'authentification se produit dans le Cloud.

Lorsque la fédération entre AD DS et Azure AD est déployée, les utilisateurs sont en mesure de se connecter à des services Cloud Microsoft, comme Office 365, Microsoft Dynamics CRM et Intune, en utilisant le même mot de passe qu'ils utilisent lors de la connexion à leur réseau local. Les utilisateurs sont redirigés vers leur infrastructure AD FS sur site pour l'authentification.

Aperçu de la synchronisation d'annuaire

La synchronisation d'annuaire est la synchronisation des objets d'annuaire (utilisateurs, groupes, contacts et ordinateurs) entre votre environnement AD DS sur site et l'infrastructure d'annuaire de Cloud, Azure AD.

Bien que la synchronisation d'annuaire est le plus souvent utilisée pour synchroniser les données à Azure AD, de nouvelles fonctionnalités permettent une synchronisation bidirectionnelle de répertoire Azure AD à votre AD DS local.

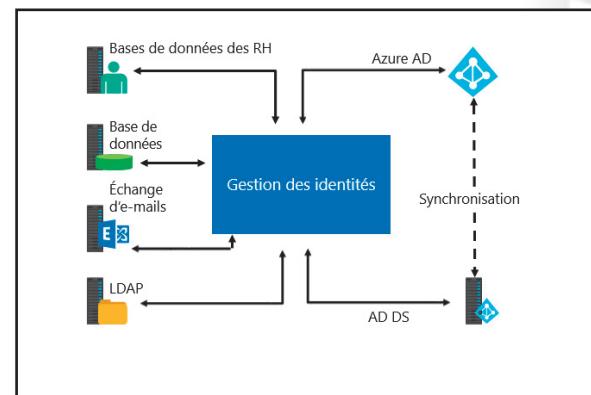
En plus des objets d'annuaire, la synchronisation d'annuaire peut également fournir une synchronisation bidirectionnelle des mots de passe utilisateur. Les outils de synchronisation d'annuaire, comme Azure AD Connect, effectuent cette synchronisation et vous les installez sur un ordinateur dédié dans votre environnement local.

L'intégration de vos répertoires locaux avec Azure AD rend vos utilisateurs plus productifs en fournissant une identité commune pour l'accès au Cloud et aux ressources locales. Grâce à cette intégration, les utilisateurs et les entreprises bénéficient des avantages suivants :

- Les organisations peuvent fournir aux utilisateurs une identité hybride commune pour les services locaux ou basés sur le cloud, y compris l'appartenance à un groupe cohérent, en utilisant l'AD DS puis en se connectant à Azure AD ;
- Les administrateurs peuvent utiliser les politiques établies par l'AD DS pour fournir un accès conditionnel basé sur les ressources d'application, le périphérique et l'identité de l'utilisateur, l'emplacement du réseau et l'authentification multifactorielle sans avoir à effectuer de tâches supplémentaires dans le cloud ;
- Les utilisateurs peuvent utiliser leur identité commune pour les comptes dans Azure AD pour accéder à Office 365, Intune, les applications SaaS et les applications qui ne sont pas de Microsoft ;
- Le personnel de support pourrait avoir moins d'appels d'assistance, parce que si les utilisateurs ont moins de mots de passe à retenir, ils sont moins susceptibles de les oublier ;
- La sécurité est plus assurée dans le sens où les identités des utilisateurs et l'information sont protégées, parce que tous les serveurs et services utilisés dans SSO sont masterisés et contrôlés sur place ;
- Pour la sécurité, une plus grande confiance peut être accordée au service du cloud quand il a la possibilité d'utiliser l'authentification forte, également appelée authentification à deux facteurs ;
- Les développeurs peuvent créer des applications qui exploitent le modèle d'identité commune.

Pour bénéficier de l'intégration de vos répertoires locaux avec Azure AD, vous devez déployer un outil de synchronisation d'annuaire. Par conséquent, l'outil de synchronisation d'annuaire fournit les fonctionnalités suivantes :

- SSO ;
- Synchronisation bidirectionnelle des mots de passe utilisateur ;
- Environnement hybride Skype pour les entreprises ;
- Environnement hybride Microsoft SharePoint Server ;
- Environnement hybride Microsoft Exchange Server, y compris :



- Une liste commune d'adresses globale (GAL) entre votre environnement local Exchange Server et Exchange Online ;
 - Une information de GAL synchronisée à partir de systèmes de messagerie différents ;
 - La possibilité d'ajouter et de supprimer des utilisateurs des services d'Office 365 nécessite une synchronisation bidirectionnelle de votre environnement AD DS sur site à l'infrastructure d'annuaire Azure AD et un déploiement hybride d'Exchange Server sur site ;
 - La possibilité de déplacer certaines ou toutes les boîtes aux lettres vers Office 365 à partir d'un serveur Exchange sur site ou vice versa ;
 - Les expéditeurs sûrs et bloqués qui sont activés sur site, se synchronisent sur Exchange Online ;
 - La possibilité d'envoyer un courriel avec une délégation de base et celle d'envoyer pour le compte de quelqu'un se synchronisent sur Exchange Online.
- La synchronisation bidirectionnelle de photos, vignettes, boîtes aux lettres de salle de conférence et des groupes de sécurité et de distribution ;
 - Le filtrage et le contrôle de la portée à des unités d'organisation individuelles.

Lorsque vous synchronisez les comptes utilisateur avec l'outil de synchronisation d'annuaire pour la première fois, ils sont marqués comme non activés. Ces utilisateurs ne peuvent pas avoir accès aux services du cloud et ils ne disposent d'aucune licence.

Planification de la synchronisation des annuaires

Lors de la planification pour la synchronisation d'annuaire, vous devez :

- Identifier les tâches de préparation de l'AD DS sur site ; par exemple, vous pouvez avoir besoin de faire des mises à jour des attributs AD DS ou des extensions de schéma ; vérifier si une mise à niveau AD DS est nécessaire pour répondre à la version des exigences minimales pour le niveau fonctionnel de la forêt ;
- Déterminer les comptes et les autorisations nécessaires à l'utilisation pendant le déploiement, la configuration et le fonctionnement de l'outil de synchronisation d'annuaire ;
- Identifier les exigences de ports réseau ;
- Identifier toutes les exigences pour l'audit après avoir activé la synchronisation ;
- Identifier tout problème de placement de contrôleur de domaine susceptible d'affecter les performances de synchronisation et de fiabilité ;
- Prévoir plusieurs scénarios de forêts ou domaines AD DS ;
- Effectuer la planification des capacités ; Par exemple, préparer des déploiements à grande échelle nécessitant des bases de données Microsoft SQL Server et des limites de quota AD Azure ;
- Prévoir la synchronisation bidirectionnelle d'annuaire ;
- Prévoir les noms de domaine non routables, tels que.LOCAL, en utilisant les suffixes du nom d'utilisateur principal (UPN) ;

Meilleures pratiques pour le déploiement de la synchronisation de répertoires :

- Avoir un plan approprié pour son projet ;
- Si le filtrage AD DS est utilisé, le configurer avant de synchroniser des objets à Azure AD ;
- Travailler avec un partenaire de services cloud ;
- Faire une planification de capacité approfondie ;
- Corriger AD DS avant de déployer la synchronisation d'annuaires ;
- Ajouter tous les domaines SMTP à la liste des domaines vérifiés avant la synchronisation.

- Prévoir le filtrage Active Directory pour affiner le champ d'application des objets AD DS pour le synchroniser à Azure AD.

Les meilleures pratiques pour le déploiement de la synchronisation de répertoire comprennent :

- Un plan de projet approprié ;
- Si le filtrage AD DS est utilisé, le configurer avant de synchroniser des objets à Azure AD ;
- Travailler avec un partenaire de services cloud ;
- Effectuer une planification approfondie de la capacité ;
- Corriger l'AD DS avant de déployer la synchronisation d'annuaire ;
- Ajouter tous les domaines du protocole SMTP comme domaines vérifiés avant la synchronisation. Vous ne pouvez pas supprimer un domaine tant que tous les objets synchronisés n'ont pas cessé d'utiliser le domaine comme adresse proxy ou UPN.

Considérations pour le déploiement de plusieurs forêts

Même si l'outil de synchronisation d'annuaire peut se synchroniser avec plusieurs forêts AD DS sur site, le déploiement sera plus complexe. Si votre organisation possède plusieurs forêts pour l'authentification (forêts d'ouverture de session) et préfère une option de déploiement plus simple, vous pouvez avoir besoin de planifier les activités suivantes :

- Evaluer la consolidation de vos forêts. En général, plus le soutien est nécessaire pour maintenir plusieurs forêts AD DS. Sauf si vous avez des contraintes de sécurité qui requièrent des forêts séparées, envisagez de simplifier votre environnement AD DS local avant de déployer l'outil de synchronisation d'annuaire ;
- Déployez la synchronisation d'annuaire pour soutenir uniquement votre forêt AD DS principale.

Synchronisation d'annuaire bidirectionnelle

Par défaut, l'outil de synchronisation d'annuaire écrit des informations d'annuaire de votre AD DS local dans votre environnement Azure AD. Lorsque vous configurez la synchronisation bidirectionnelle dans l'outil, vous activez la fonctionnalité de réécriture à l'endroit où l'outil de synchronisation d'annuaire copie un nombre limité d'attributs d'objets AD DS de l'Azure AD et les écrit dans votre AD DS local.

La synchronisation d'annuaire bidirectionnelle est nécessaire dans les scénarios où votre organisation prévoit de tirer parti des fonctionnalités avancées, telles que l'archivage Exchange Online, les expéditeurs sûrs et bloqués et la messagerie vocale Exchange. Dans la synchronisation d'annuaire bidirectionnelle, l'outil de synchronisation d'annuaire réécrira les attributs de l'objet AD DS requis depuis Azure AD sur votre AD DS local.



Lectures supplémentaires : Pour plus d'informations, consultez : « Guide des Considérations relatives à la conception d'identités hybrides Azure » à l'adresse : <http://aka.ms/ibuqek>

Prérequis et préparation à la synchronisation d'annuaire

Après avoir terminé un plan pour la synchronisation d'annuaire, vous aurez besoin d'examiner les conditions préalables. Ces tâches vous permettront de préparer l'environnement pour la synchronisation d'annuaire :

- Planifier la capacité de votre serveur de base de données de synchronisation d'annuaire ;
- Identifier les besoins en matériel pour votre ordinateur de synchronisation d'annuaire ;
- Déterminer si votre environnement dépasse le quota d'objet AD Azure ;
- Passer en revue les ports réseau requis par la synchronisation d'annuaire.

Lors de l'examen des prérequis à la synchronisation de répertoires, vos tâches sont les suivantes :

- Planification de capacité du serveur de base de données de synchronisation d'annuaires ;
- Identification des spécifications matérielles pour l'ordinateur de synchronisation d'annuaires ;
- Déterminer si votre environnement dépasse le quota d'objets Azure AD ;
- Révision des ports réseau requis pour la synchronisation d'annuaires ;
- Déterminer si des extensions de schéma pour AD DS sont nécessaires.

Planification de capacité

La synchronisation d'annuaire est un outil essentiel pour l'intégration avec vos offres de services du cloud ; vous devez donc planifier en conséquence afin de la mettre en œuvre. Dans la plupart des organisations, les objets utilisateur d'AD DS constituent la majeure partie de la charge utile de synchronisation d'annuaire et influencent à la fois le temps de synchronisation et le dimensionnement de votre infrastructure.

L'outil de synchronisation d'annuaire dépend fortement de la base de données, de sorte que vous allez devoir planifier les besoins de capacité de base de données. Si votre forêt AD DS possède moins de 50 000 objets, alors la base de données interne de Windows par défaut (IFD) doit suffire. Toutefois, si votre environnement a plus de 50 000 objets, alors une version complète de SQL Server est nécessaire. La plupart des outils de synchronisation d'annuaire prennent en charge des forêts de 600 000 objets ou plus.

Configuration matérielle requise.

Les déploiements de plus de 50 000 objets dans AD DS requièrent une augmentation significative des besoins en mémoire (de 4 gigaoctets [Go] de mémoire à accès aléatoire [RAM] à 16 Go) ; par conséquent, il est important de mettre en œuvre des ressources matérielles suffisantes lors du passage du pilote à la phase de production.

| Nombre d'objets dans AD DS | Unité de traitement centrale (UC) | Mémoire | Disque dur |
|----------------------------|-----------------------------------|---------|------------|
| Moins de 10 000 | 1,6 gigahertz (GHz) | 4 Go | 70 Go |
| 10 000–50 000 | 1,6 GHz | 4 Go | 70 Go |
| 50 000–100 000 | 1,6 GHz | 16 Go | 100 Go |
| 100 000–300 000 | 1,6 GHz | 32 Go | 300 Go |
| 300 000–600 000 | 1,6 GHz | 32 Go | 4 500 Go |
| Plus de 600 000 | 1,6 GHz | 32 Go | 5 000 Go |

Quota d'objet AD Azure

Par défaut, Azure AD permettra 50 000 objets (utilisateurs, contacts de messagerie et groupes). Le quota de l'objet augmente automatiquement à 300 000 après la vérification du premier domaine. Si le quota d'objet est dépassé lors de la synchronisation d'annuaire, l'administrateur du locataire recevra le message suivant :

Le traitement par lots de synchronisation d'annuaire a été achevé le <date/heure> pour le locataire <nom>.

Les erreurs suivantes sont survenues lors de la synchronisation :

- La synchronisation a été arrêtée. L'entreprise a dépassé le nombre d'objets pouvant être synchronisés. Contactez le support technique et demandez une augmentation du quota de votre entreprise.

Si vous avez un besoin de synchroniser plus de 300 000 objets, vous devez contacter le support technique Microsoft pour demander une extension de la limite du quota d'objet. Si vous devez synchroniser plus de 500 000 objets, vous aurez besoin d'une licence telle qu'Office 365, Azure AD Basic, Microsoft Azure AD Premium, ou Enterprise Mobility Suite. Au cours de la phase de planification, il est important de planifier de manière appropriée toutes les demandes d'augmentation de quota. Si cette tâche est effectuée à la dernière minute, cela peut entraîner le blocage du déploiement.



Lectures supplémentaires : Pour plus d'informations, reportez-vous à Vous recevez un message d'erreur dans un rapport de synchronisation d'annuaire « Cette entreprise a dépassé le nombre d'objets pouvant être synchronisés » à l'adresse : <http://aka.ms/r4x1q4>

Ports réseau

Le trafic réseau pour la synchronisation d'annuaire entre l'outil de synchronisation d'annuaire et Azure AD est sur un Secure Socket Layer (SSL). La plupart du trafic est sortant. Il est initié par l'ordinateur de synchronisation d'annuaire et utilise le port 443. L'écriture différée des mots de passe utilise un relais Microsoft Azure Service Bus comme un canal de communication sous-jacent, ce qui signifie que vous n'avez pas à ouvrir de nouveaux ports sur votre pare-feu pour que cette fonctionnalité fonctionne.

Le trafic réseau entre l'ordinateur de synchronisation d'annuaire et AD DS local utilise les ports standards liés à Active Directory. Pour la synchronisation d'annuaire sans interruption, l'ordinateur de synchronisation d'annuaire doit être capable de communiquer avec tous les contrôleurs de domaine dans la forêt.

Autorisations d'AD DS

Lorsque vous préparez le déploiement de la synchronisation d'annuaire, votre plan de projet doit inclure la préparation AD DS ainsi que les exigences et les fonctionnalités de Azure AD. Pour préparer AD DS :

- Identifier la source de l'autorité ;
- Répondre aux exigences de contrôleur de domaine ;
- Nettoyer AD DS en supprimant des objets anciens ou inutiles ;
- Mettre en place l'audit.

Source de l'autorité

Pour la synchronisation d'annuaire, la source de l'autorité se réfère à l'emplacement où les objets de service Active Directory, tels que les utilisateurs et les groupes, sont maîtrisés (une source originale qui définit des copies d'un objet) dans un déploiement inter-site. Vous pouvez modifier la source de l'autorité d'un objet en utilisant l'un de ces scénarios : activer, désactiver ou réactiver la synchronisation d'annuaire à partir du portail classique Azure ou avec Windows PowerShell.

Exigences du contrôleur de domaine

La forêt locale AD DS doit répondre à des exigences spécifiques pour le maître de schéma, les serveurs de catalogue global et les contrôleurs de domaine. Il est important de lire attentivement les exigences les plus récentes et de vous assurer que vos serveurs locaux AD DS répondent à ces exigences.

Nettoyage AD DS

Si vous effectuez la synchronisation d'annuaire pour utiliser Office 365, vous devez préparer votre forêt AD DS avant de commencer le déploiement de synchronisation d'annuaire Office 365. Vos efforts d'assainissement d'annuaire doivent se concentrer sur les tâches suivantes :

- Supprimer les doublons **proxyAddresses** et les attributs **Nom principal utilisateur** ;
- Mettre à jour les attributs blancs et invalides **Nom principal utilisateur** en les remplaçant par des attributs valides **Nom principal utilisateur** ;
- Supprimer des caractères non valides et douteux dans le **prénom, nom (sn), sAMAccountName, Afficher un nom, courrier, proxyAddresses, mailNicknameet userPrincipalName** les attributs.

Auditer AD DS

Vous pouvez utiliser l'audit AD DS pour capturer et évaluer les événements qui sont associés à la synchronisation d'annuaire, tels que la création de l'utilisateur, la réinitialisation du mot de passe, l'ajout d'utilisateurs à des groupes et ainsi de suite. Lorsque vous implémentez la synchronisation d'annuaire, l'audit capture les journaux de services d'annuaire des contrôleurs de domaine AD DS. La connexion sécurisée peut être désactivée par défaut, donc vous devez l'activer pour que les événements apparaissent dans les journaux.

Configuration d'un locataire pour la synchronisation d'annuaire

Avant d'utiliser la synchronisation d'annuaire pour lancer la synchronisation, vous devez d'abord activer la synchronisation Active Directory dans votre locataire AD Azure. Ce processus peut prendre un certain temps, il est donc important de prévoir cette exigence avant le déploiement de la synchronisation d'annuaire. Vous pouvez activer la synchronisation Active Directory dans le portail classique Azure ou en utilisant Windows PowerShell.

Pour activer la synchronisation Active Directory dans le portail classique, procédez comme suit :

1. Dans le volet de navigation de gauche, cliquez sur **TOUS LES ARTICLES**, puis sur votre instance Azure AD.
2. Dans la barre d'outils, cliquez sur **INTÉGRATION ANNUAIRE**.
3. Sous **Intégration avec le répertoire local actif**, cliquez sur **Activer**.

Pour activer la synchronisation Active Directory en utilisant le portail Azure :

1. Dans le volet de navigation de gauche, cliquez sur **TOUS LES ARTICLES**, puis cliquez sur votre instance Azure AD.
2. Dans la barre d'outils, cliquez sur **INTÉGRATION ANNUAIRE**.
3. Sous **Intégration avec le répertoire local actif**, cliquez sur **Activer**.



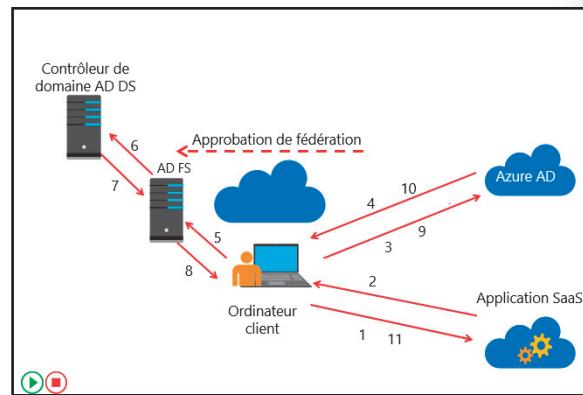
Remarque : Au moment de la rédaction de ce cours, l'option pour activer la synchronisation d'annuaire n'était pas disponible dans le nouveau portail Azure.

Pour activer la synchronisation Active Directory en utilisant le module Active Directory Microsoft Azure pour Windows PowerShell, tapez la commande suivante et appuyez sur Entrée :

```
Set-MsolsDirSyncEnabled -EnableDirSync $ true -Force
```

AD FS et Azure AD

Alors que les organisations déplacent des services et des applications vers des services basés sur le cloud, il est de plus en plus important qu'elles familiarisent les utilisateurs avec les procédés d'authentification et d'autorisation. Les services du cloud ajoutent un autre niveau de complexité à l'environnement informatique, car ils se trouvent en dehors du contrôle administratif direct des administrateurs informatiques et ils peuvent fonctionner sur de nombreuses plates-formes différentes.



Vous pouvez utiliser AD FS pour fournir une expérience d'authentification unique (SSO) aux utilisateurs à travers diverses plates-formes disponibles basées sur le cloud. Par exemple, après que les utilisateurs se sont authentifiés avec les informations d'identification AD DS, ils peuvent accéder à des services Azure tels que des sites Web, des services sur le cloud ou des services Microsoft Online qui reposent sur l'authentification AD Azure, comme Exchange Online ou Microsoft SharePoint Online et les applications SaaS intégrées à AD Azure. Cette fonctionnalité requiert l'utilisation des outils de synchronisation d'annuaire pour synchroniser les informations de compte d'utilisateur depuis le déploiement local vers le locataire AD Azure correspondant.

Les étapes suivantes décrivent le processus de connexion à une application SaaS basée sur un navigateur qui est intégré à AD Azure en utilisant AD FS. Les étapes décrivent ce qui se passe lorsqu'un utilisateur tente d'accéder à une application SaaS basée sur Azure en utilisant un navigateur Web :

1. L'utilisateur ouvre un navigateur Web et envoie une demande HTTPS à l'application SaaS.
2. L'application SaaS détermine que l'utilisateur appartient à une instance intégrée AD Azure. Le fournisseur d'applications SaaS redirige l'utilisateur vers l'instance Azure AD de l'utilisateur.
3. Le navigateur de l'utilisateur envoie une demande d'authentification HTTPS à l'instance Azure AD.
4. Si le compte Azure AD de l'utilisateur représente une identité fédérée, le navigateur de l'utilisateur est redirigé à nouveau sur le serveur de fédération local.
5. Le navigateur de l'utilisateur envoie d'une demande HTTPS au serveur de fédération local.
6. Si l'utilisateur est connecté au domaine AD DS local, le serveur de fédération demandera automatiquement l'authentification AD DS basée sur le ticket existant Kerberos de l'utilisateur. Sinon, l'utilisateur reçoit une invite pour une authentification avec AD DS local.
7. Le contrôleur de domaine AD DS authentifie l'utilisateur, puis renvoie le message d'authentification réussie au serveur de fédération.
8. Le serveur de fédération crée la revendication de l'utilisateur en se basant sur des règles définies dans le cadre de la configuration Active Directory Federation Services (AD FS). Le serveur de fédération place les données de revendication dans un jeton de sécurité connecté numériquement et le transmet au navigateur de l'utilisateur.
9. Le navigateur de l'utilisateur transmet le jeton de sécurité contenant les revendications à Azure AD.
10. Azure AD vérifie la validité du jeton de sécurité AD FS en se basant sur l'approbation de la fédération existante. Il crée un nouveau jeton afin d'accéder à l'application SaaS puis l'envoie au navigateur de l'utilisateur.
11. L'utilisateur utilise le jeton émis par Azure AD pour accéder à l'application SaaS.

Question : Vérifiez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|--|---------|
| Lorsque vous appliquez la synchronisation d'annuaire, des comptes et des groupes d'utilisateurs se déplacent depuis votre AD DS vers Azure AD. | |

Leçon 2

Mise en œuvre de synchronisation de répertoires en utilisant Azure AD Connect

Pour mettre en œuvre la synchronisation d'annuaire, vous devez utiliser les outils appropriés. Microsoft fournit Azure AD Connect en tant qu'outil dédié à l'établissement de la connexion et de la synchronisation entre votre AD DS et Azure AD locaux. Dans cette leçon, vous allez apprendre à déployer Azure AD Connect. Cette leçon comprend un examen des exigences d'installation Azure AD Connect et les options pour l'installation et la configuration de l'outil. Vous allez également examiner le suivi d'Azure AD Connect.

Objectifs de la leçon

À la fin de cette leçon, vous allez pouvoir effectuer les tâches suivantes :

- Expliquer le but et les utilisations d'Azure AD Connect ;
- Décrire les exigences Azure AD Connect ;
- Décrire comment la synchronisation expresse d'Azure AD Connect fonctionne ;
- Décrire comment la synchronisation personnalisée d'Azure AD Connect fonctionne ;
- Décrire comment installer et configurer Azure AD Connect ;
- Décrire les fonctionnalités de contrôle d'Azure AD Connect ;
- Décrire la gestion privilégiée des identités Azure AD.

Vue d'ensemble d'Azure AD Connect

L'outil Azure AD Connect, autrefois connu sous le nom de Windows Azure

Synchronisation Active Directory ou DirSync, est l'outil de synchronisation d'annuaire le plus récent pris en charge par Microsoft. Azure AD Connect est conçu pour fonctionner comme un appareil « place et oublie » basé sur un logiciel. Le but de cet outil est de permettre la coexistence entre votre environnement local Active Directory et des services basés sur le Cloud tels que Office 365 ou Microsoft Intune. Lorsque vous utilisez Azure AD Connect pour la synchronisation d'annuaire :

- Les objets nouvel utilisateur, groupe et contact de l'AD DS local sont ajoutés à AD Azure.
- Les attributs des objets utilisateur, groupe ou contact existants qui sont modifiés dans l'AD DS local sont modifiés dans AD Azure ; cependant, tous les attributs de l'AD DS local ne sont pas synchronisés sur Azure AD.
- Les objets utilisateur, groupe et contact existants qui sont supprimés de l'AD DS local sont supprimés d'Azure AD.
- Les objets utilisateur existants qui sont désactivés dans l'AD DS local sont désactivés dans Azure AD.

Lorsque vous utilisez Azure AD Connect pour la synchronisation de répertoires :

- Les nouveaux utilisateurs, groupes et objets contacts dans les AD DS locaux sont ajoutés à Azure AD ;
- Les attributs d'utilisateur, groupe ou objets contacts existants qui sont modifiés dans AD DS local sont modifiés dans Azure AD ;
- Les utilisateurs, groupes ou objets contacts existants qui sont supprimés d'AD DS local sont supprimés dans Azure AD ;
- Les objets utilisateurs existants qui sont désactivés sur site sont désactivés dans Azure AD.

Dans un déploiement de cloud uniquement, tous les objets Azure AD sont créés à l'origine (maîtrisés) dans le nuage et doivent être modifiés en utilisant des outils basés sur le Cloud (en utilisant le portail classique Azure, ou en utilisant des applets de commande Windows PowerShell). Dans ce scénario, Azure AD est appelé une source d'autorité pour tous les objets Active Directory.

Azure AD n'a besoin que d'une seule source d'autorité pour chaque objet. Il est donc essentiel de bien comprendre que dans le scénario où vous avez déployé Azure AD Connect pour la synchronisation Active Directory, vous maîtrisez les objets depuis votre AD DS local en utilisant des outils tels qu'utilisateurs et ordinateurs Active Directory ou Windows PowerShell—La source d'autorité est l'AD DS local. À la fin du premier cycle de synchronisation, la source d'autorité est transférée à partir du nuage vers l'AD DS local. Toutes les modifications ultérieures d'objets du nuage (sauf pour les licences) sont maîtrisées à partir des outils AD DS local. Les objets du nuage correspondant sont en lecture seule et les administrateurs Azure AD ne peuvent pas modifier les objets de nuage si la source d'autorité est l'AD DS local.

Exigences Azure AD Connect

Azure AD Connect est le successeur de DirSync, Azure AD Sync et Microsoft Forefront Identity Manager avec le connecteur AD Azure. Il est pré-configuré pour la synchronisation d'objets utilisateur, groupe, contact et informatique depuis votre AD DS local vers Azure AD.

Exigences Azure AD

Pour utiliser Azure AD Connect, vous devez tenir compte des exigences suivantes d'Azure AD :

- Un abonnement Azure ou un abonnement d'essai Azure. Ceci est uniquement nécessaire pour accéder au portail classique Azure et non pour l'utilisation d'Azure AD Connect. Si vous utilisez Windows PowerShell ou Office 365, vous n'avez pas besoin d'un abonnement Azure pour utiliser Azure AD Connect. Si vous avez une licence Office 365, vous pouvez utiliser le portail Office 365 à partir duquel vous pouvez accéder au portail classique Azure.
- Ajoutez et vérifiez le domaine que vous envisagez d'utiliser dans Azure AD. Par exemple, si vous prévoyez d'utiliser Adatum.com pour vos utilisateurs, vous devrez vous assurer que le nom du domaine a été vérifié dans Azure AD et qu'il est possible de lui affecter des utilisateurs.
- Un répertoire Azure AD permet, par défaut, 50 000 objets. Comme indiqué précédemment dans le module, lorsque vous vérifiez votre domaine, la limite passe à 300 000 objets. Si vous avez besoin de plus d'objets dans Azure AD, vous devez ouvrir un cas d'assistance pour augmenter la limite. Si vous avez besoin de plus de 500 000 objets, vous avez besoin d'une licence telle qu'Office 365, Azure AD Basic, Azure AD Premium, ou Enterprise Mobility Suite.

Lorsque vous identifiez les exigences Azure AD Connect, il vous faut vérifier :

- Exigences Azure AD
- Exigences de domaine et de forêt
- Exigences de système d'exploitation et du logiciel de prise en charge
- Autorisations et comptes
- Exigences de base de données

Exigences de domaine et de forêt

Azure AD Connect requiert Windows Server 2003 ou sa version ultérieure comme version du schéma Active Directory et niveau fonctionnel de la forêt. Azure AD Connect prend en charge une seule forêt AD DS avec des paramètres express et prend en charge plusieurs scénarios forestiers AD DS et plusieurs organisations Exchange avec des paramètres personnalisés.



Remarque : Utiliser Azure AD Connect pour Identity Manager Forefront 2010 R2, utiliser Azure AD Connect avec un service d'annuaire non Microsoft et installer Azure AD Connect sur un ordinateur non Windows ne sont pas traités dans ce cours.

Pour s'intégrer à Azure AD Connect, les contrôleurs de domaine Active Directory doivent exécuter l'un des systèmes d'exploitation suivants :

- Windows Server 2003 édition standard ou Windows Server 2003 édition d'entreprise avec Service Pack 1 (SP1) ou version ultérieure.
- Si vous prévoyez d'utiliser la fonction écriture différée du mot de passe, les contrôleurs de domaine Active Directory doivent être sur Windows Server 2008 ou version ultérieure.

Lorsque vous installez Azure AD Connect avec les paramètres express, l'ordinateur de synchronisation d'annuaire doit être membre d'un domaine et pour les scénarios de forêt unique, vous devez relier cet ordinateur à un domaine dans la même forêt qui sera synchronisée. Par contre, avec des paramètres personnalisés, vous pouvez installer Azure AD Connect sur un ordinateur qui n'est pas relié à un domaine. Azure AD Connect prend également en charge l'installation sur les contrôleurs de domaine. Toutefois, pour les scénarios de production, nous vous recommandons d'utiliser un serveur membre pour Azure AD Connect.

Lors de l'installation d'Azure AD Connect, vous devez sélectionner un attribut AD DS pour l'ancre source. Cet attribut, aussi appelé **sourceAnchor**, doit être un attribut immuable au cours de la durée de vie d'un objet utilisateur, car il est le lien entre l'AD DS local et Azure AD. Dans la plupart des scénarios, il s'agit de **objectGUID**. Cet attribut ne changera pas sauf si vous déplacez le compte d'utilisateur entre les forêts / domaines.

Cependant, dans un scénario de forêts multiples où vous déplacez des comptes d'utilisateurs entre les forêts, un autre attribut doit être utilisé, tel **employeeID**.

 **Remarque :** Les attributs à éviter sont ceux qui changeront si une personne se marie ou modifie les affectations. D'autres attributs qui ne peuvent pas être utilisés comprennent les attributs avec un signe (@). Par conséquent, les adresses e-mail et le **NomPrincipalutilisateur** ne peuvent pas être utilisés.

Exigences de système d'exploitation et du logiciel de prise en charge

Azure AD Connect nécessite les versions suivantes du système d'exploitation Windows Server (édition 64 bits uniquement) :

- Windows Server 2008, ou une version ultérieure.
- Windows Server 2012, ou une version ultérieure.
- Si vous prévoyez d'utiliser la fonctionnalité de synchronisation des mots de passe, le serveur doit être sur Windows Server 2008 R2 SP1 ou version ultérieure.

En outre, Azure AD Connect nécessite les conditions logicielles suivantes :

- Microsoft.NET Framework ou version ultérieure
- Windows PowerShell 3.0 ou version ultérieure
- Microsoft Azure Module AD pour Windows PowerShell (version 64 bits)

Autorisations et comptes

Pour installer et configurer Azure AD Connect, vous avez besoin des comptes suivants :

- Un compte administrateur Azure AD Global pour l'annuaire Azure AD avec lequel vous souhaitez vous intégrer.
- Un compte administrateur d'entreprise pour vos AD DS locaux si vous utilisez des paramètres express ou la mise à niveau à partir de l'outil de synchronisation Microsoft Azure Active Directory (DirSync).

Azure AD Connect utilise le compte administrateur mondial Azure AD pour fournir et mettre à jour des objets dans le locataire Azure AD lorsque vous lancez la synchronisation d'annuaire. Si vous créez un compte de service dédié dans Azure AD pour la synchronisation d'annuaire à la place du compte

d'administrateur locataire Azure AD, il est important de désactiver la valeur par défaut de l'expiration du mot de passe dans 90 jours ; sinon, le service de synchronisation cessera de fonctionner lorsque le mot de passe expirera pour le compte administrateur locataire Azure AD. Dans ce scénario, vous devrez reconfigurer Azure AD Connect pour mettre à jour le mot de passe.

Pour désactiver l'expiration du mot de passe pour le compte de service dans Azure AD en utilisant le module Azure AD pour Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
Set-MsolUser -UserPrincipalName <service account>@<domain>.onmicrosoft.com -  
PasswordNeverExpires $true
```

Le compte utilisé pour installer et configurer Azure AD Connect doit avoir les autorisations suivantes :

- Autorisation de l'administrateur d'entreprise dans votre AD DS local. Cela est nécessaire pour créer le compte de service de synchronisation d'annuaire dans AD DS.
- Autorisation d'administrateur local sur l'ordinateur Azure AD Connect. Cela est nécessaire pour installer l'outil Azure AD Connect.

Le compte utilisé pour configurer Azure AD Connect et exécuter l'assistant de configuration doit résider dans le groupe local **ADSyncAdmins** sur l'ordinateur Azure AD Connect. Par défaut, le compte utilisé pour installer Azure AD Connect (le compte administrateur d'entreprise) est automatiquement ajouté à ce groupe lors de l'installation.

Le compte administrateur d'entreprise est uniquement requis lors de l'installation et de la configuration d'Azure AD Connect et les informations d'identification de l'administrateur d'entreprise ne sont pas stockées ou enregistrées par l'assistant de configuration.

Le compte administrateur d'entreprise est nécessaire pour :

- Créer le MSOL_<*id*> Compte de service de domaine dans le **CN = Utilisateurs** conteneur du domaine racine ;
- Déléguer les autorisations suivantes à MSOL_<*id*> sur chaque partition de domaine dans la forêt :
 - Réplication des changements d'annuaire ;
 - Réplication de tous les changements d'annuaire ;
 - Synchronisation de réplication.



Remarque : Parce que cela pose un risque de sécurité avec le compte de service qu'il utilise, Azure AD Connect ne prend pas en charge l'utilisation d'un groupe de comptes de services gérés pour se connecter à vos environnements locaux AD DS. Par défaut, Azure AD Connect crée des comptes de services avec un minimum de priviléges, mais avec des mots de passe qui n'expirent pas sur l'ordinateur qui exécute Azure AD Connect et à la fois dans l'AD DS local et le locataire Azure AD.

Lors d'une configuration Azure AD Connect, vous pouvez activer la fonctionnalité de déploiement hybride Exchange. Auparavant connue sous le nom *rich coexistence*, cette fonction permet la coexistence des boîtes aux lettres Exchange à la fois locales et dans Azure en synchronisant un ensemble spécifique d'attributs depuis Azure AD vers votre AD DS local. Au cours du déploiement, le compte administrateur d'entreprise va automatiquement créer un groupe **MSOL_Active Directory_Sync_RichCoexistence** dans le conteneur du domaine racine **CN=Utilisateurs**. En outre, le compte administrateur d'entreprise déléguera des autorisations d'écriture pour des attributs AD DS particuliers qui écrivent depuis Azure AD vers votre AD DS local.

Les comptes suivants sont créés dans votre AD DS local lors de la configuration Azure AD Connect :

- MSOL_<id>. Ce compte est créé lors de l'installation d'Azure AD Connect. Il est configuré pour se synchroniser avec Azure AD. Le compte dispose des autorisations de réPLICATION d'annuaire dans votre AD DS local et des autorisations d'éCRIPTION sur certains attributs afin de permettre le déploiement hybride Exchange.
- AAD_<id>. Ceci est le compte de service pour le moteur de synchronisation. Il est créé avec un mot de passe complexe généré automatiquement de façon aléatoire et configuré pour ne jamais expirer. Lorsque le service de synchronisation d'annuaire est en cours d'exécution, il utilise les informations d'identification du compte de service pour lire depuis votre AD DS local, puis pour écrire le contenu de la base de données de synchronisation vers Azure AD en utilisant les informations d'identification de l'administrateur locataire Azure AD renseignées lors de la configuration d'Azure AD Connect.

 **Remarque :** Ne modifiez pas ce compte de service après l'installation d'Azure AD Connect, car la synchronisation d'annuaire va tenter d'utiliser le compte de service créé lors de l'installation. Si le compte est modifié, la synchronisation d'annuaire cessera de fonctionner et les synchronisations d'annuaire programmées n'auront pas lieu.

Exigences de base de données

Azure AD Connect requiert une base de données SQL Server pour stocker des données d'identité. Par défaut, SQL Server 2012 express LocalDB (une version allégée de SQL Server Express 2012 SP1) est installé et le compte de service pour le service est créé sur l'ordinateur local. SQL Server Express a une limite de base de données de 10 Go, ce qui vous permet de gérer environ 100 000 objets. Lors de déploiements massifs, vous pourriez avoir à gérer un plus grand volume d'objets. Dans ce scénario, configurez Azure AD Connect sur une version complète de SQL Server. Azure AD Connect prend en charge toutes les versions de SQL Server, depuis Microsoft SQL Server 2008 (avec SP4 ou version ultérieure) jusqu'à Microsoft SQL Server 2014.

Lorsque vous déployez sur une autre version de SQLServer, les droits de SQL Server sont requis pour créer la base de données utilisée par Azure AD Connect et pour activer le compte de service de SQL Server avec le rôle de **db_propriétaire**. Pour ce faire, assurez-vous que le compte utilisé pour installer Azure AD Connect a l'autorisation sysadmin pour la base de données SQL Server et que le compte de service utilisé pour exécuter Azure AD Connect a l'autorisation publique pour la base de données utilisée par Azure AD Connect.

Synchronisation expresse Azure AD Connect

Lors de l'installation d'Azure AD Connect, vous pouvez choisir les paramètres express. Ceci est l'option par défaut et l'un des scénarios les plus courants. Lorsque vous faites cela, Azure AD Connect déploie la synchronisation avec l'option de synchronisation des mots de passe. Ceci est valable pour une seule forêt et permet à vos utilisateurs d'utiliser leurs mots de passe locaux pour se connecter aux services du cloud basés sur Azure AD. Il est conseillé d'utiliser un modèle.

Lors de l'installation d'Azure AD Connect avec les paramètres express, le programme d'installation :

- Installe le moteur de synchronisation ;
- Configure le connecteur AD DS sur site ;
- Active la synchronisation du mot de passe ;

• Les scénarios pour l'utilisation des paramètres de configuration rapide comprennent :

- Vous avez une forêt AD DS unique ;
- Les utilisateurs se connectent avec un mot de passe identique en utilisant la synchronisation des mots de passe.

• L'installation d'Azure AD Connect avec les paramètres de configuration rapide :

- Installe le moteur de synchronisation ;
- Configure Azure AD Connector ;
- Configure le connecteur AD DS sur site ;
- Active la synchronisation de mot de passe ;
- Configure les services de synchronisation ;
- Configure les services de synchronisation pour le déploiement Exchange hybride (facultatif) ;
- Active les mises à jour automatiques pour Azure AD Connect.

- Configure les services de synchronisation ;
- Configure les services de synchronisation pour le déploiement hybride Exchange (facultatif) ;
- Active la mise à jour automatique de Azure AD Connect ;

Lorsque vous utilisez les paramètres express, la synchronisation commence automatiquement lorsque l'installation est terminée (bien que vous puissiez choisir de ne pas le faire).

Synchronisation personnalisée Azure AD Connect

Une alternative à l'option de paramètres express est l'installation d'Azure AD Connect avec des paramètres personnalisés. Cette option est utile si vous avez des options de configuration supplémentaires ou que vous avez besoin de fonctionnalités facultatives qui ne figurent pas dans l'installation express. Vous pouvez sélectionner les paramètres personnalisés pour les scénarios suivants :

- Lorsque vous avez plusieurs forêts ;
- Lorsque vous personnalisez votre option de connexion, tel que AD FS pour la fédération, ou utilisez un fournisseur d'identité non-Microsoft ;
- Lorsque vous personnalisez les fonctionnalités de synchronisation, telles que le filtrage et l'écriture différée.

Vous pouvez sélectionner les paramètres personnalisés pour les scénarios suivants :

- Quand vous avez plusieurs forêts ;
- Quand vous personnalisez votre option de connexion, comme AD FS pour la fédération, ou que vous utilisez un fournisseur d'identité qui n'est pas Microsoft ;
- Quand vous personnalisez les fonctions de synchronisation telles que le filtrage et l'écriture différée.

Outre les composants nécessaires qui sont installés comme faisant partie des paramètres express, vous pouvez sélectionner les composants facultatifs suivants lors de l'installation :

- Spécifier un emplacement d'installation personnalisé. Ce composant facultatif vous permet de spécifier un autre emplacement pour l'installation d'Azure AD Connect.
- Utiliser un serveur existant qui exécute SQL Server. Ce composant facultatif vous permet de sélectionner un serveur de base de données existant.
- Utiliser un compte de service existant. Ce composant facultatif vous permet de spécifier un compte de service existant. Par défaut, Azure AD Connect crée un compte de service local pour les services de synchronisation à utiliser. Le mot de passe est généré automatiquement et n'est pas connu de la personne installant Azure AD Connect. Si vous spécifiez un serveur à distance exécutant SQL Server, alors vous avez besoin d'un compte de service avec un mot de passe que vous connaissez.
- Spécifier des groupes de synchronisation personnalisés. Ce composant facultatif vous permet de spécifier des groupes de gestion existants pour Azure AD Connect. Par défaut, Azure AD Connect va créer quatre groupes sur le serveur lors de l'installation des services de synchronisation. Ces groupes comprennent le groupe Administrateurs, le groupe Opérateurs, le groupe de navigation et le groupe de réinitialisation de mot de passe. Utilisez cette option si vous préférez spécifier vos propres groupes. Les groupes doivent être sur le serveur et ne peuvent pas se trouver dans le domaine.

Lors de l'installation d'Azure AD Connect avec des paramètres personnalisés, le programme d'installation vous permet d'activer les fonctionnalités suivantes :

- Sélectionner la méthode d'authentification unique (SSO). Cette fonctionnalité vous permet de spécifier la méthode d'authentification unique pour les utilisateurs. Les méthodes d'authentification unique comprennent la **synchronisation des mots de passe**, la **fédération avec AD FS** et la **non-configuration**.

- Connecter des répertoires multiples sur site ou des forêts. Cette fonctionnalité vous permet de vous connecter à un ou plusieurs domaines ou forêts AD DS.
- Appariement des forêts. Cette fonctionnalité vous permet de définir la façon dont Azure AD représente les utilisateurs à partir de vos forêts AD DS. Un utilisateur peut soit n'être représenté qu'une seule fois dans toutes les forêts ou avoir à la fois des comptes activés et désactivés.
- Filtrage de la synchronisation basé sur des unités d'organisation. Cette fonctionnalité vous permet d'exécuter un petit pilote où seul un petit sous-ensemble d'objets est créé dans AD Azure. Pour utiliser cette fonctionnalité, créez une unité d'organisation dans votre système de domaine AD DS, puis ajoutez les utilisateurs et les groupes qui doivent se synchroniser avec AD Azure à l'unité d'organisation. Vous pouvez ensuite ajouter ou supprimer des utilisateurs de ce groupe pour maintenir la liste des objets qui doivent être présents dans Azure AD.
- Sélectionner l'ancre Source. Cette fonctionnalité vous permet de choisir la clé primaire qui permettra de relier l'utilisateur local avec l'utilisateur dans Azure AD.
- Sélectionner l'attribut de connexion. Cette fonctionnalité vous permet de choisir les attributs que les utilisateurs utilisent lorsqu'ils se connectent aux services Azure AD et aux services du cloud tels que Office 365. En règle générale, cela devrait être l'attribut **Nomutilisateurprincipal**. Toutefois, si cet attribut est non-routable et ne peut pas être vérifié, alors il est possible de sélectionner un autre attribut, par exemple de messagerie électronique, comme l'attribut contenant l'identifiant de connexion, connu sous le nom d'**ID secondaire**.

 **Lectures supplémentaires :** Pour plus d'informations, consultez : « Configuration d'ID de connexion secondaire » sur : <http://aka.ms/nqh5gc>

- Déploiement hybride Exchange. Cette fonctionnalité facultative permet la coexistence de boîtes de messagerie Exchange à la fois sur site et dans Office 365 en synchronisant un ensemble spécifique d'attributs de Azure AD sur votre système de domaine AD DS sur site.
- Filtrage des applications et attributs Azure AD. Cette fonctionnalité facultative vous permet d'adapter l'ensemble des attributs synchronisés à un ensemble spécifique, basé sur les applications Azure AD.
- Synchronisation de hachage de mot de passe. Vous pouvez activer cette fonctionnalité facultative si vous avez sélectionné la fédération comme solution SSO. Vous pouvez ensuite utiliser la synchronisation de mot de passe comme option de sauvegarde.
- Ecriture différée de mot de passe. Avec cette fonctionnalité facultative, les changements de mot de passe qui proviennent de Azure AD sont réécrits sur votre système de domaine AD DS sur site. Vous déployez généralement cette fonctionnalité lorsque vous souhaitez accorder aux utilisateurs la réinitialisation en libre-service de leur mot de passe Azure AD.
- Ecriture différée de groupe. Avec cette option, si vous utilisez les groupes dans la fonctionnalité Office 365, vous pouvez synchroniser ces groupes Office 365 sur votre système de domaine AD DS sur site en tant que groupe de distribution. Cette option est disponible uniquement si vous avez déployé Exchange Server sur site.
- Ecriture différée du périphérique. Avec cette fonctionnalité facultative, les objets de périphérique dans Azure AD sont réécrits sur votre système de domaine AD DS sur site pour les cas d'accès conditionnel.
- Synchronisation des attributs des extensions d'annuaire. Non disponible dans les versions précédentes de synchronisation d'annuaire, cette fonctionnalité facultative vous permet d'étendre le schéma dans Azure AD avec des attributs personnalisés ajoutés par votre organisation ou d'autres attributs dans votre système de domaine AD DS sur site.

Après avoir sélectionné les fonctionnalités facultatives, le programme d'installation Azure AD Connect offre la possibilité de déployer une nouvelle batterie AD FS sur Windows Server 2012 R2 ou une version ultérieure ou de sélectionner une batterie AD FS existante sur Windows Server 2012 R2 ou une version ultérieure. En outre, le programme d'installation Azure AD Connect offre la possibilité de configurer la relation de fédération entre AD FS et Azure AD. Il configure AD FS pour qu'il émette des jetons de sécurité sur Azure AD et configure Azure AD pour qu'il approuve les jetons de cette instance spécifique AD FS.



Remarque : Le programme d'installation Azure AD Connect ne vous permet de configurer l'approbation que pour un seul domaine. Vous pouvez configurer des domaines supplémentaires à tout moment en ouvrant à nouveau Azure AD Connect et en exécutant cette tâche.

Au cours de la phase finale de l'installation d'Azure AD Connect, vous avez la possibilité de lancer automatiquement la synchronisation une fois l'installation terminée (bien que vous puissiez choisir de ne pas le faire). Vous avez également la possibilité d'activer le mode de préproduction. Ce processus vous permet de configurer un nouveau serveur de synchronisation d'annuaire en parallèle à un serveur existant.

Vous pouvez avoir un serveur de synchronisation d'annuaire connecté à un annuaire Azure AD dans le cloud. Si vous voulez changer de serveur à partir, par exemple, d'un serveur exécutant DirSync, vous pouvez activer le mode de préproduction d'Azure AD Connect. Lorsqu'il est activé, le moteur de synchronisation importe et synchronise les données comme d'habitude, mais n'exporte pas n'importe quoi sur Azure AD et désactive la synchronisation et l'écriture différée de mot de passe.

Pendant que vous travaillez en mode de préproduction, il est possible d'apporter les modifications nécessaires au moteur de synchronisation et d'examiner ce qui est sur le point d'être exporté. Lorsque la configuration semble bonne, vous pouvez exécuter l'assistant d'installation à nouveau et désactiver le mode de préproduction. Cela permettra aux données d'être exportées vers Azure AD.



Remarque : Assurez-vous de désactiver l'autre serveur de synchronisation d'annuaire en même temps que vous configurez Azure AD Connect de sorte que seul un serveur expore activement vers Azure AD.

Démonstration : Installer et configurer Azure AD Connect

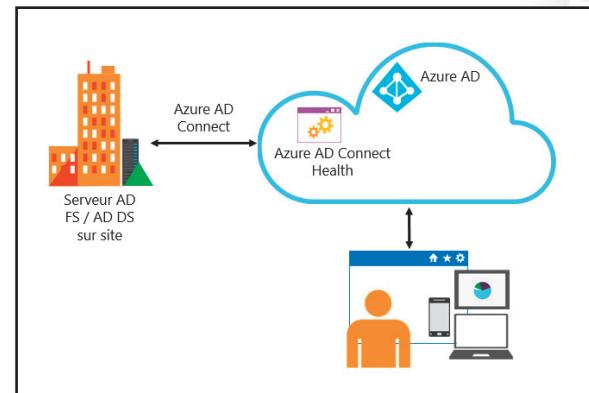
Procédure de démonstration

1. Sur **LON-SVR1**, téléchargez et exécutez la configuration Azure AD Connect à partir de <http://www.microsoft.com/fr-fr/download/details.aspx?id=47594>.
2. Choisissez de personnaliser le processus de configuration.
3. Choisissez **Synchronisation de mot de passe** comme mode de configuration.
4. Utilisez **SYNC@yourdomain.onmicrosoft.com** pour vous connecter à Azure AD et utilisez **Adatum\administrateur** pour vous connecter au système de domaine AD DS local.
5. Choisissez de synchroniser uniquement le groupe **Recherche** sur Azure AD.
6. Activez l'**écriture différée de mot de passe**.
7. Attendez que Azure AD Connect effectue la synchronisation initiale.
8. Connectez-vous au portail classique Azure, puis vérifiez que les objets sont synchronisés en allant dans l'onglet **UTILISATEURS**.
9. Sur **LON-SVR1**, ouvrez le **Gestionnaire de services de synchronisation**, puis examinez les tâches de synchronisation terminées.

Fonctionnalités de contrôle d'Azure AD Connect

Azure AD Connect Health vous permet de surveiller et d'avoir un aperçu de votre infrastructure d'identité sur site et des services de synchronisation disponibles au moyen d'Azure AD Connect. Il vous offre la possibilité d'afficher les alertes, les performances, les modèles d'utilisation, les paramètres de configuration et vous permet de maintenir une connexion fiable à Azure AD. Pour ce faire, vous devez utiliser un agent installé sur les serveurs ciblés.

La page Azure AD Connect Health présente les informations récupérées à partir de l'agent. En utilisant le portail Azure AD Connect Health, vous pouvez afficher les alertes, effectuer le suivi des performances et examiner les analyses de l'utilisation. Cette information se trouve dans un endroit facile à utiliser pour votre commodité.



Azure AD Connect Health pour AD FS surveille votre environnement AD FS sur site et Azure AD Connect Health pour la synchronisation contrôle et fournit des informations sur les synchronisations qui se produisent entre vos AD DS et Azure AD sur site. Azure AD Connect Health pour la synchronisation fournit l'ensemble des fonctionnalités clés suivantes :

- Affichage et prise en charge des alertes pour garantir des synchronisations fiables entre votre infrastructure sur site et Azure AD ;
- Notifications par courriel pour les alertes critiques ;
- Affichage des données de performance.

Pour démarrer avec Azure AD Connect Health, effectuez ces quatre étapes :

1. Connectez-vous au portail classique Azure.
2. Accédez à Azure AD Connect Health en allant sur Marketplace et en recherchant ou en sélectionnant **Marketplace**, puis en sélectionnant **Sécurité+Identité**.
3. Dans la fenêtre d'introduction, cliquez sur **Créer**. Cela ouvre une autre fenêtre avec vos informations d'annuaire.
4. Dans la fenêtre d'annuaire, cliquez sur **Créer**.



Remarque : Vous avez besoin d'une licence Azure AD Premium pour utiliser Azure AD Connect Health.

Lorsque vous accédez pour la première fois à Azure AD Connect Health, vous voyez une fenêtre. Dans cette fenêtre, vous pouvez accéder aux informations suivantes :

- **Démarrage rapide.** Cette option ouvre la fenêtre de démarrage rapide. Ici vous pouvez télécharger l'agent Azure AD Connect Health en sélectionnant **Obtenir les outils, la documentation d'accès et fournir un commentaire**.
- **AD FS.** Cette option représente tous les services AD FS qu'Azure AD Connect Health est en train de surveiller. Lorsque vous sélectionnez l'une des instances, une fenêtre contenant des informations sur cette instance s'ouvre. Ces informations comprennent un aperçu, les propriétés, les alertes, la surveillance et les analyses de l'utilisation.

- **Configurer.** Cette option vous permet d'activer ou de désactiver les sous-options suivantes :
 - **Mise à jour automatique.** Utilisez cette option pour mettre à jour automatiquement l'agent Azure AD Connect Health vers la dernière version. Cette option met automatiquement à jour l'agent sur votre serveur vers la dernière version de l'agent Azure AD Connect Health lorsqu'il est disponible. Azure AD Connect Health permet cela par défaut.
 - **Autoriser l'accès Microsoft aux données d'intégrité de votre annuaire Azure AD uniquement à des fins de dépannage.** Lorsque vous activez cette option, Microsoft peut voir les mêmes données que celles que vous voyez. Cette option peut aider au dépannage et à la résolution de problèmes. Azure AD Connect Health désactive cette fonction par défaut.



Lectures supplémentaires : Pour plus d'informations, consultez : « Surveiller votre infrastructure d'identité sur site et vos services de synchronisation sur le cloud » sur : <http://aka.ms/dqaaps>

Gestion privilégiée des identités Azure AD

Vous pouvez utiliser Azure AD Privileged Identity Management pour contrôler et surveiller les identités privilégiées et leur accès aux ressources qui se trouvent dans le cloud. Azure AD Privileged Identity Management vous permet d'accorder un accès administratif sur demande, ce qui minimise le risque pour la sécurité d'accorder un accès permanent aux ressources Azure ou Office 365. Les administrateurs temporaires doivent terminer le processus d'activation du rôle attribué pour qu'il devienne actif. Le processus d'activation de rôle consiste à fournir des informations sur la durée du rôle et des informations que l'utilisateur doit fournir lors de l'affectation de rôle. En outre, vous pouvez utiliser Azure AD Privileged Identity Management pour découvrir des utilisateurs qui ont des rôles administratifs, recevoir des alertes concernant l'utilisation des rôles privilégiés et générer des rapports pour un accès administratif.

AD Azure Privileged Identity Management vous permet de :

- Découvrir quels utilisateurs sont les administrateurs Azure AD ;
- Activer l'accès administrateur aux ressources du répertoire à la demande et juste-à-temps ;
- Obtenir des rapports sur l'historique des accès d'administrateurs et sur les modifications des attributions d'administrateurs ;
- Obtenir des alertes sur l'accès à un rôle privilégié.

Vous pouvez activer Azure AD Privileged Identity Management dans le portail classique Azure en utilisant un compte d'administrateur global pour l'annuaire. Après avoir activé Azure AD Privileged Identity Management, vous pouvez utiliser le tableau de bord de Privileged Identity Management pour surveiller le nombre d'utilisateurs auxquels des rôles privilégiés ont été attribués et le nombre d'administrateurs temporaires ou permanents.

Question : Lorsque vous mettez en place la synchronisation entre AD DS et Azure AD, où maîtrisez-vous les objets AD DS ?

Leçon 3

Gestion des identités avec la synchronisation de répertoires

Après avoir implémenté la synchronisation d'annuaire avec Azure AD Connect, vous devez choisir comment gérer les identités dans votre organisation. En outre, il est important de surveiller attentivement le processus de synchronisation pour pouvoir réagir en cas de problème.

Dans cette leçon, vous en apprenez plus sur la gestion des identités avec Azure AD Connect et AD FS. Cette leçon explique également comment gérer les utilisateurs et les groupes avec Azure AD Connect et comment maintenir la synchronisation d'annuaire.

Objectifs de la leçon

À la fin de cette leçon, vous allez pouvoir effectuer les tâches suivantes :

- Comparer les options disponibles pour la synchronisation d'identité ;
- Décrire comment gérer les utilisateurs avec la synchronisation d'annuaire ;
- Décrire comment gérer les groupes avec la synchronisation d'annuaire ;
- Décrire comment modifier la synchronisation d'annuaire ;
- Décrire comment surveiller la synchronisation d'annuaire ;
- Décrire comment résoudre la synchronisation d'annuaire.

Comparaison des options pour la synchronisation d'identité

Lorsque vous exécutez Azure AD Connect, vous pouvez choisir de synchroniser ou de fédérer les comptes à partir de votre système de domaine AD DS sur site avec Azure AD. La synchronisation a lieu en reproduisant les objets, mais peut éventuellement inclure la synchronisation de mot de passe. Il est important de comprendre la différence entre les trois options pour permettre la synchronisation entre votre système de domaine AD DS sur site et Azure AD. Ces trois options sont :

- Synchronisation d'annuaire ;
- Synchronisation d'annuaire avec synchronisation de mot de passe ;
- Synchronisation de répertoires avec SSO.

| Fonctionnalité | Synchronisation de répertoires seulement | Synchronisation d'annuaire avec synchronisation de mot de passe | Synchronisation d'annuaire avec l'authentification unique (SSO) |
|--|--|---|---|
| Sync les utilisateurs, groupes et contacts avec Azure | Oui | Oui | Oui |
| Sync les mises à jour incrémentielles avec Azure | Oui | Oui | Oui |
| Activer des scénarios Office 365 hybride | Oui, assistance limitée | Oui, assistance limitée | Oui, assistance complète |
| Les utilisateurs peuvent se connecter avec des informations d'identification sur site | Non | Oui | Oui |
| Réduire les coûts d'administration des mots de passe | Non | Oui | Oui |
| Contrôler les stratégies de mot de passe depuis un répertoire sur site | Non | Oui | Oui |
| Activer MFA dans le cloud | Oui | Oui | Oui |
| Activer MFA sur site | Non | Non | Oui |
| Authentifier contre un répertoire local | Non | Non | Oui |
| Mettre en œuvre l'authentification unique SSO avec des informations d'identification de votre organisation | Non | Non | Oui |
| Personnaliser la page de connexion | Non | Non | Oui |
| Limiter l'accès à des services basés sur l'emplacement ou le type de client | Non | Non | Oui |

Synchronisation d'annuaire :

Avec la synchronisation d'annuaire, les objets du système de domaine AD DS sont répliqués sur Azure AD. Par exemple, la synchronisation d'annuaire mappe **user.one@contoso.com** à partir du système de domaine AD DS sur site sur **utilisateur.un@contoso.onmicrosoft.com** dans Azure AD. Si vous créez et vérifiez un domaine personnalisé dans Azure AD, alors vous pouvez configurer un nom d'utilisateur correspondant entre les deux annuaires, de sorte que utilisateur.un@contoso.com existe dans les deux. Bien que cela ne soit pas obligatoire pour la synchronisation d'annuaire, vous devez l'implémenter pour l'authentification unique (SSO) et devez avoir la même arborescence pour qu'il prenne effet. Tout changement dans les attributs de l'utilisateur un dans Active Directory sur site, tels que les changements de numéro de

téléphone, d'emplacement du bureau et ainsi de suite, est répliqué au moyen de la synchronisation d'annuaire pour Azure AD. À ce stade, les deux systèmes maintiennent les mots de passe séparés.

Synchronisation d'annuaire avec synchronisation de mot de passe

L'activation de la synchronisation des mots de passe avec le processus de synchronisation fournit les mêmes facilités de connexion. Donc, si l'utilisateur un se connecte à son ordinateur faisant partie du domaine avec le nom d'utilisateur **utilisateur.un@contoso.com** et le mot de passe **Pa55w.rd**, l'utilisateur est authentifié par l'Active Directory sur site. Si l'utilisateur se connecte ensuite à un service ou une application basé sur Azure, il ou elle verra une invite d'authentification. Si l'UPN de l'utilisateur correspond entre le système de domaine Ad DS sur site et Azure AD, sur l'invite de commandes, l'utilisateur doit saisir les mêmes informations d'identification —avec **utilisateur.un@contoso.com** comme nom d'utilisateur et **Pa55w.rd** comme mot de passe— pour accéder aux ressources Azure. Lorsque l'utilisateur accède à la ressource Azure, Azure AD authentifie l'utilisateur.

En arrière-plan, le composant de synchronisation de mot de passe prend le hachage du mot de passe de l'utilisateur à partir de Active Directory local, le crypte et l'envoie sous forme de chaîne à Azure. Azure déchiffre le hachage chiffré et stocke le hachage de mot de passe en tant qu'attribut d'utilisateur dans Azure AD.

Lorsque l'utilisateur se connecte à un service Azure, la boîte de dialogue **test de connexion** génère un hachage du mot de passe de l'utilisateur et transmet ce hachage vers Azure. Azure compare ensuite le hachage avec celui dans le compte de cet utilisateur. Si les deux hachages correspondent, les deux mots de passe doivent également correspondre et l'utilisateur reçoit l'accès à la ressource.

La boîte de dialogue **test de connexion** offre la possibilité d'enregistrer les informations d'identification de telle sorte que la prochaine fois que l'utilisateur accède à la ressource Azure, il ou elle ne verra pas d'invite d'authentification. Cependant, il est important de comprendre qu'il s'agit de la même connexion, pas d'un SSO. L'utilisateur s'identifie toujours auprès de deux services d'annuaire distincts, mais avec le même nom d'utilisateur et le même mot de passe. Cependant, pour de nombreuses organisations, la simplicité de cette solution, sans la complexité et les coûts de mise en œuvre supplémentaires d'AD FS, fait du manque de vrai SSO un faible prix à payer.

Synchronisation de répertoires avec SSO

Azure AD Connect fournit un simple assistant pour déployer et configurer AD FS qui, en arrière-plan utilise la synchronisation d'annuaires pour répliquer des objets vers Azure AD. Avec SSO, la synchronisation d'annuaires synchronise les informations de contact, d'utilisateur et de groupe à partir de l'AD DS local vers Azure AD. Ces objets apparaissent comme des objets de service d'annuaire dans Azure AD.

La différence entre la synchronisation de mot de passe et SSO est que dans SSO, au lieu de deux processus d'authentification distincts, un sur l'AD DS local et l'autre dans Azure AD, une approbation de fédération s'établit entre Azure AD et l'AD DS local. Cette relation d'approbation permet aux utilisateurs d'accéder à des applications et à des ressources dans Azure en utilisant leurs comptes de domaine dans AD DS. Ces utilisateurs apparaissent aussi comme utilisateurs dans Azure AD, car SSO intègre Azure AD avec AD DS local. Cependant, l'authentification de ces utilisateurs ne se fait pas dans Azure AD, mais dans AD DS local.

L'autorisation d'accéder aux ressources Azure est séparée de l'authentification et elle a lieu du côté des ressources, dans le cas présent Azure. L'AD DS local génère un jeton, qui passe dans AD FS, puis dans Azure en utilisant la relation d'approbation de fédération.

Comparaison des fonctionnalités

Le tableau suivant répertorie les fonctionnalités que chaque option de synchronisation d'annuaire prend en charge.

| Fonctionnalité | Synchronisation de répertoires seulement | Synchronisation d'annuaire avec synchronisation de mot de passe | Synchronisation de répertoires avec SSO |
|---|--|---|---|
| Sync les utilisateurs, groupes et contacts avec Azure | Oui | Oui | Oui |
| Sync les mises à jour incrémentielles avec Azure | Oui | Oui | Oui |
| Active les scénarios hybrides Microsoft Office 365 | Oui, assistance limitée | Oui, assistance limitée | Oui, assistance complète |
| Les utilisateurs peuvent se connecter avec des informations d'identification sur site | Non | Oui | Oui |
| Réduire les coûts d'administration des mots de passe | Non | Oui | Oui |
| Contrôler les stratégies de mot de passe depuis un répertoire sur site | Non | Oui | Oui |
| Active l'authentification multifacteur dans le cloud (MFA) | Oui | Oui | Oui |
| Activer MFA sur site | Non | Non | Oui |
| Authentifie par rapport à un répertoire local | Non | Non | Oui |
| Mettre en œuvre SSO avec des informations d'identification organisationnelles | Non | Non | Oui |
| Personnaliser la page de connexion | Non | Non | Oui |
| Limiter l'accès à des services basés sur l'emplacement ou le type de client | Non | Non | Oui |

Exigences

Le tableau suivant dresse la liste des exigences de haut niveau pour chaque option de synchronisation d'annuaire.

| Configuration requise | Synchronisation de répertoires seulement | Synchronisation d'annuaire avec synchronisation de mot de passe | Synchronisation de répertoires avec SSO |
|---|--|---|---|
| Serveur local d'Azure AD Connect | Oui | Oui | Oui |
| Infrastructure de serveur AD FS | Non | Non | Oui |
| Proxy AD FS ou infrastructure Proxy d'application Web | Non | Non | Oui |

Si AD FS est indisponible, les utilisateurs ne sont pas en mesure de s'authentifier et ils ne sont pas en mesure d'utiliser les ressources d'Azure. Si l'Azure AD Connect avec le serveur de synchronisation d'annuaires est indisponible, les changements d'attributs récents, y compris les hachages de mots de passe si activés, ne se synchronisent pas, mais les utilisateurs seront toujours en mesure d'accéder aux ressources. En effet, le déploiement de SSO fiable et hautement disponible a des exigences plus élevées en matière de ressources et de gestion que l'option de synchronisation d'annuaires seule ou l'option de synchronisation d'annuaires avec synchronisation de mot de passe.

Gestion des utilisateurs avec synchronisation d'annuaire

Après avoir déployé Azure AD Connect avec succès et activé la synchronisation planifiée, plusieurs tâches de gestion sont requises pour assurer la synchronisation efficace des utilisateurs.

Écriture conditionnelle utilisateur

Les comptes d'utilisateurs créés dans Azure AD peuvent maintenant se resynchroniser vers l'AD DS local. Pour activer la fonction d'écriture différée des utilisateurs pour Azure AD Connect, vous devez activer l'option **écriture différée des utilisateurs** lors de l'installation d'Azure AD Connect, avec des réglages personnalisés, puis exécutez les applets de commande Windows PowerShell suivants sur le serveur Azure AD Connect :

```
Import-Module 'C:\Program Files\Microsoft Azure Active Directory Connect\AdPrep\AdSyncPrep.psm1'
Initialize-ADSyncUserWriteBack -AdConnectorAccount $accountName -UserWriteBackContainerDN $userOU
```

Après avoir déployé Azure AD Connect avec succès et activé la synchronisation planifiée, effectuez ces tâches de gestion requises pour assurer la synchronisation efficace des utilisateurs :

- Écriture conditionnelle utilisateur
- Écriture conditionnelle mot de passe
- Écriture conditionnelle appareil
- Gestion de l'adresse SMTP principale
- Récupération de suppressions accidentnelles
- Récupération de suppressions désynchronisées
- Suppression de compte accidentelle
- Activation en bloc de nouveaux comptes



Remarque : **\$accountName** est le compte utilisé par Azure AD Connect pour gérer les objets dans AD DS ; il s'agit généralement d'un compte sous la forme d'un numéro Azure AD. **\$userOU** est l'unité d'organisation où ces utilisateurs de nuages sont stockés dans l'AD DS local.



Remarque : l'écriture différée des utilisateurs exige que la forêt AD DS exécute Windows Server 2012 R2 ou une version plus récente.

Une fois que ces applets de commande ont fini de s'exécuter, le compte de service Azure AD Connect pour l'AD DS local a la permission d'écrire des objets dans l'unité d'organisation **\$userOU**. Vous pouvez afficher les autorisations dans Utilisateurs et ordinateurs Active Directory pour cette unité d'organisation si vous activez le mode **Avancé** dans la console. Il devrait y avoir une entrée d'autorisation pour ce compte qui n'est pas hérité des unités d'organisation parentes.

Une fois la synchronisation terminée, les utilisateurs d'Azure AD apparaîtront dans le conteneur local que vous avez sélectionné lors de la configuration.



Remarque : Une licence Azure AD Premium est nécessaire pour permettre une écriture conditionnelle du périphérique.

Écriture conditionnelle mot de passe

Les utilisateurs peuvent désormais changer leurs mots de passe via la page **s'identifier** ou dans les paramètres utilisateur dans Azure AD et le renvoyer vers AD DS local. Pour activer la fonction d'écriture différée du mot de passe pour Azure AD Connect, vous devez activer l'option écriture différée du mot de passe lors de l'installation d'Azure AD Connect, avec des réglages personnalisés, puis exécutez les applets de commande Windows PowerShell suivants sur le serveur Azure AD Connect :

```
Get-ADSyncConnector | fl name,AADPasswordResetConfiguration
Get-ADSyncAADPasswordResetConfiguration -Connector "adatum.onmicrosoft.com - AAD"
Set-ADSyncAADPasswordResetConfiguration -Connector "adatum.onmicrosoft.com - AAD" -Enable
$true
$cmd = "dsaccls.exe '$passwordOU' /I:S /G `"$accountName`":CA;`"Reset Password`";user`"
Invoke Expression-$ cmd | Out-Null
$cmd = "dsaccls.exe '$passwordOU' /I:S /G `"$accountName`":CA;`"Change Password`";user`"
Invoke Expression-$ cmd | Out-Null
$cmd = "dsaccls.exe '$passwordOU' /I:S /G `"$accountName`":WP;lockoutTime;user`"
Invoke Expression-$ cmd | Out-Null
$cmd = "dsaccls.exe '$passwordOU' /I:S /G `"$accountName`":WP;pwdLastSet;user`"
Invoke Expression-$ cmd | Out-Null
```



Remarque : Azure AD Connect utilise le compte **\$accountName** pour gérer les objets dans AD DS. Il s'agit généralement d'un compte sous la forme d'un numéro Azure AD. **\$passwordOU** est l'unité d'organisation où ces utilisateurs de nuages sont stockés dans l'AD DS local.



Remarque : l'écriture différée du mot de passe exige que la forêt AD DS exécute Windows Server 2012 R2 ou une version plus récente.

Une fois que ces applets de commande ont été exécutés, la configuration suivante se produit :

- Les connecteurs Azure AD Connect sont activés pour une réinitialisation du mot de passe.
- Le compte de service Azure AD Connect pour l'AD DS local a alors l'autorisation de réinitialiser les mots de passe pour les objets dans l'unité d'organisation **\$passwordOU**. Vous pouvez afficher les autorisations dans Utilisateurs et ordinateurs Active Directory pour cette unité d'organisation si vous activez le mode **Avancé** dans la console. Il devrait y avoir une entrée d'autorisation pour ce compte qui n'est pas hérité des unités d'organisation parentes.



Remarque : Une licence Azure AD Premium est nécessaire pour permettre une écriture conditionnelle du périphérique.

Écriture conditionnelle périphérique

Les périphériques qui sont inscrits avec la gestion des périphériques mobiles (MDM) ou Intune Office 365 peuvent se connecter aux ressources contrôlées par AD FS basées sur l'utilisateur et l'appareil sur lequel elles se trouvent. Vous utilisez l'écriture différée des appareils pour permettre l'accès conditionnel, en fonction des dispositifs, afin d'accéder à des applications AD FS protégées ou qui dépendent des approbations de partie de confiance. Cela fournit une sécurité supplémentaire et l'assurance que seuls les appareils approuvés peuvent accéder à des applications.

Pour activer la fonction d'écriture différée des appareils pour Azure AD Connect, vous devez activer l'option **écriture différée des appareils** lors de l'installation d'Azure AD Connect, avec des réglages personnalisés, puis exécutez les trois applets de commande Windows PowerShell suivants sur le serveur Azure AD Connect :

```
Install-WindowsFeature –Name AD-DOMAIN-Services –IncludeManagementTools  
Import-Module 'C:\Program Files\Microsoft Azure Active Directory  
Connect\AdPrep\AdSyncPrep.psm1'  
Initialize-ADSyncDeviceWriteback {Optional:–Nom de domaine [nom] Optional:–  
CompteConnecteurAD [compte]}
```



Remarque : **Nom de domaine** est le domaine AD DS où les objets de périphériques sont créés. **CompteConnecteurAD** est le compte AD DS qu'Azure AD Connect utilise pour gérer les objets dans le répertoire. Ceci est le compte utilisé par Azure AD Connect pour se connecter à AD DS. Si vous avez installé Azure AD Connect en utilisant les paramètres express, alors ce nom de compte a le préfixe **MSOL_**.



Remarque :

- L'écriture différée des appareils nécessite que la forêt AD DS exécute Windows Server 2012 R2 ou une version ultérieure.
- L'écriture différée des appareils nécessite qu'AD FS soit hébergé sur Windows Server 2012 R2 (AD FS v3.0) ou une version ultérieure.

Une fois que les applets de commande mentionnés précédemment ont été exécutés, la configuration suivante se produit :

- S'il n'y en a pas, ils créent et configurent de nouveaux conteneurs et objets sous **CN=Configuration de l'enregistrement du périphérique, CN=Services, CN=Configuration, [forêt-dn]**, où **forêt-dn** est le nom unique de votre forêt AD DS.
- S'il n'y en a pas, ils créent et configurent de nouveaux conteneurs et objets sous **CN=AppareilsEnregistrés, [domain-dn]**, où **forêt-dn** est le nom unique de votre forêt AD DS. Les objets de périphérique sont créés dans ce conteneur.
- Ils fixent les autorisations nécessaires sur le compte Azure AD Connector pour gérer les périphériques sur votre AD DS.



Remarque : Une licence Azure AD Premium est nécessaire pour permettre une écriture conditionnelle du périphérique.

Gestion de l'adresse SMTP principale

L'une des principales tâches de maintenance de l'utilisateur est de gérer les attributs de boîte aux lettres de l'utilisateur, en particulier les adresses SMTP principales. Pour qu'un compte utilisateur local obtienne l'adresse SMTP principale correcte, il doit être autorisé pour boîte aux lettres, soit en utilisant le centre d'administration Microsoft Exchange 2016, soit en définissant l'attribut **courrier** manuellement pour activer la messagerie de l'utilisateur.

 **Remarque :** si une adresse SMTP principale n'est pas définie pour un compte d'utilisateur, Office 365 utilise un @domaine.onmicrosoft.com comme adresse SMTP par défaut de l'utilisateur.

S'il est impossible de garantir que tous les utilisateurs synchronisés auront une adresse SMTP principale valide avant la synchronisation, vous pouvez utiliser le filtrage d'attribut utilisateur pour vous assurer que tous les comptes sans UPN valide sont exclus du champ d'application de la synchronisation.

Récupération de suppressions accidentelles

Azure AD prend désormais en charge les suppressions réversibles. Après avoir supprimé un utilisateur dans Azure AD, soit à la suite d'une synchronisation ou si vous supprimez manuellement un utilisateur désynchronisé dans Azure AD, les données de l'utilisateur sont supprimées et les licences de l'utilisateur peuvent être réaffectées ; toutefois, les comptes restent récupérables pendant 30 jours. Une fois la corbeille du cloud vidée (suppression définitive), il n'est plus possible de récupérer les comptes supprimés.

Récupération de suppressions désynchronisées

Une autre tâche importante de maintenance est de faire face à une suppression locale qui ne se synchronise pas avec Azure AD de sorte que l'objet lié n'est pas retiré d'Azure AD. Cette situation peut se produire si la synchronisation d'annuaires n'est pas encore terminée ou si elle n'a pas réussi à supprimer un objet cloud spécifique, ces deux éventualités se traduisant par un objet Azure AD orphelin.

Pour résoudre ce problème, procédez comme suit :

1. Exécuter manuellement une mise à jour de la synchronisation d'annuaires ;
2. Forcer la synchronisation des annuaires ;
3. Vérifier que la synchronisation d'annuaires a bien eu lieu correctement ;
4. Vérifier la synchronisation des annuaires.

Si les étapes ci-dessus confirment que la synchronisation d'annuaires fonctionne correctement, mais que la suppression des objets AD DS ne s'est pas encore propagée à Azure AD, vous pouvez supprimer manuellement l'objet orphelin en utilisant l'un des modules AD Azure suivants pour applets de commande Windows PowerShell :

```
Remove-MsolContact
Remove-MsolGroup
Remove-MsolUser
```

Par exemple, pour supprimer manuellement un utilisateur orphelin créé à l'origine en utilisant la synchronisation d'annuaires, exécutez l'applet de commande suivant :

```
Retirez-MsolUser -UserPrincipalName <Nom d'utilisateur> @ <Domain cloud>
```

Suppression de compte accidentelle

Si vous supprimez accidentellement un compte d'utilisateur alors qu'un cycle de synchronisation d'annuaires est en cours, cette action supprime l'utilisateur dans Azure AD. Toutefois, si vous avez la fonctionnalité de la corbeille activée dans AD DS, vous pouvez récupérer le compte à partir de la corbeille

et le lien entre les comptes est rétabli. Si vous ne disposez pas de la corbeille activée, vous devez peut-être créer un autre compte avec un nouveau GUID.

Activation en bloc de nouveaux comptes

Les comptes d'utilisateur que vous créez dans Azure AD grâce à la synchronisation d'annuaires ne sont pas automatiquement activés pour les services cloud tels qu'Office 365. Nous vous recommandons d'utiliser des scripts pour gérer cette exigence. Une approche simple utilise le module AD Azure pour applets de commande Windows PowerShell. Par exemple :

```
Get-MsolAccountSku (to report the Office365 SKUs that, such as EXCHANGESTANDARD)
Get-MsolUser -UnlicensedUsersOnly | Set-MsolUser -UsageLocation <location>, such as "US"
Get-MsolUser -UnlicensedUsersOnly | Set-MsolUserLicense -AddLicenses SKU
```

L'attribut utilisateur **isLicensed** indique si un utilisateur possède une licence attribuée (True) ou non attribuée (False). Windows PowerShell peut, par conséquent, faire un rapport sur des comptes d'utilisateurs avec licence d'Office 365. Pour voir tous les utilisateurs avec licence dans Office 365, tapez la commande suivante dans le module Azure AD pour l'invite Windows PowerShell :

```
Get-MsolUser | Where-Object { $_.isLicensed -eq "True" }
Pour exporter une liste d'utilisateurs avec licence d'Office 365 dans CSV, utilisez la commande suivante :
Get-MsolUser | Where-Object { $_.isLicensed -eq "True" } | Export-Csv
C:\Labfiles\LicensedUsers.csv
```

Gérer les groupes avec synchronisation d'annuaire

Comme pour la synchronisation d'annuaires des utilisateurs d'AD DS local sur Azure AD, les groupes (ainsi que leur adhésion) dans AD DS se synchronisent aussi à partir de l'AD DS local sur Azure AD. Comme pour la fonction d'écriture différée des utilisateurs, la fonction d'écriture différée de groupe écrit aussi des groupes à partir d'Azure AD sur l'AD DS local. Le processus que Azure AD Connect utilise, est très similaire pour les objets d'utilisateur et de groupe et a beaucoup des mêmes limitations et mises en garde.

Même si vous activez la fonction d'écriture différée de groupe lors de l'installation de Azure AD Connect en sélectionnant la fonction d'écriture différée de groupe après l'installation, avec des paramètres personnalisés, vous devez également créer l'unité d'organisation et les autorisations appropriées requises pour l'écriture différée de groupe dans AD DS. Pour vous aider à faire cela, Azure AD Connect dispose d'un applet de commande intégré appelé **Initialisation-ADSyncGroupWriteBack** qui prépare automatiquement AD DS.

- La fonctionnalité d'écriture différée de groupe copie les groupes d'Azure AD dans AD DS local
- Cmdlet **Initialize-ADSyncGroupWriteBack** prépare automatiquement AD DS à l'écriture différée de groupe
- **\$groupOU** est l'unité d'organisation dans laquelle les groupes cloud sont stockés dans AD DS local
- Les groupes d'Azure AD sont représentés comme des groupes de distribution dans AD DS local
- Il vous faut une licence Azure AD Premium pour activer l'écriture différée de groupe sans la fonctionnalité d'écriture différée hybride de Serveur Exchange



Remarque : l'écriture différée de groupe exige que la forêt AD DS exécute Windows Server 2012 R2 ou une version plus récente.

Par exemple, utilisez la commande suivante pour préparer AD DS à l'écriture différée de groupe :

```
Import-Module 'C:\Program Files\Microsoft Azure Active Directory Connect\AdPrep\AdSyncPrep.psm1'
Initialize-ADSyncGroupWriteBack -AdConnectorAccount $accountName -GroupWriteBackContainerDN $groupOU
```

 **Remarque :** Azure AD Connect utilise le compte **\$accountName** pour gérer les objets dans AD DS, il s'agit généralement d'un compte sous la forme d'un numéro Azure AD. **\$groupOU** est l'unité d'organisation où ces groupes du cloud sont stockés dans AD DS local.

Une fois que ces applets de commande ont fini de s'exécuter, le compte de service Azure AD Connect pour l'AD DS local a la permission d'écrire des objets dans cette unité d'organisation. Vous pouvez afficher les autorisations dans Utilisateurs et ordinateurs Active Directory pour cette unité d'organisation si vous activez le mode **Avancé** dans la console. Il devrait y avoir une entrée d'autorisation pour ce compte qui n'est pas hérité des unités d'organisation parentes.

Une fois la synchronisation terminée, des groupes apparaissent dans le conteneur local que vous avez sélectionné lors de la configuration. Ces groupes sont représentés comme des groupes de distribution dans AD DS local.

 **Remarque :** À ce moment, l'écriture différée de groupe dans Azure AD Connect ne supporte que les écritures différées des groupes de distribution.

Comme pour des comptes utilisateurs synchronisés à partir de Azure AD sur l'AD DS local, les groupes synchronisés ne sont pas visibles dans la liste d'adresses globale locale. Ainsi, vous devez d'abord exécuter l'applet de commande **Update-Recipient** comme illustré dans l'exemple suivant :

```
Update-Recipient Group_af905347-5322-4183-a1aa-9522a85bfeb9ad
```

 **Remarque :** Sinon, vous pouvez utiliser les applets de commande **Update-AddressList** ou **Update-GlobalAddressList** pour faire apparaître le groupe synchronisé. Cependant, ces applets de commande nécessitent plusieurs cycles sur les serveurs exécutant Exchange Server par rapport à l'applet de commande **Update-Recipient**.

Après que cet applet de commande a fini de s'exécuter, le groupe s'affiche dans la liste d'adresses globale locale. Les groupes synchronisés depuis Azure AD sur l'AD DS local comprennent également l'attribut d'appartenance. Si vous avez activé l'écriture différée des utilisateurs dans Azure AD Connect, les appartенноances aux groupes pour les comptes d'utilisateurs créés dans Azure AD sont également incluses. Toutefois, si vous n'avez pas activé l'écriture différée des utilisateurs dans Azure AD Connect, seules les appartенноances aux groupes pour les comptes d'utilisateurs créés localement sont incluses.

Modification de la synchronisation des annuaires

Dans la synchronisation Azure AD Connect, vous pouvez activer le filtrage à tout moment. Si vous avez déjà déployé les configurations par défaut de la synchronisation d'annuaires et activé le filtrage, les objets filtrés ne sont plus synchronisés sur Azure AD. De ce fait, tous les objets dans Azure AD qui ont été précédemment synchronisés mais ont ensuite été filtrés sont supprimés dans Azure AD. Si des objets ont été supprimés par inadvertance en raison d'une erreur de filtrage, vous pouvez recréer les objets dans Azure AD en supprimant vos configurations de filtrage puis en synchronisant à nouveau vos répertoires.

Les types de configuration de filtrage que vous appliquez à Azure AD Connect comprennent :

- Domaine :
 - Vous permet de sélectionner les domaines AD DS qui sont autorisés à se synchroniser avec Azure AD
 - Utilise Azure AD Connect ou Synchronisation Service Manager
- L'unité d'organisation :
 - Vous permet de sélectionner les unités d'organisation d'AD DS qui sont autorisés à se synchroniser avec Azure AD
 - Utilise Azure AD Connect ou Synchronisation Service Manager
- Attribut :
 - Vous permet de contrôler quels objets d'AD DS devraient se synchroniser avec Azure AD en se basant sur des critères d'attributs des objets ;
 - Utilise l'Éditeur de règles de synchronisation (SRE, Synchronization Rules Editor).



Remarque : Bien que vous puissiez activer plusieurs personnalisations de filtrage dans Azure AD Connect, Microsoft ne supporte pas toutes les modifications ou opérations de synchronisation Azure AD Connect en dehors des actions formellement documentées. Chacune de ces actions pourrait conduire à un état de la synchronisation de Azure AD Connect incohérent ou non pris en charge. Par conséquent, Microsoft ne peut pas fournir de support technique pour de tels déploiements.

Vous pouvez vous demander : « pourquoi voudrais-je activer le filtrage si Azure AD Connect synchronise tout ce dont j'ai besoin après la mise en œuvre ? » Dans la plupart des cas, votre environnement AD DS local contient beaucoup plus d'objets (par exemple, les comptes utilisateurs, les contacts et les groupes) que ce qui est requis dans Azure AD. Par exemple, les comptes de services ou les comptes administratifs qui ne sont nécessaires que localement peuvent ne pas devoir être synchronisés sur Azure AD.

Heureusement, vous pouvez filtrer les objets de sorte que seuls les objets dont vous avez besoin en ligne se synchronisent. Le filtrage rend la synchronisation plus sécurisée, sans comptes oubliés dans les services en ligne et fournit donc une surface d'attaque plus petite. Le filtrage peut également vous aider à limiter le nombre d'objets, ce qui à son tour vous aide à minimiser la taille de votre base de données Azure AD Connect et peut empêcher d'avoir à effectuer un déploiement complet de SQL Server. N'oubliez pas, si votre environnement comporte plus de 50.000 objets, alors vous pouvez avoir besoin d'une version complète de SQL Server. À bien des égards, ce qui permet le filtrage dans Azure AD Connect favorise une complexité moins grande et augmente la vitesse de la synchronisation d'annuaires.

Voici quelques scénarios où le filtrage peut être nécessaire pour personnaliser la configuration par défaut :

- Vous prévoyez d'utiliser la topologie de répertoires Azure AD multiples. Pour ce scénario, vous devez appliquer un filtre pour contrôler quel objet doit se synchroniser avec un répertoire particulier d'Azure AD.
- Vous exécutez un pilote pour Azure ou Office 365 et ne souhaitez qu'un sous-ensemble d'utilisateurs dans Azure AD. Dans un petit projet pilote comme celui-ci, il n'est pas important d'avoir une liste d'adresses globale complète pour démontrer la fonctionnalité.
- Vous avez beaucoup de comptes de service et d'autres comptes non personnels ou comptes administratifs que vous ne voulez pas dans Azure AD.
- Pour des raisons de conformité, votre entreprise ne supprime pas les comptes d'utilisateur dans l'AD DS local ; vous vous contentez de les désactiver. Cependant, dans Azure AD, vous voulez que seuls les comptes actifs soient présents.



Remarque : À l'exception du filtrage à base d'attributs sortants, les configurations dans Azure AD Connect sont conservées lorsque vous installez ou mettez à niveau vers une version plus récente d'Azure AD Connect. Il est toujours recommandé de vérifier que la configuration n'a pas été modifiée par inadvertance après une mise à niveau vers une version plus récente avant de lancer le premier cycle de synchronisation.

Il existe trois types de configuration de filtrage que vous pouvez appliquer à Azure AD Connect (classées ici du filtrage le plus large au filtrage plus détaillé) :

- Domaine. Ce type de configuration de filtrage vous permet de sélectionner les domaines AD DS qui sont autorisés à se synchroniser avec Azure AD. Utilisez l'outil Synchronization Service Manager pour gérer les propriétés du Connecteur AD Source dans Azure AD Connect. Cet outil est automatiquement installé sur le serveur de synchronisation d'annuaire lors du déploiement d'Azure AD Connect.
- UO. Ce type de configuration de filtrage vous permet de sélectionner les UO dans AD DS qui sont autorisées à se synchroniser avec Azure AD. La plupart des organisations ont déjà une structure UO qui sépare les objets qui sont éligibles pour la synchronisation et ceux qui ne sont pas, comme les UO de groupes de comptes Exchange Security, les UO de services/administratifs, ou les UO pour les groupes de sécurité spécifiques. Vous pouvez utiliser Azure AD Connect ou l'outil Synchronization Service Manager pour gérer les propriétés du Connecteur AD Source dans Azure AD Connect.
- Attribut : Ce type de configuration de filtrage vous permet de contrôler les objets dans AD DS qui devraient se synchroniser avec Azure AD basé sur des critères d'attributs des objets. Même avec le filtrage de domaine et le filtrage UO, il est possible que certains objets dans une unité d'organisation doivent être exclus de la synchronisation. Il peut également s'avérer peu pratique de changer la conception UO dans le but de filtrer les objets qui se synchronisent avec Azure AD. Bien que beaucoup plus complexe que l'outil Synchronization Service Manager, vous devez utiliser l'outil Éditeur de règles de synchronisation pour gérer les règles de synchronisation dans Azure AD Connect. Cet outil est automatiquement installé sur le serveur de synchronisation d'annuaire lors du déploiement de Azure AD Connect.



Remarque : Vous utilisez Source AD comme nom pour votre connecteur AD DS. Si vous avez plusieurs forêts, vous avez un connecteur par forêt et la configuration doit se répéter pour chaque forêt.

Vous pouvez utiliser tous les types de configuration de filtrage, n'en utiliser que deux ou n'en utiliser qu'un seul. Les champs que vous choisissez dépendent de la façon dont vos domaines AD DS locaux sont structurés, de quels objets doivent se synchroniser avec Azure AD et des critères de filtrage.



Remarque : Avant de procéder à la modification du filtrage, vous devez désactiver la tâche planifiée pour la synchronisation sur le serveur de synchronisation d'annuaires pour vous assurer de ne pas exporter accidentellement des changements qui ne sont pas vérifiés vers Azure AD.

Étant donné que le filtrage dans Azure AD Connect peut enlever beaucoup d'objets dans un temps très court, vous devez vérifier les modifications apportées aux filtres avant de les exporter vers Azure AD.

Après avoir terminé les étapes de configuration, nous vous recommandons fortement de suivre les étapes de vérification avant d'exporter et d'apporter des modifications à Azure AD.

Pour vous protéger contre la suppression de plusieurs objets par accident, la fonction qui empêche les suppressions accidentelles est activée par défaut. Si vous supprimez de nombreux objets en raison du filtrage (500 par défaut), vous devez suivre les étapes décrites dans l'article suivant pour permettre aux suppressions de passer par Azure AD.



Lectures supplémentaires : Pour plus d'informations, consultez : « Synchronisation Azure AD Connect : configurer le filtrage » à l'adresse : <http://aka.ms/au8smo>

Surveillance de la synchronisation des annuaires

Nous vous recommandons d'utiliser System Center Operations Manager (Operations Manager) pour la surveillance du serveur de synchronisation d'annuaires et des services tels que AD DS pour vous assurer que les problèmes sont détectés et communiqués efficacement à tous les administrateurs responsables. À cet effet, vous pouvez utiliser le pack d'administration de System Center Operations Manager pour Azure.

Outils pour surveiller la synchronisation d'annuaires :

- Operations Manager : utilise le pack d'administration System Center pour Azure
- Le portail classique Azure
- Windows PowerShell
- Gestion du service de synchronisation
- Journaux d'événements

Le portail classique Azure

Le portail classique Azure fournit plusieurs méthodes pour la surveillance de synchronisation d'annuaires. S'il y a des erreurs lors de la synchronisation d'annuaires, une notification est envoyée par e-mail à l'adresse enregistrée en tant que *contact technique* du service cloud lors de votre inscription pour un service.

Pour vérifier la synchronisation d'annuaires en temps réel en utilisant le portail classique Azure :

1. Cliquez sur votre instance de répertoire dans le portail classique Azure.
2. Dans la barre d'outils, cliquez sur **INTÉGRATION D'ANNUAIRE**. Dans le champ **DERNIÈRE SYNCHRONISATION**, vous verrez la dernière fois qu'une synchronisation a eu lieu.

Windows PowerShell

Vous pouvez également utiliser des applets de commande et des scripts Windows PowerShell pour aider à gérer AD Azure, faire des rapports sur l'état de synchronisation et ainsi de suite. Après la connexion à Azure AD dans Windows PowerShell, vous pouvez utiliser l'applet de commande suivant pour vérifier la dernière fois qu'une synchronisation d'annuaires a été complétée avec succès dans AD Azure :

```
Import-Module MSOnline  
Connect-MsolService  
Get-MsolCompanyInformation | fl LastDirSyncTime
```



Lectures supplémentaires : Pour plus d'informations, consultez : « Applets de commande Azure Active Directory » sur : <http://aka.ms/pfsm1x>

Gestion du service de synchronisation

Le Synchronization Service Manager est installé automatiquement avec Azure AD Connect. Cet outil vous permet de vérifier et de modifier le service de synchronisation d'annuaire. Dans l'onglet **Opérations**, vous pouvez sélectionner la liste des différentes opérations de connecteur pour examiner l'**Heure de début**, l'**Heure de fin** et le **Statut** des tâches précédentes déjà terminées.

Journaux d'événements

L'outil de synchronisation d'annuaire écrit des entrées dans le journal des événements de synchronisation d'annuaire de l'ordinateur. Ces entrées indiquent le début et la fin d'une session de synchronisation d'annuaires. Les erreurs de synchronisation d'annuaires sont également rapportées dans le journal des événements et envoyées par e-mail à un contact technique désigné de votre organisation. Lors de l'examen du journal des événements, recherchez les entrées dont la source est la synchronisation d'annuaires. Une entrée marquée Événement 4 et accompagnée de la description **L'exportation est terminée** indique que la synchronisation d'annuaires est terminée.

Résolution des problèmes liés à la synchronisation des annuaires

Les tâches de résolution des problèmes importantes pour la synchronisation d'annuaires comprennent les analyses des journaux à la recherche d'erreurs et la remédiation à des erreurs de synchronisation avec Azure AD Connect. Les points typiques qui peuvent mener à des problèmes sont notamment :

- Les erreurs d'installation, telles que l'utilisation d'informations d'identification locales ou Azure AD incorrectes ;
- La désactivation par inadvertance de la synchronisation d'annuaires dans le portail classique Azure ou au moyen de Windows PowerShell ;
- Des changements imprévus dans AD DS qui affectent l'étendue de UO ou le filtrage des attributs ;
- Une corruption de AD DS nécessitant la récupération d'annuaires.

- Les tâches de résolution des problèmes pour la synchronisation d'annuaires comprennent :
 - Analyse du journal à la recherche d'erreurs ;
 - Correction des erreurs de synchronisation à l'aide de l'outil.
- Les points typiques qui peuvent mener à des problèmes sont notamment :
 - Les erreurs d'installation, telles que l'utilisation d'informations d'identification incorrectes comme les identifiants locaux ou ceux d'Azure AD ;
 - La désactivation accidentelle de la synchronisation d'annuaires dans le portail Azure Classic ou via Windows PowerShell ;
 - Des modifications inattendues dans AD DS qui affectent l'étendue de l'unité d'organisation ou le filtrage des attributs ;
 - Un AD DS endommagé qui nécessite une récupération du répertoire.

Il est très important que vous compreniez ce qui se passe lorsque vous désactivez puis réactivez la synchronisation dans le portail classique Azure. Lorsque la synchronisation d'annuaires est désactivée, la source de l'autorité est transférée de AD DS local à Azure AD. La désactivation est nécessaire lorsque AD DS local n'est plus utilisé pour créer et gérer des utilisateurs, des groupes, des contacts et des boîtes mails, comme après une migration Exchange progressive vers le cloud, lorsque l'organisation ne veut plus gérer des objets depuis l'environnement local. Des problèmes peuvent ensuite survenir si la synchronisation d'annuaires est alors réactivée, avec la source de l'autorité transférée de Azure AD à AD DS local.

Par exemple, supposons qu'une organisation a activé la synchronisation d'annuaires en janvier puis a créé de nouveaux utilisateurs locaux, qui se sont synchronisés avec Azure AD. Dans ce cas, la source de l'autorité est AD DS local. En juillet, l'organisation a désactivé la synchronisation d'annuaires, ce qui entraîne le transfert de la source de l'autorité vers Azure AD ; à partir de ce moment, des objets ont été édités dans Azure AD. En septembre, la société a décidé de déployer AD FS et SSO. Pour répondre à cette exigence, la synchronisation d'annuaires a été réactivée, provoquant un nouveau transfert de la source de l'autorité vers AD DS local. Dans cet exemple, lorsque vous réactivez et exécutez la synchronisation d'annuaires, les modifications apportées aux objets Azure AD de juillet à septembre sont écrasées et perdues.



Lectures supplémentaires : Pour plus d'informations, consultez : « L'intégration de vos identités locales avec Azure Active Directory » sur : <http://aka.ms/cdm2kk>

Mise à jour de la synchronisation d'annuaires

Il est important d'utiliser la dernière version de l'outil de synchronisation d'annuaires. Lors de la mise à niveau vers une nouvelle version de l'outil de synchronisation d'annuaires, des filtres existants et d'autres personnalisations d'agent de gestion peuvent ne pas s'importer automatiquement dans la nouvelle installation. Si vous mettez à niveau vers une version plus récente de synchronisation d'annuaire, vous devez toujours réappliquer manuellement les configurations de filtrage après mise à niveau, mais avant de lancer le premier cycle de synchronisation.

Gestion du service de synchronisation

Pour vérifier s'il n'y a pas de problèmes avec l'outil de synchronisation d'annuaires, vous devez ouvrir le **Synchronisation Service Manager** dans le groupe **Azure AD Connect** dans le menu **Démarrer**.

Dans l'application, vous devez consulter l'onglet **Opérations**. Sur cet onglet, vous pouvez confirmer que les opérations suivantes ont été complétées avec succès :

- L'importation sur le connecteur AD ;
- L'importation sur le connecteur Azure AD ;
- La synchronisation complète sur le connecteur AD ;
- La synchronisation complète sur le connecteur Azure AD.

Passez en revue le résultat de ces opérations pour valider l'état de la synchronisation d'annuaires et pour identifier les erreurs.

Par défaut, ces opérations sont programmées pour s'exécuter une fois toutes les trois heures. Si vous ne voulez pas attendre aussi longtemps pour résoudre un problème, utilisez la procédure suivante pour forcer une synchronisation manuelle :

1. Ouvrez l'outil **Azure AD Connect** dans le menu **Démarrer**.
2. Fournissez les informations demandées sur les pages de l'assistant (vous devez pouvoir accepter les paramètres par défaut si l'outil a déjà été déployé).
3. Sur la page **Configurer**, sélectionnez l'option **Démarrer le processus de synchronisation dès que la configuration initiale est terminée**, puis cliquez sur **Terminer**.



Lectures supplémentaires : Pour plus d'informations, consultez : « Comment résoudre les erreurs dans l'installation de l'outil de synchronisation Azure Active Directory et dans l'Assistant de configuration » sur : <http://aka.ms/bz5cjw>

Testez vos connaissances

| Question | |
|---|------------------------------|
| Si vous voulez disposer de l'authentification unique à la fois pour les services basés dans le cloud et sur site, que vous faut-il déployer ? Choisissez toutes les réponses applicables. | |
| Sélectionnez la réponse correcte. | |
| | Intégrité d'AD Azure Connect |
| | AD FS |
| | Azure AD Connect |
| | Office 365 |
| | Azure AD : |

Question : Vérifiez l'exactitude de la déclaration en plaçant une marque dans la colonne à droite.

| Déclaration | Réponse |
|--|---------|
| Si vous appliquez AD FS et une fédération entre AD DS et Azure AD déployés localement, alors vous n'avez pas besoin d'utiliser Azure AD Connect. | |

Atelier pratique : Configuration de la synchronisation des annuaires

Scénario

Dans le cadre de la phase de preuve de concept, votre équipe doit configurer et tester la synchronisation entre AD DS local et Azure AD. Vous devez préparer AD DS pour la synchronisation l'annuaire, installer et exécuter Azure AD Connect, puis vérifier que les annuaires se synchronisent.

Objectifs

À la fin de cet atelier pratique, vous allez pouvoir effectuer les tâches suivantes :

- Préparer un domaine AD DS local pour la synchronisation d'annuaires ;
- Installer et configurer la synchronisation d'annuaires avec Azure AD Connect ;
- Gérer les comptes d'utilisateurs et de groupes en utilisant la synchronisation d'annuaires.

Configuration de l'atelier pratique

Durée approximative : **60 minutes**

Ordinateurs virtuels. **22742A-LON-DC1**, **22742A-LON-DC2**, **22742A-LON-SVR1** et **22742A-LON-CL1**

Accès Internet : **MSL-tmg1**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa55w.rd**

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V Microsoft, cliquez sur **22742A-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 : **Pa55w.rd**
5. Répétez les étapes 2 à 4 pour les ordinateurs virtuels **22742A-LON-DC2**, **22742A-LON-SVR1** et **22742A-LON-CL1**.
6. Pour l'accès à Internet, vous avez également besoin de démarrer **MSL-TMG1**.

Cet atelier pratique requiert un Pass Microsoft Azure pour activer votre abonnement d'essai. Votre instructeur fournit le Pass Azure et entre les détails nécessaires à la réalisation de l'atelier pratique.

Exercice 1 : Préparation de la synchronisation des annuaires

Scénario

Avant de configurer la synchronisation d'annuaire, vous devez créer votre client Azure AD. Dans cet exercice, vous allez créer les comptes requis et créer un nouveau client Azure AD.

Les tâches principales de cet exercice sont les suivantes :

1. Créer un compte Microsoft ;
2. Créer un abonnement d'évaluation Azure ;
3. Créer un client Azure AD.

► Tâche 1 : Créer un compte Microsoft

D'autres tâches dans ce Microsoft Office 365 exigent un compte Microsoft actif sans abonnement Azure attribué à celui-ci. Si vous ne voulez pas utiliser votre compte Microsoft privé, si vous ne possédez pas de compte ou si vous avez déjà un abonnement Azure, veuillez suivre les étapes de cette tâche pour créer un nouveau compte Microsoft.

1. Dans **LON-CL1**, démarrez **Internet Explorer**, puis accédez à www.live.com.
2. Cliquez sur le lien « **Créer un compte** », puis utilisez l'assistant pour créer un nouveau compte Microsoft.
3. Lorsque vous avez terminé, fermez Internet Explorer.



Remarque : Assurez-vous que vous écrivez le nom d'utilisateur que vous avez choisi.

Par exemple, vous pouvez choisir un nom d'utilisateur dans le format *VosInitiales-
Date@outlook.com*, par exemple **JB-080615@outlook.com**. Utilisez **Pa55w.rd1** comme mot de passe. Nous vous recommandons de saisir votre adresse e-mail professionnelle dans la zone de texte **Autre adresse de messagerie**.

► Tâche 2 : Créer un abonnement d'évaluation Azure.

1. Sur **LON-CL1**, ouvrez **Internet Explorer** et accédez à la page Web **Try Microsoft Azure Pass** à l'adresse <http://aka.ms/cu92vo>.
2. Sélectionnez votre pays/région, puis utilisez le bon Azure que l'instructeur vous a fourni pour activer l'abonnement d'essai Azure.
3. Sur la page **Se connecter**, utilisez l'ID d'utilisateur que vous avez configuré dans la tâche précédente ou utilisez votre compte Microsoft personnel.
4. Attendez quelques minutes jusqu'à la création de votre abonnement Azure, puis vérifiez qu'un nouveau portail Azure s'ouvre. Vous pouvez cliquer sur le portail pour voir les options disponibles, mais n'apportez pas de modifications.
5. Fermez le navigateur Internet Explorer.

► Tâche 3 : Créer un client Azure AD

1. Sur **LON-CL1**, ouvrez **Internet Explorer** et accédez à <https://manage.windowsazure.com>.
2. Utilisez le compte Microsoft que vous avez utilisé dans la tâche précédente pour créer votre abonnement d'essai Azure pour vous connecter.
3. Lorsque le Portail Azure Classic s'ouvre, accédez à **ACTIVE DIRECTORY**, puis créez un nouveau répertoire :
 - NOM : **Adatum**
 - NOM DE DOMAINE : Utilisez vos initiales avec Adatum et des chiffres aléatoires (par exemple, « DDA datum111 ») pour créer le nom de domaine; si vous recevez un message **Déjà inscrit dans un autre répertoire**, changez les chiffres jusqu'à ce que vous receviez une coche verte.



Remarque : À partir d'ici, tout au long du cours, vous devez utiliser ce nom lorsque vous voyez la variable *nomdevotredomaine* dans les ateliers pratiques.

- PAYS OU RÉGION : **États-Unis**

Résultats : À la fin de cet exercice, vous devez avoir créé le client Azure AD.

Exercice 2 : Configuration de la synchronisation des annuaires

Scénario

Maintenant que l'environnement est préparé pour la synchronisation d'annuaire, l'étape suivante consiste à installer et à configurer l'outil Azure AD Connect et configurer une synchronisation initiale.

Les tâches principales de cet exercice sont les suivantes :

1. Configurer le compte de synchronisation et ajouter un domaine à Azure ;
2. Installer et configurer Azure AD Connect ;
3. Vérifier la synchronisation initiale et gérer des paramètres.

► Tâche 1 : Configurer le compte de synchronisation et ajoutez un domaine à Azure



Remarque : En raison de l'importance de la configuration des prochaines étapes correctement, ces étapes de haut niveau sont une copie des étapes détaillées dans le corrigé de l'atelier pratique.

1. Sur votre machine hôte, sur l'écran Démarrer, cliquez sur **Internet Explorer**.
2. Dans la barre d'adresses, tapez <https://manage.windowsazure.com>, puis appuyez sur Entrée.
3. Sur la page **Microsoft Azure**, cliquez sur **Utiliser un autre compte**.
4. Sur la page **Microsoft Azure**, saisissez votre compte Microsoft qui est associé à votre abonnement Azure, puis cliquez sur **Continuer**.
5. Connectez-vous à Azure en utilisant le compte Microsoft qui est associé à votre abonnement d'évaluation. Il s'agit du compte que vous aviez utilisé dans l'exercice 1 pour créer votre abonnement Azure.
6. Dans le portail classique Azure, cliquez sur l'instance d'annuaire **Adatum**.

7. Cliquez sur l'onglet **UTILISATEURS**, puis sur **AJOUTER UN UTILISATEUR**.
8. Dans la liste **TYPE D'UTILISATEUR**, cliquez sur **Nouvel utilisateur dans votre organisation**.
9. Dans la zone de texte **NOM D'UTILISATEUR**, saisissez **Sync**.



Remarque : Notez le nom complet de l'utilisateur. Il s'agit du **NOM D'UTILISATEUR** ainsi que le suffixe qui apparaît à droite du signe (@), tel que Sync@votredomaine.onmicrosoft.com.

10. Cliquez sur **Suivant**.
11. Sur la page **profil utilisateur**, dans la zone de texte de **NOM D'AFFICHAGE**, saisissez **SYNC**.
12. Dans la liste **RÔLE**, cliquez sur **Administrateur général**.
13. Dans la zone de texte **AUTRE ADRESSE DE MESSAGERIE**, saisissez votre propre adresse e-mail, puis cliquez sur **Suivant**.
14. Cliquez sur **Créer**.
15. Notez le mot de passe temporaire qui s'affiche.
16. Cliquez sur **Terminé**.
17. Fermez Internet Explorer, puis rouvrez-le.
18. Dans la barre d'adresses, tapez <https://manage.windowsazure.com>, puis appuyez sur Entrée.
19. Cliquez sur **Utiliser un autre compte**.
20. Saisissez le nom d'utilisateur pour l'utilisateur **SYNC** que vous avez enregistré précédemment. Il s'agit de **SYNC@votredomaine.onmicrosoft.com**. Cliquez sur **Continuer**
21. Saisissez le mot de passe temporaire que vous avez noté lors de la création de votre compte de synchronisation, puis cliquez sur **Se connecter**.
22. Lorsque vous êtes invité, saisissez votre ancien mot de passe que vous avez saisi à l'étape 21, dans la zone de texte **Ancien mot de passe**, puis dans les zones de texte **Nouveau mot de passe** et **Confirmer le mot de passe**, saisissez **Pa55w.rd**, puis cliquez sur **Mettre à jour le mot de passe et se connecter**.
23. Si vous êtes invité à vous connecter de nouveau sur le portail, utilisez les informations d'identification du compte **SYNC** et le mot de passe **Pa55w.rd**. Vous allez recevoir un message stipulant qu'aucun abonnement n'est trouvé.
24. Fermez et rouvrez Internet Explorer.
25. Dans la barre d'adresses, tapez <https://manage.windowsazure.com>, puis appuyez sur Entrée.
26. Connectez-vous à Azure en utilisant le compte Microsoft qui est associé à votre abonnement d'évaluation. Le compte doit figurer dans la liste.
27. Dans le portail classique Azure, cliquez sur **Adatum**. La page **COMMENCER** se charge.
28. Cliquez sur **Ajouter un domaine**.
29. Dans l'**Assistant AJOUTER UN DOMAINE**, dans la zone de texte **NOM DE DOMAINE**, saisissez **Adatum.com**, cliquez sur **ajouter**, puis sur **Suivant**.
30. Sur la page **Vérifier Adatum.com**, cliquez sur **Terminer** (l'icône en forme de coche).
31. Réduisez la fenêtre **Internet Explorer**.

► Tâche 2 : Installer et configurer Azure AD Connect

En raison de l'importance de la configuration des prochaines étapes correctement, ces étapes de haut niveau sont une copie des étapes détaillées dans le corrigé de l'atelier pratique.

1. Sur **LON-SVR1**, connectez-vous en tant qu'**Adatum\Administrateur**.
2. Ouvrez **Internet Explorer**, puis accédez à <http://www.microsoft.com/en-us/download/details.aspx?id=47594>.
3. Sur la page **Microsoft Azure Active Directory Connect**, cliquez sur **Télécharger**, puis sur **Exécuter**.



Remarque : Si vous rencontrez des problèmes pour lancer le téléchargement, ajoutez le site **Webhttps://download.microsoft.com** à vos sites de confiance.

4. Dans l'**Assistant Microsoft Azure Active Directory Connect**, sur la page **Bienvenue sur Azure AD Connect**, activez la case à cocher **Je suis d'accord avec les termes de la licence et la déclaration de confidentialité**, puis cliquez sur **Continuer**.
5. Sur la page **Configuration rapide**, cliquez sur **Utiliser la configuration rapide**.
6. Sur la page **Connexion à Azure AD**, dans la zone de texte **NOM D'UTILISATEUR**, saisissez le nom de compte utilisateur **SYNC**. Dans la zone de texte **MOT DE PASSE**, tapez **Pa55w.rd**, puis cliquez sur **Suivant**.
7. Sur la page **Connexion à Azure AD**, dans la zone de texte **NOM D'UTILISATEUR**, saisissez **Adatum\administrateur**. Dans la zone **MOT DE PASSE**, tapez **Pa55w.rd**, puis cliquez sur **Suivant**.
8. Sur la page **Configuration de la connexion à Azure AD**, activez la case à cocher à côté de **Continuer sans aucun domaine vérifié**, puis cliquez sur **Suivant**.
9. Cliquez **Installer**. Lorsque l'installation est terminée, cliquez sur **Quitter**.
10. À ce moment, la synchronisation des objets à partir de votre AD DS local et Azure AD commence. Vous devez attendre environ 10 minutes pour que ce processus se termine.
11. Fermez la fenêtre Internet Explorer sur **LON-SVR1**.

► Tâche 3 : Vérifier la synchronisation initiale et gérer les paramètres

1. Basculez vers Internet Explorer sur votre ordinateur hôte.
2. Sur la page **annuaire** dans le Portail Azure Classic, cliquez sur l'onglet **UTILISATEURS**.
3. Vérifiez que vous pouvez voir les comptes d'utilisateurs de vos AD DS locaux.
4. Basculez vers **LON-SVR1**.
5. Ouvrez **Synchronization Service Manager**, puis basculez vers l'onglet **Opérations**.
6. Assurez-vous que vous voyez les tâches **Exporter**, **Synchronisation complète** et **Importation complète**.
7. Assurez-vous que toutes les tâches indiquent une heure et une date dans actuelles les colonnes **Heure de début** et **Heure de fin**. En outre, assurez-vous que toutes les tâches sont classées sous succès dans la colonne **Statut**.
8. Sur **LON-SVR1**, ouvrez **Windows PowerShell**.
9. Utilisez l'applet de commande **Get-ADSyncScheduler** pour examiner les paramètres de synchronisation.
10. Utilisez l'applet de commande **Set-ADSyncScheduler -CustomizedSyncCycleInterval** pour définir l'intervalle de synchronisation sur **1 heure**.

11. Utilisez l'applet de commande **Start-ADSyncSyncCycle -PolicyType Delta** pour démarrer la synchronisation manuellement.
12. Utilisez l'applet de commande **Get-ADSyncScheduler** pour examiner les nouveaux paramètres de synchronisation.

Résultats : À la fin de cet exercice, vous devez avoir installé Azure AD Connect avec des paramètres personnalisés, terminé la synchronisation d'annuaires pour Azure AD et vérifié que la synchronisation est réussie.

Exercice 3 : Gestion des utilisateurs et des groupes Active Directory

Scénario

Maintenant que la synchronisation d'annuaire est en place et fonctionne, vous devez identifier la façon dont la gestion des comptes d'utilisateur et de groupe a changé avec la synchronisation d'annuaire.

Les tâches principales de cet exercice sont les suivantes :

1. Ajouter de nouveaux objets dans AD DS ;
2. Vérifier la synchronisation des nouveaux objets USER ;
3. Préparer le module suivant.

► Tâche 1 : Ajouter de nouveaux objets dans AD DS

1. Sur **LON-DC1**, ouvrir **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'**UO Sales**, créez un nouveau compte d'utilisateur avec votre nom.
3. Ajoutez le nouveau compte d'utilisateur au groupe **Sales**.

► Tâche 2 : Vérifier la synchronisation des nouveaux objets User

1. Sur **LON-SVR1**, ouvrez **Windows PowerShell** en mode **Administrateur**.
2. Forcez la synchronisation delta en exécutant la commande **Start-ADSyncSyncCycle**.
3. Ouvrez le Portail Azure Classic, puis vérifiez que le nouvel utilisateur créé dans les tâches précédentes apparaît dans l'onglet **UTILISATEURS** et dans le groupe **Ventes**.

Résultats : Après avoir terminé cet exercice, vous devriez avoir identifié la façon dont la gestion des comptes d'utilisateur et de groupe a changé avec la synchronisation d'annuaire.

► Tâche 3 : Préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour rétablir **22742A-LON-DC2**, **22742A-LON-SVR1** et **22742A-LON-CL1**.

Question : Que devez-vous faire avant de commencer à configurer Azure AD Connect ?

Question : Quel applet de commande devez-vous utiliser pour modifier le calendrier de synchronisation pour Azure AD Connect ?

Contrôle des acquis et éléments à retenir

Enjeux et scénarios du monde réel

Étant donné que la synchronisation d'annuaire est le lien entre vos objets AD DS sur site et les services dans Azure AD, soyez prudent lorsque vous modifiez Azure AD Connect ou Synchronization Service Manager après le déploiement de production. Par exemple, une erreur mineure dans le filtrage pourrait accidentellement supprimer toutes les boîtes aux lettres utilisateur dans Office 365.

Dans certains environnements, par exemple, dans un environnement de test, vous pouvez tester toutes les modifications sur un serveur de synchronisation de répertoire distinct qui est connecté à un client Azure AD séparé (essai). En outre, vous devez lancer manuellement les profils gérés pour chaque agent de gestion de Synchronization Service Manager et observez les actions en suspens avant d'exporter vers Azure AD. Dans certains cas, ce serait une bonne idée de créer un nouveau profil d'exécution pour l'exportation vers Azure AD qui comprend une limite maximale du nombre de suppressions permises.

Question de contrôle des acquis

Question : Quelle fonctionnalité devez-vous configurer de sorte que les objets se synchronisent depuis Azure AD à votre AD DS sur site ?

Outils

Le tableau suivant répertorie les outils référencés par ce module :

| Outil | Utilisation | Emplacement |
|------------------------------|---|---|
| Azure AD Connect | Établissement d'une synchronisation entre AD DS et Azure AD | Centre de téléchargement Microsoft |
| Intégrité d'AD Azure Connect | Surveillance de l'état de synchronisation entre AD DS et Azure AD | Le portail classique Azure |
| Le portail classique Azure | Gestion d'Azure AD | http://aka.ms/n2l3cb |

Meilleures Pratiques

- Pour les environnements simples, utilisez la configuration rapide d'Azure AD Connect.
- Permettez aux utilisateurs d'utiliser la fonctionnalité de réinitialisation de mot de passe en libre-service avec au moins deux méthodes d'authentification.
- Pensez à utiliser les fonctionnalités de réécriture.
- Implémentez Azure AD Connect Health si vous avez un abonnement premium à Azure AD.

Problèmes courants et conseils de résolution des problèmes

| Problème courant | Conseil pour la résolution du problème |
|---|--|
| Le filtrage de synchronisation d'annuaire ne fonctionne plus. | |
| Après avoir installé Azure AD Connect, vous pouvez recevoir une invite avec le message d'erreur suivant lorsque vous ouvrez Synchronization Service Manager : Impossible de se connecter au service de synchronisation. | |

Module 13

Surveillance, gestion et récupération de AD DS

Sommaire :

| | |
|--|-------|
| Vue d'ensemble du module | 13-1 |
| Leçon 1 : Surveillance de AD DS | 13-2 |
| Leçon 2 : Gestion de la base de données Active Directory | 13-12 |
| Leçon 3 : Sauvegarde de Active Directory et options de récupération pour AD DS et autres solutions d'identité et d'accès | 13-19 |
| Atelier pratique : Récupération d'objets dans AD DS | 13-28 |
| Contrôle des acquis et éléments à retenir | 13-33 |

Vue d'ensemble du module

En tant que responsable professionnel de la technologie de l'information (IT) prenant en charge le système d'exploitation Windows Server et les services de domaine Active Directory (AD DS), le maintien de l'intégrité de votre domaine est un aspect essentiel de votre travail. Dans ce module, vous apprendrez tout sur les technologies et les outils disponibles pour vous aider à assurer l'intégrité et la fiabilité de AD DS. Vous explorerez des outils qui vous aident à surveiller les performances en temps réel et vous apprendrez à enregistrer les performances au fil du temps pour repérer les problèmes potentiels en observant les tendances des performances. Vous apprendrez également comment optimiser et protéger votre service d'annuaire et les solutions d'identité et d'accès connexes pour pouvoir redémarrer le plus rapidement possible en cas de défaillance d'un service.

Objectifs

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

- Surveiller AD DS ;
- Gérer la base de données Active Directory ;
- Décrire les options de sauvegarde et de récupération pour AD DS et autres solutions d'accès d'identité.

Leçon 1

Surveillance de AD DS

Les problèmes de performance sont fréquents dans les environnements du monde réel. Par conséquent, vous devez savoir comment analyser, évaluer et résoudre ces problèmes. Dans cette leçon, vous apprendrez à utiliser les outils de surveillance de la performance et des événements dans Windows Server pour surveiller l'intégrité de vos contrôleurs de domaine et de AD DS.

Objectifs de la leçon

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

- Décrire le suivi des performances et expliquer les goulots d'étranglement en lien avec la performance ;
- Décrire les outils de surveillance dans le système d'exploitation Windows Server ;
- Décrire comment utiliser l'Analyseur de performances pour surveiller les performances enregistrées et en temps réel ;
- Décrire comment utiliser les ensembles de collecteurs de données pour surveiller les performances ;
- Expliquer comment surveiller un contrôleur de domaine en utilisant l'Analyseur de performances.

Comprendre les performances et les goulots d'étranglement

Les mauvaises performances du système de contrôleur de domaine peuvent être attribuées à des ressources système insuffisantes. Les quatre ressources clés du système sont l'unité centrale (CPU), le sous-système de disque, la mémoire et le réseau. L'identification et la résolution des goulots d'étranglement impliquent un examen minutieux des journaux système et des compteurs de performance pour déterminer quelle ressource est actuellement limitée. Après l'augmentation de cette ressource, la performance sera améliorée, mais elle pourra stagner à un certain niveau quand elle rencontrera un nouveau goulot d'étranglement dans une autre ressource du système.

- Un *goulot d'étranglement* est une ressource qui fonctionne au maximum de sa capacité
- Ressources clés du système :
 - Processeur ;
 - Disque ;
 - Mémoire ;
 - Réseau.

Analyse des principaux composants matériels

Pour optimiser les performances du serveur, vous devez comprendre comment votre système d'exploitation interagit avec les composants matériels suivants :

- Le processeur. La vitesse du processeur est un facteur important dans la détermination de la capacité globale de traitement de votre serveur. Le nombre d'opérations que l'unité centrale effectue dans une période donnée détermine la vitesse du processeur. Les serveurs équipés de plusieurs processeurs ou de processeurs à plusieurs cœurs exécutent généralement les tâches qui sollicitent beaucoup le processeur avec une plus grande efficacité. Ils sont souvent plus rapides que les ordinateurs équipés d'un processeur unique ou de processeurs à cœur unique. Les contrôleurs de domaine n'exigent généralement pas une performance de processeur plus élevée, mais la performance du processeur peut être importante si votre contrôleur de domaine exécute également d'autres rôles.

- Le disque. Les disques durs stockent des données et des programmes. Par conséquent, le *débit* des disques (la quantité totale de données que le sous-système de disque traite pour chaque unité de temps) affecte la vitesse d'un poste de travail ou d'un serveur, en particulier lorsque le serveur exécute des tâches sollicitant fortement les disques, telles que la restauration de la base de données AD DS ou la réPLICATION d'une grande quantité de données AD DS dans la base de données. Les disques durs ont des composants mobiles, et le positionnement des têtes de lecture et d'écriture sur la partie appropriée du disque pour récupérer les informations demandées peut prendre du temps.

 **Remarque :** La *charge de travail* est le nombre de demandes disque de traitement de tâche que le sous-système de disque exécute dans un temps donné.

Vous pouvez réduire les goulots d'étranglement potentiels du sous-système de disque en sélectionnant des disques plus rapides et en utilisant des collections de disques tels que des contrôleurs RAID ou des espaces de stockage qui optimisent les temps d'accès. Rappelez-vous que les informations sur les disques se déplacent sur la mémoire avant que le système d'exploitation ne les utilise. S'il y a un excédent de mémoire, le système d'exploitation Windows Server crée un cache de fichier pour les éléments récemment écrits ou lus à partir des disques. L'installation d'une mémoire supplémentaire sur un serveur peut souvent améliorer les performances du sous-système de disque, car l'accès au cache est plus rapide que le déplacement des informations sur la mémoire.

- La mémoire. Les programmes et les données sont chargés depuis le disque dans la mémoire avant que le programme ne traite les données. Vous pouvez augmenter la quantité de mémoire pour améliorer les performances du serveur dans les serveurs qui exécutent plusieurs programmes, ou lorsque les ensembles de données sont extrêmement grands.

Windows Server utilise un modèle de mémoire dans lequel les demandes de mémoire excessives ne sont pas rejetées, mais sont gérées par un processus connu sous le nom de *pagination*. Pendant la pagination, les données et les programmes en mémoire, qui ne sont pas actuellement utilisés par les processus, sont déplacés dans une zone sur le disque dur, connue sous le nom de *fichier de pagination*. Cela libère de la mémoire physique pour satisfaire les demandes excessives, mais cela a un effet négatif sur les performances du poste de travail, car un disque dur est relativement lent. En ajoutant plus de mémoire, vous pouvez réduire le besoin de pagination.

- Le réseau. Il est courant de sous-estimer l'impact d'un réseau peu performant, car il n'est pas aussi facile à voir ou à mesurer que dans le cas des trois autres composants. Cependant, le réseau est un élément essentiel pour la surveillance des performances, car AD DS est un service réseau qui nécessite une connectivité réseau fiable entre les serveurs et les clients.

Vue d'ensemble des outils de surveillance

Vous pouvez utiliser plusieurs outils dans Windows Server pour divers types de surveillance. La plupart de ces outils sont disponibles par défaut en tant que composants de Windows Server. Vous pouvez les utiliser pour une surveillance en temps réel et historique de AD DS et d'autres services. Les outils les plus couramment utilisés sont le Gestionnaire des tâches, le Moniteur de ressources, l'Observateur d'événements et l'Analyseur de performances.

Windows Server fournit les outils suivants pour aider en cas de problèmes de performance de surveillance :

- Gestionnaire des tâches ;
- Moniteur de ressources ;
- Observateur d'événements ;
- Analyseur de performances ;
- Windows PowerShell.

Gestionnaire des tâches

Le Gestionnaire des tâches fournit des informations pour vous aider à identifier et résoudre les problèmes liés à la performance dans Windows Server. L'interface utilisateur (IU) du Gestionnaire des tâches comprend les onglets suivants :

- **Processus.** L'onglet **Processus** affiche la liste des programmes en cours d'exécution, subdivisés en processus d'arrière-plan et en processus Windows internes. Pour chaque processus en cours d'exécution, cet onglet affiche un résumé de l'utilisation du processeur et de la mémoire.
- **Performance.** L'onglet **Performance** affiche un résumé de l'utilisation du processeur et de la mémoire, ainsi que des statistiques réseau.
- **Utilisateurs.** L'onglet **Utilisateurs** affiche la consommation de ressources par utilisateur. Vous pouvez également développer la vue Utilisateur pour afficher des informations plus détaillées sur les processus spécifiques exécutés par un utilisateur.
- **Détails.** L'onglet **Détails** répertorie toutes les tâches en cours d'exécution sur le serveur et fournit des statistiques sur la consommation du processeur, de la mémoire et sur toute autre consommation de ressources. Vous pouvez utiliser cet onglet pour gérer les tâches en cours d'exécution. Vous pouvez par exemple arrêter seulement un processus, arrêter un processus et tous les processus associés ou modifier les valeurs de priorité des processus. En modifiant la priorité d'un processus, vous déterminez sa consommation de ressources de processeur. En augmentant la priorité, vous autorisez le processus à demander plus de temps processeur.
- **Prestations de service.** L'onglet **Services** fournit une liste des services Windows en cours d'exécution ainsi que des informations connexes. Il indique par exemple si le service est en cours d'exécution, ainsi que la valeur de l'identifiant de processus (PID) du service en cours d'exécution. Vous pouvez démarrer et arrêter des services en utilisant la liste située dans l'onglet **Services**.

De manière générale, pensez à utiliser le Gestionnaire des tâches lorsqu'un problème lié aux performances se produit pour la première fois. Par exemple, vous pouvez examiner les tâches en cours d'exécution pour déterminer si un programme particulier utilise des ressources de processeur excessives. Gardez toujours à l'esprit que le Gestionnaire des tâches affiche une capture instantanée de la consommation de ressources actuelle, et que vous pouvez également être amené à examiner les données d'historique pour avoir une idée précise des performances et de la réponse sous la charge d'un serveur.

Moniteur de ressources

Le moniteur de ressources permet d'examiner de manière approfondie la performance en temps réel de votre serveur. Utilisez-le pour analyser en temps réel l'utilisation et les performances des ressources de l'UC, du disque, du réseau et de la mémoire. Grâce à lui, vous pouvez identifier les conflits de ressources et les goulets d'étranglement afin de les résoudre.

En développant les éléments analysés, les administrateurs système peuvent identifier les processus utilisant des ressources spécifiques. En outre, vous pouvez utiliser le Moniteur de ressources pour suivre un ou plusieurs processus en cochant les cases correspondantes. Lorsque vous sélectionnez un processus, il reste sélectionné en haut de l'écran dans chaque volet du Moniteur de ressources, qui fournit les informations dont vous avez besoin au sujet de ce processus où que vous soyez dans l'interface.

Observateur d'événements

L'Observateur d'événements fournit un accès aux journaux d'événements de Windows Server. Les *journaux d'événements* sont les journaux qui fournissent des informations sur les événements système qui se produisent dans le système d'exploitation Windows. Ces événements comprennent les messages d'information, d'avertissement et d'erreur sur les composants Windows et les applications.

L'Observateur d'événements fournit des listes de catégorie des événements essentiels du journal Windows, y compris les événements d'application, de sécurité, de configuration et système, ainsi que des groupements de journaux pour les applications individuelles et des catégories de composants spécifiques Windows. Les événements individuels fournissent des informations détaillées concernant le type d'événement qui s'est produit, la date à laquelle l'événement s'est produit, la source de l'événement, ainsi que des informations détaillées pour vous aider à résoudre l'événement.

En outre, l'Observateur d'événements vous permet de consolider les journaux de plusieurs ordinateurs sur un ordinateur centralisé à l'aide d'abonnements. Enfin, vous pouvez configurer l'Observateur d'événements pour effectuer une action basée sur un événement spécifique ou la surveillance d'événements multiples. Cela peut inclure l'envoi d'un message électronique, le lancement d'une application, l'exécution d'un script ou d'autres actions de maintenance qui peuvent vous informer d'un problème potentiel ou tenter de le résoudre.

L'Observateur d'événements de Windows Server contient les fonctionnalités importantes suivantes :

- La possibilité d'afficher plusieurs journaux. Vous pouvez filtrer des événements spécifiques dans plusieurs journaux, ce qui facilite l'examen et la résolution des problèmes susceptibles d'apparaître dans plusieurs journaux.
- L'inclusion des affichages personnalisés. Vous pouvez utiliser le filtrage pour limiter la recherche aux événements qui vous intéressent. Vous pouvez sauvegarder ces vues filtrées.
- La possibilité de configurer des tâches planifiées à exécuter en réponse à des événements. Vous pouvez automatiser les réponses aux événements. L'Observateur d'événements est intégré au Planificateur de tâches pour effectuer ces tâches.
- La capacité de créer et gérer des abonnements aux événements. Vous pouvez collecter des événements à partir d'ordinateurs distants et les enregistrer localement.



Remarque : Pour collecter des événements à partir d'ordinateurs distants, vous devez créer une règle entrante dans le Pare-feu Windows pour permettre la gestion du journal des événements Windows.

L'observateur d'événements suit les informations dans plusieurs journaux différents. Ces journaux fournissent des informations détaillées qui comprennent :

- Une description de l'événement ;
- Un numéro d'identification de l'événement ;
- Le composant ou sous-système qui a généré l'événement ;
- Le statut Information, Avertissement ou Erreur ;
- La date de l'occurrence ;
- Le nom de l'utilisateur au nom duquel l'événement est survenu ;
- L'ordinateur sur lequel l'événement s'est produit ;
- Un lien vers Microsoft TechNet pour obtenir des informations supplémentaires sur l'événement.

L'Observateur d'événements comporte plusieurs journaux intégrés, y compris ceux contenus dans le tableau suivant.

| Journal intégré | Description et utilisation |
|------------------------|---|
| Journal d'application | Ce journal contient les erreurs, avertissements et événements d'information qui concernent le fonctionnement des applications telles que Microsoft Exchange Server. |
| Journal de sécurité | Ce journal enregistre les résultats de l'audit, si vous l'activez. Les événements d'audit sont décrits comme ayant réussi ou échoué, selon l'événement. Par exemple, le journal enregistre les succès ou les échecs de l'accès d'un utilisateur à un fichier. |
| Journal d'installation | Ce journal contient les événements relatifs à la configuration des composants du système d'exploitation. |
| Journal système | Les événements généraux sont enregistrés par les composants et services Windows, et sont classés en tant qu'erreur, avertissement ou information. Windows prédétermine les événements enregistrés par les composants système. |
| Événements transférés | Par défaut, ce journal enregistre les événements collectés à partir d'ordinateurs distants. Pour collecter des événements à partir d'ordinateurs distants, vous devez créer un abonnement aux événements. |

Analyseur de performances

Avec l'Analyseur de performances, vous pouvez voir les performances du système dans un rapport ou sous forme de graphique. Il peut surveiller les logiciels et composants matériels en temps réel et dans l'historique. Cet outil est expliqué plus en détail dans la rubrique suivante.

Windows PowerShell

Vous pouvez utiliser les applets de commande dans l'interface de ligne de commande Windows PowerShell pour surveiller les performances du serveur. Par exemple, vous pouvez utiliser la commande suivante pour récupérer les valeurs regroupées du % **temps processeur** pour tous les processeurs sur l'ordinateur local toutes les deux secondes jusqu'à ce qu'il obtienne 100 valeurs et affiche les données capturées :

```
Get-counter -Counter "\Processor(_Total)\% Pourcentage de temps processeur" -SampleInterval 2 -MaxSamples 100
```



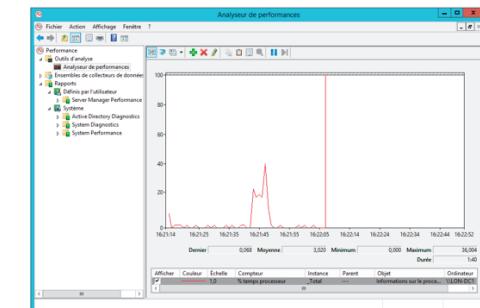
Lectures supplémentaires : Pour plus d'informations, consultez : « Utilisation de PowerShell pour recueillir des données de performance » à l'adresse : <http://aka.ms/F8mxnr>

Qu'est-ce que l'Analyseur de performances ?

Vous pouvez utiliser l'Analyseur de performance pour afficher les statistiques de performance actuelles ou les données d'historique recueillies en utilisant des ensembles de collecteurs de données. Avec Windows Server, vous pouvez surveiller les performances du système d'exploitation grâce à des objets de performance et des compteurs dans les objets. Windows Server collecte des données en provenance des compteurs sous différentes formes, notamment :

- Un aperçu en temps réel ;
- Le total depuis le dernier démarrage de l'ordinateur ;
- Une moyenne sur un intervalle de temps spécifique ;
- Une moyenne des valeurs ;
- Le nombre par seconde ;
- Une valeur maximum ;
- Une valeur minimum.

Vous pouvez utiliser l'Analyseur de performance pour afficher les statistiques de performance actuelles ou les données historiques recueillies en utilisant des ensembles de collecteurs de données



L'Analyseur de performance fonctionne en vous offrant une collection d'objets et de compteurs qui enregistrent les données d'utilisation des ressources de l'ordinateur. Vous pouvez chercher et examiner beaucoup de compteurs pour répondre à vos besoins spécifiques.

Compteurs du processeur principaux

Les compteurs du CPU, une caractéristique du CPU de l'ordinateur, stockent le nombre d'événements liés au matériel. Les compteurs du processeur principaux comprennent :

- Processeur > % temps processeur. Ce compteur mesure le pourcentage de temps que le processeur utilise pour exécuter un *thread* actif. En d'autres termes, ce compteur affiche le pourcentage du temps d'un processeur qu'un *thread* donné utilise pour exécuter des *instructions*. (Une *instruction* est l'unité de base de l'exécution dans un processeur et un *thread* est l'objet qui exécute les instructions.) Si ce pourcentage est supérieur à 85 %, le processeur est surchargé et le serveur peut nécessiter un processeur plus rapide. Le code qui gère certaines interruptions matérielles et les conditions d'interruption est inclus dans ce compteur.
- Processeur > Interruptions/s. Ce compteur affiche le taux, en incidents par seconde, auquel le processeur a connu et géré des interruptions matérielles. Cette valeur est un indicateur indirect de l'activité des périphériques qui génèrent des interruptions, telles que l'horloge système, la souris, les pilotes de disque, les lignes de communication de données, les cartes d'interface réseau et d'autres périphériques. Normalement, ces périphériques interrompent le processeur quand ils ont terminé une tâche ou nécessitent votre attention. L'exécution normale du *thread* est suspendue.
- Système > Longueur de la file d'attente du processeur. Ce compteur affiche le nombre approximatif de threads dont chaque processeur s'occupe. Si la valeur est plus de deux fois le nombre de CPU sur un temps donné, le serveur n'a pas assez de puissance processeur. La longueur de la file du processeur (parfois appelée *profondeur de la file du processeur*) signalée par ce compteur est une valeur à un instant *t* qui représente seulement un instantané actuel du processeur. Par conséquent, vous devez observer ce compteur dans la durée pour observer les tendances des données. En outre, le

compteur Système > Longueur de la file du processeur rend compte d'une longueur de file d'attente totale pour tous les processeurs, et non d'une longueur pour chaque processeur.

Compteurs de mémoire principaux

L'objet de performances Mémoire se compose de compteurs qui décrivent le comportement de la mémoire physique et virtuelle de l'ordinateur. La *mémoire physique* est la quantité de mémoire vive (RAM) de l'ordinateur. La *mémoire virtuelle* se compose de l'espace dans la mémoire physique et sur le disque. La plupart des compteurs de mémoire surveillent la *pagination*, à savoir le mouvement des pages de code et de données entre le disque et la mémoire physique.

- Le compteur Mémoire > Pages/s mesure la fréquence à laquelle les pages sont lues ou écrites sur le disque pour résoudre les défauts de page matérielle. Une augmentation de ce compteur indique que la pagination est plus importante, ce qui suggère un manque de mémoire physique.

Compteurs de disque principaux

L'objet de performance Disque physique est constitué de compteurs qui surveillent les lecteurs de disques durs ou fixes. Les disques stockent des fichiers, des programmes et des données de pagination. Les disques sont lus pour récupérer ces éléments et sont écrits lors de l'enregistrement des modifications qui leur sont apportées. Les valeurs totales des compteurs de disque physique sont la somme de toutes les valeurs des disques ou des partitions logiques dans lesquels ils sont divisés. Les compteurs de disque principaux comprennent :

- Disque physique > % Temps du disque. Ce compteur indique comment un disque particulier est occupé et mesure le pourcentage de temps d'occupation du disque au cours de l'intervalle d'échantillonnage. Un compteur approchant 100 % indique que le disque est occupé presque tout le temps et que la survenance d'un goulot d'étranglement est peut-être imminente. Vous pouvez éventuellement remplacer le système de disque actuel par un autre plus rapide.
- Disque physique > Longueur moyenne de la file d'attente du disque. Ce compteur indique le nombre de demandes de disque en attente d'être traité par le gestionnaire entrée/sortie (E/S) dans Windows Server à un moment donné. Si cette valeur est plus de deux fois plus importante que le nombre de broches, le disque lui-même peut être engorgé. Plus la file d'attente est longue, moins le débit du disque est satisfaisant.

Compteurs du réseau principaux

La plupart des charges de travail nécessitent l'accès à des réseaux de production pour assurer la communication avec d'autres applications et services et la communication avec les utilisateurs. Les exigences du réseau comprennent des éléments tels que le débit et la présence de multiples connexions réseau.

Les charges de travail peuvent nécessiter l'accès à plusieurs réseaux différents qui doivent rester sécurisés. Par exemple, des connexions pour :

- Un accès au réseau public ;
- Des réseaux afin d'effectuer des sauvegardes et d'autres tâches de maintenance ;
- Des connexions dédiées gérées à distance ;
- Une association d'adaptateurs réseau pour la performance et le basculement ;
- Des connexions à l'ordinateur hôte physique ;
- Des connexions à des baies de stockage en réseau.

En surveillant les compteurs de performance du réseau, vous pouvez évaluer les performances de votre réseau. Les compteurs de réseau principaux comprennent :

- Interface réseau > Bande passante actuelle. Ce compteur indique la bande passante actuelle qui est consommée, sur l'interface réseau, en bits par seconde (bits/s). La plupart des topologies de réseau ont des bandes passantes potentielles maximales estimées en mégabits par seconde (Mbps). Par exemple, Ethernet peut fonctionner avec des bandes passantes de 10 Mbps, 100 Mbps, 1 gigabit par seconde (Gbps) et plus. Pour interpréter ce compteur, divisez la valeur donnée par 1 048 576 pour les Mbps. Si la valeur se rapproche de la bande passante potentielle maximale du réseau, vous devriez envisager la mise en place d'un réseau commuté ou la mise à niveau vers un réseau qui prend en charge des bandes passantes plus élevées.
- Interface réseau > Longueur de la file d'attente de sortie. Ce compteur indique la longueur actuelle de la file d'attente des paquets en sortie sur l'interface réseau sélectionnée. Une valeur croissante ou toujours supérieure à deux pourrait indiquer un goulot d'étranglement du réseau, que vous devriez examiner.
- Interface réseau > Total des octets/s. Ce compteur mesure la fréquence à laquelle les octets sont envoyés et reçus sur chaque adaptateur réseau, y compris les caractères de trame. Si plus de 70 % de l'interface est utilisée, le réseau est saturé.

Compteurs Active Directory principaux

Sur un contrôleur de domaine, vous devez également surveiller au moins les compteurs de performance suivants, exposés par l'objet Service d'annuaire Active Directory NT (NTDS).

Compteurs de l'Agent de réPLICATION d'annuaire (DRA)

- Total des octets entrants NTDS\DRa par sec. Ce compteur indique le nombre total d'octets répliqués dans la base de données AD DS.
- Objet entrant NTDS\DRa. Ce compteur indique le nombre d'objets Active Directory reçus de la part des voisins par la réPLICATION entrante.
- Total des octets sortants NTDS\DRa par sec. Ce compteur indique le nombre total d'octets répliqués en sortie.
- Synchronisations de réPLICATION NTDS\DRa en attente. Il s'agit du nombre de synchronisations d'annuaire qui sont en attente pour ce serveur, mais pas encore traitées.

Autres compteurs

- Statistiques de sécurité à l'échelle système\ authentifications Kerberos par sec. Ce compteur suit le nombre de fois où les clients utilisent un ticket pour s'authentifier sur cet ordinateur par seconde.
- Statistiques de sécurité à l'échelle système\ authentifications NTLM par sec. Ce compteur suit le nombre d'authentifications NTLM traitées par seconde.

Que sont les ensembles de collecteurs de données ?

Un ensemble de collecteurs de données est à la base de la surveillance des performances de Windows Server et des rapports dans l'Analyseur de performances. Vous pouvez utiliser les ensembles de collecteurs de données pour recueillir des informations liées à la performance et d'autres statistiques du système sur lesquelles vous pouvez effectuer une analyse avec des outils au sein de l'Analyseur de performances ou avec des outils tiers.

Bien qu'il soit utile de suivre les performances en cours sur un serveur, vous trouverez peut-être plus utile de recueillir des données de performance sur une période définie, puis de les analyser et de les comparer avec les données que vous avez collectées précédemment. Vous pouvez utiliser cette comparaison de données pour déterminer l'utilisation des ressources afin de planifier la croissance et pour identifier les problèmes potentiels de performance.

- Vous pouvez utiliser les ensembles de collecteurs de données pour recueillir des informations liées à la performance
- Les ensembles de collecteurs de données peuvent contenir les types de collecteurs de données suivants :
 - Compteurs de performance
 - Données de suivi d'événements
 - Informations de la configuration système

Les ensembles de collecteurs de données peuvent contenir les types de collecteurs de données suivants :

- Compteurs de performance. Ce collecteur de données fournit des données sur les performances du serveur.
- Données de suivi des événements. Ce collecteur de données fournit des informations sur les activités et les événements du système, ce qui est souvent utile pour la résolution des problèmes.
- Informations sur la configuration du système. Ce collecteur de données vous permet d'enregistrer l'état actuel des clés de registre et d'enregistrer les modifications apportées à ces clés.

Vous pouvez créer un ensemble de collecteurs de données à partir d'un modèle, à partir d'un ensemble existant de collecteurs de données présent dans l'Analyseur de performances ou en sélectionnant les collecteurs de données individuels et en réglant chaque option dans les propriétés de l'ensemble de collecteurs de données.

Démonstration : Surveillance de AD DS

Dans cette démonstration, vous apprendrez à :

- Configurer l'Analyseur de performances pour surveiller AD DS ;
- Créer un ensemble de collecteurs de données ;
- Démarrer un ensemble de collecteurs de données ;
- Analyser les données obtenues dans un rapport.

Étapes de la démonstration

Configurer l'analyseur de performances pour surveiller AD DS

1. Sur **LON-DC1**, ouvrez l'**Analyseur de performances**.
2. Ajouter les compteurs de performance d'objet suivants :
 - **DirectoryServices\Nb total d'octets DRA entrants/s**
 - **DirectoryServices\Nb total d'octets DRA sortants/s**

- **DirectoryServices\Nb de threads Active Directory utilisés**
 - **DirectoryServices\Lectures Active Directory/s.**
 - **DirectoryServices\Écritures Active Directory/s.**
 - **DirectoryServices\Recherches Active Directory/s.**
 - **NTDS\Nb d'objets DRA entrants/s.**
 - **NTDS\Nb de synchronisations de réPLICATION DRA en attente**
 - **Statistiques de sécurité système\authentifications NTLM**
 - **Statistiques de sécurité système\authentifications Kerberos**
3. Regardez la performance pendant quelques instants. Puis, dans la liste des compteurs en dessous du graphique, sélectionnez **Recherches Active Directory/s.**
 4. Dans la barre d'outils, cliquez sur **Surlignage** pour surligner **Recherches Active Directory/s.** dans le graphique. Puis cliquez **Surlignage** dans la barre d'outils pour désactiver le surlignage.

Créer un ensemble de collecteurs de données

1. Créez un nouvel Ensemble de collecteurs de données depuis la vue actuelle de l'Analyseur de performances.
2. Nommez l'Ensemble de collecteurs de données **Compteurs de performances ADDS personnalisés**.
3. Notez le répertoire racine par défaut dans lequel l'Ensemble de collecteurs de données sera sauvegardé.

Démarrer l'ensemble de collecteurs de données

1. Cliquez sur le nœud **Ensembles de collecteurs de données\Définis par l'utilisateur**, cliquez avec le bouton droit sur **Compteurs de performances ADDS personnalisés**, puis cliquez sur **Démarrer**. Le nœud Compteurs de performances ADDS personnalisés est sélectionné automatiquement.

 **Remarque :** notez que vous pouvez identifier les collecteurs de données individuels dans l'ensemble de collecteurs de données. Dans ce cas, un seul collecteur de données (le compteur de performances Journal de Moniteur système) est contenu dans l'ensemble de collecteurs de données. Vous pouvez également identifier l'emplacement d'enregistrement de la sortie du collecteur de données.

2. Dans l'arborescence de la console, cliquez avec le bouton droit sur l'ensemble de collecteurs de données **Compteurs de performance ADDS personnalisés**, puis cliquez sur **Arrêter**.

Analyser les données obtenues dans un rapport

- Dans l'arborescence de la console, depuis le nœud **Rapports\Définis par l'utilisateur**, développez **Compteurs de performances ADDS personnalisés**, puis cliquez sur **Journal de Moniteur système.blg**. Le graphique des compteurs de performance du journal apparaît.

Leçon 2

Gestion de la base de données Active Directory

La base de données Active Directory se trouve au cœur de l'environnement Active Directory. Elle contient toutes les informations essentielles requises pour fournir la fonctionnalité Active Directory. Un entretien correct de cette base de données est un aspect essentiel pour la gestion de Active Directory. Vous devrez connaître plusieurs outils et les bonnes pratiques afin de gérer efficacement votre base de données Active Directory. Cette leçon vous présentera la gestion de base de données Active Directory et vous montrera les outils et les méthodes pour la maintenance.

Objectifs de la leçon

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

- Gérer la base de données Active Directory ;
- Décrire les outils de gestion de la base de données ;
- Expliquer comment gérer la base de données Active Directory avec Ntdsutil.exe ;
- Expliquer l'AD DS en redémarrage ;
- Gérer la base de données AD DS ;
- Expliquer comment gérer les instantanés Active Directory.

Vue d'ensemble de la base de données AD DS

Les informations Active Directory sont stockées dans la base de données de l'annuaire. Chaque partition d'annuaire (également appelé *contexte d'appellation*) contient des objets d'une étendue et d'un but de réPLICATION spécifiques. Les quatre partitions Active Directory sur chaque contrôleur de domaine sont les suivantes :

- Domaine. La partition de domaine contient tous les objets stockés dans un domaine, y compris les utilisateurs, les groupes, les ordinateurs et les conteneurs de stratégie de groupe.
- Configuration. La partition de configuration contient les objets qui représentent la structure logique de la forêt (y compris des informations sur les domaines), en plus de la topologie physique, notamment les sites, les sous-réseaux et les services.
- Schéma. La partition de schéma définit les classes d'objets et leurs attributs pour l'ensemble du répertoire.
- Application. Les contrôleurs de domaine peuvent également héberger des partitions d'application. Vous pouvez utiliser les partitions d'application pour limiter la réPLICATION des données spécifiques à une application sur un sous-ensemble de contrôleurs de domaine. Le DNS (Domain Name System) intégré à Active Directory est un exemple courant d'une application qui utilise des partitions d'application. Les partitions d'application ne sont pas un composant obligatoire de la base de données AD DS.

- La base de données du répertoire stocke des informations d'Active Directory
- Les quatre partitions Active Directory sur chaque contrôleur de domaine sont : Domaine, Configuration, Schéma et Application (en option).
- Les composants de niveau du fichier de la base de données AD DS sont :

| Fichier | Description |
|-----------------|---|
| Ntds.dit | <ul style="list-style-type: none">• Fichier de base de données AD DS principal• Contient des partitions et des objets Active Directory |
| Edb *.log | Journaux des transactions |
| Edb.chk | Fichier de point de contrôle de base de données |
| Edbres00001.jrs | Réserver un fichier de journal des transactions qui permet au répertoire de traiter les transactions si le serveur manque d'espace disque |
| Edbres00002.jrs | |

Chaque contrôleur de domaine conserve une copie (ou *réplica*) de plusieurs partitions. La partition de configuration réplique sur chaque contrôleur de domaine de la forêt, comme le fait la partition de schéma. La partition de domaine pour un domaine réplique sur tous les contrôleurs de domaine d'un domaine, mais pas aux contrôleurs de domaine d'autres domaines, à l'exception des serveurs de catalogue globaux. Par conséquent, chaque contrôleur de domaine a au moins trois réplicas : les partitions de domaine pour son domaine, la configuration et le schéma.

Fichiers de la base de données AD DS

La base de données AD DS est stockée dans un fichier nommé **Ntds.dit**. Lorsque vous installez et configurez AD DS, vous pouvez spécifier l'emplacement du fichier. La localisation par défaut est **%SystemRoot%\NTDS**. Toutes les partitions hébergées par le contrôleur de domaine se trouvent dans **Ntds.dit** : le schéma de la forêt et de la configuration, le contexte d'appellation de domaine et, en fonction de la configuration du serveur, les partitions d'application et de jeu d'attributs partiel.

D'autres fichiers prenant en charge la base de données AD DS se trouvent dans le dossier NTDS. Les fichiers **Edb*.log** sont les journaux de transactions pour AD DS. Quand une modification doit être effectuée dans le répertoire, elle est d'abord écrite dans le fichier journal. La modification est réalisée dans le répertoire comme une transaction. Si la transaction échoue, AD DS annule les modifications.

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

| Fichier | Description |
|--|--|
| Ntds.dit | <ul style="list-style-type: none"> Fichier de base de données AD DS principal Contient des partitions et des objets Active Directory |
| Edb*.log | Journaux des transactions |
| Edb.chk | Fichier de point de contrôle de base de données |
| Edbres00001.jrs Edbres00002.jrs | Fichier journal des transactions en réserve qui permet au répertoire de traiter les transactions si le serveur manque d'espace disque |

Modifications et réPLICATION de la base de données AD DS

Dans le cadre d'opérations normales, le journal des transactions s'ajuste, les nouvelles transactions s'écrivant au dessus des anciennes. Toutefois, si un grand nombre de transactions est effectué dans une courte période, AD DS crée des fichiers journaux de transaction supplémentaires. Par conséquent, si vous regardez dans le dossier NTDS d'un contrôleur de domaine particulièrement occupé, vous pourriez voir plusieurs fichiers **Edb*.log**. Au fil du temps, ces fichiers sont supprimés automatiquement.

Le fichier **Edb.chk** agit comme un signet dans les fichiers journaux, marquant l'emplacement avant que les transactions ne soient réalisées avec succès dans la base de données et indiquant par la suite les transactions qui doivent toujours être réalisées.

Si un lecteur de disque manque d'espace, cela représente un problème important pour le serveur. C'est encore plus problématique si ce disque est l'hôte de la base de données AD DS, car les transactions qui pourraient être en attente ne peuvent pas écrire dans les journaux. Par conséquent, AD DS gère deux fichiers journaux supplémentaires : **Edbres00001.jrs** et **Edbres00002.jrs**. Ce sont des fichiers vides de 10 mégaoctets (Mo) chacun. Lorsqu'un disque manque d'espace pour les journaux de transaction normaux, AD DS récupère l'espace utilisé par ces deux fichiers pour écrire les transactions qui sont dans une file d'attente à ce moment-là. Après cela, il arrête les services Active Directory en toute sécurité et démonte la base de données. Bien sûr, il sera important pour un administrateur de trouver une solution à ce faible espace disque aussi rapidement que possible. Les fichiers offrent une solution temporaire pour forcer le service d'annuaire à traiter les nouvelles transactions.

Qu'est-ce que NtdsUtil ?

NtdsUtil.exe est un fichier exécutable de ligne de commande que vous pouvez utiliser pour effectuer la maintenance de base de données, y compris la création d'instantanés, la relocalisation des fichiers de base de données et la défragmentation hors connexion.

Vous pouvez également utiliser Ntdsutil.exe pour nettoyer les métadonnées du contrôleur de domaine. Si un contrôleur de domaine est supprimé du domaine hors connexion, le contrôleur de domaine ne peut pas supprimer des informations importantes à partir du service d'annuaire. Cependant, vous pouvez utiliser Ntdsutil.exe pour nettoyer les restes du contrôleur de domaine. Il est très important que vous le fassiez pour empêcher vos données d'être compromises.

En outre, vous pouvez utiliser **NtdsUtil.exe** pour réinitialiser le mot de passe utilisé pour se connecter au mode restauration des services d'annuaire (DSRM). Vous configurez ce mot de passe au début lors de la configuration d'un contrôleur de domaine. Si vous oubliez le mot de passe, vous pouvez utiliser la commande **NtdsUtil.exe set dsrm** pour le réinitialiser.

- Gérer et contrôler les opérations de base simples
- Effectuer la maintenance de la base de données Active Directory :
 - Effectuer une défragmentation hors ligne ;
 - Créer et organiser des captures instantanées ;
 - Déplacer les fichiers de la base de données ;
- Nettoyer les métadonnées du contrôleur de domaine :
 - Retrait du contrôleur de domaine ou rétrogradation sans être connecté à un domaine.
- Réinitialiser DSRM :
 - Mot de passe
 - **Initialiser dsrm**



Remarque : Vous pouvez également utiliser des outils graphiques tels qu'Utilisateurs et ordinateurs Active Directory et Sites et services Active Directory pour gérer les objets Active Directory et nettoyer les métadonnées automatiquement.

Comprendre l'AD DS redémarrable

Dans la plupart des scénarios où la gestion Active Directory est nécessaire, vous devez redémarrer le contrôleur de domaine dans DSRM. Windows Server permet aux administrateurs d'arrêter et de démarrer AD DS comme tout autre service, sans redémarrer un contrôleur de domaine, pour effectuer rapidement certaines tâches de gestion. Cette fonction est appelée *AD DS redémarrable*. Vous pouvez utiliser la console **Services**, l'invite de commande ou Windows PowerShell pour redémarrer AD DS.

L'AD DS redémarrable réduit le temps nécessaire pour effectuer certaines opérations. Par exemple, vous pouvez arrêter AD DS afin de réaliser les mises à jour d'un contrôleur de domaine. En outre, les administrateurs peuvent arrêter AD DS pour effectuer des tâches telles que la défragmentation hors connexion de la base de données AD DS, sans redémarrer le contrôleur de domaine. D'autres services s'exécutant sur le serveur qui ne dépendent pas de AD DS pour fonctionner, comme le protocole DHCP, restent disponibles pour répondre aux demandes client lorsque AD DS est arrêté. L'AD DS redémarrable est disponible par défaut sur tous les contrôleurs de domaine qui exécutent Windows Server ou une version ultérieure. Il n'y a pas d'exigence de niveau fonctionnel ou d'autres conditions préalables à l'utilisation de cette fonctionnalité.

- Utiliser la console de **services** pour démarrer ou arrêter AD DS
- Trois états d'AD DS :
 - AD DS démarré ;
 - AD DS arrêté ;
 - DSRM.
- Il est impossible d'effectuer une restauration d'état du système, tandis qu'AD DS est arrêté



Remarque : Pour restaurer l'état du système d'un contrôleur de domaine, vous devez commencer dans DSRM.

L'AD DS redémarrable nécessite de légèrement modifier les composants logiciels enfichables existants Microsoft Management Console (MMC). En utilisant le composant logiciel enfichable, un administrateur peut arrêter et redémarrer AD DS plus facilement, ainsi que tout autre service qui s'exécute localement sur le serveur.

Bien que l'arrêt de AD DS soit similaire à la connexion au DSRM, l'AD DS redémarrable fournit un état unique, connu sous le nom de *AD DS arrêté*, à un contrôleur de domaine qui exécute Windows Server 2012 ou une version ultérieure.

États du contrôleur de domaine

Les trois états possibles pour un contrôleur de domaine qui exécute Windows Server 2012 ou une version ultérieure sont les suivants :

- AD DS démarré. Dans cet état, AD DS est démarré. Le contrôleur de domaine est en mesure d'effectuer normalement des tâches liées à AD DS.
- AD DS arrêté. Dans cet état, AD DS est arrêté. Bien que ce mode soit unique à Windows Server 2012 ou aux versions ultérieures, le serveur a des caractéristiques à la fois d'un contrôleur de domaine dans DSRM et d'un serveur membre joint au domaine.
- DSRM. Dans cet état, la base de données AD DS (**Ntds.dit**) sur le contrôleur de domaine local est hors connexion. Un autre contrôleur de domaine peut être contacté pour la connexion s'il est disponible. Si aucun autre contrôleur de domaine ne peut être contacté, vous pouvez par défaut réaliser une des actions suivantes :
 - Connectez-vous au contrôleur de domaine local dans DSRM en utilisant le mot de passe DSRM ;
 - Redémarrez le contrôleur de domaine pour vous connecter avec un compte de domaine.

Comme avec un serveur membre, le contrôleur de domaine dans l'état Arrêté est encore joint au domaine. Cela signifie que la stratégie de groupe et d'autres paramètres s'appliquent toujours à l'ordinateur. Cependant, un contrôleur de domaine ne doit pas rester dans l'état AD DS arrêté pendant une période prolongée, car dans cet état, il ne peut pas traiter les demandes de connexion aux services ou répliquer avec d'autres contrôleurs de domaine.

Démonstration : Gestion de la base de données

Vous pouvez utiliser plusieurs tâches et d'outils pour effectuer la maintenance base de données Active Directory.

Dans cette démonstration, vous apprendrez à :

- Arrêter AD DS ;
- Effectuer une défragmentation hors connexion de la base de données Active Directory ;
- Vérifier hors connexion l'intégrité de la base de données Active Directory ;
- Démarrer AD DS.

Étapes de la démonstration

Arrêter AD DS

1. Sur **LON-DC1**, ouvrez la console **Services**.

2. Arrêtez le service **Services de domaine Active Directory**.

Effectuer une défragmentation hors ligne de la base de données Active Directory

- Exécutez les commandes suivantes dans une invite de commande de l'interface de ligne de commande Windows PowerShell, en appuyant sur Entrée après chaque ligne :

```
ntdsutil.exe
activev instance NTDS
files
compact to C:\
```

Vérifier l'intégrité de la base de données Active Directory en mode hors ligne

- Exécutez les commandes suivantes à partir de l'interface de ligne de commande Windows PowerShell, en appuyant sur Entrée après chaque ligne :

```
Integrity
quit
quit
```

- Fermez la fenêtre **Windows PowerShell**.

Démarrer AD DS

- Ouvrez la console **Services**.
- Démarrez le service Services de domaine Active Directory.
- Vérifiez que la colonne d'état pour les services de domaine Active Directory est répertoriée comme Exécution en cours.

Gestion des Captures instantanées de Active Directory

Vous pouvez utiliser NtdsUtil.exe pour créer et monter des instantanés de AD DS. Un *instantané* est la capture exacte d'un état historique du service d'annuaire, au moment de l'instantané. Vous pouvez utiliser des outils pour explorer le contenu d'un instantané afin d'examiner l'état du service d'annuaire au moment où le cliché a été fait. Par exemple, vous pouvez utiliser l'instantané pour parcourir le contenu de la base de données AD DS, dans l'état où il était lors de la sauvegarde. Vous pouvez utiliser l'outil de ligne de commande Ldifde pour vous connecter à un instantané monté et exporter des objets depuis AD DS.

- Créer une capture instantanée d'AD DS avec NtdsUtil
- Introduire la capture instantanée avec NtdsUtil
- Afficher la capture instantanée :
 - Cliquez avec le bouton droit sur le nœud racine de **Utilisateurs et ordinateurs d'Active Directory**, puis cliquez sur **Se connecter au contrôleur de domaine**
 - Saisissez **serverFQDN:port**
- Vue en lecture seule de la capture instantanée :
 - Les données ne peuvent être récupérées directement à partir de la capture instantanée
- Récupérer des données :
 - Connectez-vous à la capture instantanée introduite, puis aux attributs des objets d'exportation / de réimportation avec Ldifde
 - Restaurez une sauvegarde à partir de la même date que la capture instantanée

Création d'un instantané Active Directory

Pour créer un instantané Active Directory, procédez comme suit :

- Ouvrez une invite de commandes avec élévation de privilèges.
- Tapez les commandes ci-dessous, en appuyant sur Entrée après chaque commande :

```
NtdsUtil.exe
activate instance ntds
snapshot
Create
List all
```



Remarque : La commande **list all** renvoie un message qui indique que l'ensemble d'instantanés a été généré avec succès.

Le GUID qui apparaît est important pour les commandes dans les tâches ultérieures. Notez donc le GUID ou copiez-le dans le Presse-papiers.

3. Tapez **terminer**, puis appuyez sur Entrée.

Vous devez planifier des instantanés AD DS régulièrement. Vous pouvez utiliser le Planificateur de tâches pour exécuter un fichier de commandes en utilisant les commandes NtdsUtil.exe appropriées.

Montage d'un instantané AD DS

Pour afficher le contenu d'un instantané, vous devez monter l'instantané comme une nouvelle instance AD DS. Vous pouvez y parvenir en utilisant NtdsUtil.exe.

Pour monter un instantané, procédez comme suit :

1. Ouvrez une invite de commandes avec élévation de priviléges.
2. Tapez les commandes ci-dessous, en appuyant sur Entrée après chaque commande :

```
ntdsutil.exe
activate instance ntds
snapshot
list all
```



Remarque : La commande **list all** retourne une liste de tous les instantanés.

3. Entrez la commande suivante, puis appuyez sur Entrée :

```
mount <GUID>
```



Remarque : **GUID** est le GUID retourné par la commande de création de l'instantané.

4. Tapez les commandes ci-dessous, en appuyant sur Entrée après chaque commande :

```
quit
quit
dsamain -dbpath c:\$snap_datetime_volumec$\windows\ntds\ntds.dit -ldapport 50000
```

Un message indique que le démarrage des Services de domaine Active Directory est terminé.



Remarque : La propriété **dbpath** est fournie lorsque vous exécutez la commande **mount <GUID>**. 1 Le numéro de port 50000 peut être n'importe quel numéro de port du protocole TCP non utilisé.

5. Ne fermez pas la fenêtre d'invite de commandes. Laissez la commande que vous venez de lancer, **Dsamain.exe**, s'exécuter tandis que vous passez à la prochaine étape.

Affichage d'un instantané AD DS

Après le montage de l'instantané, vous pouvez utiliser des outils pour vous connecter à l'instantané et l'explorer. Utilisateurs et ordinateurs Active Directory est l'un des outils que vous pouvez utiliser pour vous connecter à l'instance.

Pour se connecter à un instantané avec Utilisateurs et ordinateurs Active Directory, suivez la procédure suivante :

1. Ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Cliquez avec le bouton droit sur le nœud racine, puis cliquez sur **Modifier le contrôleur de domaine**.
3. Dans la boîte de dialogue **Changer de serveur d'annuaire**, cliquez sur <**Tapez ici un nom de serveur d'annuaire:[port]**>.
4. Saisissez **LON-DC1:50000**, puis appuyez sur Entrée.



Remarque : **LON-DC1** est le nom du contrôleur de domaine sur lequel vous avez monté l'instantané, et 50000 est le numéro de port TCP que vous avez configuré pour l'instance.

5. Après avoir vérifié que vous êtes maintenant connecté à l'instantané, cliquez sur **OK**.



Remarque : Notez que les instantanés sont en lecture seule. Vous ne pouvez pas modifier le contenu d'un instantané. De plus, il n'y a pas de méthodes directes pour déplacer, copier ou restaurer des objets ou des attributs de l'instantané à l'instance AD DS de production.

Démontage d'un instantané AD DS

Pour démonter l'instantané Active Directory, procédez comme suit :

1. Passez sur l'invite de commande dans lequel l'instantané est monté.
2. Appuyez sur Ctrl+C pour arrêter Dsamain.exe.
3. Saisissez les commandes ci-dessous, en appuyant sur ENTRÉE après chaque commande :

```
ntdsutil.exe
activate instance ntds
snapshot
unmount <GUID>,
quit
quit
```



Remarque : *GUID* est le GUID de l'instantané.

Leçon 3

Sauvegarde de Active Directory et options de récupération pour AD DS et autres solutions d'identité et d'accès

Il est important de maintenir la fiabilité des données Active Directory. Des sauvegardes régulières peuvent jouer un rôle dans ce processus, mais savoir comment restaurer ou récupérer des données après une défaillance est vital. La restauration d'objets supprimés dans AD DS pouvant souvent causer des temps d'arrêt de AD DS, Windows Server comprend la fonctionnalité Corbeille Active Directory, qui fournit un moyen beaucoup plus facile de restaurer des objets supprimés sans que AD DS ne connaisse de temps d'arrêt. Cette leçon se penche sur les fonctionnalités de sauvegarde et de récupération de Active Directory.

Objectifs de la leçon

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

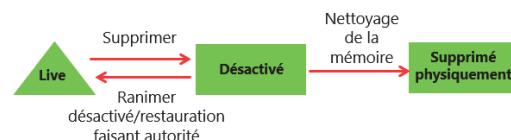
- Expliquer comment restaurer des objets Active Directory supprimés ;
- Expliquer comment configurer la Corbeille Active Directory ;
- Implémenter la Corbeille Active Directory ;
- Décrire les outils de sauvegarde et de récupération ;
- Expliquer la sauvegarde et la récupérer de Active Directory.

Suppression et restauration d'objets de AD DS

Lorsque vous supprimez un objet dans AD DS, il est déplacé dans le conteneur Objets supprimés et de nombreux attributs importants lui sont enlevés. Vous pouvez étendre la liste des attributs qui restent lorsque vous supprimez un objet, mais vous ne pouvez jamais conserver les valeurs d'attributs liés, tels que l'appartenance à un groupe.

Vos options de récupération dépendent de l'activation ou non de la fonctionnalité Corbeille Active Directory. Si vous n'avez pas activé la Corbeille Active Directory, vous pouvez réanimer l'objet supprimé si l'objet n'a pas encore atteint la fin de sa durée de vie de temporisation (qui est de 180 jours par défaut) et s'il n'a pas été récupéré par le processus de nettoyage de la mémoire. (Le *nettoyage* est un processus de nettoyage de base de données qui supprime les enregistrements obsolètes.)

- Les objets supprimés sont récupérés grâce à la réanimation des objets désactivés
- Lorsqu'un objet est supprimé, la plupart de ses attributs sont effacés
- La restauration faisant autorité exige un temps d'arrêt d'Active Directory



Remarque : La base de données AD DS s'entretient presque toute seule. Par défaut, toutes les 12 heures, chaque contrôleur de domaine exécute un nettoyage de la mémoire. Deux tâches sont alors réalisées. Premièrement, le nettoyage supprime les objets supprimés qui ont survécu à leur durée de vie de temporisation. Deuxièmement, le processus de nettoyage de la mémoire procède à une défragmentation en ligne.

Pour réanimer un objet supprimé, vous pouvez utiliser l'outil LDP pour effectuer la procédure suivante :

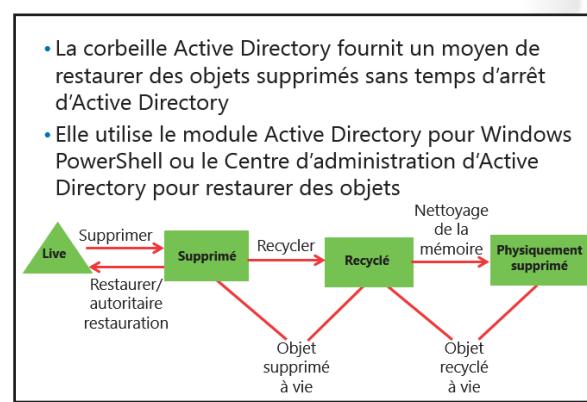
1. Cliquez sur **Démarrer** et dans la zone de texte **Rechercher**, tapez **Ldp.exe**. Appuyez sur Ctrl + Maj + Entrée, ce qui exécute la commande en tant qu'administrateur.
2. Dans la boîte de dialogue **Contrôle de compte d'utilisateur**, cliquez sur **Utiliser un autre compte**.
3. Dans la zone de texte **Nom d'utilisateur**, saisissez le nom d'utilisateur d'un administrateur.
4. Dans la zone de texte **Mot de passe**, saisissez le mot de passe pour le compte Administrateur, puis appuyez sur Entrée. Ldp s'ouvre.
5. Dans le menu **Connexion**, cliquez sur **Se connecter**, puis sur **OK**.
6. Dans le menu **Connexion**, cliquez sur **Liaison**, puis sur **OK**.
7. Cliquez sur le menu **Options**, puis sur **Contrôles**.
8. Dans la liste **Chargement prédefini**, cliquez sur **Retourner les objets supprimés**, puis cliquez sur **OK**.
9. Dans le menu **Afficher**, cliquez sur **Arborescence**, puis sur **OK**.
10. Développez le domaine, puis double-cliquez sur **CN=Objets supprimés,DC=adatum,DC=com**.
11. Cliquez avec le bouton droit sur l'objet supprimé, puis sur **Modifier**.
12. Dans la zone de texte **Attribut**, saisissez **isDeleted**. Dans la section **Opération**, cliquez sur **Supprimer**, puis appuyez sur Entrée.
13. Dans la zone de texte **Attribut**, saisissez **NomUnique**.
14. Dans la zone de texte **Valeurs**, saisissez le nom unique de l'objet dans le conteneur parent ou dans l'unité d'organisation (UO) dans lequel vous souhaitez que l'objet soit restauré. Par exemple, saisissez le nom unique de l'objet avant qu'il ne soit supprimé.
15. Dans la section **Opération**, cliquez sur **Remplacer**, puis appuyez sur Entrée.
16. Cochez la case **Étendu**, cliquez sur **Exécuter**, puis sur **Fermer**.
17. Fermez LDP.
18. Utilisez **Utilisateurs et ordinateurs Active Directory** pour remplir à nouveau les attributs de l'objet, réinitialiser le mot de passe pour un objet utilisateur et activer l'objet s'il est désactivé.



Remarque : *Ldp.exe* est un outil de ligne de commande que vous utilisez pour réaliser des recherches de protocole LDAP recherches auprès de Active Directory. Vous pouvez également l'utiliser pour effectuer la maintenance de AD DS ou des Services AD LDS (Active Directory Lightweight Directory Services)

Configuration de la Corbeille Active Directory

Vous pouvez activer la Corbeille Active Directory pour bénéficier d'un processus simplifié pour la restauration des objets supprimés. Cette fonctionnalité permet de surmonter les problèmes de restauration faisant autorité ou de réanimation de la désactivation. Avec la Corbeille Active Directory, les administrateurs peuvent restaurer des objets supprimés avec toutes leurs fonctionnalités sans avoir à restaurer des données Active Directory à partir de sauvegardes, puis de redémarrer AD DS ou les contrôleurs de domaine. La Corbeille Active Directory repose sur l'infrastructure existante de réanimation de désactivation et améliore votre capacité à préserver et à récupérer des objets Active Directory supprimés accidentellement.



Fonctionnement de la Corbeille Active Directory

Lorsque vous activez la Corbeille Active Directory, tous les attributs liés ou non liés par les valeurs des objets Active Directory supprimés sont conservés. Les objets sont restaurés dans leur intégralité, avec le même état logique cohérent juste avant la suppression. Par exemple, les comptes d'utilisateurs restaurés retrouvent automatiquement toutes les appartenances à des groupes et les droits d'accès correspondants qu'ils avaient juste avant la suppression, à l'intérieur et à travers les domaines. La Corbeille Active Directory fonctionne pour les environnements AD DS et AD LDS.

Après avoir activé la Corbeille Active Directory, lorsqu'un objet Active Directory est supprimé, le système conserve tous attributs liés et non liés par les valeurs de l'objet, qui devient logiquement supprimé. Un objet supprimé se déplace vers le conteneur Objets supprimés et son nom distinctif est obscurci. Un objet supprimé reste dans le conteneur Objets supprimés dans un état logiquement effacé pendant toute la durée de vie de l'objet supprimé. Durant la durée de vie de l'objet supprimé, vous pouvez récupérer un objet supprimé avec la Corbeille Active Directory et en faire un objet AD DS actif de nouveau.

La durée de vie de l'objet supprimé est déterminée par la valeur de l'attribut **msDS-deletedObjectLifetime**. Pour un élément supprimé après l'activation Corbeille Active Directory (objet recyclé), la durée de vie de l'objet recyclé est déterminée par la valeur de l'attribut hérité **tombstoneLifetime**. Par défaut, cette valeur est nulle, ce qui signifie que la durée de vie de l'objet supprimé est réglée sur la valeur de la durée de vie de l'objet recyclé.

Par défaut, la durée de vie de l'objet recyclé, qui est stockée dans l'attribut **tombstoneLifetime** est également nulle. Cela signifie la durée de vie par défaut de l'objet recyclé est de 180 jours. Vous pouvez modifier ces deux valeurs à tout moment. Quand **msDS-deletedObjectLife** est réglé sur une valeur autre que nulle, elle ne prend plus la valeur de **tombstoneLifetime**.

Pour modifier ces valeurs, vous pouvez utiliser Windows PowerShell. Par exemple, pour définir **tombstoneLifetime** sur 365 jours, exécutez la commande suivante, en appuyant sur Entrée à la fin de chaque ligne :

```
Set-ADObject -Identity "CN=Annuaire,CN=Windows
NT,CN=Services,CN=Configuration,DC=Adatum,DC=com" -Partition
"CN=Configuration,DC=Adatum,DC=com" -Replace:@>{"tombstoneLifetime" = 365}
```

Pour définir la durée de vie de l'objet supprimé à 365 jours, exécutez la commande suivante, en appuyant sur Entrée à la fin de chaque ligne :

```
Set-ADObject -Identity "CN=Annuaire,CN=Windows  
NT,CN=Services,CN=Configuration,DC=Adatum,DC=com" -Partition  
"CN=Configuration,DC=Adatum,DC=com" -Replace:@>{"msDS-DeletedObjectLifetime" = 365}
```

Vous pouvez utiliser l'outil de ligne de commande Ldp.exe pour configurer ces valeurs.

Activation de la Corbeille Active Directory

Vous pouvez activer la corbeille Active Directory uniquement lorsque le niveau fonctionnel de la forêt est défini sur Windows Server 2008 R2 ou une version ultérieure.

Pour activer la Corbeille Active Directory, vous pouvez effectuer une des opérations suivantes :

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

Seuls les éléments supprimés après que la Corbeille Active Directory soit activée peuvent être restaurés à partir de la Corbeille Active Directory.

 **Remarque :** Une fois que vous avez activé la Corbeille Active Directory, vous ne pouvez pas la désactiver.

Restauration d'éléments depuis la Corbeille Active Directory

Le Centre d'administration Active Directory fournit une interface graphique pour la restauration d'objets Active Directory supprimés. Une fois que vous activez la Corbeille Active Directory, le conteneur Objets supprimés apparaît dans le Centre d'administration Active Directory. Les objets supprimés seront visibles dans ce conteneur jusqu'à l'expiration de leur durée de vie d'objet supprimé. Vous pouvez choisir de restaurer les objets soit à leur emplacement d'origine, soit à un autre emplacement dans AD DS.

Démonstration : Implémentation de la Corbeille Active Directory

Dans cette démonstration, vous apprendrez à :

- Activer la Corbeille Active Directory ;
- Créer, puis supprimer les comptes de test ;
- Restaurer les comptes supprimés.

Étapes de la démonstration

Activez la Corbeille Active Directory

1. Sur **LON-DC1**, à partir du **Gestionnaire de serveur**, ouvrez **Centre d'administration Active Directory**.
2. Activez la Corbeille.

Créez, puis supprimez les comptes d'essai

1. Dans le Centre d'administration Active Directory, créez les utilisateurs suivants dans l'UO **Rechercher**.
Donnez-leur le mot de passe **Pa\$\$w0rd** :
 - o **Test1**

- **Test2**
- 2. Supprimer les comptes **Test1** et **Test2**.

Restaurez les comptes supprimés

1. Dans le Centre d'administration Active Directory, accédez au dossier **Objets supprimés** pour le domaine Adatum.
2. Restaurez **Test1** à son emplacement d'origine.
3. Restaurer **Test2** dans l'UO **IT**.
4. Assurez-vous que **Test1** est maintenant situé dans l'UO **Rechercher** et que **Test2** est dans le l'UO **IT**.

Outils de sauvegarde et de récupération supplémentaires

Sauvegarde Windows Server

La fonctionnalité de sauvegarde Windows Server dans Windows Server se compose d'un composant logiciel enfichable MMC, de la commande **Wbadm** et des commandes de Windows PowerShell. Vous pouvez utiliser des assistants dans l'interface utilisateur de sauvegarde de Windows Server pour vous guider à travers les sauvegardes en cours d'exécution et les récupérations.

- Sauvegarde Windows Server
- Sauvegarde Windows Azure
- Data Protection Manager

Vous pouvez utiliser Windows Server Backup pour sauvegarder :

- Un serveur complet (tous les volumes) ;
- Les volumes sélectionnés.
- Sélectionnez des éléments spécifiques pour la sauvegarde, tels que des dossiers spécifiques ou l'État du système.

La sauvegarde de Windows Server vous permet aussi :

- D'effectuer une récupération dépourvue de système d'exploitation. Une sauvegarde dépourvue de système d'exploitation contient tous les volumes critiques et vous permet de restaurer sans avoir à installer d'abord un système d'exploitation. Pour cela, vous utilisez le support de produit sur une clé USB ou DVD et l'Environnement de récupération Windows (Windows RE). Vous pouvez utiliser ce type de sauvegarde ainsi que Windows RE pour récupérer d'une défaillance de disque dur, ou si vous devez récupérer toute l'image de l'ordinateur vers un nouveau matériel.
- D'utiliser l'État du système. La sauvegarde contient des informations importantes pour restaurer un serveur à un point précis dans le temps. Cependant, vous devez avoir un système d'exploitation installé avant de récupérer l'état du système.
- Récupérez des fichiers et des dossiers individuels ou des volumes. L'option des fichiers et des dossiers individuels vous permet de sélectionner quels fichiers, dossiers ou volumes spécifiques sauvegarder et restaurer. Vous pouvez également ajouter des fichiers, des dossiers ou des volumes spécifiques à la sauvegarde lorsque vous utilisez une option telle que le volume critique ou de l'état du système.
- D'exclure des fichiers sélectionnés ou des types de fichiers. Par exemple, vous pouvez exclure les fichiers temporaires de la sauvegarde.

- De choisir les emplacements de stockage. Vous pouvez stocker des sauvegardes sur des partages distants ou des volumes non dédiés.
- D'utiliser Microsoft Azure Backup. Azure Backup est une solution de sauvegarde hors-site sur le cloud pour Windows Server qui permet de sauvegarder et de récupérer des fichiers et des dossiers sur le cloud privé ou public.

Si un sinistre survient, tel qu'une panne de disque dur, vous pouvez effectuer la récupération du système en utilisant une sauvegarde complète du serveur et Windows RE. Vous allez restaurer votre système complet sur le nouveau disque dur.

Azure Backup

Azure Backup est un service d'abonnement que vous pouvez utiliser pour fournir une protection hors site contre la perte de données critiques causée par des sinistres. Vous sauvegardez des fichiers et des dossiers. Vous les récupérez à partir du cloud public ou privé, selon les besoins.

Azure Backup est conçu sur la plate-forme Windows Azure et utilise le stockage Windows Azure Blob pour stocker les données des clients. Vous pouvez utiliser l'agent d'Azure Backup téléchargeable pour transférer des données de fichiers et de dossiers en toute sécurité sur Azure Backup depuis Windows Server. Après avoir installé l'agent d'Azure Backup, l'agent intègre ses fonctionnalités grâce à l'interface de Sauvegarde Windows Server. Vous pouvez télécharger l'agent Azure Backup sur le site Web de Microsoft.

Les principales fonctionnalités d'Azure Backup proposées dans Windows Server comprennent :

- Une configuration et une gestion simplifiées. L'intégration avec l'outil de Sauvegarde Windows Server fournit une expérience de sauvegarde et de récupération fluide sur un disque local ou une plate-forme cloud. Les autres caractéristiques comprennent :
 - Une interface utilisateur simplifiée pour configurer et surveiller les sauvegardes.
 - Une expérience de récupération intégrée pour récupérer des fichiers et des dossiers à partir d'un disque local ou d'une plate-forme cloud.
 - Une recouvrabilité facile des données pour les données qui ont été sauvegardées sur le serveur de votre choix.
 - Une capacité de script fournie par Windows PowerShell.
- Des sauvegardes incrémentielles de niveau bloc. L'agent d'Azure Backup effectue des sauvegardes incrémentielles en suivant les changements de fichiers et de niveau bloc. Il transfère uniquement les blocs modifiés. L'utilisation du stockage et de la bande passante s'en trouve réduite. Différentes versions à un moment donné de sauvegardes utilisent le stockage efficacement en stockant uniquement les blocs modifiés entre ces versions.
- Compression des données, chiffrement et limitation. L'agent Azure Backup s'assure que les données sont compressées et chiffrées sur le serveur avant d'être envoyées à Azure Backup sur le réseau. Par conséquent, Azure Backup stocke uniquement les données chiffrées dans un stockage sur le cloud. La phrase secrète de chiffrement n'est pas disponible sur Azure Backup et donc, les données ne sont jamais déchiffrées dans le cloud. En outre, les utilisateurs peuvent configurer la limitation et la façon dont Azure Backup utilise la bande passante du réseau lors de la sauvegarde ou de la restauration des informations.
- Vérification de l'intégrité des données dans le cloud. En plus des sauvegardes sécurisées, l'intégrité des données sauvegardées est également vérifiée automatiquement après la fin de la sauvegarde. Par conséquent, vous pouvez identifier rapidement les altérations qui pourraient survenir en raison du transfert de données. Ces altérations sont résolues automatiquement lors de la prochaine sauvegarde.
- Des stratégies de rétention configurables pour le stockage des données dans le nuage. Azure Backup accepte et met en œuvre des stratégies de rétention pour recycler les sauvegardes qui dépassent la

plage de rétention souhaitée. Cela contribue à répondre aux stratégies métiers et à la gestion des coûts de sauvegarde.

Data Protection Manager

Data Protection Manager (DPM) est un produit de protection des données d'entreprise et de récupération du Microsoft System Center. DPM comprend les fonctionnalités suivantes :

- La centralisation de sauvegarde. DPM utilise une architecture client / serveur où le logiciel client est installé sur tous les ordinateurs qui doivent être sauvegardés. Ces clients diffusent les données de sauvegarde sur le serveur DPM. Ainsi, chaque serveur DPM peut prendre en charge des organisations de petite à moyenne taille, en entières. Vous pouvez également gérer plusieurs serveurs DPM à partir d'une console centralisée Microsoft System Center Operations Manager.
- Un objectif de point de récupération de 15 minutes (RPO). DPM permet d'obtenir des instantanés de 15 minutes des produits pris en charge. Cela inclut la plupart des suites de produits de Microsoft pour entreprise, y compris Windows Server avec ses rôles et services, Exchange Server, Microsoft Hyper-V et Microsoft SQL Server.
- La prise en charge des charges de travail Microsoft. DPM a été spécialement conçu par Microsoft pour prendre en charge les applications Microsoft comme Exchange Server, SQL Server et Hyper-V. Cependant, DPM n'a pas été conçu pour prendre en charge d'autres applications serveur tierces qui ne disposent pas d'états cohérents sur le disque ou qui ne prennent pas en charge VSS.
- Une sauvegarde sur disque. DPM peut effectuer des sauvegardes planifiées sur des baies de disques et des réseaux de zone de stockage (SAN). Vous pouvez également configurer DPM pour exporter des données de sauvegarde spécifiques sur la bande pour la rétention et les tâches liées à la conformité.
- Une sauvegarde à distance du site. DPM utilise une architecture qui lui permet de sauvegarder les clients qui sont situés dans des sites distants. Cela signifie qu'un serveur DPM qui se trouve au siège social peut effectuer des sauvegardes de serveurs et de clients reliés par le réseau étendu (WAN).
- La prise en charge des stratégies de sauvegarde sur le cloud. DPM prend en charge la sauvegarde des serveurs DPM sur une plate-forme cloud. Cela signifie que vous pouvez utiliser un serveur DPM dans une installation d'hébergement cloud pour sauvegarder le contenu d'un serveur DPM du siège social. Pour la redondance en cas de sinistre, vous pouvez également configurer les serveurs DPM pour se sauvegarder les uns des autres.

Sauvegarde et récupération de Active Directory

Dans les versions antérieures du système d'exploitation Windows, la sauvegarde AD DS impliquait la création d'une sauvegarde de l'état du système, qui était une petite collection de fichiers comprenant la base de données AD DS et le registre.

Dans Windows Server 2016, le concept d'état système existe toujours, mais il est beaucoup plus étendu. En raison des interdépendances entre les rôles de serveur, la configuration physique et AD DS, l'état du système est maintenant un sous-ensemble d'une sauvegarde complète du serveur et, dans certaines configurations, pourrait être tout aussi important. Pour sauvegarder un contrôleur de domaine, vous devez sauvegarder pleinement tous les volumes critiques.

- | |
|--|
| <ul style="list-style-type: none"> • Restauration non autoritaire ou normale : <ul style="list-style-type: none"> • Restaure le contrôleur de domaine à la dernière bonne configuration ; • Le contrôleur de domaine fait les mises à jour en utilisant la réplication standard des partenaires. • Restauration autoritaire : <ul style="list-style-type: none"> • Restaure le contrôleur de domaine à la dernière bonne configuration ; • Marque les objets devant faire autorité ; • Le contrôleur de domaine fait les mises à jour à partir de celles de ses partenaires ; • Le contrôleur de domaine envoie des mises à jour faisant autorité à ses partenaires. • Restauration complète du serveur : <ul style="list-style-type: none"> • Elle est effectuée généralement dans Windows RE • Autre emplacement de restauration |
|--|

Restauration des données Active Directory

Quand un contrôleur de domaine ou son répertoire est corrompu, endommagé, ou défaillant, vous avez plusieurs options pour restaurer le système. Pour effectuer une restauration de AD DS, vous devez avoir un accès complet aux fichiers sur le contrôleur de domaine. Cela nécessite le redémarrage du contrôleur de domaine dans DSRM. Si vous redémarrez localement un contrôleur de domaine, appuyez sur **F8** au démarrage et choisissez DSRM dans le menu de démarrage.

Lorsque vous démarrez un contrôleur de domaine dans DSRM, connectez-vous en tant qu'administrateur avec le mot de passe DSRM. Vous pouvez ensuite utiliser la Sauvegarde Windows Server pour restaurer la base de données de l'annuaire. Après avoir terminé la restauration, vous devez redémarrer le serveur. Le contrôleur de domaine veillera à ce que cette base de données soit cohérente avec le reste du domaine en tirant de ses partenaires de réPLICATION les modifications apportées au répertoire depuis la date de la sauvegarde.

Restauration ne faisant pas autorité

Lors d'une restauration normale, vous restaurez une sauvegarde de AD DS d'une date adéquate. Fondamentalement, vous restaurez le contrôleur de domaine dans le temps. Lorsque AD DS redémarre sur le contrôleur de domaine, le contrôleur de domaine contacte ses partenaires de réPLICATION et demande toutes les mises à jour ultérieures. En d'autres termes, le contrôleur de domaine rattrape le reste du domaine en utilisant des mécanismes de réPLICATION standard.

Une restauration normale est utile lorsque le répertoire sur un contrôleur de domaine a été endommagé ou corrompu, mais que le problème ne s'est pas propagé sur d'autres contrôleurs de domaine. Toutefois, pour certaines situations, une restauration normale n'est pas suffisante. Par exemple, la restauration normale ne fonctionnera pas si les dommages ont répliqué, par exemple lorsque vous supprimez un ou plusieurs objets et que la suppression a répliqué. Si vous restaurez une bonne version connue de AD DS et redémarrez le contrôleur de domaine, la suppression, qui est arrivée à la suite de la sauvegarde, sera tout simplement répliquée vers le contrôleur de domaine.

Restauration faisant autorité

Une restauration faisant autorité est nécessaire quand une bonne copie connue de AD DS est restaurée et contient des objets qui doivent prévaloir sur les objets existants dans la base de données AD DS. Dans une restauration faisant autorité, vous restaurez la bonne version connue de AD DS comme vous le faites dans une restauration normale. Cependant, avant de redémarrer le contrôleur de domaine, vous marquez les objets supprimés accidentellement ou préalablement corrompus que vous souhaitez conserver comme faisant autorité, afin qu'ils répliquent à partir du contrôleur de domaine restauré jusqu'à ses partenaires de réPLICATION. En réalité, lorsque vous marquez des objets comme faisant autorité, Windows incrémente le numéro de version de tous les attributs d'objet pour être si élevé que la version est virtuellement garantie d'être plus élevée que le numéro de version sur tous les autres contrôleurs de domaine.

Lorsque le contrôleur de domaine restauré redémarre, il réplique depuis ses partenaires de réPLICATION tous les changements qui ont été apportés à l'annuaire. Il informe également ses partenaires qu'il y a des changements. Les numéros de version des modifications assurent que les partenaires prennent les changements en compte et les répliquent à travers le service d'annuaire.

Dans les forêts dotées d'une Corbeille Active Directory activée, vous pouvez utiliser la Corbeille Active Directory comme une alternative plus simple à une restauration faisant autorité.



Remarque : Vous ne pouvez pas utiliser la Corbeille Active Directory pour récupérer des objets corrompus.

Pour faire autorité, l'opération de restauration est réalisée ainsi :

1. Redémarrez le contrôleur de domaine dans DSRM ;

2. Connectez-vous avec le compte d'administrateur et le mot de passe DSRM ;
3. Restaurez le répertoire avec Sauvegarde Windows Server, comme décrit dans la rubrique précédente.

Avant de redémarrer le contrôleur de domaine, vous devez d'abord marquer comme faisant autorité les objets que vous voulez garder après le redémarrage, c'est-à-dire, les objets supprimés que vous essayez de restaurer. Ouvrez une fenêtre d'invite de commandes, puis saisissez les commandes ci-dessous, en appuyant sur Entrée à la fin de chaque ligne :

```
ntdsutil.exe
authoritative restore
restore object <DN objet>
```

DN objet est le nom unique de l'objet en cours de restauration. Par exemple, si vous souhaitez restaurer l'objet utilisateur Candy Spoon qui était dans l'UO IT, vous devez taper :

```
Restore object "CN=Candy Spoon,OU=IT,DC=adatum,DC=com"
```

Pour marquer une UO ou un conteneur et tous ses sous-objets comme faisant autorité, saisissez les commandes suivantes dans l'invite de commande :

```
ntdsutil.exe
authoritative restore
restore subtree <DN objet>
```

4. Redémarrez le contrôleur de domaine.

Le contrôleur de domaine va répliquer depuis ses partenaires tous les changements qui se sont produits dans le répertoire depuis la date de la sauvegarde. Cependant, pour les objets qui ont été marqués comme faisant autorité, tous les attributs de ces objets ont reçu un très grand nombre de version. Par conséquent, ces objets se répliquent à partir du contrôleur de domaine restauré vers le reste du service d'annuaire.

Autres options de restauration

La troisième option pour restaurer le service d'annuaire est de restaurer le contrôleur de domaine complet. Vous pouvez le faire en commençant dans Windows RE, puis en restaurant une sauvegarde complète du serveur sur le contrôleur de domaine. Par défaut, il s'agit de la méthode de restauration normale. Si vous avez aussi besoin de marquer des objets comme faisant autorité, vous devez redémarrer le serveur dans le DSRM et définir les objets désirés comme faisant autorité, avant de lancer le contrôleur de domaine en fonctionnement normal.

Enfin, vous pouvez restaurer une sauvegarde de l'état du système à un autre emplacement. Cela vous permet d'examiner les fichiers et potentiellement pour monter le fichier Ntds.dit. Vous ne devez pas copier les fichiers sur les versions de production de ces fichiers à partir d'un emplacement de restauration autre. En outre, ne faites pas une restauration partielle de AD DS. Cependant, vous pouvez utiliser ces fichiers copiés pour prendre en charge l'option **Installation à partir du support** pour la création d'un nouveau contrôleur de domaine. La plupart des procédures impliquées dans l'exécution de restauration faisant autorité sont identiques à celles d'une restauration ne faisant pas autorité.

Atelier pratique : Récupération d'objets dans AD DS

Scénario

Hier, vous avez été averti qu'un compte d'utilisateur a été supprimé par accident. Il y a quelques jours, d'autres comptes d'utilisateurs ont été supprimés accidentellement. Vous voulez récupérer ces comptes.

Il est de votre responsabilité de veiller à ce que le service d'annuaire soit sauvegardé. Aujourd'hui, vous avez remarqué que la sauvegarde de la veille n'a pas été effectuée comme prévu. Vous avez donc décidé d'effectuer une sauvegarde interactive. Peu de temps après la sauvegarde, un administrateur de domaine supprime accidentellement l'UO informatique. Vous devez récupérer cette unité d'organisation.

Objectifs

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

- Sauvegarde et restauration de AD DS ;
- Récupération d'objets dans AD DS.

Configuration de l'atelier pratique

Durée approximative : **60 minutes**

Ordinateurs virtuels. **22742A-LON-DC1, 22742A-LON-DC2**

Nom d'utilisateur : **Adatum\Administrateur**

Mot de passe : **Pa\$\$w0rd**

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

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans le Gestionnaire Hyper-V, cliquez sur **22742A-LON-DC1**, et dans le volet **Actions**, cliquez sur **Démarrer**.
3. Dans le volet d'**Actions**, cliquez sur **Se connecter**. Attendez que l'ordinateur virtuel démarre.
4. Connectez-vous en utilisant les informations d'identification suivantes :
 - Nom d'utilisateur : **Administrateur**
 - Mot de passe : **Pa\$\$w0rd**
 - Domaine : **Adatum**
5. Répétez les étapes 1 à 4 pour **22742A-LON-DC2**.

Exercice 1 : Sauvegarde et restauration de système de domaine Active Directory (AD DS)

Scénario

Vous avez remarqué que AD DS n'a pas été sauvegardé dernièrement. Vous décidez de créer un calendrier de sauvegarde et d'effectuer une sauvegarde interactive unique, pour plus de sécurité. Vous avez eu raison d'effectuer la sauvegarde interactive, car peu de temps après, un objet AD DS a été supprimé par inadvertance. Vous devez restaurer cet objet de manière qui fasse autorité.

Les tâches principales de cet exercice sont les suivantes :

1. Installer la fonction de sauvegarde Windows Server ;

2. Créer une sauvegarde planifiée ;
3. Réaliser une sauvegarde interactive ;
4. Supprimer une unité d'organisation (UO) ;
5. Redémarrer en mode restauration des services d'annuaire (DSRM) ;
6. Restaurer les données d'état du système ;
7. Marquer des données restaurées comme faisant autorité ;
8. Vérifier que les données ont été restaurées.

► **Tâche 1 : Installer la fonction de sauvegarde Windows Server**

- Sur **LON-DC1**, depuis le **Gestionnaire de serveur**, installez la fonctionnalité Sauvegarde Windows Server.

► **Tâche 2 : Créer une sauvegarde planifiée**

1. Sur **LON-DC1**, exécutez **Sauvegarde Windows Server**.
2. Créez une configuration de sauvegarde personnalisée en utilisant les informations suivantes :
 - Eléments à sauvegarder : récupération dépourvue de système d'exploitation ;
 - Intervalle entre les sauvegardes : **Tous les jours** ;
 - Heure : **12:00** ;
 - Type de destination : **Sauvegarde sur un disque dur qui est dédié pour les sauvegardes** ;
 - Disque de destination : **Disque 1** ;
3. Quand la boîte de dialogue **Sauvegarde de Windows Server** apparaît, vous informant que toutes les données sur le disque seront supprimées, cliquez sur **Oui**.



Remarque : Vous annulerez le processus à l'étape suivante pour éviter le formatage du lecteur E.

4. Cliquez sur **Annuler**. Ne pas formater le lecteur E.

► **Tâche 3 : Réaliser une sauvegarde interactive**

1. Dans le volet **Actions**, cliquez sur **Sauvegarde unique**.
2. Configurez la sauvegarde avec les paramètres suivants :
 - Sauvegarde de la configuration : **Personnalisée** ;
 - Eléments de sauvegarde : **état du système** ;
 - Paramètres avancés : **sauvegarde totale VSS**.



Remarque : La sauvegarde prendra environ 10 à 15 minutes. Une fois la sauvegarde terminée, fermez la fenêtre Sauvegarde Windows Server.

► Tâche 4 : Supprimer une unité d'organisation (UO)



Remarque : Attendez que la sauvegarde se termine avant de continuer.

1. Sur l'ordinateur **LON-DC1**, à partir du **Gestionnaire de serveurs**, ouvrez **Utilisateurs et ordinateurs Active Directory**.

2. Supprimez l'UO **Research**.

► Tâche 5 : Redémarrer en mode restauration les services d'annuaire (DSRM)

1. Sur **LON-DC1**, exécutez Windows PowerShell en tant qu'administrateur.
2. Dans l'invite de commandes, saisissez la commande suivante pour configurer le serveur afin de commencer dans DSRM :

```
bcdedit /set safeboot dsrepair
```

3. Redémarrez **LON-DC1**.

► Tâche 6 : Restaurer les données d'état du système

1. Connectez-vous à **LON-DC1** en tant que **.\Administrateur** avec le mot de passe **Pa\$\$w0rd**.
2. Exécutez Windows Powershell en tant qu'administrateur.
3. Pour obtenir l'identifiant de la version pour la sauvegarde, dans l'invite de commande, saisissez la commande suivante, puis appuyez sur Entrée :

```
wbadmin get versions -backuptarget:E: -machine:LON-DC1
```

4. Restaurez les informations du système d'état en saisissant la commande suivante dans le format suivant :

```
wbadmin start systemstaterecovery -version:<version> -backuptarget:E: -machine:LON-DC1.
```

Par exemple :

```
wbadmin start systemstaterecovery -version:01/22/2011-10:37 -backuptarget:E: -machine:LON-DC1
```



Remarque : La restauration prendra environ 30 à 35 minutes.

5. Lorsque vous êtes invité à redémarrer, tapez **O**, puis appuyez sur Entrée.

► Tâche 7 : Marquer les données restaurées comme faisant autorité

1. Connectez-vous à **LON-DC1** en tant que **.\Administrateur** avec le mot de passe **Pa\$\$w0rd**.
2. Ouvrez Windows PowerShell en tant qu'administrateur.
3. Dans l'invite de commandes Windows PowerShell, utilisez **NtdsUtil.exe** pour effectuer une restauration faisant autorité de "**OU=Research,DC=adatum,DC=com**".
4. Pour redémarrer le serveur normalement après avoir effectué l'opération de restauration, saisissez la commande suivante, puis appuyez sur Entrée.

```
bcdedit /deletevalue safeboot
```

5. Redémarrez le serveur.

► **Tâche 8 : Vérifier que les données ont été restaurées**

1. Après le redémarrage du serveur, connectez-vous à **LON-DC1** en tant qu'**adatum\Administrateur** avec le mot de passe **Pa\$\$w0rd**.
2. À partir du **Gestionnaire de serveur**, ouvrez **Utilisateurs et ordinateurs Active Directory**.
3. Vérifiez la présence de l'UO **Research**. Notez que vous pouvez avoir à forcer une réplication de site dans Sites et services Active Directory pour voir immédiatement le changement.

Résultats : Après avoir terminé cet exercice, vous devriez avoir effectué une sauvegarde interactive et une restauration faisant autorité de AD DS avec succès.

Exercice 2 : Récupération d'objets dans AD DS

Scénario

Un certain nombre de comptes d'utilisateurs ont été récemment supprimés par erreur. Vous décidez d'activer la Corbeille Active Directory pour faciliter la récupération de compte à l'avenir.

Les tâches principales de cet exercice sont les suivantes :

1. Vérifier les exigences pour la Corbeille Active Directory ;
2. Activer la fonctionnalité Corbeille Active Directory ;
3. Supprimer les objets pour simuler la suppression accidentelle ;
4. Effectuer la restauration de l'objet avec le module Active Directory pour Windows PowerShell ;
5. Vérifier la restauration de l'objet ;
6. Préparez-vous à terminer le cours.

► **Tâche 1 : Vérifier les exigences pour la corbeille Active Directory**

- Sur **LON-DC1**, ouvrez **Domaines et approbations Active Directory** et vérifier le niveau fonctionnel de la forêt. Ce devrait être Windows Server2012 R2.

► **Tâche 2 : Activer la fonctionnalité Corbeille Active Directory**

1. Sur **LON-DC1**, ouvrez **Sites et services Active Directory**, puis répliquer Active Directory entre **LON-DC1** et **LON-DC2**.
2. Démarrez le module Active Directory pour Windows PowerShell.
3. Autorisez la fonctionnalité de Corbeille Active Directory en saisissant la commande suivante, puis appuyez sur Entrée :

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory service,CN=Windows NT,CN=Services,CN=Configuration,DC=adatum,DC=com' adatum -Scope ForestOrConfigurationSet -Target 'Adatum.com'
```

4. Répétez l'étape 1 pour resynchroniser le domaine.

► **Tâche 3 : Supprimer les objets pour simuler la suppression accidentelle**

1. Ouvrez **Utilisateurs et ordinateurs Active Directory**. Connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa\$\$w0rd**.
2. Accédez à l'unité d'organisation **Sales**.
3. Effacer **Abbie Parsons**.
4. Fermez la fenêtre Utilisateurs et ordinateurs Active Directory.

► **Tâche 4 : Effectuer la restauration de l'objet avec le module Active Directory pour Windows PowerShell**

1. Démarrez le module Active Directory pour Windows PowerShell.
2. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Get-ADObject -Filter {displayName -eq "Abbie Parsons"} -IncludeDeletedObjects |  
Restore-ADObject
```

3. Fermez la fenêtre **Windows PowerShell**.

► **Tâche 5 : Vérifier la restauration de l'objet**

1. Sur **LON-DC1**, ouvrez la console **Utilisateurs et ordinateurs Active Directory**.
2. Assurez-vous qu'**Abbie Parsons** existe dans l'unité d'organisation **Sales**.

Résultats : Après avoir terminé l'exercice, vous devez avoir activé et testé la fonctionnalité Corbeille Active Directory avec succès.

► **Tâche 6 : Se préparer pour la fin du cours.**

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-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 rétablir **22742A-LON-DC2**.

Question : Lorsque vous restaurez un utilisateur supprimé ou une unité d'organisation avec des objets utilisateur à l'aide de restauration faisant autorité, les objets sont-ils exactement les mêmes qu'avant ? Quels attributs pourraient ne pas être les mêmes ?

Question : Pendant l'atelier pratique, serait-il possible de restaurer ces objets supprimés s'ils ont été supprimés avant que la Corbeille Active Directory soit activée ?

Contrôle des acquis et éléments à retenir

Question de contrôle des acquis

Question : Quel type de restauration pouvez-vous effectuer avec AD DS ?

Bonnes Pratiques

- Sauvegarder vos contrôleurs de domaine régulièrement.
- Envisager la récupération de la base de données AD DS comme l'un de vos scénarios de restauration pour les contrôleurs de domaine.
- Activer la Corbeille Active Directory pour faciliter la récupération des objets supprimés.
- Utiliser l'AD DS redémarrable lors de l'exécution des tâches de maintenance de base de données.

Évaluation du cours

Votre évaluation de ce cours aidera Microsoft à comprendre la qualité de votre expérience d'apprentissage.

Veuillez travailler avec votre fournisseur pour accéder au formulaire d'évaluation de formation.

Microsoft gardera privées et confidentielles vos réponses à cette enquête et les utilisera pour améliorer vos expériences d'apprentissage futures. Vos commentaires ouverts et honnêtes sont précieux et appréciés.

- Votre évaluation de ce cours aidera Microsoft à comprendre la qualité de votre expérience d'apprentissage.
- S'il vous plaît travaillez avec votre fournisseur pour accéder au formulaire d'évaluation de formation.
- Microsoft gardera privées et confidentielles vos réponses à cette enquête et les utilisera pour améliorer vos expériences d'apprentissage futures. Vos commentaires ouverts et honnêtes sont précieux et appréciés.

Module 1 : Installation et configuration de contrôleurs de domaine

Atelier pratique : Déploiement et administration de AD DS

Exercice 1 : Déploiement d'AD DS

► Tâche 1 : Installer des binaires AD DS

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Windows PowerShell**.
2. À l'invite de commandes dans l'interface de ligne de commande Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Install-WindowsFeature -Name AD-Domain-Services -ComputerName LON-SVR1
```

3. Entrez la commande suivante pour vérifier que le rôle des services de domaine Active Directory (AD DS) est installé sur **LON-SVR1**, puis appuyez sur Entrée.

```
Get-WindowsFeature -ComputerName LON-SVR1
```

4. Dans la sortie de la commande précédente, faites défiler et recherchez **Services de domaine Active Directory**. Vérifiez que la case à cocher est activée. Recherchez **Outils d'administration de serveur distant**. Recherchez le nœud **Outils d'administration de rôles** sous ce dernier, puis recherchez le nœud **Outils AD DS et AD LDS**.



Remarque : En dessous de ce nœud, seul le **Module Active Directory pour Windows PowerShell** a été installé et non les outils graphiques, tels que le Centre d'administration Active Directory. Si vous gérez de manière centralisée vos serveurs, vous n'aurez généralement pas besoin de ces derniers sur chaque serveur. Si vous souhaitez les installer, vous devez spécifier les outils AD DS en exécutant l'applet de commande **Add-WindowsFeature** avec le nom de commande **RSAT-ADDS**.



Remarque : Vous devrez peut-être patienter quelques instants une fois le processus d'installation terminé avant de vérifier que le rôle AD DS a été installé. Si les résultats attendus de la commande **Get-WindowsFeature** ne sont pas visibles, vous pouvez réessayer après quelques minutes.

► Tâche 2 : Préparer l'installation de AD DS et promouvoir un serveur distant

Ajouter LON-SVR1 au Gestionnaire de serveur sur LON-DC1

1. Sur **LON-DC1**, dans **Gestionnaire de serveur**, sélectionnez l'affichage **Tous les serveurs**.
2. Dans le menu **Gérer**, cliquez sur **Ajouter des serveurs**.
3. Dans la boîte de dialogue **Ajouter des serveurs**, conservez les paramètres par défaut, puis cliquez sur **Rechercher maintenant**.
4. Dans la liste des serveurs **Active Directory**, sélectionnez **LON-SVR1**, cliquez sur la flèche pour l'ajouter à la liste **Sélectionnés**, puis cliquez sur **OK**.

Configurer AD DS à distance à l'aide du Gestionnaire de serveur

1. Sur **LON-DC1**, vérifiez que l'installation du rôle AD DS sur **LON-SRV1** est complète et que le serveur a été ajouté au **Gestionnaire de serveur**. Puis cliquez sur le symbole du drapeau **Notifications**.
2. Notez la configuration post-déploiement de **LON-SVR1**, puis cliquez sur le lien **Promouvoir ce serveur en contrôleur de domaine**.
3. Dans l'**Assistant Configuration des services de domaine Active Directory**, sur la page **Configuration de déploiement**, sous **Sélectionner l'opération de déploiement**, vérifiez que **Ajouter un contrôleur de domaine à un domaine existant** est sélectionné.
4. Vérifiez que le domaine **Adatum.com** est spécifié, puis, dans la section **Fournir les informations d'identification pour effectuer cette opération**, cliquez sur **Modifier**.
5. Dans la boîte de dialogue **Informations d'identification pour l'opération de déploiement**, dans la boîte de dialogue **Nom d'utilisateur**, saisissez **Adatum\Administrateur**, puis, dans la boîte de dialogue **Mot de passe**, saisissez **Pa55w.rd**.
6. Cliquez sur **OK**, puis sur **Suivant**.
7. Sur la page **Options de contrôleur de domaine**, désactivez les sélections pour **Serveur Système nom de domaine (DNS)** et **Catalogue global (GC)**. Assurez-vous que **Contrôleur de domaine en lecture seule (RODC)** est désactivé.
8. Dans la section **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)**, saisissez et confirmez le mot de passe **Pa55w.rd**, puis cliquez sur **Suivant**.
9. Sur la page **Options supplémentaires**, cliquez sur **Suivant**.
10. Sur la page **Chemins d'accès**, conservez les paramètres de chemin par défaut pour le **Dossier de base de données**, le **Dossier des fichiers journaux** et le **Dossier SYSVOL**, puis cliquez sur **Suivant**.
11. Sur la page **Examiner les options**, cliquez sur **Afficher le script** pour ouvrir le script Windows PowerShell généré.
12. Dans le Bloc-notes Microsoft, modifiez le script Windows PowerShell généré :
 - Supprimez les lignes de commentaires qui commencent par le signe dièse (#).
 - Supprimez la ligne **Import-Module**.
 - Supprimez les accents graves (`) à la fin de chaque ligne.
 - Supprimez les sauts de ligne.
13. Maintenant, la commande **Install-ADDSDomainController** et tous les paramètres sont sur une seule ligne. Placez le curseur en face de la ligne, puis appuyez sur Maj+Fin pour sélectionner toute la ligne. dans le menu, cliquez sur **Édition**, puis cliquez sur **Copier**.
14. Passez à l'**Assistant de configuration des services de domaine Active Directory**, puis cliquez sur **Annuler**.
15. Lorsque vous êtes invité à confirmer, cliquez sur **Oui** pour annuler l'assistant.
16. Rebasculez vers le **Gestionnaire de serveur**. Dans le menu, cliquez sur **Outils**, puis sur **Windows PowerShell**.
17. À l'invite de commandes de Windows PowerShell, entrez la commande suivante.

```
Invoke-Command -ComputerName LON-SVR1 { }
```

18. Placez le curseur entre les crochets ({}), puis collez le contenu de la ligne de script copié à partir du Presse-papiers. La ligne entière doit se présenter comme suit.

```
Invoke-Command -ComputerName LON-SVR1 {Install-ADSDomainController -NoGlobalCatalog:$true -(Credential (Get-Credential)) -CriticalReplicationOnly:$false -DatabasePath "C:\Windows\NTDS" -DomainName "Adatum.com" -InstallDns:$false -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:$false -SiteName "Default-First-Site-Name" -SysvolPath "C:\Windows\SYSVOL" -Force:$true }
```

19. Appuyez sur Entrée pour lancer la commande.
20. Dans la boîte de dialogue **Demande d'informations d'identification Windows PowerShell**, saisissez **Adatum\Administrateur** dans la boîte de dialogue **Nom d'utilisateur**, saisissez **Pa55w.rd** dans la boîte de dialogue **Mot de passe**, puis cliquez sur **OK**.
21. Lorsque vous êtes invité pour le mot de passe, dans la zone de texte **SafeModeAdministratorPassword**, saisissez **Pa55w.rd**, puis appuyez sur Entrée.
22. Lorsque vous êtes invité à confirmer, dans la zone de texte **Confirmer le mot de passe**, saisissez **Pa55w.rd**, puis appuyez sur Entrée.
23. Patientez jusqu'à ce que la commande soit exécutée et que **Statut réussi** soit renvoyé. L'ordinateur virtuel **LON-SVR1** redémarre.
24. Fermer le Bloc-notes sans enregistrer le fichier.
25. Après le redémarrage de **LON-SVR1**, sur **LON-DC1**, basculez vers **Gestionnaire de serveur**, puis sur le côté gauche, cliquez sur le nœud **AD DS**. Notez que **LON-SVR1** a été ajouté en tant que serveur et que la notification d'avertissement a disparu. Vous pourriez avoir à cliquer sur **Actualiser**.

► **Tâche 3 : Exécuter l'AD DS Best Practices Analyzer**

1. Sur **LON-DC1**, dans **Gestionnaire de serveur**, allez sur la vue du tableau de bord AD DS.
2. Faites défiler jusqu'à la section **Best Practice Analyzer**, cliquez sur le menu **Tâches**, puis sur **Commencer l'analyse BPA**.
3. Dans la boîte de dialogue **Sélection des Serveurs**, sélectionnez **LON-DC1.Adatum.com** et **LON-SVR1.Adatum.com**.
4. Cliquez sur **Démarrer scan**, puis patientez jusqu'à ce que l'Analyseur des meilleures pratiques (BPA) ait terminé l'analyse.
5. Vérifiez les résultats du BPA.

Résultats : Une fois cet exercice terminé, vous aurez créé un nouveau contrôleur de domaine et vérifié les résultats de l'AD DS Best Practices Analyzer (BPA) pour ce contrôleur de domaine.

Exercice 2 : Déploiement de contrôleurs de domaine en procédant à un clonage du contrôleur de domaine

► **Tâche 1 : Vérifier les prérequis pour le clone du contrôleur de domaine**

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Dans **Centre d'administration Active Directory**, double-cliquez sur **Adatum (local)**, puis dans la liste de gestion, double-cliquez sur l'unité organisationnelle (UO) **Domain Controllers**.
3. Dans la liste de gestion, sélectionnez **LON-DC1** si elle n'est pas déjà sélectionnée, puis dans le volet **Office**, dans la section **LON-DC1**, cliquez sur **Ajouter au groupe**.

4. Dans la boîte de dialogue **Sélectionner un groupe**, dans la zone **Entrer les noms d'objets à sélectionner**, saisissez **Clonable**, puis cliquez sur **Vérifier les noms**.
5. Assurez-vous que le nom du groupe est élargi à **Contrôleurs de domaine clonables**, puis cliquez sur **OK**.
6. Sur **LON-DC1**, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
7. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Get-ADCCloningExcludedApplicationList
```

8. Vérifiez la liste des applications critiques, le cas échéant. (Dans la production, vérifiez chaque application ou utilisez un contrôleur de domaine qui a moins d'applications installées par défaut.) Entrez la commande suivante, puis appuyez sur Entrée :

```
Get-ADCCloningExcludedApplicationList -GenerateXML
```

9. Exécutez la commande suivante pour créer le fichier DCCloneConfig.xml.

```
New-ADCCloneConfigFile
```

► Tâche 2 : Copier le contrôleur de domaine source

1. Entrez la commande suivante pour arrêter **LON-DC1**, puis appuyez sur Entrée.

```
Stop-Computer
```

2. Sur l'ordinateur hôte, dans Gestionnaire Microsoft Hyper-V, dans la liste de gestion, sélectionnez l'ordinateur virtuel **22742A-LON-DC1**.
3. Dans le volet **Actions**, dans la section **22742A-LON-DC1**, cliquez sur **Exporter**.
4. Dans la boîte de dialogue **Exporter l'ordinateur virtuel**, saisissez l'emplacement **D:\Program Files\Microsoft Learning\22742**, puis cliquez sur **Exporter**. Patientez jusqu'à ce que l'exportation soit terminée.



Remarque : Selon la configuration de votre salle de classe, le dossier **Program Files\Microsoft Learning\22742** pourrait être sur le lecteur C. Veuillez localiser et utiliser le dossier existant pour le reste de l'atelier pratique.

5. Dans le volet **Actions**, dans la section **22742-LON-DC1**, cliquez sur **Démarrer**, puis connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.

► Tâche 3 : Effectuer le clonage du contrôleur de domaine

1. Sur l'ordinateur hôte, dans le Gestionnaire Hyper-V, dans le volet **Actions**, dans la section qui porte le nom de l'ordinateur hôte, cliquez sur **Importer l'ordinateur virtuel**.
2. Dans l'**Assistant Importer ordinateur virtuel**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Localiser le dossier**, cliquez sur **Parcourir**, accédez au dossier **D:\Program Files\Microsoft Learning\22742\22742A-LON-DC1**, cliquez sur **Sélectionner le dossier**, puis cliquez sur **Suivant**.
4. Sur la page **Sélectionner un ordinateur virtuel**, sélectionnez **22742A-LON-DC1** (si elle n'est pas déjà sélectionnée), puis cliquez sur **Suivant**.

5. Sur la page **Choisir le type d'importation**, sélectionnez **Copiez l'ordinateur virtuel (créer un nouvel ID unique)**, puis cliquez sur **Suivant**.
6. Sur la page **Choisir les dossiers pour fichiers d'ordinateur virtuel**, cochez la case **Stocker l'ordinateur virtuel dans un emplacement différent**.
7. Pour chaque emplacement du dossier, spécifiez **D:\Program Files\Microsoft Learning\22742** comme chemin, puis cliquez sur **Suivant**.
8. Sur la page **Choisir les dossiers pour stocker des disques durs virtuels**, indiquez le chemin d'accès **D:\Program Files\Microsoft Learning\22742**, puis cliquez sur **Suivant**.
9. Sur la page **Fin de l'Assistant Importation**, cliquez sur **Terminer**.
10. Dans la liste de gestion, identifiez et sélectionnez la machine virtuelle nouvellement importée nommée **22742A-LON-DC1** et dont le **Statut** indique **Arrêté**. Dans la section basse du volet **Actions**, cliquez sur **Renommer**.
11. Saisissez le nom **22742A-LON-DC3**, puis appuyez sur Entrée.
12. Dans le volet **Actions** dans la section **22742A-LON-DC3**, cliquez sur **Démarrer**, puis cliquez sur **Connecter** pour voir l'ordinateur virtuel démarrer.
13. Pendant le démarrage du serveur, vous pouvez voir le message **Le clonage du contrôleur de domaine est achevé à x%**.

Résultats : Une fois cet exercice terminé, vous aurez déployé un contrôleur de domaine en le fermant dans Hyper-V.

Exercice 3 : Administration AD DS

► Tâche 1 : Utiliser le Centre d'administration Active Directory

Naviguer dans le Centre d'administration Active Directory

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Dans le volet de navigation, cliquez sur l'onglet **Arborescence**, puis développez **Adatum (local)**.

Effectuer une tâche administrative au sein du Centre d'administration Active Directory

1. Dans le **Centre d'administration Active Directory**, cliquez sur **Aperçu**.
2. Dans la section **Réinitialiser le mot de passe**, dans la zone **Nom d'utilisateur**, saisissez **Adatum\Adam**.
3. Dans les zones **Mot de passe** et **Confirmer le mot de passe**, saisissez **Pa55w.rd**.
4. Désactivez la case à cocher **Changer le mot de passe à la prochaine session**, puis cliquez sur **Appliquer**.
5. Dans la section **Recherche globale**, dans la boîte **Rechercher**, saisissez **Lon**, puis appuyez sur Entrée.

Créer des objets

1. Dans le **Centre d'administration Active Directory**, dans l'arborescence du volet de navigation, développez **Adatum (local)**, puis cliquez sur le conteneur **Computers**.

2. Dans le volet **Tâches** dans la section **Computers**, cliquez sur **Nouveau**, puis sélectionnez **Ordinateur**.
3. Dans la boîte de dialogue **Créer un ordinateur**, fournissez les détails suivants, puis cliquez sur **OK** :
 - o Nom de l'ordinateur : **LON-CL4**
 - o Ordinateur (NetBIOS) : **LON-CL4**

Voir tous les attributs de l'objet

1. Dans le **Centre d'administration Active Directory**, double-cliquez sur **Adatum (local)**, puis dans la liste de gestion, double-cliquez sur **Ordinateurs**.
2. Sélectionner **LON-CL4**, puis dans le volet **Tâches** dans la section **LON-CL4**, cliquez sur **Propriétés**.
3. Dans la fenêtre **Propriétés LON-CL4**, faites défiler jusqu'à la section **Extensions**, cliquez sur l'onglet **Éditeur d'attributs**, puis vous verrez que tous les attributs de l'objet ordinateur sont disponibles ici.
4. Fermez la fenêtre **Propriétés de LON-CL4** en cliquant sur **Annuler**.

Utiliser la visionneuse Windows PowerShell History

1. Dans le **Centre d'administration Active Directory**, cliquez sur la barre d'outils **Historique Windows PowerShell** en bas de l'écran.
2. Voir les détails de l'applet de commande **New AD-Computer** qui a été utilisée pour exécuter la tâche la plus récente.
3. Sur **LON-DC1**, fermez toutes les fenêtres actives.

Résultats : Une fois cet exercice terminé, vous aurez utilisé le Centre d'administration Active Directory pour gérer AD DS et vérifié les applets de commande Windows PowerShell qui fonctionnent dans les coulisses.

► Tâche 2 : Préparer le module suivant

Une fois l'atelier terminé, rétablissez l'état initial de tous les ordinateurs virtuels :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-DC2** et **22742A-LON-SVR1**.

Module 2 : Gestion d'objets dans AD DS

Atelier pratique A : Gestion des objets AD DS

Exercice 1 : Création et gestion des groupes dans AD DS

► Tâche 1 : Créer des groupes et ajouter des membres

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Cliquez sur **Adatum (local)**, puis sur **Managers**.
3. Dans le volet **Tâches**, sous **Gestionnaires**, cliquez sur **Nouveau**, puis sur **Groupe**.
4. Dans le champ **Nom de groupe** : entrez **Gestionnaires de l'entreprise**.
5. Sous **Étendue du groupe**, cliquez sur **Universel**.
6. Cliquez sur **OK** pour fermer la fenêtre **Créer le groupe : Gestionnaires de l'entreprise**.
7. Cliquez **Adatum (local)**, puis cliquez sur l'unité organisationnelle (UO) **Research**.
8. Dans le volet **Tâches**, sous **Rechercher**, cliquez sur **Nouveau**, puis sur **Groupe**.
9. Dans le champ **Nom de groupe** : entrez **Research mail**.
10. Dans la section **Type de groupe**, sélectionnez **Distribution**.
11. Dans le champ **E-mail**, saisissez **Research@adatum.com**.
12. Dans la section **Géré par**, cliquez sur **Modifier**.
13. Dans la boîte de dialogue **Sélectionnez les utilisateurs, contacts, ordinateurs, comptes de service ou groupes**, dans **Entrez les noms des objets à sélectionner (exemples)**, saisissez **Cai**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
14. Cochez la case **Le gestionnaire peut mettre à jour la liste des membres**.
15. Cliquez sur **OK** pour fermer la fenêtre **Créer le groupe : Research mail**.
16. Dans le volet **Tâches**, sous **Rechercher**, cliquez sur **Nouveau**, puis sur **Groupe**.
17. Dans le champ **Nom de groupe** : entrez **Research gestionnaires**.
18. Faites défiler jusqu'à la section **Membres**, puis sur **Ajouter**.
19. Dans la boîte de dialogue **Sélectionnez les utilisateurs, contacts, ordinateurs, comptes de service ou groupes**, dans **Entrez les noms des objets à sélectionner (exemples)**, saisissez **Cai ; Vera**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
20. Cliquez sur **OK** pour fermer la fenêtre **Créer le groupe : Research gestionnaires**.

► Tâche 2 : Configurer l'imbrication du groupe

1. Double-cliquez sur l'UO **Managers**.
2. Cliquez avec le bouton droit sur **Gestionnaires de l'entreprise**, puis cliquez sur **Propriétés**.
3. Dans le volet de navigation, cliquez sur **Membres**, puis sur **Ajouter**.

4. Dans la boîte de dialogue **Sélectionnez les utilisateurs, contacts, ordinateurs, comptes de service ou groupes**, dans **Entrez les noms des objets à sélectionner (exemples)**, saisissez **Managers** ; **Rechercher Gestionnaires**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
 5. Cliquez sur **OK** pour fermer la fenêtre **Gestionnaires de l'entreprise**.
- **Tâche 3 : Convertir un type de groupe de la distribution à la sécurité**
1. Dans le volet de navigation, cliquez sur **Adatum (local)** puis sur l'UO **Research Gestionnaires**
 2. Double-cliquez sur le groupe **Research mail**.
 3. Sous **Type de groupe**, cliquez sur **Sécurité**, puis cliquez sur **OK**.

Résultats : Une fois cet exercice terminé, vous aurez :

- Crée des groupes et ajouté des membres ;
- Configuré l'imbrication du groupe ;
- Converti un type de groupe.

Exercice 2 : Création et configuration de comptes d'utilisateurs dans AD DS

- **Tâche 1 : Créer et configurer un modèle utilisateur pour le département de recherche**
1. Assurez-vous que l'UO **Research** est sélectionnée.
 2. Dans le volet **Tâches**, sous **Rechercher**, cliquez sur **Nouveau**, puis sur **Utilisateur**.
 3. Dans la fenêtre **Créer un utilisateur**, dans le champ **Prénom**, entrez **Modèle de Research**.
 4. Dans le champ **Ouverture de session Utilisateur UPN**, entrez **Modèle de Research**.
 5. Dans les champs **Mot de passe** et **Confirmer le mot de passe**, entrez **Pa55w.rd**.
 6. Dans le volet de navigation, cliquez sur **Organisationet** dans le champ **Service**, entrez **Recherche**.
 7. Dans le champ **Société**, saisissez **Adatum**.
 8. Dans le champ **Responsable**, cliquez sur **Modifier**.
 9. Dans la boîte de dialogue **Sélectionnez les utilisateurs, contacts, ordinateurs, comptes de service ou groupes**, dans **Entrez les noms des objets à sélectionner (exemples)**, saisissez **Cai**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
 10. Dans le volet de navigation, cliquez sur **Membre de**.
 11. Cliquez sur **Ajouter**.
 12. Dans la boîte de dialogue **Sélectionnez les utilisateurs, contacts, ordinateurs, comptes de service ou groupes**, dans **Entrez les noms des objets à sélectionner (exemples)**, saisissez **Research**, puis cliquez sur **Vérifier les noms**. Dans la boîte de dialogue **Noms multiples trouvés**, sélectionnez **Rechercher**, puis cliquez sur **OK** deux fois.
 13. Dans le volet de navigation, cliquez sur **Profil**.
 14. Dans le champ **Se connecter**, entrez **\LON-DC1\Netlogon\Logon.bat**, puis cliquez sur **OK**.
 15. Cliquez sur le compte **Modèle de recherche**, puis dans le volet **Tâches**, sous **Modèle de Research**, cliquez sur **Désactiver**.

16. Fermez le Centre d'administration Active Directory.

► **Tâche 2 : Créer de nouveaux utilisateurs pour la succursale de recherche basés sur le modèle**

1. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Développez **Adatum.com**, puis cliquez sur l'UO **Research**.
3. Cliquez avec le bouton droit sur le compte **Modèle de recherche**, puis cliquez sur **Copier**.
4. Dans la boîte de dialogue **Copier l'objet - Utilisateur**, saisissez **Research** dans le champ **Prénom**, puis saisissez **Utilisateur** dans le champ **Nom de famille**.
5. Dans le champ **Nom d'ouverture de session de l'utilisateur**, entrez **ResearchUser** et cliquez sur **Suivant**.
6. Dans les champs **Mot de passe** et **Confirmer le mot de passe**, entrez **Pa55w.rd**.
7. Désactivez la case à cocher **Le compte est désactivé**, puis cliquez sur **Suivant**.
8. Cliquez sur **Terminer**.

► **Tâche 3 : Valider le modèle**

1. Double-cliquez sur **Recherche utilisateur**.
2. Cliquez sur l'onglet **Profil**, puis assurez-vous que le chemin du script d'ouverture de session est **\LON-DC1\Netlogon\Logon.bat**.
3. Cliquez sur l'onglet **Organisation**, puis vérifiez que le **Service** est **Recherche**, que **Département** est **Adatum** et que le gestionnaire est **Cai Chu**.
4. Cliquez sur l'onglet **Membre de**, puis vérifiez que l'utilisateur est un membre du groupe **Research**.
5. Cliquez sur **Annuler** pour rejeter la boîte de dialogue **Propriétés Utilisateur Recherche**.

Résultats : Une fois cet exercice terminé, vous aurez :

- Crée et configuré un modèle utilisateur pour les utilisateurs de la recherche ;
- Crée trois nouveaux utilisateurs à partir du modèle ;
- Vérifié, en vous authentifiant, que les comptes fonctionnent comme prévu.

Exercice 3 : Gestion des objets ordinateur dans AD DS

► **Tâche 1 : Réinitialiser un compte d'ordinateur**

1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez sur le conteneur **Computers**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur le compte d'ordinateur **LON-CL1**, puis cliquez sur **Réinitialiser le compte**.
3. Dans la boîte de dialogue **Services de domaine Active Directory**, cliquez sur **Oui**.
4. Dans la boîte de message **Services de domaine Active Directory**, cliquez sur **OK**.

► **Tâche 2 : Observer le comportement lorsqu'un client tente de se s'authentifier**

- Redémarrez **LON-CL1** et connectez-vous en tant qu'**Adatum\Adam** avec le mot de passe **Pa55w.rd**.

Question : Quel message s'affiche ?

Réponse : La relation d'approbation entre ce poste de travail et le domaine principal a échoué.

► **Tâche 3 : Résoudre le problème de l'ordinateur**

- Connectez-vous à **LON-CL1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
- Cliquez avec le bouton droit sur le bouton **Démarrer**, puis cliquez sur **Exécuter**.
- Saisissez **PowerShell** et appuyez sur Entrée.
- Dans la fenêtre **Administrateur : Windows PowerShell**, entrez la commande suivante, puis appuyez sur Entrée :

```
Test-ComputerSecureChannel -Repair
```

- Fermez la fenêtre **Windows PowerShell**, puis déconnectez-vous.
- Connectez-vous en tant qu'**Adatum\Adam** avec le mot de passe **Pa55w.rd**. L'ouverture de session réussira maintenant.
- Déconnectez-vous de **LON-CL1**.
- Laissez les ordinateurs virtuels en cours d'exécution pour la démonstration suivante.

Résultats : Une fois cet exercice terminé, vous aurez :

- Réinitialisé un compte d'ordinateur ;
- Observé le comportement lorsqu'un client s'authentifie ;
- Résolu le problème de l'ordinateur.

Atelier pratique B : Administration AD DS

Exercice 1 : Déléguer l'administration pour les UO

► Tâche 1 : Créer une nouvelle UO pour la succursale

1. Sur **LON-DC1**, dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur **Adatum.com**, cliquez sur **Nouveau**, puis cliquez sur **Unité organisationnelle**.
2. Dans **Nouvel objet - Unité organisationnelle**, saisissez **Londres** dans le champ **Nom**, puis cliquez sur **OK**.

► Tâche 2 : Créer des groupes pour les administrateurs de succursales et le personnel du Help-desk de la succursale

1. Cliquez avec le bouton droit sur l'UO **Londres**, cliquez sur **Nouveau**, puis sur **Groupe**.
2. Dans la boîte de dialogue **Nouvel objet - Groupe**, saisissez **Admins Londres**, puis cliquez sur **OK**.
3. Répétez les étapes 1 et 2 pour créer un groupe nommé **Helpdesk Londres**.

► Tâche 3 : Ajouter des membres au groupe

1. Cliquez sur l'UO **IT**.
2. Cliquez avec le bouton droit sur le compte utilisateur **Beth Burke**, puis cliquez sur **Ajouter à un groupe**.
3. Dans la boîte de dialogue **Sélectionner des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemple)** : saisissez **Admins Londres**. Cliquez sur **Vérifier les noms**, puis sur **OK**.
4. Dans la boîte de message **Services de domaine Active Directory**, cliquez sur **OK**.
5. Cliquez avec le bouton droit sur le compte utilisateur **Dante Dabney**, ensuite cliquez sur **Ajouter à un groupe**.
6. Dans la boîte de dialogue **Sélectionner des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemple)** : saisissez **Helpdesk Londres**. Cliquez sur **Vérifier les noms**, puis sur **OK**.
7. Dans la boîte de message **Services de domaine Active Directory**, cliquez sur **OK**.

► Tâche 4 : Déléguer des autorisations au groupe

1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez sur **Affichage**, puis cliquez sur **Fonctionnalités avancées**.
2. Cliquez avec le bouton droit sur l'UO **Londres**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Sécurité**, puis sur **Ajouter**.
4. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemple)** : saisissez **Admins Londres**. Cliquez sur **Vérifier les noms**, puis sur **OK**.
5. Vérifiez que le groupe **Londres Admins** est sélectionné, cochez **Contrôle total** dans la colonne **Autoriser**, puis cliquez sur **OK**.
6. Cliquez avec le bouton droit sur l'UO **Londres**, puis cliquez sur **Délégation de contrôle**.
7. Dans l'**Assistant Délégation de contrôle**, cliquez sur **Suivant**.
8. Sur la page **Utilisateurs ou groupes**, cliquez sur **Ajouter**.

9. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs ou des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemple)** : saisissez **Helpdesk Londres**. Cliquez sur **Vérifier les noms**, cliquez sur **OK** puis sur **Suivant**.
10. Sur la page **Tâches à déléguer**, cliquez sur **Créer une tâche personnalisée à déléguer**, puis sur **Suivant**.
11. Sur la page **Type d'objet Active Directory**, cliquez sur **Seul l'objet suivant dans ce dossier**.
12. Faites défiler vers le bas de la liste. Cliquez sur **Objets utilisateur**, sélectionnez les cases à cocher pour **Créer les objets sélectionnés dans ce dossier** et **Supprimer les objets sélectionnés dans ce dossier**, puis cliquez sur **Suivant**.
13. Sur la page **Autorisations**, cliquez sur **Contrôle total**, puis sur **Suivant**.
14. Cliquez sur **Terminer**.

► Tâche 5 : Tester les autorisations

1. Basculez vers **LON-SVR1**.
2. Cliquez sur **Démarrer**, cliquez sur **Gestionnaire de serveur**, puis sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner les fonctionnalités**, développez **Outils d'administration de serveur distant**, puis développez **Outils d'administration de rôles**. Développez les **Outils AD DS et AD LDS**. Cochez la case à côté de **Outils AD DS** puis cliquez sur **Suivant**.
8. Cliquez sur **Installer**. Patientez jusqu'à la fin de l'installation.
9. Une fois l'installation terminée, cliquez sur **Fermer**.
10. Déconnectez-vous de **LON-SVR1**.

Tester les autorisations pour Admins Londres

1. Connectez-vous à **LON-SVR1** en tant que **Beth** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, puis cliquez sur la vignette **Gestionnaire de serveur**.
3. Cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
4. Développez **Adatum.com**, puis cliquez sur l'UO **Research**. Notez que les icônes de la barre d'outils pour créer des utilisateurs, des groupes ou des UO sont grises.
5. Cliquez sur l'UO **Londres**. Notez que ces icônes sont maintenant activées.
6. Cliquez avec le bouton droit sur l'UO **Londres**, cliquez sur **Nouveau**, puis sur **Unité organisationnelle**.
7. Dans la boîte de dialogue **Nouvel objet - Unité organisationnelle**, saisissez **Laptops** dans le champ **Nom**, puis cliquez sur **OK**. La création réussira.
8. Déconnectez-vous de **LON-SVR1**.

Tester les autorisations pour le Helpdesk de Londres

1. Connectez-vous à **LON-SVR1** en tant que **Dante** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, puis cliquez sur la vignette **Gestionnaire de serveur**.
3. Cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
4. Développez **Adatum.com**, puis cliquez sur l'UO **Londres**. Notez que la seule icône non grisée est l'icône créer un utilisateur.

Résultats : Une fois cet exercice terminé, vous aurez :

- Crée une nouvelle UO pour la succursale ;
- Crée des groupes pour les administrateurs de succursales et le personnel de support technique de la succursale ;
- Ajouté des membres au groupe ;
- Délgué des autorisations aux groupes ;
- Installé les outils AD DS et testé les autorisations.

Exercice 2 : Création et modification d'objets AD DS dans Windows PowerShell

► Tâche 1 : Créer un compte utilisateur en utilisant Windows PowerShell

1. Basculez vers **LON-DC1**.
2. Cliquez avec le bouton droit sur le bouton **Démarrer**, puis cliquez sur **Windows PowerShell (Admin)**.
3. Créez un compte utilisateur pour Ty Carlson dans l'UO Londres en exécutant la commande suivante :

```
New-ADUser -Name Ty -DisplayName "Ty Carlson" -GivenName Ty -Surname Carlson -Path "ou=Londres,dc=adatum,dc=com"
```

4. Définissez le mot de passe pour le compte en exécutant la commande suivante :

```
Set-ADAccountPassword Ty
```

5. Lorsque vous recevez une invite pour le mot de passe actuel, appuyez sur Entrée.
6. Lorsque vous recevez une invite pour le mot de passe souhaité, entrez **Pa55w.rd** et appuyez sur Entrée.
7. Lorsque vous recevez une invite pour répéter le mot de passe, entrez **Pa55w.rd** et appuyez sur Entrée.
8. Pour activer le compte, exécutez la commande suivante :

```
Enable-ADAccount Ty
```

9. Testez le compte en allant sur **LON-CL1**, puis connectez-vous en tant que **Ty** avec le mot de passe **Pa55w.rd**.

► Tâche 2 : Créer un nouveau groupe en utilisant Windows PowerShell

- Sur **LON-DC1**, dans la fenêtre **Administrateur : Windows PowerShell**, exécutez la commande suivante :

```
New-ADGroup LondonBranchUsers -Path "ou=Londres,dc=adatum,dc=com" -GroupScope Global  
-GroupCategory Security
```

► **Tâche 3 : Ajouter un membre au groupe en utilisant Windows PowerShell**

1. Dans la fenêtre **Administrateur : Windows PowerShell**, exécutez la commande suivante :

```
Add-ADGroupMember LondonBranchUsers -Members Ty
```

2. Confirmez que l'utilisateur est dans le groupe en exécutant la commande suivante :

```
Get-ADGroupMember LondonBranchUsers
```

► **Tâche 4 : Modifier le fichier .csv**

1. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
2. Dans l'Explorateur de fichiers, développez **AllFiles (E:)**, développez **Labfiles**, puis cliquez sur **Mod02**.
3. Cliquez avec le bouton droit sur **LabUsers.ps1**, puis cliquez sur **Modifier**. Dans **Administrateur : Windows PowerShell (ISE)**, lisez les commentaires au début du script, puis identifier les conditions requises pour l'en-tête dans le fichier csv.
4. Dans l'Explorateur de fichiers, double-cliquez sur **LabUsers.csv**.
5. Dans le message **Comment voulez-vous ouvrir ce type de fichier (.csv)?**, cliquez sur **Bloc-notes**. Cliquez sur **OK**.

6. Dans le Bloc-notes, entrez la ligne suivante en haut du fichier :

```
FirstName,LastName,Department,DefaultPassword
```

7. Cliquez sur **Fichier**, puis sur **Enregistrer**.

8. Fermez le **Bloc-notes**.

► **Tâche 5 : Modifier le script**

1. Dans la fenêtre **Administrateur : Fenêtre Windows PowerShell (ISE)**, sous **Variables**, remplacez **C:\path\file.csv** par **E:\Labfiles\Mod02\LabUsers.csv**.
2. De nouveau sous **Variables**, remplacez **ou=orgunit,dc=domain,dc=com** par **ou=London,dc=adatum,dc=com**.
3. Cliquez sur **Fichier**, puis sur **Enregistrer**. Faites défiler vers le bas et révisez le contenu du script.
4. Fermez la fenêtre **Administrateur : Fenêtre Windows PowerShell (ISE)**.

► **Tâche 6 : Exécuter le script**

1. Allez sur la fenêtre **Administrateur : Windows PowerShell**.
2. À l'invite de commande, entrez **cd E:\Labfiles\Mod02**, puis appuyez sur Entrée.
3. Entrez **.\LabUsers.ps1**, puis appuyez sur Entrée
4. Pour afficher les utilisateurs tout juste créés, entrez la commande suivante et appuyez sur Entrée :

```
Get-ADUser -Filter * -SearchBase "ou=London,dc=adatum,dc=com"
```

► Tâche 7 : Préparer le module suivant

Une fois l'atelier terminé, rétablissez l'état initial de tous les ordinateurs virtuels :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-DC2**, **22742A-LON-SVR1** et **22742A-LON-CL1**.

Résultats : Une fois cet exercice terminé, vous aurez :

- Crée un compte utilisateur à l'aide de Windows powershell ;
- Crée un groupe à l'aide de Windows powershell ;
- Ajouté un utilisateur à un groupe à l'aide de Windows powershell ;
- Modifié le fichier .csv ;
- Modifié le script ;
- Exécuté le script.

Module 3 : Gestion avancée de l'infrastructure AD DS

Atelier pratique : Domaine et gestion des approbations dans AD DS

Exercice 1 : Implémenter des approbations de forêts

► Tâche 1 : Configurer les zones de stub pour résolution de nom DNS

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur le menu **Outils** puis sur **DNS** dans la liste déroulante.
2. Dans le volet d'**arborescence DNS**, développez **LON-DC1**, cliquez avec le bouton droit sur **Zones de recherche directes**, puis cliquez sur **Nouvelle zone**.
3. Dans l'**Assistant Nouvelle zone**, cliquez sur **Suivant**.
4. Sur la page **Type de zone**, cliquez sur **Zone de stub**, puis sur **Suivant**.
5. Sur la page **Étendue de la zone de réPLICATION Active Directory**, cliquez sur **Vers tous les serveurs DNS exécutés sur des contrôleurS de domaine dans cette forêt : adatum.com**, puis sur **Suivant**.
6. Dans la zone de texte **Nom de zone** : tapez **treyresearch.net**, puis cliquez sur **Suivant**.
7. Sur la page **Serveurs DNS maîtres**, cliquez sur <**Cliquez ici pour ajouter une adresse IP ou un nom DNS**>, tapez **172.16.10.10**, cliquez sur l'espace libre, puis sur **Suivant**.
8. Sur la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Suivant**, puis sur **Terminer**.
9. Développez **Zones de recherche directes**, cliquez avec le bouton droit sur la nouvelle zone de stub **treyresearch.net**, puis cliquez sur **Transfert de Maître**.
10. Cliquez avec le bouton droit sur **treyresearch.net**, puis cliquez sur **Actualiser**.
11. Vérifiez que la zone de stub **treyresearch.net** contient des enregistrements et fermez **Gestionnaire DNS**.
12. Basculez vers **TREY-DC1**.
13. Dans le **Gestionnaire de serveur**, cliquez sur le menu **Outils** puis sur **DNS** dans la liste déroulante.
14. Dans le volet d'**arborescence**, développez **TREY-DC1**, cliquez avec le bouton droit sur **Zones de recherche directes**, puis cliquez sur **Nouvelle zone**.
15. Dans l'**Assistant Nouvelle zone**, cliquez sur **Suivant**.
16. Sur la page **Type de zone**, cliquez sur **Zone de stub**, puis sur **Suivant**.
17. Sur la page **Étendue de la zone de réPLICATION Active Directory**, cliquez sur **Vers tous les serveurs DNS exécutés sur des contrôleurS de domaine dans cette forêt : Treyresearch.net**, puis cliquez sur **Suivant**.
18. Dans la zone de texte **Nom de zone**, entrez **adatum.com**, puis cliquez sur **Suivant**.
19. Sur la page **Serveurs DNS maîtres**, cliquez sur <**Cliquez ici pour ajouter une adresse IP ou un nom DNS**>, tapez **172.16.0.10**, cliquez sur l'espace libre, puis sur **Suivant**.
20. Sur la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Suivant**, puis sur **Terminer**.
21. Développez **Zones de recherche directes**, cliquez avec le bouton droit sur la nouvelle zone stub **adatum.com**, puis cliquez sur **Transfert de Maître**.

22. Cliquez avec le bouton droit sur **adatum.com**, puis cliquez sur **Actualiser**.
 23. Vérifiez que la zone stub **adatum.com** contient des enregistrements.
 24. Fermez le **Gestionnaire DNS**.
- **Tâche 2 : Configurer une approbation de forêt avec l'authentification sélective**
1. Sur **LON-DC1**, dans le menu **Outils**, cliquez sur **Domaines et approbations Active Directory**.
 2. Dans la console de gestion **Domaines et approbations Active Directory**, cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Propriétés**.
 3. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur l'onglet **Approbations**, puis sur **Nouvelle approbation**.
 4. Sur la page **Assistant nouvelle approbation**, cliquez sur **Suivant**.
 5. Sur la page **Nom d'approbation**, dans la zone de texte **Nom**, tapez **treyresearch.net**, puis cliquez sur **Suivant**.
 6. Sur la page **Type d'approbation**, cliquez sur **Approbation de forêt**, puis sur **Suivant**.
 7. Sur la page **Sens de l'approbation**, cliquez sur **Sens unique : en sortie**, puis sur **Suivant**.
 8. Sur la page **Sens de l'approbation**, cliquez sur **Ce domaine et le domaine spécifié**, puis sur **Suivant**.
 9. Sur la page **Nom d'utilisateur et mot de passe**, entrez **Administrateur** comme nom d'utilisateur et **Pa55w.rd** comme mot de passe dans les cases appropriées, puis cliquez sur **Suivant**.
 10. Sur la page **Niveau d'authentification d'approbation sortante**, cliquez sur **Authentification sélective**, puis sur **Suivant**.
 11. Sur la page **Fin de la sélection des approbations**, cliquez sur **Suivant**.
 12. Sur la page **Fin de la création de l'approbation**, cliquez sur **Suivant**.
 13. Sur la page **Confirmer l'approbation sortante**, cliquez sur **Suivant**.
 14. Sur la page **Fin de l'Assistant Nouvelle approbation**, cliquez sur **Terminer**.
 15. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur l'onglet **Approbations**.
 16. Sous l'onglet **Approbations**, sous **Domaines approuvés par ce domaine (approbations sortantes)**, cliquez sur **treyresearch.net**, puis sur **Propriétés**.
 17. Dans la boîte de dialogue **Propriétés treyresearch.net**, cliquez sur **Valider**.
 18. Lisez le message qui s'affiche : **L'approbation a été validée. Elle est en place et active.**
 19. Cliquez **OK**, puis à l'invite, cliquez sur **Non**.
 20. Cliquez sur **OK** dans la boîte de dialogue **Propriétés TreyResearch.net**, puis cliquez sur **OK** dans la boîte de dialogue **Propriétés Adatum.com**.
 21. Fermez **Domaines et approbations Active Directory**.
- **Tâche 3 : Configurer un serveur pour l'authentification sélective**
1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur le menu **Outils** puis sur **Utilisateurs et ordinateurs Active Directory**.
 2. Dans la console **Utilisateurs et ordinateurs Active Directory**, dans le menu **Affichage**, cliquez sur **Fonctionnalités avancées**.
 3. Développez **Adatum.com**, puis cliquez sur **Computers**.

4. Cliquez avec le bouton droit sur **LON-SVR2**, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés LON-SVR2**, cliquez sur l'onglet **Sécurité**, puis sur **Ajouter**.
6. Dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, cliquez sur **Emplacements**.
7. Cliquez sur **treyresearch.net**, puis sur **OK**.
8. Dans la zone de texte **Entrer le nom de l'objet à sélectionner (exemples :)**, tapez **IT**, puis cliquez sur **Vérifier les noms**. Lorsque vous êtes invité à entrer des informations d'identification, entrez **treyresearch\administrator** avec le mot de passe **Pa55w.rd**, puis cliquez sur **OK**.
9. Sur la page **Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, cliquez sur **OK**.
10. Dans la fenêtre **Propriétés LON-SVR2**, assurez-vous que **IT (TreyResearch\IT)** est sélectionné, activez la case à cocher **Autoriser** en ligne avec **Autorisation d'authentifier**, puis cliquez sur **OK**.
11. Basculez vers **LON-SVR2**.
12. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
13. Dans la fenêtre de l'**Explorateur de fichiers**, cliquez sur **Disque local (C:)**.
14. Cliquez avec le bouton droit dans le volet d'informations, cliquez sur **Nouveau**, puis sur **Dossier**.
15. Dans la zone de texte **Nom**, entrez **IT-Données**, puis appuyez sur Entrée.
16. Cliquez avec le bouton droit sur **IT-Données**, pointez sur **Partager avec**, puis cliquez sur **Personnes spécifiques**.
17. Dans la boîte de dialogue **Partage de fichiers**, entrez **TreyResearch\IT**, puis cliquez sur **Ajouter**.
18. Cliquez sur **Lire**, sous **Niveau d'autorisation** de **IT**, puis cliquez sur **Lecture/écriture**. Cliquez sur **Partager**, puis sur **Terminer**.
19. Sur **TREY-DC1**, dans le **Gestionnaire de serveur**, cliquez sur le menu **Outils** puis sur **Utilisateurs et ordinateurs Active Directory**.
20. Dans la console **Utilisateurs et ordinateurs Active Directory**, développez **TreyResearch.net**, puis cliquez sur **Users**.
21. Double-cliquez sur le groupe **Admins du Domaine**. Dans l'onglet **Membres**, cliquez sur **Ajouter**, entrez **Alice**, puis cliquez deux fois sur **OK**.
22. Déconnectez-vous de **TREY-DC1**.
23. Connectez-vous à **TREY-DC1** comme **TreyResearch\Alice** avec le mot de passe **Pa55w.rd**.
24. Cliquez sur **Démarrer**, puis sur **Rechercher**.
25. Dans la zone de texte **Rechercher**, entrez **\LON-SVR2\IT-Données**, puis appuyez sur Entrée. Le dossier s'ouvre.

Résultats : Une fois cet exercice terminé, vous aurez implémenté les approbations de forêts.

Exercice 2 : Mise en œuvre des domaines enfants dans AD DS

► Tâche 1 : Installer un contrôleur de domaine dans un domaine enfant

1. Sur **TOR-DC1**, cliquez sur **Démarrer**, puis cliquez sur **Gestionnaire de serveur**. Dans le **Gestionnaire de serveur**, cliquez sur **Gérer** et dans la zone de liste déroulante, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, confirmez que l'option **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, assurez-vous que **Sélectionner un serveur du pool de serveurs** est sélectionné et que **TOR-DC1.adatum.com** est surligné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionnez les rôles du serveur**, cliquez sur **Services du domaine Active Directory**.
6. Sur la page **Ajouter des fonctionnalités requises pour les services de domaine Active Directory ?**, cliquez sur **Ajouter des fonctionnalités**.
7. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Sur la page **Services de domaine Active Directory**, cliquez sur **Suivant**.
10. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**. Ce processus dure plusieurs minutes.
11. Lorsque les Services de domaine Active Directory (AD DS) binaires ont été installés, cliquez sur le lien bleu **Promouvoir ce serveur à un contrôleur de domaine**.
12. Dans la fenêtre **Configuration de déploiement**, cliquez sur **Ajouter un nouveau domaine à une forêt existante**.
13. Vérifier que **Sélectionnez le type de domaine** est ajusté sur **Domaine enfant** et que **Nom de domaine parent** est ajusté sur **Adatum.com**. Dans la zone de texte **Nouveau nom de domaine**, tapez **na**.
14. Assurez-vous que **Fournir les informations d'identification pour effectuer cette opération** est ajusté sur **Adatum\Administrateur (utilisateur actuel)**, puis cliquez sur **Suivant**.



Remarque : Si les informations d'identification ne sont pas ajustées sur **Adatum\Administrateur**, utilisez le bouton **Modifier** pour entrer les informations d'identification **Adatum\Administrateur** et le mot de passe **Pa55w.rd**.

15. Dans la fenêtre **Options de contrôleur de domaine**, assurez-vous que **Niveau fonctionnel de domaine** est défini sur **Windows Server Technical Preview**.
16. Assurez-vous que les deux cases à cocher **Système de nom de domaine (DNS)** et **Catalogue global (GC)** sont activées.
17. Confirmez que **Nom du site** : est défini sur **Nom-Premier-Site-Par défaut**.
18. Sous **Entrer le mot de passe du mode de restauration des services d'annuaire (DSRM)**, entrez **Pa55w.rd** dans les deux zones de texte, puis cliquez sur **Suivant**.
19. Sur la page **Options DNS**, cliquez sur **Suivant**.
20. Sur la page **Options supplémentaires**, cliquez sur **Suivant**.

21. Sur la page **Chemins**, cliquez sur **Suivant**.
22. Sur la page **Examiner les options**, cliquez sur **Suivant**.
23. Sur la page **Vérification de la configuration requise**, confirmez qu'il n'y a pas de problèmes, puis cliquez sur **Installer**.



Remarque : Si vous recevez l'avertissement suivant qui empêche les algorithmes de cryptographie les plus faibles lors de l'établissement des sessions de canal de sécurité, vous pouvez l'ignorer en toute sécurité : « Prévisualisation technique Windows Server 2016, 5 contrôleurs de domaines ont une valeur par défaut pour le paramètre de sécurité appelé Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0. »

Une fois la configuration terminée, le serveur redémarre automatiquement.

► Tâche 2 : Vérifier la configuration de la confiance par défaut

1. Connectez-vous à **TOR-DC1** en tant que **NA\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, puis sur **Gestionnaire de serveur**. Dans le Gestionnaire de serveur, cliquez sur **Serveur local**.
3. Vérifiez que **Pare-feu Windows** affiche **Domaine : Désactivé**. Si ce n'est pas le cas, procédez comme suit :
 - a. Cliquez sur le texte souligné en bleu à côté de **Pare-feu Windows**. Dans la fenêtre **Pare-feu Windows**, cliquez sur **Activer ou désactiver le pare-feu Windows**.
 - b. Sous chaque section, sélectionnez **Désactivez le pare-feu Windows (non recommandé)**, puis cliquez sur **OK**. Ignorer les messages d'avertissement qui apparaissent concernant le Pare-feu Windows.
 - c. Dans **Gestionnaire de serveur**, cliquez sur l'icône **Actualiser le « serveur local »**, indiqué par des doubles flèches.
 - d. Après la mise à jour terminée, vérifiez que **Pare-feu Windows** affiche **Public : Désactivé**.
4. Dans **Gestionnaire de serveur**, dans le menu **Outils**, cliquez sur **Domaines et approbations Active Directory**.
5. Dans la console **Domaines et approbations Active Directory**, développez **Adatum.com**, cliquez avec le bouton droit sur **na.adatum.com**, puis cliquez sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés na.adatum.com**, cliquez sur l'onglet **Approbations**, puis dans la boîte de dialogue **Domaine de confiance pour ce domaine (approbations sortantes)**, cliquez sur **Adatum.com**, puis sur **Propriétés**,
7. Dans la boîte de dialogue **Propriétés adatum.com**, cliquez sur **Valider**, puis cliquez sur **Oui, valider l'approbation entrante**.
8. Dans la zone de texte **Nom d'utilisateur**, tapez **Administrateur** et dans le champ **Mot de passe**, tapez **Pa55w.rd**, puis cliquez sur **Oui**.
9. Lorsque le message « La relation d'approbation a été validée. Elle est en place et activée » apparaît, cliquez sur **OK**.



Remarque : Si vous recevez un message indiquant que la relation d'approbation ne peut pas être validée ou que la vérification de canal sécurisé a échoué, assurez-vous que vous avez terminé l'étape 3, puis patientez au moins 10 à 15 minutes avant de réessayer.

10. Cliquez deux fois sur **OK** pour fermer la boîte de dialogue **Propriétés Adatum.com**.

Résultats : Une fois cet exercice terminé, vous aurez implémenté des domaines enfants dans AD DS.

► **Tâche : Préparer le module suivant**

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-DC2**, **22742A-TOR-DC1**, **22742A-TREY-DC1** et **22742A-LON-SVR2**.

Module 4 : Mise en œuvre et administration des sites AD DS et réPLICATION

Atelier pratique : Mise en œuvre des sites AD DS et réPLICATION

Exercice 1 : Modification du site par défaut

► Tâche 1 : Installer le contrôleur de domaine Toronto

1. Sur **TOR-DC1**, cliquez sur **Démarrer**, puis cliquez sur **Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Gérer** et dans la zone de liste déroulante, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, confirmez que **Installation basée sur un rôle ou une fonctionnalité** est sélectionné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, assurez-vous que **Sélectionner un serveur du pool de serveurs** est sélectionné et que **TOR-DC1.adatum.com** est surligné, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, cochez la case **Services de domaine Active Directory**.
7. Sur le **Ajouter des fonctionnalités requises pour les services de domaine Active Directory ?** cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
8. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Sur la page **Services de domaine Active Directory**, cliquez sur **Suivant**.
10. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.



Remarque : Ce processus durera plusieurs minutes.

11. Lorsque les Services de domaine Active Directory (AD DS) binaires ont été installés, ne cliquez pas sur **Fermer** mais cliquez sur le lien bleu **Promouvoir ce serveur à un contrôleur de domaine**.
12. Dans la fenêtre **Configuration de déploiement**, cliquez sur **Ajouter un contrôleur de domaine à un domaine existant**, puis cliquez sur **Suivant**.
13. Dans la fenêtre **Options du contrôleur de domaine**, assurez-vous que les deux cases à cocher **Système de nom de domaine (DNS)** et **Catalogue global (GC)** sont activées.
14. Confirmez que **Nom du site** : est réglé sur **Default-First-Site-Name**, puis sous **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)**, entrez **Pa55w.rd** dans les deux boîtes **Mot de passe** et **Confirmer le mot de passe**. Cliquez sur **Suivant**.
15. Sur la page **Options DNS**, cliquez sur **Suivant**.
16. Sur la page **Options supplémentaires**, cliquez sur **Suivant**.
17. Dans la fenêtre **Chemins**, cliquez sur **Suivant**.
18. Dans la fenêtre **Examiner les options**, cliquez sur **Suivant**.

19. Dans la fenêtre **Confirmer les conditions préalables**, cliquez sur **Installer**. Le serveur redémarre automatiquement.
20. Après le redémarrage de **TOR-DC1**, connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.

► **Tâche 2 : Renommer le site par défaut**

1. Si nécessaire, sur **LON-DC1**, ouvrez la console **Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
3. Dans **Sites et services Active Directory**, dans le volet de navigation, développez **Sites**.
4. Cliquez avec le bouton droit sur **Default-First-Site-Name**, puis cliquez sur **Renommer**.
5. Entrez **LondonHQ**, puis appuyez sur Entrée.
6. Développez **LondonHQ**, développez le dossier **Serveurs**, puis vérifiez que **LON-DC1** et **TOR-DC1** appartiennent au site **LondonHQ**.

► **Tâche 3 : Configurer des sous-réseaux IP associés au site par défaut**

1. Si nécessaire, sur **LON-DC1**, ouvrez la console **Gestionnaire de serveur**, puis ouvrez **Sites et services Active Directory**.
2. Dans la console **Sites et services Active Directory**, dans le volet de navigation, développez **Sites**, puis cliquez sur le dossier **Subnets**.
3. Cliquez avec le bouton droit sur **Sous-réseaux**, puis cliquez sur **Nouveau sous-réseau**.
4. Dans la boîte de dialogue **Nouvel objet - Sous-réseau**, sous **Préfixe**, saisissez **172.16.0.0/24**.
5. Sous **Sélectionner un objet de site pour ce préfixe**, cliquez sur **LondonHQ**, puis cliquez sur **OK**.

Résultats : Une fois cet exercice terminé, vous aurez reconfiguré le site par défaut et attribué des sous-réseaux d'adresses IP au site.

Exercice 2 : Création de sites et sous-réseaux supplémentaires

► **Tâche 1 : Créer les sites AD DS pour Toronto**

1. Si nécessaire, sur **LON-DC1**, ouvrez la console **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
2. Dans la console **Sites et services Active Directory**, dans le volet de navigation, cliquez avec le bouton droit sur **Sites**, puis cliquez sur **Nouveau Site**.
3. Dans la boîte de dialogue **Nouvel objet - Site**, dans la zone de texte **Nom**, saisissez **Toronto**.
4. Sous **Sélectionnez un objet de lien de sites pour ce site**, cliquez sur **DEFAULTSITELINK**, puis cliquez sur **OK**.
5. Dans la boîte de dialogue **Services de domaine Active Directory**, cliquez sur **OK**. Le site de Toronto s'affiche dans le volet de navigation.
6. Dans la console **Sites et services Active Directory**, dans le volet de navigation, cliquez avec le bouton droit sur **Sites**, puis cliquez sur **Nouveau Site**.
7. Dans la boîte de dialogue **Nouvel objet - Site**, dans la zone de texte **Nom**, entrez **Test**.

8. Sous **Sélectionnez un objet de lien de sites pour ce site**, sélectionnez **DEFAULTIPSITELINK**, puis cliquez sur **OK**. Le site de test s'affiche dans le volet de navigation.
- **Tâche 2 : Créer des sous-réseaux IP qui sont associés avec les sites de Toronto**
1. Si nécessaire, sur **LON-DC1**, ouvrez la console **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
 2. Dans la console **Sites et services Active Directory**, dans le volet de navigation, développez **Sites**, puis cliquez sur le dossier **Sous-réseaux**.
 3. Cliquez avec le bouton droit sur **Sous-réseaux**, puis cliquez sur **Nouveau sous-réseau**.
 4. Dans la boîte de dialogue **Nouvel objet - Sous-réseau**, sous **Préfixe**, saisissez **172.16.1.0/24**.
 5. Sous **Sélectionnez un objet de site pour ce préfixe**, cliquez sur **Toronto**, puis cliquez sur **OK**.
 6. Cliquez avec le bouton droit sur **Sous-réseaux**, puis cliquez sur **Nouveau sous-réseau**.
 7. Dans la boîte de dialogue **Nouvel objet - Sous-réseau**, sous **Préfixe**, saisissez **172.16.100.0/24**.
 8. Sous **Sélectionnez un objet de site pour ce préfixe**, cliquez sur **Test**, puis cliquez sur **OK**.
 9. Dans le volet de navigation, cliquez sur le dossier **Sous-réseaux**. Vérifiez dans le volet d'informations que les deux sous-réseaux sont créés et associés à leur site approprié.



Remarque : Il y a trois sous-réseaux au total (**172.16.0.0** a été créé dans l'exercice 1, Tâche 3, « Configurer des sous-réseaux IP associés au site par défaut »).

Résultats : Une fois cet exercice terminé, vous aurez créé deux sites supplémentaires représentant les adresses de sous-réseau IP à Toronto.

Exercice 3 : Configuration de la réPLICATION AD DS

► **Tâche 1 : Configurer les liens du site entre les sites AD DS**

1. Si nécessaire, sur **LON-DC1**, ouvrez la console **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
2. Dans la console **Sites et services Active Directory**, dans le volet de navigation, développez **Sites**, développez **Transports Inter-Site**, puis cliquez sur le dossier **IP**.
3. Cliquez avec le bouton droit sur **IP**, puis cliquez sur **Nouveau lien de sites**.
4. Dans la boîte de dialogue **Nouvel objet - lien de sites**, dans la zone de texte **Nom**, entrez **TOR-TEST**.
5. Sous **Sites exclus de ce lien de sites**, appuyez sur la touche Ctrl du clavier, cliquez successivement sur **Toronto**, **Test** et **Ajouter**, puis cliquez sur **OK**.
6. Cliquez avec le bouton droit sur **TOR-TEST**, puis cliquez sur **Propriétés**.
7. Dans la boîte de dialogue **Propriétés TOR-TEST**, cliquez sur **Modifier la planification**.
8. Dans la boîte de dialogue **Calendrier de TOR-TEST**, sélectionnez la plage de **Lundi 9 heures** à **Vendredi 15 heures**, comme suit :
 - o Cliquez sur la vignette **Lundi à 9h00**, appuyez et maintenez le bouton de la souris, puis faites glisser le curseur vers la vignette **Vendredi à 15h00**.

9. Cliquez sur **RéPLICATION non disponible**, puis cliquez sur **OK**.
10. Cliquez sur **OK** pour fermer **Propriétés TOR-TEST**.
11. Cliquez avec le bouton droit sur **DEFAULTIPSITELINK**, puis cliquez sur **Renommer**.
12. Entrez **LON-TOR**, puis appuyez sur Entrée.
13. Cliquez avec le bouton droit sur **LON-TOR**, puis cliquez sur **Propriétés**.
14. Sous **Sites dans ce lien de sites**, cliquez sur **Test**, puis sur **Supprimer**.
15. Dans la zone de sélection numérique **Répliquer toutes les**, modifiez la valeur à **60** minutes, puis cliquez sur **OK**.

► Tâche 2 : Déplacer TOR-DC1 sur le site Toronto

1. Si nécessaire, dans **LON-DC1**, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
2. Dans la console **Sites et services Active Directory**, dans le volet de navigation, développez **Sites**, développez **LondonHQ**, puis cliquez sur le dossier **Serveurs**.
3. Cliquez avec le bouton droit sur **TOR-DC1**, puis cliquez sur **Déplacer**.
4. Dans la boîte de dialogue **Déplacer serveurs**, cliquez sur **Toronto**, puis sur **OK**.
5. Dans le volet de navigation, développez le site **Toronto**, développez **Serveurs**, puis cliquez sur **TOR-DC1**.

► Tâche 3 : Surveiller la réPLICATION de site AD DS

1. Sur **LON-DC1**, cliquez sur **Démarrer**, puis sur l'icône **Windows PowerShell**.
2. À l'invite Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Repadmin / kcc
```

Cette commande recalcule la topologie de réPLICATION entrante pour le serveur.

3. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Repadmin /showrep1
```

4. Vérifiez que la dernière réPLICATION avec **TOR-DC1** s'est déroulée avec succès.

5. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Repadmin /bridgeheads
```

Cette commande affiche les serveurs têtes de pont pour la topologie de site.

6. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Repadmin /replsummary
```

Cette commande affiche un résumé des tâches de réPLICATION. Vérifiez qu'aucune erreur n'apparaisse.

7. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
DCDiag /test:replications
```

8. Vérifiez que tous les tests de connectivité et de réPLICATION se déroulent avec succès.

9. Basculez vers **TOR-DC1**, puis répétez les étapes 1 à 8 pour afficher les informations de **TOR-DC1**. Pour l'étape 4, vérifiez que la dernière réPLICATION avec **LON-DC1** a été réussie.

Résultats : Une fois cet exercice terminé, vous aurez configuré les liens du site et contrôlé la réPLICATION.

Exercice 4 : Surveillance et dépannage de la réPLICATION AD DS

► Tâche 1 : Produire une erreur

1. Si nécessaire, sur **LON-DC1**, ouvrez **Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
3. Dans la console **Sites et services Active Directory** dans le volet de navigation, développez successivement **Sites**, **LondonHQ**, **Serveurs** et **LON-DC1**, puis sélectionnez **Paramètres NTDS**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur l'objet de connexion **TOR-DC1**, puis cliquez sur **Répliquer maintenant**.
5. Dans la boîte de dialogue **Répliquer maintenant**, cliquez sur **OK**.
6. Dans **Sites et services Active Directory**, examinez tous les objets que vous avez créés précédemment, puis sur la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
7. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Get-ADReplicationUpToDateNessVectorTable -Target "adatum.com"
```

 **Remarque :** Cette cmdlet vous montrera les derniers événements de réPLICATION. Notez la date et l'heure du dernier événement (en haut).

8. Allez à **TOR-DC1**.

9. Cliquez sur **Démarrer**, puis cliquez sur **Windows PowerShell**.

10. À l'invite de commandes Windows PowerShell, entrez les commandes suivantes et appuyez sur Entrée après chaque commande :

```
CD \Labfiles\Mod04
.\Mod04Ex4.ps1
```

► Tâche 2 : Surveiller la réPLICATION de site AD DS

1. Si nécessaire, sur **TOR-DC1**, ouvrez la console **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
2. Dans la console **Sites et services Active Directory** dans le volet de navigation, développez successivement **Sites**, **Toronto**, **Serveurs** et **TOR-DC1**, puis sélectionnez **Paramètres NTDS**.
3. Dans le volet d'informations, cliquez avec le bouton droit sur **LON-DC1**, puis sélectionnez **Répliquer maintenant**.
4. Cliquez sur **OK** sur le menu déroulant **Répliquer maintenant**.
5. Sur **TOR-DC1**, dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
6. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Get-ADReplicationUpToDateNessVectorTable -Target "adatum.com"
```

-  **Remarque :** Cette cmdlet vous montrera les derniers événements de réPLICATION. Notez que la dernière date et heure indiquée (**RéPLICATION de LON-DC1**) n'est pas mise à jour. Ceci indique que la réPLICATION unidirectionnelle ne se produit pas.

7. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Get-AdReplicationSubnet -filter *
```

-  **Remarque :** Cette applet de commande affiche des informations détaillées sur tous les sous-réseaux affectés à tous les sites. Notez que rien n'est retourné.

8. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Get-AdReplicationSiteLink -filter *
```

-  **Remarque :** Cette applet de commande affiche des informations détaillées sur tous les liens de site affectés à des sites en particulier. Notez que rien n'est retourné.

► Tâche 3 : Dépanner la réPLICATION AD DS

1. Si nécessaire, sur **TOR-DC1**, ouvrez **Windows PowerShell**.

2. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Ipconfig /all
```

3. Examinez les résultats. L'adresse du serveur DNS doit être **10.0.0.1**.

4. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Get-DNSClient | Set-DnsClientServerAddress -ServerAddresses ("172.16.0.10",  
"172.16.0.25")
```

5. Exécutez de nouveau la commande **Ipconfig/all**. Les adresses du serveur DNS doivent être **172.16.0.10** et **172.16.0.25**.

6. Si nécessaire, sur **TOR-DC1**, ouvrez la console **Gestionnaire de serveur**, cliquez sur **Outils**, puis cliquez sur **Sites et services Active Directory**.

7. Dans la console **Sites et services Active Directory** dans le volet de navigation, développez successivement **Sites**, **Toronto**, **Serveurs** et **TOR-DC1**, puis sélectionnez **Paramètres NTDS**.

8. Dans le volet d'informations, cliquez avec le bouton droit sur **LON-DC1**, puis sélectionnez **Répliquer maintenant**.

9. Dans **Sites et services Active Directory**, examinez tous les objets que vous avez créés précédemment. Manque-t-il quelque chose ?

10. Sur **TOR-DC1**, ouvrez l'**Explorateur de fichiers**. Recherchez **C:\Labfiles\Mod04**.

11. Cliquez avec le bouton droit sur le dossier **Mod04EX4Fix.ps1**, puis sélectionnez **Exécuter à l'aide de PowerShell**. Entrez **O** à l'invite concernant la stratégie d'exécution, puis appuyez sur Entrée.

12. Dans **Sites et services Active Directory**, examinez tous les objets que vous avez créés précédemment. Assurez-vous que le lien de sites a été créé dans le nœud **Transports Inter-Site** et que les sous-réseaux ont été créés dans le nœud **Subnets**.
13. Sur **LON-DC1** et **TOR-DC1**, fermez toutes les fenêtres ouvertes, puis déconnectez-vous des deux ordinateurs virtuels.

Résultats : Une fois cet exercice terminé, vous aurez diagnostiqué et résolu les problèmes liés à la réplication.

► Tâche 4 : Préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-DC2** et **22742A-TOR-DC1**.

Module 5 : Implémentation d'une stratégie de groupe

Atelier pratique A : Implémentation d'une infrastructure de stratégie de groupe

Exercice 1 : Création et configuration des GPO

► Tâche 1 : Créer et modifier un GPO

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans le volet de navigation, développez **Forêt : Adatum.com**, **Domaines** et **Adatum.com**, puis cliquez sur **Objets de stratégie de groupe**.
3. Dans le volet de navigation, cliquez avec le bouton droit sur le conteneur **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
4. Dans la zone de texte **Nom**, saisissez **Normes ADATUM**, puis cliquez sur **OK**.
5. Dans le volet d'informations, cliquez avec le bouton droit sur l'Objet de stratégie de groupe (GPO) **Normes ADATUM**, puis cliquez sur **Modifier**.
6. Dans la fenêtre **Éditeur de gestion de la stratégie de groupe** fenêtre, dans le volet de navigation, développez **Configuration Utilisateur**, développez successivement **Stratégies** et **Modèles d'administration**, puis cliquez sur **Système**.
7. Double-cliquez sur le paramètre de stratégie **Empêcher l'accès aux outils de modification du registre**.
8. Dans la boîte de dialogue **Empêche l'accès aux outils de modifications du Registre**, cliquez sur **Activé**, puis sur **OK**.
9. Dans le volet de navigation, développez successivement **Configuration utilisateur**, **Stratégies**, **Modèles d'administration** et **Panneau de configuration**, puis cliquez sur **Personnalisation**.
10. Dans le volet d'informations, double-cliquez sur le paramètre de stratégie **Dépassement du délai d'expiration de l'écran de veille**.
11. Dans la boîte de dialogue **Dépassement du délai d'expiration de l'écran de veille**, cliquez sur **Activé**, dans la zone de texte **Secondes**, entrez **600**, puis cliquez sur **OK**.
12. Double-cliquez sur le paramètre de stratégie **Le mot de passe protège l'écran de veille**.
13. Dans la boîte de dialogue **Un mot de passe protège l'écran de veille**, cliquez sur **Activé**, puis sur **OK**.
14. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.

► Tâche 2 : Lier le GPO

1. Dans la fenêtre **Gestion de la stratégie de groupe**, dans le volet de navigation, cliquez avec le bouton droit sur le domaine **Adatum.com**, puis cliquez sur **Lier un GPO existant**.
2. Dans la boîte de dialogue **Sélectionner GPO**, cliquez sur **Normes ADATUM**, puis cliquez sur **OK**.

► Tâche 3 : Voir les effets des paramètres du GPO

1. Basculez vers **LON-CL1**, puis connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Cliquez avec le bouton droit sur **Démarrer**, puis sur **Panneau de configuration**.

3. Cliquez sur **Système et sécurité**, puis sur **Autoriser une application via le Pare-feu Windows**.
4. Dans la liste **Applications et fonctionnalités autorisées**, cochez les cases suivantes, puis cliquez sur **OK** :
 - **Gestion à distance des journaux des événements**
 - **Infrastructure de gestion Windows (WMI)**
5. Déconnectez-vous, puis connectez-vous en tant que **Adatum\Connie** avec le mot de passe **Pa\$\$w0rd**.
6. Cliquez sur **Démarrer**, saisissez **écran de veille**, puis cliquez sur **Modifier l'écran de veille**. (La modification de l'état peut prendre quelques minutes).
7. Dans la boîte de dialogue **Paramètres de l'écran de veille**, notez que l'option **Paramètres** est grisée : vous ne pouvez pas modifier le délai d'attente. Notez que l'option **À la reprise, afficher l'écran d'ouverture de session** est sélectionnée et grisée et que vous ne pouvez pas modifier les paramètres. Si l'option **À la reprise, afficher l'écran d'ouverture de session** est désactivée et grisée, effectuez les étapes suivantes :
 - a. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Exécuter**.
 - b. Dans la boîte de dialogue **Exécuter**, dans la zone de texte **Ouvrir**, saisissez **gpupdate/force**, puis cliquez sur **OK**.
 - c. Cliquez sur **Démarrer**, saisissez **écran de veille**, puis cliquez sur **Modifier l'écran de veille**.
8. Cliquez sur **OK**.
9. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Exécuter**.
10. Dans la boîte de dialogue **Exécuter**, dans la zone de texte **Ouvrir**, saisissez **regedit**, puis cliquez sur **OK**.
11. Dans la boîte de dialogue **Éditeur du Registre**, cliquez sur **OK**.

Résultats : Une fois cet exercice terminé, vous aurez créé, édité et partagé le GPO requis.

Exercice 2 : Gestion de l'étendue des GPO

► Tâche 1 : Créer et lier les GPO requis

1. Sur **LON-DC1**, dans **Console de gestion des stratégies de groupe**, dans le volet de navigation, développez successivement **Forêt : Adatum.com**, **Domaines** et **Adatum.com**, puis cliquez sur **Research**.
2. Cliquez avec le bouton droit sur l'UO **Recherche**, puis cliquez sur **Créer un GPO dans ce domaine et le lier ici**.
3. Dans la boîte de dialogue **Nouveau GPO**, dans la zone de texte **Nom**, saisissez **Rechercher remplacement application**, puis cliquez sur **OK**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur **Rechercher remplacement application GPO**, puis cliquez sur **Modifier**.
5. Dans l'arborescence de la console, développez successivement **Configuration utilisateur**, **Stratégies**, **Modèles d'administration** et **Panneau de configuration**, puis cliquez sur **Personnalisation**.

6. Double-cliquez sur le paramètre de stratégie **Dépassement du délai d'expiration de l'écran de veille**.
7. Cliquez sur **Désactivé**, puis sur **OK**.
8. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.

► **Tâche 2 : Vérifier l'ordre de priorité**

- Dans l'arborescence **Console de gestion de stratégie de groupe**, cliquez sur l'OU **Research**, puis cliquez sur l'onglet **Héritage de stratégie de groupe**. Notez que le GPO **Rechercher remplacement application** a une priorité supérieure au GPO **Normes ADATUM**. Le paramètre de stratégie de Dépassement du délai d'expiration de l'écran de veille que vous venez de configurer dans le GPO **Recherche remplacement application** est appliqué après le réglage dans le GPO **Normes ADATUM**. Par conséquent, le nouveau réglage remplacera le paramètre de normes et prévaudra. La mise en veille automatique de l'écran ne sera pas disponible pour les utilisateurs dans le cadre du GPO **Modification de l'application de recherche**.

► **Tâche 3 : Configurer l'étendue d'un GPO avec filtrage de sécurité**

1. Sur **LON-DC1**, dans la **Console de gestion Stratégie de groupe**, dans le volet de navigation, si nécessaire, développez l'UO **Research**, puis cliquez sur le GPO **Recherche remplacement application** sous l'UO **Research**.
2. Dans la boîte de dialogue **Console de gestion Stratégie de groupe**, lisez le message, cochez la case **Ne plus afficher ce message**, puis cliquez sur **OK**.
3. Dans la section **Filtrage de sécurité**, vous verrez que le GPO s'applique par défaut à tous les utilisateurs authentifiés.
4. Dans la section **Filtrage de sécurité**, cliquez sur **Utilisateurs authentifiés**, puis cliquez sur **Supprimer**.
5. Dans la boîte de dialogue **Gestion des stratégies de groupe**, cliquez sur **OK**.
6. Dans le volet d'informations, cliquez sur **Ajouter**.
7. Dans la boîte de dialogues **Sélectionner un utilisateur, un ordinateur ou un groupe**, dans la zone **Entrez les noms des objets à sélectionner (exemple)** : entrez **Research** et cliquez ensuite sur **OK**.

► **Tâche 4 : Configurer le traitement de bouclage**

1. Sur **LON-DC1**, dans la **Console de gestion de stratégie de groupe**, dans le volet de navigation, cliquez sur **Adatum.com**, cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvelle unité organisationnelle**.
2. Dans la boîte de dialogue **Nouvelle unité organisationnelle**, dans la zone de texte **Nom**, entrez **Kiosques**, puis cliquez sur **OK**.
3. Cliquez avec le bouton droit sur **Kiosques**, puis cliquez sur **Nouvelle unité organisationnelle**.
4. Dans la boîte de dialogue **Nouvelle unité organisationnelle**, dans la zone de texte **Nom**, entrez **Salles de conférence**, puis cliquez sur **OK**.
5. Dans le volet de navigation, développez l'UO **Kiosques**, puis cliquez sur l'UO **Salles de conférence**.
6. Cliquez avec le bouton droit sur l'UO **Salles de conférence**, puis cliquez sur **Créer un GPO dans ce domaine et le lier ici**.
7. Dans la boîte de dialogue **Nouveau GPO**, dans la zone **Nom**, saisissez **Paramètres de salle de conférence**, puis cliquez sur **OK**.

8. Dans le volet de navigation, développez **Salles de conférence**, puis cliquez sur le GPO **Paramètres de salle de conférence**.
9. Dans le volet de navigation, cliquez avec le bouton droit sur le GPO **Paramètres de salle de conférence**, puis cliquez sur **Modifier**.
10. Dans la fenêtre **Éditeur de gestion de la stratégie de groupe** fenêtre, dans le volet de navigation, développez successivement **Configuration Utilisateur**, **Stratégies**, **Modèles d'administration** et **Panneau de configuration** puis cliquez sur **Personnalisation**.
11. Dans le volet d'informations, double-cliquez sur le paramètre de stratégie **Dépassement du délai d'expiration de l'écran de veille**, puis cliquez sur **Activé**.
12. Dans la zone **Secondes**, saisissez **7200**, puis cliquez sur **OK**.
13. Dans le volet de navigation, développez successivement **Configuration ordinateur**, **Stratégies**, **Modèles d'administration** et **Système**, puis cliquez sur **Stratégie de groupe**.
14. Dans le volet d'informations, double-cliquez sur le paramètre de stratégie **Configurer le mode de traitement en boucle de la stratégie de groupe utilisateur**, puis cliquez sur **Activé**.
15. Dans la liste déroulante **Mode**, sélectionnez **Fusionner**, puis cliquez sur **OK**.
16. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.

Résultats : Une fois cet exercice terminé, vous aurez configuré l'étendue requise des objets de stratégie de groupe (GPO).

► **Tâche 5 : Préparer l'atelier suivant**

- Après avoir terminé cet atelier pratique, laissez tous les ordinateurs virtuels s'exécuter pour l'atelier pratique suivant.

Atelier pratique B : Dépannage de l'infrastructure de stratégie de groupe

Exercice 1 : Vérifier l'application GPO

► Tâche 1 : Effectuer une analyse RSOP

1. Basculez vers **LON-CL1**, puis vérifiez que vous êtes connecté en tant **Adatum\Connie**. Si nécessaire, utilisez le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, saisissez **cmd**, puis appuyez sur Entrée.
3. À l'invite de commandes, entrez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

4. Patientez jusqu'à ce que la commande ait terminé. Prenez note de l'heure actuelle du système, que vous aurez besoin de savoir pour une tâche ultérieure dans cet exercice. Pour enregistrer l'heure du système, entrez la commande suivante et appuyez deux fois sur Entrée :

```
Time
```

5. Redémarrez **LON-CL1**. Patientez jusqu'au redémarrage de **LON-CL1** avant de passer à la tâche suivante. Ne pas se connecter à **LON-CL1**.
6. Basculez vers **LON-DC1**.
7. Passez à la **Console Gestion de stratégie de groupe**.
8. Dans le volet de navigation, si nécessaire, développez **Forêt : Adatum.com**, puis cliquez sur **Résultats de stratégie de groupe**.
9. Cliquez avec le bouton droit sur **Résultats de stratégie de groupe**, puis cliquez sur **Assistant Résultats de stratégie de groupe**.
10. Sur la page **Bienvenue dans l'Assistant Résultats de stratégie de groupe**, cliquez sur **Suivant**.
11. Sur la page **Sélection des ordinateurs**, sélectionnez l'option **Autre ordinateur**, saisissez **LON-CL1**, puis cliquez sur **Suivant**.
12. Sur la page **Sélection des utilisateurs**, cliquez sur **ADATUM\Connie**, puis sur **Suivant**.
13. Sur la page **Aperçu des sélections**, vérifiez vos paramètres, puis cliquez sur **Suivant**.
14. Cliquez sur **Terminer**. Le rapport RSOP apparaît dans le volet d'informations de la **Console de gestion de la stratégie de groupe**.
15. Vérifiez les résultats du résumé. Pour la configuration de l'utilisateur et de l'ordinateur, identifiez l'heure de la dernière actualisation de la stratégie et la liste des GPO autorisées et refusées. Identifier les composants utilisés pour traiter les paramètres de stratégie.
16. Cliquez sur l'onglet **Détails**. Vérifiez les paramètres qui ont été appliqués au cours de l'application des stratégies d'utilisateur et d'ordinateur, puis identifiez le GPO à partir duquel les paramètres ont été obtenus.
17. Cliquez sur l'onglet **Événements de stratégie**, puis localisez l'événement qui enregistre l'actualisation de la stratégie que vous avez déclenchée avec la commande **gpupdate**.
18. Cliquez sur l'onglet **Résumé**, cliquez avec le bouton droit sur un espace vide sur la page, puis cliquez sur **Enregistrer le rapport**.

19. Dans le volet de navigation, cliquez sur **Bureau**, puis sur **Enregistrer**.
20. Sur le bureau, cliquez avec le bouton droit sur **Connie sur LON-CL1.htm**, pointez vers **Ouvrir avec**, puis cliquez sur **Internet Explorer**.
21. Lorsque vous avez examiné le rapport, fermez Microsoft Internet Explorer.

► Tâche 2 : Analyser RSoP avec GPResult

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Connie** avec le mot de passe **Pa55w.rd**.
2. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Invite de commandes**.
3. À l'invite de commandes, entrez la commande suivante et appuyez sur Entrée :

```
gpresult /r
```
4. Les résultats du résumé RSoP s'affichent. Notez que l'information est très similaire à l'onglet **Résumé** du rapport RSoP qui a été produit par l'**Assistant Résultats de stratégie de groupe**.
5. À l'invite de commandes, entrez la commande suivante et appuyez sur Entrée :

```
gpresult /v | more
```
6. Appuyez sur la barre d'espace pour parcourir le rapport. Notez que la plupart des paramètres de stratégie de groupe qui ont été appliqués par le client sont énumérés dans le présent rapport.
7. À l'invite de commandes, entrez la commande suivante et appuyez sur Entrée :

```
gpresult /z | more
```
8. Appuyez sur la barre d'espace pour parcourir le rapport. Ce rapport est le rapport RSoP le plus détaillé.
9. À l'invite de commandes, entrez la commande suivante et appuyez sur Entrée :

```
gpresult /h:"%userprofile%\Desktop\RSOP.html"
```

Un rapport RSoP est enregistré en fichier HTML sur votre bureau.

10. Ouvrez le rapport RSoP enregistré à partir de votre bureau. Comparez le rapport, ses informations et sa mise en forme avec le rapport RSoP que vous avez enregistré dans la tâche précédente.
11. Déconnectez-vous de **LON-CL1**.

► Tâche 3 : Évaluer les résultats GPO en utilisant l'Assistant Modélisation de stratégie de groupe

1. Sur **LON-DC1**, dans **Console de gestion des stratégies de groupe**, dans le volet de navigation, cliquez sur **Modélisation de la stratégie de groupe**.
2. Cliquez avec le bouton droit sur **Modélisation de la stratégie de groupe**, puis cliquez sur **Assistant de modélisation de stratégie de groupe**.
3. Dans l'**Assistant Modélisation de stratégie de groupe**, cliquez sur **Suivant**.
4. Sur la page **Sélection du contrôleur de domaine**, cliquez sur **Suivant**.
5. Sur la page **Sélection d'ordinateurs et d'utilisateurs**, dans la section **Informations sur l'utilisateur**, sélectionnez l'option **Utilisateur**, puis cliquez sur **Parcourir**. Dans la boîte de dialogue **Sélectionner utilisateur**, entrez **Connie**, puis appuyez sur Entrée.

6. Dans la section **Informations sur l'ordinateur**, sélectionnez l'option **Ordinateur**, puis cliquez sur **Parcourir**. Dans la boîte de dialogue **Sélectionner un ordinateur**, saisissez **LON-CL1**, puis appuyez sur Entrée.
7. Dans l'**Assistant Modélisation de stratégie de groupe**, cliquez sur **Suivant**.
8. Sur la page **Options de simulation avancées**, cochez la case **Traitement en boucle**, puis sélectionnez l'option **Fusionner**. Même si le GPO **Paramètres Salle de conférence** spécifie un traitement de bouclage, vous devez demander à **Assistant Modélisation de stratégie de groupe** d'envisager le traitement en boucle dans sa simulation. Cliquez sur **Suivant**.
9. Sur la page **Autres chemins Active Directory**, à côté de **Emplacement de l'ordinateur**, cliquez sur **Parcourir**.
10. Dans la boîte de dialogue **Sélectionner conteneur ordinateur**, développez successivement **Adatum** et **Kiosques**, puis cliquez sur **Salles de conférence**. Vous simulez l'effet de **LON-CL1** comme ordinateur de salle de conférence. Cliquez sur **OK**, puis sur **Suivant**.
11. Sur la page **Groupes de sécurité utilisateur**, cliquez sur **Suivant**.
12. Sur la page **Groupes de sécurité ordinateur**, cliquez sur **Suivant**.
13. Sur la page **Filtres WMI pour Utilisateurs**, cliquez sur **Suivant**.
14. Sur la page **Filtres WMI pour Ordinateurs**, cliquez sur **Suivant**.
15. Sur la page **Aperçu des sélections**, cliquez sur **Suivant**, puis sur **Terminer**.
16. Dans le volet d'informations, cliquez sur l'onglet **Détails**, si nécessaire développez successivement **Détails de l'utilisateur**, **Objets de stratégie de groupe** et **GPOs appliqués**.
17. Vérifiez si le GPO **Paramètres Salle de conférence** s'applique à Connie en tant que stratégie utilisateur quand elle se connecte à **LON-CL1**, si **LON-CL1** est dans l'UO **Salles de conférence**.
18. Faites défiler jusqu'à, et si nécessaire développez, **Détails de l'utilisateur**, **Paramètres**, **Stratégies**, **Modèles d'administration** et **Panneau de configuration/Personnalisation**.
19. Vérifiez que le délai d'attente de l'écran de veille est de 7200 secondes (2 heures), le paramètre configuré par le GPO **Paramètres Salle de conférence** qui remplace la norme 10 minutes configurée par le GPO **Normes ADATUM**.

► **Tâche 4 : Examiner les événements de stratégie et déterminer l'état de l'infrastructure GPO**

1. Basculez vers **LON-CL1**. Connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Observateur d'événements**.
3. Dans le volet de navigation, développez **Journaux Windows**, puis cliquez sur le journal **Système**.
4. Cliquez sur l'en-tête de colonne **Source** pour trier le journal **Système** par source.
5. Repérez l'événement **1500, 1501, 1502** ou **1503** avec **Stratégie de groupe** comme source.
6. Passez en revue l'information qui est associée aux événements de stratégie de groupe.
7. Dans le volet de navigation, développez successivement **Journaux d'applications et services**, **Microsoft**, **Windows** et **Stratégie de groupe**, puis cliquez sur **Opérationnel**.
8. Localisez le premier événement lié à l'actualisation de la stratégie de groupe que vous avez lancée lors de la première opération avec la commande **gpupdate**. Examinez cet événement et les événements qui ont suivi.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

9. Déconnectez-vous de **LON-CL1**.
10. Basculez vers **LON-DC1**.
11. Dans la fenêtre **Gestion des stratégies de groupe**, dans le volet de navigation, cliquez sur le domaine **Adatum.com**.
12. Sous l'onglet **Etat**, vérifiez que **LON-DC1.Adatum.com** est répertorié en tant que contrôleur de domaine de base.
13. Cliquez sur **Détecter maintenant**.
14. Développez la flèche à côté de la coche verte. Vérifiez que **LON-DC2.Adatum.com** est répertorié en tant que contrôleur de domaine avec la réPLICATION synchrone. Certains stagiaires pourraient voir **LON-DC2.Adatum.com** répertorié comme contrôleur de domaine avec réPLICATION en cours. Cela est dû à l'environnement de l'atelier pratique.

Résultats : Une fois cet exercice terminé, vous aurez utilisé les outils RSOP pour vérifier l'application correcte de vos GPO, examiné les événements de stratégie de groupe et vérifié l'intégrité de l'infrastructure de stratégie de groupe.

Exercice 2 : Dépannage des GPO

► Tâche 1 : Lire l'enregistrement d'incident du service d'assistance et simuler le problème

1. Lisez l'**Enregistrement d'incident du service d'assistance 604531** dans le scénario du manuel d'exercices.
2. Dans **LON-DC1**, dans la barre des tâches, cliquez sur **Explorateur de fichiers**.
3. Dans l'Explorateur de fichiers, dans le volet de navigation, développez successivement **AllFiles (E:)** et **Labfiles**, puis cliquez sur **Mod05**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur **Mod05-1.ps1**, puis cliquez sur **Exécuter avec PowerShell**. Appuyez sur **Y**, puis appuyez sur Entrée lorsque vous y êtes invité.

► Tâche 2 : Mettre à jour le Plan d'action de l'enregistrement d'incident

1. Lisez la section **Information additionnelle** de l'Enregistrement des incidents dans le scénario de l'exercice du manuel du stagiaire.
2. Mettez à jour la section **Plan d'action** de l'enregistrement d'incident dans le manuel du stagiaire avec vos recommandations :
 - o Vérifiez la configuration pour **Connie Vaughn**.
 - o RSOP de **Assistant Résultats de stratégie de groupe** va ensuite fournir les informations de configuration pour **Connie Vaughn**.
 - o Le GPO **Rechercher remplacement application** doit fournir la configuration correcte. S'informer sur la configuration du GPO.

► Tâche 3 : Dépanner et résoudre le problème

1. Sur **LON-CL1**, connectez-vous en tant qu'**Adatum\Connie** avec le mot de passe **Pa55w.rd**.
2. Cliquez avec le bouton droit sur **Démarrer**, puis sur **Panneau de configuration**.

3. Dans le Panneau de configuration, cliquez sur **Apparence et personnalisation**, puis sur **Modifier l'écran de veille**.
4. Vérifiez que **Patienter** est grisé et a une valeur de **10 minutes**.
5. Déconnectez-vous de **LON-CL1**.
6. Basculez vers **LON-DC1**.
7. Dans la fenêtre **Gestion des stratégies de groupe**, dans le volet de navigation, cliquez sur **Résultats de la stratégie de groupe**.
8. Cliquez avec le bouton droit sur **Résultats de stratégie de groupe**, puis cliquez sur **Assistant Résultats de stratégie de groupe**.
9. Sur la page **Bienvenue dans l'Assistant Résultats de stratégie de groupe**, cliquez sur **Suivant**.
10. Sur la page **Sélection des ordinateurs**, sélectionnez l'option **Autre ordinateur**, saisissez **LON-CL1**, puis cliquez sur **Suivant**.
11. Sur la page **Sélection des utilisateurs**, cliquez sur **ADATUM\Connie**, puis sur **Suivant**.
12. Sur la page **Aperçu des sélections**, vérifiez vos paramètres, puis cliquez sur **Suivant**.
13. Cliquez sur **Terminer**.
14. Cliquez sur l'onglet **Détails**, puis cliquez sur **Tout afficher**.
15. Dans la section **Détails de l'utilisateur**, recherchez la section **Paramètres**, puis dans **Panneau de configuration/Personnalisation**, vérifiez que le délai d'attente de l'écran de veille est de 600 secondes et que le GPO gagnant est **Normes ADATUM**.
16. Dans la section **Détails de l'utilisateur**, recherchez les GPO refusés et vérifier que le GPO **Rechercher remplacement application** est dans la liste des GPO refusés une raison de **Vide**.
Dans ce cas, il semble que Connie Vaugh ne soit plus un membre du groupe Recherche.
17. Basculez vers la fenêtre **Gestionnaire Serveur**.
18. Cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
19. Dans la fenêtre **Utilisateurs et ordinateurs Active Directory**, si nécessaire développez le domaine **Adatum.com**, puis cliquez sur l'UO **Recherche**.
20. Dans le volet d'informations, double-cliquez sur le groupe **Recherche**.
21. Dans la boîte de dialogue **Propriétés de recherche**, cliquez sur l'onglet **Membres**, puis vérifiez que Connie Vaugh ne figure pas en tant que membre du groupe.
22. Cliquez sur **Ajouter**. Dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, saisissez **Connie**, puis cliquez sur **OK**.
23. Dans la boîte de dialogue **Propriétés de recherche**, cliquez sur **OK**.
24. Fermez la fenêtre **Utilisateurs et ordinateurs Active Directory**.
25. Basculez vers **LON-CL1**.
26. Sur **LON-CL1**, connectez-vous en tant qu'**Adatum\Connie** avec le mot de passe **Pa55w.rd**.
27. Cliquez avec le bouton droit sur **Démarrer**, puis sur **Panneau de configuration**.
28. Dans le Panneau de configuration, cliquez sur **Apparence et personnalisation**, puis sur **Modifier l'écran de veille**.
29. Vérifiez que **Patienteze** est grisé et a une valeur de **1 minute**.
30. Si **Patienteze** est toujours grisé, procédez comme suit :

- a. Cliquez avec le bouton droit sur **Démarrer**, survolez **Arrêter ou se déconnecter**, puis cliquez sur **Redémarrer**.
 - b. Connectez-vous en tant qu'**Adatum\Connie** avec le mot de passe **Pa55w.rd**.
 - c. Effectuer les étapes 27-29.
31. Déconnectez-vous de **LON-CL1**.

Résultats : Une fois cet exercice terminé, vous aurez résolu le problème d'application GPO.

► Tâche 4 : Préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-CL1** et **22742A-LON-DC2**.

Module 6 : Gestion des paramètres de l'utilisateur avec la stratégie de groupe

Atelier pratique : Gestion des paramètres de l'utilisateur avec la stratégie de groupe

Exercice 1 : Utilisation de modèles d'administration pour gérer les paramètres utilisateur

► Tâche 1 : Importer des modèles d'administration pour Microsoft Office 2016

1. Sur **LON-DC1**, dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
2. Dans l'Explorateur de fichiers, dans le volet de navigation, développez successivement **AllFiles (E:)** et **Labfiles**, puis cliquez sur **Mod06**.
3. Double-cliquez sur **admintemplates_x64_4390-1000_en-us.exe**.
4. Dans la boîte de dialogue **Modèles d'administration Microsoft Office 2016**, cochez la case **Cliquez ici pour accepter les termes du contrat de licence Microsoft**, puis cliquez sur **Continuer**.
5. Dans la boîte de dialogue **Rechercher un dossier**, cliquez sur **Bureau**, puis sur **OK**.
6. Dans la boîte de dialogue **Modèles d'administration Microsoft Office 2016**, cliquez sur **OK**.
7. Dans l'Explorateur de fichiers, dans le volet de navigation, cliquez sur **Bureau**, puis dans le volet de contenu, double-cliquez sur **admx**.
8. Appuyez sur **Ctrl+A** pour sélectionner tous les fichiers, cliquez avec le bouton droit, puis cliquez sur **Copier**.
9. Dans le volet de navigation, développez successivement **Disque local (C:)** et **Windows**, cliquez avec le bouton droit sur **PolicyDefinitions**, puis cliquez sur **Coller**.
10. Fermez l'**Explorateur de fichiers**.

► Tâche 2 : Configurer les paramètres de Office 2016

1. Dans **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion de la stratégie de groupe**.
2. Basculez vers la fenêtre **Gestion des stratégies de groupe**.
3. Dans le volet de navigation, développez **Forêt : Adatum.com, Domaines et Adatum.com**, puis cliquez sur **Objets de stratégie de groupe (GPO)**.
4. Cliquez avec le bouton droit sur **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
5. Dans la boîte de dialogue **Nouveau GPO**, saisissez **Paramètres Office 2016**, puis cliquez sur **OK**.
6. Dans le volet d'informations, cliquez avec le bouton droit sur **Paramètres Office 2016**, puis cliquez sur **Modifier**.
7. Dans la fenêtre **Éditeur de gestion de la stratégie de groupe**, dans le volet de navigation, développez successivement **Configuration Utilisateur**, développez **Stratégies** et **Modèles d'administration**, puis cliquez sur **Microsoft Excel 2016**.
8. Développez **Microsoft Excel 2016**, développez **Options Excel**, cliquez sur **Personnaliser le ruban**, puis double-cliquez sur **Afficher l'onglet Développeur dans le ruban**.

9. Dans la boîte de dialogue **Afficher l'onglet Développeur dans le ruban**, cliquez sur **Activé**, puis cliquez sur **OK**.
 10. Dans **Éditeur de gestion des stratégies de groupe**, cliquez sur **Enregistrer**, puis double-cliquez sur **Emplacement du fichier par défaut**.
 11. Dans la boîte de dialogue **Emplacement du fichier par défaut**, cliquez sur **Activé**, dans la zone de texte **Emplacement du fichier par défaut**, saisissez **%userprofile%\Desktop**, puis cliquez sur **OK**.
 12. Fermez l'**Éditeur de gestion des stratégies de groupe**.
 13. Dans **Gestion de la stratégie de groupe**, cliquez avec le bouton droit sur le domaine **Adatum.com**, puis cliquez sur **Associer un GPO existant**.
 14. Dans la boîte de dialogue **Sélectionner GPO**, cliquez sur **Paramètres Office 2016**, puis cliquez sur **OK**.
- **Tâche 3 : Appliquer et vérifier les paramètres sur l'ordinateur client**
1. Basculez vers **LON-CL1**.
 2. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Invite de commandes**.
 3. Dans la fenêtre de l'**invite de commandes**, entrez la commande suivante et appuyez sur Entrée :
`Gpupdate /force`
 4. Fermer la fenêtre d'**invite de commandes**.
 5. Cliquez sur **Démarrer**, sur **Toutes les applications**, puis sur **Excel 2016**.
 6. Dans la boîte de dialogue **Commençons par le début**, sélectionnez l'option **Me demander ultérieurement**, puis cliquez sur **Accepter**.
 7. Cliquez sur **Classeur vide**.
 8. Vérifiez que l'onglet **Développeur** s'affiche sur le ruban.
 9. Si l'onglet **Développeur** ne s'affiche pas sur le ruban, procédez comme suit :
 - a. Cliquez avec le bouton droit sur **Démarrer**, survolez **Arrêter ou se déconnecter**, puis cliquez sur **Redémarrer**.
 - b. Après le redémarrage de l'ordinateur, connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
 - c. Répétez les étapes 5 à 8.
 10. Cliquez sur **Fichier, Enregistrer et Parcourir**.
 11. Dans la boîte de dialogue **Enregistrer sous**, dans la barre d'adresse, vérifiez que **Bureau** s'affiche, puis cliquez sur **Annuler**.
 12. Fermez **Excel 2016**.

Résultats : Une fois cet exercice terminé, vous aurez développé des modèles d'administration avec des modèles pour Office 2016 et configuré certains paramètres Office en utilisant la stratégie de groupe.

Exercice 2 : Mise en œuvre des paramètres en utilisant les préférences de stratégie de groupe

► Tâche 1 : Configurer l'environnement actuel

1. Basculez vers **LON-DC1**.
2. Sur **LON-DC1**, dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
3. Dans le volet de navigation, développez successivement **AllFiles (E:)** et **Labfiles**, puis cliquez sur **Mod06**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur **Mod06-1.ps1**, puis cliquez sur **Exécuter avec PowerShell**.
5. Si vous y êtes invité, saisissez **O**, puis appuyez sur Entrée.
6. Cliquez avec le bouton droit sur **BranchScript.cmd**, puis cliquez sur **Copier**.
7. Basculez vers la fenêtre **Gestion des stratégies de groupe**.
8. Dans le volet de navigation, cliquez avec le bouton droit sur **Objets de stratégie de groupe**, puis cliquez sur **Rafraîchir**.
9. Cliquez avec le bouton droit sur l'objet de stratégie de groupe (GPO) **Branch1**, puis cliquez sur **Modifier**.
10. Dans la fenêtre **Éditeur de gestion de la stratégie de groupe**, sous **Configuration utilisateur**, développez successivement **Stratégies** et **Paramètres Windows**, puis cliquez sur **Scripts (Connexion/Déconnexion)**.
11. Dans le volet d'informations, double-cliquez sur **Ouverture de session**.
12. Dans la boîte de dialogue **Propriétés de l'ouverture de session**, cliquez sur **Afficher les fichiers**.
13. Dans le volet d'informations, cliquez avec le bouton droit sur un espace vide, puis cliquez sur **Coller**.
14. Fermez la fenêtre **Ouverture de session**.
15. Dans la boîte de dialogue **Propriétés de l'ouverture de session**, cliquez sur **Ajouter**.
16. Dans la boîte de dialogue **Ajout d'un script**, cliquez sur **Parcourir**.
17. Cliquez sur **BranchScript.cmd**, puis sur **Ouvrir**.
18. Cliquez sur **OK** deux fois pour fermer toutes les boîtes de dialogue.
19. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.

► Tâche 2 : Tester un lecteur mappé pour utilisateurs de la succursale 1

1. Basculez vers **LON-CL1**.
2. Cliquez avec le bouton droit sur **Démarrer**, survolez **Arrêter ou se déconnecter**, puis cliquez sur **Redémarrer**.
3. Après le redémarrage de l'ordinateur, connectez-vous en tant qu'**Adatum\Abbi** avec le mot de passe **Pa55w.rd**.
4. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
5. Dans l'Explorateur de fichiers, cliquez sur **Ce PC**.
6. Vérifiez que dans le volet d'informations, dans la section **Emplacements réseau**, le lecteur **S** s'affiche.
7. Si le lecteur S n'est pas disponible, procédez comme suit :

- a. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Invite de commandes**.
- b. Dans la fenêtre **Invite de commandes**, entrez les deux commandes ci-dessous et appuyez sur Entrée après chacune :

```
Gpupdate /force  
Shutdown /r /t 0
```

- c. Répétez les étapes 3 à 6.

► **Tâche 3 : Créer un GPO de préférences avec les préférences de stratégie de groupe requises**

1. Basculez vers **LON-DC1**.
2. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils** puis sur **Utilisateurs et ordinateurs Active Directory**.
3. Dans la fenêtre **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur **IT**, cliquez sur **Nouveau**, puis cliquez sur **Groupe**.
4. Dans la boîte de dialogue **Nouvel objet - groupe**, dans la zone **Nom de groupe**, entrez **Administrateurs de l'ordinateur**, puis cliquez sur **OK**.
5. Dans **Console de gestion des stratégies de groupe**, cliquez avec le bouton droit sur le domaine **Adatum.com**, puis cliquez sur **Actualiser**.
6. Développez **Branch 1**, cliquez avec le bouton droit sur le GPO **Branch 1**, puis cliquez sur **Supprimer**.
7. Dans la boîte de dialogue **Gestion des stratégies de groupe**, cliquez sur **OK**.
8. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Créer un objet GPO dans ce domaine et le lier ici**.
9. Dans la boîte de dialogue **Nouvel objet GPO**, dans la zone **Nom**, saisissez **Préférences**, puis cliquez sur **OK**.
10. Dans le volet de navigation, cliquez avec le bouton droit sur **Préférences**, puis cliquez sur **Modifier**.
11. Développez **Configuration utilisateur**, **Préférences** et **Paramètres Windows**, cliquez avec le bouton droit sur **Raccourcis**, survolez **Nouveau**, puis cliquez sur **Raccourci**.
12. Dans la boîte de dialogue **Nouvelles propriétés de raccourci**, dans la liste **Action**, cliquez sur **Créer**.
13. Dans la zone de texte **Nom**, saisissez **Notepad**.
14. Dans la boîte **Emplacement**, cliquez sur la flèche, puis sélectionnez **Tous les utilisateurs bureau**.
15. Dans la boîte **Chemin cible**, saisissez **C:\Windows\System32\Notepad.exe**.
16. Sous l'onglet **Commun**, désactivez la case à cocher **Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de stratégie utilisateur)**.
17. Cochez la case **Cible niveau élément**, puis cliquez sur **Cible**.
18. Dans la boîte de dialogue **Éditeur de cible**, cliquez sur **Nouvel élément**, puis sur **Groupe de sécurité**.
19. Dans la partie inférieure de la boîte de dialogue, cliquez sur le bouton de sélection (...).
20. Dans la boîte de dialogues **Sélectionner un groupe**, dans la zone **Entrez les noms des objets à sélectionner (exemple)**, entrez **IT** et cliquez ensuite sur **OK**.
21. Cliquez encore deux fois sur **OK**.

22. Cliquez avec le bouton droit sur **Mappages de lecteur**, pointez sur **Nouveau**, puis cliquez sur **lecteur mappé**.
23. Dans la boîte de dialogue **Propriétés nouveau disque**, dans la zone de texte **Emplacement**, saisissez **\LON-DC1\Branch1**, puis cochez la case **Reconnecter**. Dans la zone de texte **Libeller en tant que**, saisissez **Disque pour filiale 1**, dans la zone de liste déroulante **Utilisation**, sélectionnez **S**.
24. Sous l'onglet **Commun**, cochez la case **Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de stratégie utilisateur)**.
25. Cochez la case **Cible niveau élément**, puis cliquez sur **Cible**.
26. Dans la boîte de dialogue **Éditeur de cible**, cliquez sur **Nouvel élément**, puis cliquez sur **Unité organisationnelle**.
27. Dans la partie inférieure de la boîte de dialogue, cliquez sur le bouton de sélection (...).
28. Dans la boîte de dialogue **Trouver une recherche personnalisée**, dans la liste **Résultats de la recherche**, sélectionnez **Filiale 1**, puis cliquez sur **OK**.
29. Cliquez encore deux fois sur **OK**.
30. Développez **Configuration de l'ordinateur**, développez **Préférences**, puis **Paramètres du panneau de configuration**.
31. Cliquez avec le bouton droit sur **Utilisateurs et groupes locaux**, survolez **Nouveau**, puis cliquez sur **Groupe local**.
32. Dans la boîte de dialogue **Nouvelles propriétés de groupe local**, dans la zone **Nom de groupe**, entrez **Administrateurs**, puis cliquez sur **Ajouter**.
33. Dans la boîte de dialogue **Membre du groupe local**, cliquez sur le bouton de sélection (...).
34. Dans la boîte de dialogues **Sélectionner un utilisateur, un ordinateur ou un groupe**, dans la zone **Entrez les noms des objets à sélectionner (exemple)**, entrez **Administrateurs de l'ordinateur** et cliquez deux fois sur **OK**.
35. Dans la boîte de dialogue **Nouvelles propriétés du groupe local** cliquez sur l'onglet **Common**.
36. Sous l'onglet **Commun**, cochez la case **Ciblage de niveau des articles**, puis cliquez sur **Ciblage**.
37. Dans la boîte de dialogue **Éditeur de cible**, cliquez sur **Nouvel élément**, puis cliquez sur **Système d'exploitation**.
38. Dans la zone de liste déroulante **Produit**, sélectionnez **Windows Server 2016 Aperçu technique 5**, puis cliquez deux fois sur **OK**.
39. Fermez toutes les fenêtres ouvertes, à l'exception de **Gestion des stratégies de groupe** et **Gestionnaire de serveur**.

► Tâche 4 : Tester les préférences

1. Basculez vers **LON-CL1**.
2. Cliquez avec le bouton droit sur **Démarrer**, survolez **Arrêter ou se déconnecter**, puis cliquez sur **Redémarrer**.
3. Après le redémarrage de l'ordinateur, connectez-vous en tant qu'**Adatum\Abbi** avec le mot de passe **Pa55w.rd**.
4. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
5. Dans l'Explorateur de fichiers, cliquez sur **Ce PC**.
6. Vérifiez que dans le volet d'informations, dans la section **Emplacements réseau**, le lecteur **S** s'affiche.



Remarque : Le libellé de lecteur est désormais **Lecteur pour succursale 1**, lequel vérifie si le lecteur est mappé via les préférences de la stratégie de groupe.

7. Sur le bureau, vérifiez qu'il existe un raccourci pour **Bloc-notes**.
8. Si le raccourci pour **Notepad** n'est pas disponible, procédez comme suit :
 - a. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Invite de commandes**.
 - b. Dans la fenêtre **Invite de commandes**, entrez les deux commandes ci-dessous et appuyez sur Entrée après chacune :

```
Gupdate /force  
Shutdown /r /t 0
```

 - c. Répétez l'étape 3.
 - d. Le raccourci pour **Bloc-notes** devrait maintenant s'afficher sur le bureau.
9. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Gestion ordinateur**.
10. Dans **Gestion d'ordinateur**, développez **Utilisateurs et groupes locaux**, puis cliquez sur **Groupes**.
11. Dans le volet d'informations, double-cliquez sur **Administrateurs**.
12. Vérifiez que le groupe **Administrateurs informatiques** n'est pas un membre du groupe **Administrateurs**.



Remarque : Le groupe **Administrateurs informatiques** n'est pas un membre du groupe **Administrateurs** parce que le paramètre de **Préférences** ne vaut que pour les serveurs.

13. Déconnectez-vous de **LON-CL1**.

Résultats : Une fois cet exercice terminé, vous aurez retiré les scripts d'ouverture de session et configuré les paramètres de préférence, puis vous les aurez attribués en utilisant les GPO.

Exercice 3 : Configuration de la redirection de dossiers

► Tâche 1 : Créer un dossier partagé pour stocker les dossiers redirigés

1. Sur **LON-DC1**, dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
2. Dans le volet de navigation, cliquez sur **Ce PC**.
3. Dans le volet d'informations, double-cliquez sur **Disque local (C:)**, puis sous l'onglet **Accueil**, cliquez sur **Nouveau dossier**.
4. Nommez le nouveau dossier **Branch1Redirect**.
5. Cliquez avec le bouton droit sur le dossier **Branch1Redirect**, cliquez sur **Partager avec** puis sur **Des personnes spécifiques**.
6. Dans la boîte de dialogue **Partage de fichiers**, cliquez sur la zone de liste déroulante, sélectionnez **Tout le monde**, puis cliquez sur **Ajouter**.
7. Pour le groupe **Tout le monde**, cliquez sur la zone de liste déroulante **Niveau Autorisation**, puis cliquez sur **Lecture/écriture**.

8. Cliquez sur **Partager**, puis sur **Terminer**.

9. Fermez l'**Explorateur de fichiers**.

► **Tâche 2 : Créer un nouveau GPO et le lier à l'unité organisationnelle (UO) succursale 1**

1. Sur **LON-DC1**, ouvrez **Gestion des stratégies de groupe**.

2. Dans **Gestion des stratégies de groupe**, développez et cliquez avec le bouton droit sur **Filiale 1**, puis cliquez sur **Créer un objet GPO dans ce domaine et le lier ici**.

3. Dans la boîte de dialogue **Nouvel objet GPO**, dans la zone **Nom**, saisissez **Redirection de dossiers**, puis cliquez sur **OK**.

► **Tâche 3 : Modifier les paramètres de redirection de dossiers dans la stratégie**

1. Développez **Filiale 1**, cliquez avec le bouton droit sur **Redirection de dossiers**, puis cliquez sur **Modifier**.

2. Dans la fenêtre **Éditeur de gestion de la stratégie de groupe**, sous **Configuration utilisateur**, développez **Stratégies**, **Windows Paramètres** et **Redirection de dossiers**.

3. Cliquez avec le bouton droit sur **Documents**, puis cliquez sur **Propriétés**.

4. Dans la boîte de dialogue **Propriétés du document**, sous l'onglet **Cible**, dans la zone de liste déroulante **Paramètre**, sélectionnez **De base - Rediriger les dossiers de tout le monde vers le même emplacement**.

5. Assurez-vous que la boîte **Emplacement du dossier cible** est définie sur **Créez un dossier pour chaque utilisateur sous le chemin racine**.

6. Dans la zone de texte **Chemin racine**, entrez **\\\LON-DC1\Branch1Redirect**, puis cliquez sur **OK**.

7. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.

8. Cliquez avec le bouton droit sur **Images**, puis cliquez sur **Propriétés**.

9. Dans la boîte de dialogue **Propriétés des images**, sous l'onglet **Cible**, dans la zone de liste déroulante **Paramètre**, sélectionnez **Suivre le dossier des documents** puis cliquez sur **OK**.

10. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.

11. Cliquez avec le bouton droit sur **Musique**, puis cliquez sur **Propriétés**.

12. Dans la boîte de dialogue **Propriétés musique**, sous l'onglet **Cible**, dans la zone de liste déroulante **Paramètre**, sélectionnez **Suivre le dossier des documents** puis cliquez sur **OK**.

13. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.

14. Fermez toutes les fenêtres actives sur **LON-DC1**.

► **Tâche 4 : Tester les paramètres de redirection de dossiers**

1. Basculez vers **LON-CL1**.

2. Connectez-vous en tant qu'**Adatum\Abbi** avec le mot de passe **Pa\$\$w0rd**.

3. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Invite de commandes**.

4. Dans la fenêtre de l'**invite de commandes**, entrez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

5. Lorsque vous y êtes invité, entrez le message suivant, puis appuyez sur Entrée :

Y

6. Déconnectez-vous puis reconnectez-vous à **LON-CL1** en tant qu'**Adatum\Abbi** avec le mot de passe **Pa\$\$w0rd**.
7. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
8. Dans l'Explorateur de fichiers, dans le volet de navigation, cliquez avec le bouton droit sur **Documents**, puis sélectionnez **Propriétés**.
9. Dans la boîte de dialogue propriétés **Documents**, vérifiez que l'emplacement est **\LON-DC1\Branch1\Redirect\Abbi**, puis cliquez sur **OK**.



Remarque : Si l'emplacement est **C:\Users\Abbi**, répétez les étapes 3 à 9.

10. Cliquez sur **Documents** et vérifiez que les deux sous-dossiers, **Musique** et **Photos** existent.



Remarque : Cela permet de vérifier que **Musique** et **Images** sont également redirigées.

11. Déconnectez-vous de **LON-CL1**.

Résultats : Une fois cet exercice terminé, vous aurez configuré la redirection de dossiers vers un dossier partagé sur le serveur **LON-DC1**.

Exercice 4 : Planifier la stratégie de groupe (en option)

- ▶ **Tâche 1 : Lire la documentation fournie avec le produit**
 - Lisez la documentation fournie.
- ▶ **Tâche 2 : Mettre à jour le document de proposition en fonction du plan d'action planifié**
 - Répondez aux questions de la section **Propositions** du document **Proposition de stratégie GPO A.Datum.**

Propositions

- Quelle exigence nécessitera la création d'un ou de plusieurs GPO ?

Les administrateurs informatiques centraux à Londres doivent être en mesure de gérer tous les GPO et les paramètres de l'organisation. Les administrateurs de chaque bureau devraient être en mesure de gérer uniquement les GPO applicables à ce bureau. Bien que vous pouvez compléter l'une des tâches restantes manuellement sur chaque ordinateur, utiliser les GPO nécessite moins d'effort. Vous pourriez mettre en oeuvre plusieurs autres exigences, telles que la mise en garde de sécurité ou empêcher l'accès au registre des outils d'édition, en utilisant des stratégies locales seulement. Cependant, parce que les stratégies locales sont difficiles à gérer, les GPO sont également bénéfiques pour ces paramètres.

- Pouvez-vous répondre à l'une des exigences sans créer de GPO ?
Vous pouvez remplir toutes les exigences sans créer de GPO.
- Existe-t-il des exceptions à l'application GPO par défaut que vous devez prendre en compte ?
Oui, il y a une exception : le filtrage de sécurité des bureaux de l'administrateur de sorte qu'ils auront accès aux outils d'édition du registre.
- Dressez la liste des GPO à créer pour répondre aux exigences du scénario de l'atelier pratique.
Fournissez les informations suivantes dans le tableau prévu :
 - Nom du GPO
 - Exigences auxquelles répond le GPO
 - Les paramètres de configuration (stratégies utilisateur, stratégies informatiques, préférences de l'utilisateur, ou préférences informatiques) contenus par le GPO
 - Le conteneur (domaine, UO, site) auquel le GPO sera lié

| Nom | Exigences remplies | Paramètres de configuration | S'applique aux éléments ci-dessous |
|--------------|--|---|------------------------------------|
| Tous_Clients | Configure les comptes d'administrateur locaux | Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Groupes restreints | UO=Clients |
| Tous_Clients | Configurer les paramètres Windows Update généraux. | Configuration ordinateur\Stratégies\Modèles d'administration\Composants Windows\Windows Update\Configuration du service Mises à jour automatiques | UO=Clients |

| Nom | Exigences remplies | Paramètres de configuration | S'applique aux éléments ci-dessous |
|----------------------|---|---|------------------------------------|
| All_Users_but_Admins | Empêche l'édition du registre | Configuration utilisateur\Stratégies\Modèles d'administration\Système\Accès bloqué aux outils d'édition du registre | DC=adatum |
| London_Clients | Affiche un message de conformité | Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Options de sécurité\Connexion interactive : Le texte du message pour les utilisateurs essayant de se connecter Connexion interactive : Titre du message pour les utilisateurs essayant de se connecter | UO=Londres, UO=Clients |
| Marketing_Share | Les utilisateurs doivent disposer d'un ensemble de lecteurs mappés par défaut | Configuration utilisateur\Préférences\Paramètres Windows\Plans d'entraînement | UO=Marketing |

- Listez d'autres tâches de configuration que vous devez effectuer au sein de la console de gestion des stratégies de groupe pour répondre aux exigences du scénario.

Les autres tâches de configuration comprennent :

- La stratégie All_Users_but_Admins a besoin d'un filtrage de sécurité pour refuser l'accès. Cela appliquera la stratégie aux utilisateurs, mais pas au groupe d'administrateurs, IT Groupe.

Vous devez configurer l'administration des GPO comme souhaité.

- ▶ **Tâche 3 : Examiner les propositions suggérées dans le corrigé de l'atelier pratique**
- Comparez vos propositions à celles présentées précédemment.
- ▶ **Tâche 4 : Présenter la solution que vous proposez à la classe, comme indiqué par votre instructeur**
- Préparez-vous à discuter de vos propositions avec la classe.

Résultats : Une fois cet exercice terminé, vous aurez configuré une stratégie GPO.

► Préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-DC2** et **22742A-LON-CL1**.

Module 7 : Sécurisation des services de domaine Active Directory

Atelier pratique : Sécurisation AD DS

Exercice 1 : Mise en œuvre des stratégies de sécurité pour les comptes, mots de passe et groupes d'administration

► **Tâche 1 : Identifier les paramètres requis**

1. Lisez la documentation fournie.
2. Remplissez le tableau des paramètres en fonction des exigences de A. Datum Corporation.

| Paramètre | Configuration pour tous les utilisateurs | Configuration pour les administrateurs informatiques |
|--|--|--|
| Appliquer l'historique des mots de passe | 10 | 10 |
| Antériorité maximale du mot de passe | 60 jours | 30 jours |
| Antériorité minimale du mot de passe | 1 jour | 1 jour |
| Longueur de mot de passe minimale | 8 caractères | 10 caractères |
| Les mots de passe doivent répondre à des exigences de complexité | Vrai | Vrai |
| Stocker le mot de passe en utilisant le chiffrage réversible | Faux | Faux |
| Durée de verrouillage du compte | 1 heure | Administrateur doit déverrouiller |
| Seuil de verrouillage du compte | 5 | 3 |
| Réinitialiser le compteur de verrouillage de compte après | 20 minutes | 20 minutes |

3. Répondez aux questions supplémentaires du document de proposition.
 - a. Comment pouvez-vous effectuer une configuration de sorte que les administrateurs informatiques aient des paramètres de verrouillage de compte et mot de passe différents de ceux des utilisateurs habituels ?

Réponse : Utilisez la stratégie de domaine par défaut, qui s'applique à tous les utilisateurs et créez un objet de stratégie de mots de passe détaillé qui ne vaut que pour les groupes administratifs nécessaires.

- b. Comment pouvez-vous identifier les administrateurs informatiques en termes de paramètres de verrouillage de compte et mot de passe plus restreints ?

Réponse : Les paramètres de mots de passe administratif et de verrouillage de compte devraient s'appliquer au groupe informatique et au groupe des administrateurs de domaine.

- c. Comment pouvez-vous répondre à l'exigence de limiter la liste des membres des groupes d'administrateurs locaux sur tous les serveurs membres seulement au compte de l'administrateur local, au groupe des administrateurs de domaine et au groupe informatique ?

Réponse : Assurez-vous que vous avez des serveurs membres de domaine dans la même hiérarchie d'UO. Attribuez une stratégie à cette dernière, puis utilisez la fonctionnalité de groupes restreints pour limiter le groupe Administrateurs locaux avec force pour ne contenir que les administrateurs, le groupe Admins du domaine et le groupe IT.

- d. Comment pouvez-vous répondre à l'exigence selon laquelle le groupe des administrateurs de domaine doit comprendre uniquement le compte Administrateur et les groupes Administrateurs de l'entreprise et Administrateurs du schéma doivent être vides pendant le fonctionnement normal ?

Réponse : Vous ne pouvez pas configurer d'autres groupes que les groupes locaux avec la fonctionnalité groupes restreints. Pour les Administrateurs du domaine, Administrateurs de l'entreprise et Administrateurs du schéma, vous devez configurer l'appartenance à un groupe manuellement et vérifier les modifications.

- e. Comment pouvez-vous répondre à l'exigence selon laquelle les autres groupes intégrés, tels que les opérateurs de compte et opérateurs de serveur, ne doivent pas contenir de membres ?

Réponse : Utilisez la fonctionnalité des groupes restreints.

- f. Comment pouvez-vous répondre à l'exigence de devoir vérifier toutes les modifications aux utilisateurs ou groupes dans les Services de domaine Active Directory (AD DS) ?

Réponse : Configurez les stratégies d'audit avancées pour contrôler les modifications de service Directory.

► Tâche 2 : Configurer les paramètres de mot de passe pour tous les utilisateurs

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la **Console de gestion des stratégies de groupe**, dans le volet de navigation, développez **Forêt : Adatum.com\Domaines\ adatum.com\Objets de stratégie de groupe**, puis sélectionnez **Stratégie des contrôleurs de domaine par défaut**.
3. Cliquez avec le bouton droit sur **Stratégie de domaine par défaut**, puis cliquez sur **Modifier**.
4. Dans la fenêtre **Éditeur de gestion des stratégies de groupe**, dans le volet de navigation, développez **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de comptes**, puis double-cliquez sur **Stratégie de mot de passe**.
5. Dans le volet d'informations, double-cliquez sur **Appliquer l'historique des mots de passe**.

6. Dans la boîte de dialogue **Conserver Propriétés de l'historique du mot de passe**, assurez-vous que **Définir ce paramètre de stratégie** est sélectionné.
7. Configurez **Conserver l'historique de mot de passe pour** : jusqu'à **10 mots de passe mémorisés**, cliquez sur **OK**, puis double-cliquez sur **Durée de vie maximale du mot de passe**.
8. Dans la boîte de dialogue **Propriétés Durée de vie maximale du mot de passe**, assurez-vous que **Définir ce paramètre de stratégie** est sélectionné.
9. Configurez **Le mot de passe expirera dans** jusqu'à **60 jours**, cliquez sur **OK**, puis double-cliquez sur **Durée de vie minimale du mot de passe**.
10. Dans la boîte de dialogue **Propriétés Durée de vie minimale du mot de passe**, assurez-vous que **Définir ce paramètre de stratégie** est sélectionné.
11. Configurez **Le mot de passe peut être modifié après à 1 jour**, cliquez sur **OK**, puis double-cliquez sur **longueur minimale du mot de passe**.
12. Dans la boîte de dialogue **Propriétés longueur minimale du mot de passe**, assurez-vous que **Définir ce paramètre de stratégie** est sélectionné.
13. Configurez **Le mot de passe doit être d'au moins sur 8 caractères**, cliquez sur **OK**, puis double-cliquez sur **Le mot de passe doit répondre aux exigences de complexité**.
14. Dans la boîte de dialogue **Propriétés des exigences de complexité du mot du passe**, assurez-vous que **Définir ce paramètre de stratégie** est sélectionné.
15. Sélectionnez **Activé**, cliquez sur **OK**, puis double-cliquez sur **Enregistrer les mots de passe en utilisant un chiffrement réversible**.
16. Dans la boîte de dialogue **Enregistrer les mots de passe en utilisant le cryptage réversible**, assurez-vous que **Définir ce paramètre de stratégie** est sélectionné.
17. Sélectionnez **Désactivé**, puis cliquez sur **OK**.
18. Dans le volet de navigation, cliquez pour sélectionner **Stratégie de verrouillage du compte**.
19. Dans le volet d'informations, double-cliquez sur **Durée du verrouillage de compte**.
20. Dans la boîte de dialogue **Propriétés de la durée de verrouillage du compte**, cliquez sur **Définir ce paramètre de stratégie**.
21. Configurez **Le compte est verrouillé pour** sur **60 minutes**, puis cliquez sur **OK**.
22. Dans la boîte de dialogue **Modifications de valeur suggérées**, cliquez sur **OK**, puis double-cliquez sur **Seuil de verrouillage de comptes**.
23. Dans la boîte de dialogue **Propriétés de seuil de verrouillage de compte**, configurez **Le compte sera verrouillé après** sur **5 tentatives de connexion non valides**, cliquez sur **OK**, puis double-cliquez sur **Réinitialiser le compteur de verrouillage de compte après**.
24. Dans la boîte de dialogue **Propriétés Réinitialiser le compteur de verrouillage de compte après**, configurez **Réinitialisez le compteur de verrouillage de compte après** sur **20 minutes**, puis cliquez sur **OK**.
25. Fermez la fenêtre **Éditeur de gestion des stratégies de groupe** et la **Console de gestion des stratégies de groupe**.
- Tâche 3 : Configurer un PSO pour les administrateurs informatiques
- Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.

2. Dans **Centre d'administration Active Directory**, dans le volet de navigation, cliquez sur **Adatum (local)**.
3. Dans le volet d'informations, faites défiler et double-cliquez sur **Système**, puis double-cliquez sur **Conteneur des paramètres du mot de passe**.
4. Dans le volet **Tâches**, dans le **Conteneur Paramètres de mot de passe**, cliquez sur **Nouveau**, puis cliquez sur **Paramètres de mot de passe**.
5. Dans la boîte de dialogue **Paramètres Créez mot de passe**, dans la section **Paramètres mot de passe**, dans le champ **Prénom**, entrez **Paramètres mot de passe Administrateurs Adatum**.
6. Dans le champ **Priorité**, saisissez **10**, puis vérifiez que **Appliquer la longueur minimale du mot de passe** est sélectionné.
7. Dans la zone de texte **Longueur du mot de passe minimum (caractères)**, saisissez **10**, puis vérifiez que **Appliquer l'historique des mots de passe** est sélectionné.
8. Dans la zone de texte **Nombre de mots de passe mémorisés**, saisissez **10**, vérifiez que **Le mot de passe doit répondre aux exigences de complexité** est sélectionné et que **Enregistrer le mot de passe en utilisant un cryptage réversible** n'est pas sélectionné.
9. Sous **Options d'âge de mot de passe**, vérifiez que **Appliquer l'âge minimum du mot de passe** est sélectionné.
10. Dans la zone de texte **L'utilisateur ne peut pas modifier le mot de passe avant (jours)**, saisissez **1** puis cochez la case **Appliquer l'âge maximum du mot de passe**.
11. Dans la zone de texte **L'utilisateur doit modifier le mot de passe après (jours)**, saisissez **30** puis cochez la case **Appliquer la stratégie de verrouillage du compte**.
12. Dans la zone de texte **Nombre de tentatives de connexion autorisées**, saisissez **3**.
13. Dans la zone de texte **Réinitialiser le compteur de tentatives erronées d'ouverture de session après (mn)**, saisissez **20**, puis sélectionnez **Le compte sera verrouillé, Jusqu'à ce qu'un administrateur déverrouille manuellement le compte**.
14. Dans la section **S'applique directement à**, cliquez sur **Ajouter**.
15. Dans la boîte de dialogue **Sélectionnez les utilisateurs ou les groupes**, sous **Entrez les noms des objets à sélectionner**, saisissez **IT**, puis cliquez sur **Vérifier les noms**.
16. La boîte de dialogue **Nom introuvable** apparaît, car IT n'est pas un groupe global mais un groupe universel. Cliquez sur **Annuler**.
17. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Windows PowerShell**.
18. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Get-ADGroup IT
```
19. Vérifiez que le groupe IT a une étendue de groupe **Universelle**.
20. À l'invite de commandes, entrez la commande suivante et appuyez sur Entrée :

```
Set-ADGroup IT -GroupScope Global
```
21. Revenez à la boîte de dialogue **Paramètres Créez mot de passe : Paramètres de mot de passe administratif Adatum**.
22. Dans la boîte de dialogue **Sélectionnez les utilisateurs ou les groupes**, sous **Entrez les noms des objets à sélectionner**, saisissez **IT, Admins Domaine**, puis cliquez sur **Vérifier les noms**. Les noms sont tous deux résolus. Cliquez sur **OK**.

23. Cliquez sur **OK** pour fermer la boîte de dialogue **Créer des paramètres de mot de passe : Paramètres mot de passe administratif Adatum** et créez l'objet **Paramètres mot de passe** (PSO).
24. Dans **Centre d'administration Active Directory**, dans le volet de navigation, cliquez sur **Aperçu**.
25. Dans le volet d'informations, dans la boîte **Recherche globale**, saisissez **Abbi Skinner**, puis appuyez sur Entrée. L'objet USER de **Abbi Skinner** est trouvé.
26. Dans le volet **Tâches**, cliquez sur **Afficher tous les paramètres de mot de passe résultants**. Notez que le PSO **Paramètres mot de passe administratif Adatum** s'applique (Abbi est dans le groupe IT), puis cliquez sur **Annuler**.
27. Dans la zone de texte **Recherche globale**, saisissez **Adam Hobbs** et appuyez sur Entrée.
28. Dans le volet **Tâches**, cliquez sur **Voir tous les paramètres de mot de passe résultants**. Notez que les paramètres de mot de passe détaillé non résultant s'appliquent (Adam n'est pas dans le groupe IT et les paramètres de Stratégies de domaine par défaut lui sont applicables), puis cliquez sur **OK**.
29. Fermez le **Centre d'administration Active Directory** et **Windows PowerShell**.
- **Tâche 4 : Mettre en œuvre des stratégies de sécurité administratives**
1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
 2. Dans **Centre d'administration Active Directory**, dans le volet de navigation, cliquez sur **Adatum (local)**.
 3. Dans le volet des **tâches**, sous **Adatum (local)**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
 4. Dans la boîte de dialogue **Créer Unité organisationnelle**, dans la zone de texte **Nom**, entrez **Serveurs Adatum**, puis cliquez sur **OK**.
 5. Dans **Centre d'administration Active Directory**, dans le volet d'informations, double-cliquez sur **Ordinateurs**, sélectionnez **LON-SVR1**, puis appuyez et maintenez la touche Maj enfoncee et cliquez sur **LON-SVR2**. Les deux serveurs sont maintenant sélectionnés.
 6. Dans le volet **Tâches**, dans la section **2 éléments sélectionnés**, cliquez sur **Déplacer**.
 7. Dans la boîte de dialogue **Déplacer**, cliquez sur **Serveurs Adatum**, puis sur **OK**.
 8. Fermez le **Centre d'administration Active Directory**.
 9. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
 10. Dans la **Console de gestion de stratégie de groupe**, sous **Forêt : Adatum.com\Domaines\Adatum.com**, recherchez et cliquez pour sélectionner **Serveurs Adatum**. Cliquez avec le bouton droit sur **Serveurs Adatum**, puis cliquez sur **Créer un GPO dans ce domaine et le lier ici**.
 11. Dans la boîte de dialogue **Nouveau GPO**, dans le champ **Nom**, saisissez **Administrateurs restreints sur Serveurs Membre**, puis cliquez sur **OK**.
 12. Dans le volet d'informations, cliquez avec le bouton droit sur le GPO **Administrateurs restreints sur Serveurs Membre**, puis cliquez sur **Modifier**.
 13. Dans la fenêtre **Éditeur de gestion de la stratégie de groupe**, développez **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité**, cliquez pour sélectionner **Groupes restreints**, cliquez avec le bouton droit sur **Groupes restreints**, puis cliquez sur **Ajouter un groupe**.
 14. Dans la boîte de dialogue **Ajouter Groupe**, dans le champ **Groupe**, saisissez **Administrateurs**, puis cliquez sur **OK**.

15. Dans la boîte de dialogue **Propriétés Administrateurs**, sous **Membres de ce groupe**, cliquez sur **Ajouter**.
16. Dans la boîte de dialogue **Ajouter un membre** cliquez sur **Parcourir**.
17. Dans la boîte de dialogue **Sélectionner des utilisateurs des comptes de service ou des groupes**, dans la zone de texte **Entrer les noms des objets à sélectionner**, entrez **Admins du Domaine ; IT**, cliquez sur **Vérifier les noms**, puis sur **OK**.
18. Dans la boîte de dialogue **Ajouter un membre**, dans la section **Membres de ce groupe**, ajoutez ; **Administrateur** à la chaîne, puis cliquez sur **OK**.
19. Vérifiez que la boîte de dialogue **Propriétés de l'administrateur** affiche maintenant l'élément suivant dans **Membres de ce groupe**, puis cliquez sur **OK** :
 - **ADATUM\Admins Domaine**
 - **ADATUM\IT**
 - **Administrateur**
20. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.
21. Sur **LON-SVR1**, cliquez sur **Démarrer**, saisissez **cmd**, puis cliquez sur **Invite de commandes**.
22. Dans la fenêtre **Administrateur : À l'invite de commandes**, entrez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```
23. Patientez jusqu'à ce que la commande mette à jour la Stratégie ordinateur et la Stratégie utilisateur.
24. Sur **LON-SVR1**, cliquez sur **Démarrer**, puis cliquez sur **Gestionnaire de serveur**.
25. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion ordinateur**.
26. Dans **Gestion d'ordinateur**, développez **Outils Système\Utilisateurs et groupes locaux**, puis cliquez sur **Groupes**.
27. Double-cliquez sur **Administrateurs**, puis vérifiez que **Adatum\Admins Domaine**, **ADATUM\IT** et **l'Administrateur** local soient membres de ce groupe.
28. Fermez toutes les fenêtres actives excepté **Gestionnaire de serveur**.
29. Rebasculez vers **LON-DC1** puis basculez vers **Gestion de stratégie de groupe**.
30. Dans la **Console de gestion de stratégie de groupe**, développez **Contrôleurs de domaine**, cliquez avec le bouton droit sur le lien **Stratégie de contrôleurs de domaine par défaut**, puis cliquez sur **Modifier**.
31. Dans la fenêtre **Éditeur de gestion de la stratégie de groupe**, développez **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité**, cliquez pour sélectionner **Groupes restreints**, cliquez avec le bouton droit sur **Groupes restreints**, puis cliquez sur **Ajouter un groupe**.
32. Dans la boîte de dialogue **Ajouter Groupe**, dans le champ **Groupe**, saisissez **Opérateurs de Serveur**, puis cliquez sur **OK**.
33. Dans la boîte de dialogue **Propriétés opérateurs de serveur**, conservez les paramètres par défaut de **Ce groupe ne doit contenir aucun membre**, puis cliquez sur **OK**.
34. Répétez les étapes 30 à 33 pour le groupe **Opérateurs de compte**.

35. Fermez la fenêtre **Éditeur de gestion des stratégies de groupe** et la **Console de gestion des stratégies de groupe**.

► **Tâche 5 : Mettre en œuvre la vérification administrative**

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
 2. Dans la **Console de gestion de stratégie de groupe**, développez **Forêt : Adatum.com\Domaines, Adatum.com\Objets de stratégie de groupe**, sélectionnez **Stratégie des contrôleurs de domaine par défaut**, cliquez avec le bouton droit sur **Stratégie des contrôleurs de domaine par défaut**, puis cliquez sur **Modifier**.
 3. Dans la fenêtre **Éditeur de gestion de stratégie de groupe**, développez **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Configuration avancée de la stratégie d'audit\Stratégies d'audit**, puis cliquez pour sélectionner **Accès DS**.
 4. Dans le volet d'informations, double-cliquez sur **Auditer les modifications des services d'annuaire**.
 5. Dans la boîte de dialogue **Propriétés d'audit de modification des services Directory**, sélectionnez **Configurer les événements d'audit suivants**, cochez la case **Réussite**, puis cliquez sur **OK**.
 6. Dans le volet de navigation, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Configuration avancée de la stratégie d'audit\Stratégies d'audit**, puis cliquez pour sélectionner **Gestion du compte**.
 7. Dans le volet d'informations, double-cliquez sur **Auditer la gestion des groupes de sécurité**.
 8. Dans la boîte de dialogue **Auditer la gestion des groupes de sécurité**, sélectionnez **Configurer les événements d'audit suivants**, cochez la case **Succès**, puis cliquez sur **OK**.
 9. Dans le volet de navigation, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales**, cliquez pour sélectionner **Options de sécurité**, puis double-cliquez sur le **Audit : force les paramètres de sous-catégorie de stratégie d'audit (Windows Vista ou version ultérieure) à se substituer aux paramètres de catégorie de stratégie d'audit**.
 10. Dans la boîte de dialogue **Audit : force les paramètres de sous-catégorie de stratégie d'audit (Windows Vista ou version ultérieure) à se substituer aux paramètres de catégorie de stratégie d'audit**, sélectionnez **Définir ce paramètre de stratégie**, vérifiez que **Activé** est sélectionné, puis cliquez sur **OK**.
 11. Fermez la fenêtre **Éditeur de gestion des stratégies de groupe** et la **Console de gestion des stratégies de groupe**.
 12. Sur **LON-DC1**, sur l'écran d'accueil, saisissez **cmd**, puis cliquez sur **Invite de commandes**.
 13. Dans la fenêtre **Administrateur : À l'invite de commandes**, entrez la commande suivante et appuyez sur Entrée :
- ```
gpupdate /force
```
14. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
  15. Dans la console **Utilisateurs et ordinateurs Active Directory**, dans le menu **Affichage**, cliquez sur **Fonctionnalités avancées**.
  16. Dans le volet de navigation, cliquez pour sélectionner **Adatum.com**, cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Propriétés**.
  17. Dans la boîte de dialogue **Propriétés adatum.com**, dans l'onglet **Sécurité**, cliquez sur **Avancé**.

18. Dans la boîte de dialogue **Paramètres de sécurité avancés pour Adatum**, sous l'onglet **Audit des entrées**, double-cliquez sur l'entrée d'audit **Réussite** pour **Tout le monde** avec accès **Spécial**, qui s'applique à **Cet objet uniquement**.
19. Dans la boîte de dialogue **Audit de l'entrée pour Adatum**, dans la zone de liste déroulante **S'applique à**, sélectionnez **Cet objet et tous les objets descendants**.
20. Cliquez sur **OK** trois fois pour fermer toutes les boîtes de dialogue.
21. Dans la fenêtre **Utilisateurs et ordinateurs Active Directory**, dans le volet de navigation, développez **Adatum.com** et cliquez ensuite sur **Utilisateurs**.
22. Dans le volet d'informations, double-cliquez sur **Admins du Domaine**.
23. Dans la boîte de dialogue **Propriétés Admins du Domaine**, cliquez sur l'onglet **Membres**, puis sur **Ajouter**.
24. Dans la boîte de dialogue **Sélectionner des utilisateurs, des contacts, des ordinateurs, des comptes de service ou des groupes**, dans la zone de texte **Entrer les noms des objets à sélectionner**, entrez **Abbi**, cliquez sur **Vérifier les noms**, puis deux fois sur **OK**.
25. Dans la console **Utilisateurs et ordinateurs Active Directory**, dans le volet de navigation, cliquez pour sélectionner **Marketing**.
26. Dans le volet d'informations, double-cliquez sur **Ada Russel**.
27. Dans la boîte de dialogue **Propriétés Ada Russel Propriétés**, sous l'onglet **Adresse**, dans la zone de texte **Ville**, sélectionnez **Londres**, entrez **Birmingham**, puis cliquez sur **OK**.
28. Fermez la fenêtre **Utilisateurs et ordinateurs Active Directory**.
29. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Observateur d'événements**.
30. Dans l'**Observateur d'événements**, développez **Journaux Windows**, puis cliquez sur **Sécurité**.
31. Dans le volet d'informations, recherchez l'**ID d'événement 4728** le plus récent, puis double-cliquez sur l'événement.
32. Dans la boîte de dialogue **Propriétés de l'événement - événement 4728, Audit de sécurité Microsoft Windows**, vous obtenez le message « Un membre a été ajouté à un groupe global avec sécurité activée ». Vous pouvez voir que **Adatum\Administrateur** a invoqué la modification et que **Adatum\Abbi** a été ajouté au groupe **Adatum\Admins Domaine**.
33. Dans **Observateur d'événements**, dans le nœud **Journaux Windows\Journal de sécurité**, recherchez les deux **ID d'événement 5136** les plus récents, puis double-cliquez sur le plus ancien des deux événements.
34. Dans la boîte de dialogue **Propriétés de l'événement - événement 5136, Audit de sécurité Microsoft Windows**, vous verrez le message suivant : « Un objet de service de répertoire a été modifié ». Vous pouvez voir que **Adatum\Administrateur** a modifié l'objet utilisateur **cn=Ada Russel**, puis supprimé la valeur **Londres**. Sur le côté droit de la boîte de dialogue, cliquez sur la **Flèche vers le haut** pour passer à l'événement suivant.



**Remarque :** Sur la page de détails **Propriétés de l'événement**, notez que **Adatum\Administrateur** a modifié **Ada Russel** et a ajouté la valeur **Birmingham**.

35. Fermez toutes les fenêtres actives excepté Gestionnaire de serveur.

**Résultats :** Une fois cet exercice terminé, vous aurez identifié et configuré les stratégies de sécurité pour A. Datum.

## Exercice 2 : Déploiement et configuration d'un RODC

### ► Tâche 1 : Organiser l'installation déléguée d'un RODC

#### Préparation

Pour prédéfinir un compte RODC, le nom de l'ordinateur ne doit pas être en cours d'utilisation dans le domaine. Par conséquent, vous devez d'abord retirer **LON-SVR1** du domaine en procédant comme suit :

1. Sur **LON-SVR1**, dans le **Gestionnaire de serveur**, sur le coté gauche, cliquez sur **Serveur local**.
2. Dans la section **Propriétés LON-SVR1**, cliquez sur le domaine **Adatum.com**.
3. Dans la boîte de dialogue **Propriétés système**, cliquez sur **Modifier**.
4. Dans **Modification du nom ou du domaine de l'ordinateur**, dans la section **Membre d'un**, cliquez sur **Groupe de travail**, saisissez **MUNICH**, puis cliquez sur **OK**.
5. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, cliquez sur **OK**.
6. Dans la boîte de dialogue **Nom de l'ordinateur/Changements de domaine**, vous verrez le message suivant : « Bienvenue dans le groupe de travail MUNICH ». Cliquez sur **OK**.
7. Dans la boîte de dialogue **Nom de l'ordinateur/Changements de domaine**, vous verrez le message suivant : « Vous devez redémarrer votre ordinateur pour appliquer ces modifications ». Cliquez sur **OK**.
8. Dans la boîte de dialogue **Propriétés système**, cliquez sur **Fermer**.
9. Dans la boîte de dialogue **Microsoft Windows**, cliquez sur **Redémarrer maintenant**.
10. Connexion en tant que :
  - o Nom d'utilisateur : **Administrateur**
  - o Mot de passe : **Pa55w.rd**.
11. Basculez vers **LON-DC2**. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
12. Dans le volet de navigation, développez **Adatum.com**, cliquez pour sélectionner **Serveurs Adatum**, cliquez avec le bouton droit sur **LON-SVR1**, puis cliquez sur **Supprimer**.
13. Dans la boîte de dialogue **Services de domaine Active Directory**, confirmez la suppression en cliquant sur **Oui**.
14. Dans la boîte de dialogue **Confirmer suppression sous-arborescence**, cliquez sur **Oui**

## Organiser l'installation déléguée d'un RODC

1. Sur **LON-DC2**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
  2. Dans **Sites et services Active Directory**, dans le volet de navigation, cliquez sur **Sites**. Dans le menu **Action**, cliquez sur **Nouveau site**.
  3. Dans la boîte de dialogue **Nouvel objet - Site** dans le champ **Nom**, saisissez **Munich**, sélectionnez l'objet du lien de sites **DEFAULTSITELINK**, puis cliquez sur **OK**.
  4. Dans la boîte de dialogue **Services de domaine Active Directory**, cliquez sur **OK**.
  5. Basculez sur le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
  6. Dans **Centre d'administration Active Directory**, dans le volet de navigation, cliquez sur **Adatum (local)**, puis dans le volet d'informations, double-cliquez sur l'unité d'organisation (UO) **Contrôleurs de domaine**.
  7. Dans le volet **Tâches**, dans la section **Contrôleurs de domaine**, cliquez sur **Précréer un compte de contrôleur de domaine en lecture seule**.
  8. Dans l'**Assistant Installation des services de domaine Active Directory**, sur la page **Bienvenue dans l'assistant Installation des services de domaine Active Directory**, cliquez sur **Suivant**.
  9. Sur la page **Identification Réseau**, cliquez sur **Suivant**.
  10. Sur la page **Spécifiez le nom de l'ordinateur**, saisissez le nom d'ordinateur comme **LON-SVR1**, puis cliquez sur **Suivant**.
  11. Sur la page **Sélectionner un site**, cliquez sur **Munich**, puis sur **Suivant**.
  12. Sur la page **Options supplémentaires pour le contrôleur de domaine**, acceptez les sélections par défaut de **serveur DNS** et **Catalogue global**, puis cliquez sur **Suivant**.
  13. Sur la page **Délégation de l'installation et de l'administration du RODC**, cliquez sur **Définir**.
  14. Dans la boîte de dialogue **Sélectionner un utilisateur ou un groupe**, dans la zone **Entrer le nom de l'objet à sélectionner**, saisissez **Nestor**, puis cliquez sur **Vérifier les noms**.
  15. Vérifiez que **Nestor Fiore** est résolu, ensuite cliquez sur **OK**.
  16. Sur la page **Délégation de l'installation et de l'administration du RODC**, cliquez sur **Suivant**.
  17. Sur la page **Résumé**, vérifiez vos sélections, puis cliquez sur **Suivant**.
  18. Sur la page **Fin de l'Assistant Installation des services de domaine Active Directory**, cliquez sur **Terminer**.
- **Tâche 2 : Exécuter l'Assistant Installation des services de domaine Active Directory sur un RODC pour terminer le processus de déploiement**
1. Basculez vers **LON-SVR1**. Dans le **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**.
  2. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
  3. Sur la page **Sélectionner le type d'installation**, acceptez le paramètre par défaut **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
  4. Sur la page **Sélectionner le serveur de destination**, assurez-vous que **LON-SVR1** est sélectionné, puis cliquez sur **Suivant**.

5. Sur la page **Sélectionner des rôles de serveurs**, dans la liste **Rôles**, sélectionnez **Services de domaine Active Directory**.
6. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, acceptez d'installer les fonctionnalités et les outils de gestion, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Sur la page **Services de domaine Active Directory**, cliquez sur **Suivant**.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Patientez jusqu'à ce que le rôle s'installe. Vous pouvez cliquer sur **Fermer** à tout moment, mais surveiller l'icône **Notification** dans le Gestionnaire de serveur.
11. Lorsque l'installation du nouveau rôle est terminée, cliquez sur l'icône **Notification** pour les notifications.
12. Dans la boîte de message **Configuration post-déploiement**, cliquez sur **Promouvoir ce serveur à un contrôleur de domaine**.
13. Dans l'**Assistant Configuration des services de domaine Active Directory**, sur la page **Configuration de déploiement**, laissez le paramètre par défaut **Ajouter un contrôleur de domaine à un domaine existant**.
14. Dans la section **Fournir les informations d'identification pour effectuer cette opération**, cliquez sur **Modifier**.
15. Dans la boîte de dialogue **Sécurité Windows**, saisissez les informations suivantes :
  - Nom d'utilisateur : **Adatum\NESTOR**
  - Mot de passe : **Pa55w.rd**.
16. Sous **Spécifier les informations de domaine pour cette opération**, cliquez sur **Sélectionner**, puis sélectionnez le domaine **Adatum.com**, cliquez sur **OK**, puis cliquez sur **Suivant**.
 

Vous recevrez une notification vous informant qu'un compte RODC qui correspond au nom du serveur existe dans le répertoire.
17. Sur la page **Options de contrôleur de domaine**, acceptez la valeur par défaut à **Utiliser le compte RODC existant**, dans les champs **Mot de passe** et **Confirmer le mot de passe**, entrez **Pa55w.rd**, puis cliquez sur **Suivant**.
18. Sur la page **Options supplémentaires**, acceptez les valeurs par défaut, puis cliquez sur **Suivant**.
19. Sur la page **Chemins**, acceptez les valeurs par défaut, puis cliquez sur **Suivant**.
20. Sur la page **Options de révision**, vérifiez vos options, puis cliquez sur **Suivant**.
21. Une fois la vérification des prérequis effectuée, cliquez sur **Installer**.



**Remarque :** L'ordinateur va configurer AD DS et redémarrer, mais vous pouvez passer à la tâche suivante.

#### ► Tâche 3 : Configurer la stratégie de réPLICATION de mot de passe à l'échelle du domaine

1. Basculez vers **LON-DC2**. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.

2. Dans **Centre d'administration Active Directory**, dans le volet de navigation, cliquez sur **Adatum (local)**.
3. Dans le volet d'informations, double-cliquez sur **IT**.
4. Localisez le groupe **IT**, cliquez avec le bouton droit sur le groupe, puis cliquez sur **Ajouter à un autre groupe**.
5. Dans la boîte de dialogue **Sélectionner un groupe**, dans la zone **Entrer le nom de l'objet à sélectionner**, saisissez **Groupe de réPLICATION dont le mot de passe RODC est refusé**, puis cliquez sur **Vérifier les noms**.
6. Vérifiez que le nom du groupe est élargi à **Groupe de réPLICATION dont le mot de passe RODC est refusé**, puis cliquez sur **OK**.

 **Remarque :** Les membres du groupe IT ont des autorisations élevées, de sorte que le stockage de leur mot de passe sur un RODC serait un risque de sécurité. Par conséquent, vous ajoutez le groupe Informatique à la liste mondiale Deny, qui s'applique à tous les RODC dans le domaine.

7. Fermez le **Centre d'administration Active Directory**.

► **Tâche 4 : Créer un groupe pour gérer la réPLICATION de mot de passe au RODC de la filiale**

1. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans le volet de navigation, développez **Adatum.com**, puis cliquez sur **Utilisateurs**.
3. Dans le menu **Action**, cliquez sur **Nouveau**, puis sur **Groupe**.
4. Dans la boîte de dialogue **Nouvel objet - Groupe**, saisissez le nom du groupe **Groupe de réPLICATION de mot de passe RODC autorisé Munich**, cliquez sur **OK**, puis double-cliquez sur **Groupe de réPLICATION de mot de passe RODC autorisé Munich**.
5. Dans l'onglet **Membres**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Sélectionnez les utilisateurs, contacts, ordinateurs, comptes de services ou groupes**, dans la zone de texte **Entrez les noms des objets à sélectionner**, saisissez **Ana**, puis cliquez sur **Vérifier les noms**.
7. Dans la boîte de dialogue **Plusieurs noms trouvés**, cliquez sur **Ana Cantrell**, puis sur **OK**.
8. Dans la boîte de dialogue **Sélectionner les Utilisateurs, Contacts, Ordinateurs, comptes de service ou Groupes**, cliquez sur **OK**, puis dans la boîte de dialogue **Groupe de réPLICATION de mot de passe RODC autorisé Munich**, cliquez sur **OK**.
9. Fermez la fenêtre **Utilisateurs et ordinateurs Active Directory**.
10. Dans **Centre d'administration Active Directory**, de l'UO **Contrôleurs de domaine**, visualiser les propriétés de **LON-SVR1**.
11. Dans la section **Extensions**, sous l'onglet **Stratégie de réPLICATION de mot de passe**, cliquez sur **Ajouter**.
12. Dans la boîte de dialogue **Ajouter des groupes, des utilisateurs et des ordinateurs**, sélectionnez **Autoriser la réPLICATION des mots de passe du compte sur ce contrôleur de domaine en lecture seule (RODC)**, puis cliquez sur **OK**.

13. Dans la boîte de dialogue **Sélectionnez les utilisateurs, ordinateurs, comptes de service ou groupes**, dans **Entrez les noms des objets à sélectionner**, saisissez **Munich**, puis cliquez sur **Vérifier les noms** puis sur **OK**.

14. Dans la boîte de dialogue **LON-SVR1**, cliquez sur **OK** pour fermer la boîte de dialogue.

► **Tâche 5 : Évaluer la stratégie de réPLICATION de mot de passe qui en résulte**

1. Dans **Centre d'administration Active Directory**, dans le volet **Tâches**, dans la section **LON-SVR1**, cliquez sur **Propriétés**.
2. Dans les propriétés de **LON-SVR1**, puis dans la section **Extensions**, dans l'onglet **Stratégie de réPLICATION de mot de passe**, cliquez sur **Avancé**

 **Remarque :** Notez que cette boîte de dialogue affiche tous les comptes avec des mots de passe qui sont stockés dans le RODC.

3. Sélectionnez **Comptes authentifiés sur ce contrôleur de domaine en lecture seule**, puis notez que ceci ne montre que les comptes disposant des autorisations et ayant déjà été authentifiés par ce RODC.
4. Cliquez sur l'onglet **Stratégie résultante**, puis ajoutez **Ana Cantrell**. Notez que Sybille Morin a une stratégie résultante d'**Autoriser**.
5. Fermez toutes les boîtes de dialogue ouvertes.

**Résultats :** Une fois cet exercice terminé, vous aurez déployé et configuré un RODC.

### Exercice 3 : Création et association d'un groupe MSA

► **Tâche 1 : Créer et associer un MSA**

1. Dans **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Module Active Directory pour Windows PowerShell**.
2. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Add-KdsRootKey -EffectiveTime ((get-date) .addhours (-10))
```

3. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
New-ADServiceAccount -Name Webservice -DNSHostName LON-DC1 -PrincipalsAllowedToRetrieveManagedPassword LON-DC1$
```

4. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Add-ADComputerServiceAccount -identity LON-DC1 -ServiceAccount Webservice
```

5. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Get-ADServiceAccount -Filter *
```

6. Notez la sortie de la commande, puis assurez-vous que le compte nouvellement créé est répertorié.
7. Réduisez la fenêtre de commande Windows PowerShell.

### ► Tâche 2 : Installer un groupe MSA

- Sur **LON-DC1**, à l'invite Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Install-ADServiceAccount -Identity Webservice
```

- Dans le Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur le **Gestionnaire des services d'information Internet (IIS)**.
- Développez **LON-DC1 (Adatum\Administrateur)**, puis cliquez sur **Pools d'applications**.
- Dans le volet d'informations, cliquez avec le bouton droit sur **DefaultAppPool**, puis cliquez sur **Paramètres avancés**.
- Dans la boîte de dialogue **Paramètres avancés**, dans la section **Modèle de processus**, cliquez sur **Identité**, puis cliquez sur les ellipses (...).
- Dans la boîte de dialogue **Identité du pool d'applications**, cliquez sur **Compte personnalisé**, puis cliquez sur **Définir**.
- Dans la boîte de dialogue **Modifier les identifiants**, saisissez **Adatum\Webservice\$** dans le champ **Nom d'utilisateur**, puis cliquez sur **OK** trois fois.
- Dans le volet **Actions**, cliquez sur **Arrêter** pour arrêter le pool d'applications.
- Cliquez sur **Démarrer** pour démarrer le pool d'applications.
- Fermez le **Gestionnaire de services d'information Internet (IIS)**.

**Résultats :** Une fois cet exercice terminé, vous aurez configuré un compte de service administré (MSA, Managed Service Account).

### ► Tâche 3 : Préparer le module suivant

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

- Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
- Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
- Dans la boîte de dialogue **Rétablissement de l'ordinateur virtuel**, cliquez sur **Rétablissement**.
- Répétez les étapes 2 et 3 pour **22742A-LON-DC2** et **22742A-LON-SVR1**.

## Module 8 : Déploiement et gestion AD CS

# Atelier pratique : Déploiement et configuration d'une hiérarchie AC à deux niveaux

### Exercice 1 : Déploiement d'une AC racine hors ligne

#### ► Tâche 1 : Créer des exceptions au partage de fichiers et d'imprimantes

1. Connectez-vous à **CA-SVR1** en tant qu'**Administrateur** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur Démarrer, puis sur **Panneau de Configuration**.
3. Dans la fenêtre **Panneau de configuration**, cliquez sur **Afficher l'état et la gestion du réseau**.
4. Dans la fenêtre **Centre Réseau et partage**, cliquez sur **Modifier les paramètres de partage avancés**.
5. Sous **Invité ou Public (profil actuel)**, sélectionnez l'option **Activer le partage de fichiers et d'imprimantes**, puis cliquez sur **Enregistrer les modifications**.
6. Basculez vers **LON-SVR1**.
7. Cliquez sur Démarrer, puis sur **Panneau de Configuration**.
8. Dans la fenêtre **Panneau de configuration**, cliquez sur **Afficher l'état et la gestion du réseau**.
9. Dans la fenêtre **Centre Réseau et partage**, cliquez sur **Modifier les paramètres de partage avancés**.
10. Sous **Invité ou Public (profil actuel)**, sélectionnez l'option **Activer le partage de fichiers et d'imprimantes**, puis cliquez sur **Enregistrer les modifications**.

#### ► Tâche 2 : Installer et configurer AD CS sur CA-SVR1

1. Basculez vers **CA-SVR1**.
2. Cliquez **Démarrer**, puis cliquez sur **Gestionnaire de serveur**. Dans le **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner rôles de serveur**, sélectionnez **Services de Certificats Active Directory**. Quand l'**Assistant Ajout de rôles et de fonctionnalités** s'affiche, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Sur la page **Services de certificats Active Directory**, cliquez sur **Suivant**.
9. Sur la page **Sélectionner les services de rôle**, vérifiez que **Autorité de certification** est sélectionné, puis cliquez sur **Suivant**.
10. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. Sur la page **Progression de l'installation**, après l'installation terminée, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination**.

12. Dans l'**Assistant Configuration AD CS**, sur la page **Identifiants**, cliquez sur **Suivant**.
13. Sur la page **Services de rôle**, sélectionnez **Autorité de certification**, puis cliquez sur **Suivant**.
14. Sur la page **Type d'installation**, vérifiez que l'option **AC autonome** est sélectionnée, puis cliquez sur **Suivant**.
15. Sur la page **Type d'autorité de certification**, vérifiez que l'option **AC racine** est sélectionnée, puis cliquez sur **Suivant**.
16. Sur la page **Clé privée**, vérifiez que **Créer une nouvelle clé privée** est sélectionné, puis cliquez sur **Suivant**.
17. Sur la page **Chiffrement pour l'autorité de certification**, conservez les sélections par défaut pour Fournisseur de services de cryptographie (CSP) et Algorithme de hachage, mais définissez la **longueur de la clé à 4096**, puis cliquez sur **Suivant**.
18. Sur la page **Nom d'AC**, dans la zone **Nom commun pour cette AC**, saisissez **AdatumRootCA**, puis cliquez sur **Suivant**.
19. Sur la page **Période de validité**, cliquez sur **Suivant**.
20. Sur la page **Base de données de l'autorité de certification**, cliquez sur **Suivant**.
21. Sur la page **Confirmation**, cliquez sur **Configurer**.
22. Sur la page **Résultats**, cliquez sur **Fermer**.
23. Sur la page **Progression de l'installation**, cliquez sur **Fermer**.
24. Sur **CA-SVR1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Autorité de certification**.
25. Dans la console **certsrv – [Autorité de certification (Locale)]**, cliquez avec le bouton droit sur **AdatumRootCA**, puis cliquez sur **Propriétés**.
26. Dans la boîte de dialogue **Propriétés AdatumRootCA**, cliquez sur l'onglet **Extensions**.
27. Sous l'onglet **Extensions**, dans la liste déroulante **Sélectionner l'extension**, cliquez sur **Point de distribution CRL (CDP)**, puis cliquez sur **Ajouter**.
28. Dans la boîte **Emplacement**, saisissez **http://lon-svr1.adatum.com/CertData/**, dans la liste déroulante **Variable**, cliquez sur <NomAutoritéCertification>, puis cliquez sur **Insérer**.
29. Dans la liste déroulante **Variable**, sélectionnez <SuffixeNomListeRévocationCertificats>, puis cliquez sur **Insérer**.
30. Dans la liste déroulante **Variable**, sélectionnez <ListeRévocationCertificatsDeltaAutorisée>, puis cliquez sur **Insérer**.
31. Dans la boîte **Emplacement**, placez le curseur à la fin de l'URL, entrez **.crl**, puis cliquez sur **OK**.
32. Sélectionnez les options suivantes, puis cliquez sur **Appliquer** :
  - Inclure dans l'extension CDP des certificats émis**
  - Inclure dans les CRL. Les clients utilisent cela pour trouver des emplacements Delta CRL**
33. Dans la fenêtre indépendante **Autorité de certification**, cliquez sur **Non**.
34. Dans la liste déroulante **Sélectionner l'extension**, cliquez sur **Accès aux informations de l'autorité (AIA)**, puis cliquez sur **Ajouter**.
35. Dans la boîte **Emplacement**, saisissez **http://lon-svr1.adatum.com/CertData/**, dans la liste déroulante **Variable**, cliquez sur <NomduServeurDNS>, puis cliquez sur **Insérer**.

36. Dans la boîte **Emplacement**, saisissez un tiret bas (\_), dans la liste déroulante **Variable**, cliquez sur <**NomAutoritéCertification**>, puis cliquez sur **Insérer**. Placez le curseur à la fin de l'URL.
37. Dans la liste déroulante **Variable**, cliquez sur <**NomCertificat**>, puis sur **Insérer**.
38. Dans la boîte **Emplacement**, placez le curseur à la fin de l'URL, entrez .crt, puis cliquez sur **OK**.
39. Cochez la case **Inclure dans l'extension AIA des certificats délivrés**, puis cliquez sur **OK**.
40. Cliquez **Oui** pour redémarrer le service d'autorité de certification.
41. Dans la console **Autorité de certification**, développez **AdatumRootCA**, cliquez avec le bouton droit sur **Certificats révoqués**, pointez vers **Toutes les tâches**, puis cliquez sur **Publier**.
42. Dans la fenêtre **Publier la liste de révocation des certificats**, cliquez sur **OK**.
43. Cliquez avec le bouton droit sur **AdatumRootCA**, puis cliquez sur **Propriétés**.
44. Dans la boîte de dialogue **Propriétés AdatumRootCA**, cliquez sur **Afficher Certificat**.
45. Dans la boîte de dialogue **Certificats**, cliquez sur l'onglet **Détails**.
46. Sous l'onglet **Détails**, cliquez sur **Copier dans un fichier**.
47. Dans l'**Assistant Exportation du certificat**, sur la page **Bienvenue**, cliquez sur **Suivant**.
48. Sur la page **Format de fichier d'exportation**, sélectionnez **Binaire codé DER X.509 (.CER)**, puis cliquez sur **Suivant**.
49. Sur la page **Fichier à exporter**, cliquez sur **Parcourir**. Dans la zone de texte **Nom de fichier**, saisissez \\lon-svr1\c\$, puis appuyez sur Entrée.
50. Dans la zone **Nom de fichier**, saisissez **RootCA**, cliquez sur **Enregistrer** puis cliquez sur **Suivant**.
51. Cliquez sur **Terminer**, puis sur **OK** trois fois.
52. Ouvrez l'**Explorateur de fichiers** puis accédez à **C:\Windows\System32\CertSrv\CertEnroll**.
53. Dans le dossier **CertEnroll**, Ctrl+clic sur les deux fichiers, cliquez avec le bouton droit sur les fichiers en surbrillance, puis cliquez sur **Copier**.
54. Dans la barre d'adresse de l'Explorateur de fichiers, saisissez \\lon-svr1\c\$, puis appuyez sur Entrée.
55. Cliquez avec le bouton droit sur un espace vide, puis cliquez sur **Coller**.
56. Fermez l'Explorateur de fichiers.

► **Tâche 3 : Créer un enregistrement DNS (Domain Name System) pour une AC racine hors ligne**

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.
2. Dans la console Gestionnaire DNS, développez **LON-DC1**, développez **Zones de recherche directe**, cliquez sur **Adatum.com** cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
3. Dans la fenêtre **Nouvel hôte**, dans la zone **Nom**, saisissez **CA-SVR1**.
4. Dans la fenêtre **Adresse IP**, saisissez **172.16.0.40**, cliquez sur **Ajouter un hôte**, cliquez **OK**, puis cliquez sur **Terminer**.
5. Fermez le Gestionnaire DNS.

**Résultats :** Une fois cet exercice terminé, vous aurez installé et configuré le rôle de l'AC racine autonome sur le serveur **CA-SVR1**. En outre, vous aurez créé un enregistrement DNS approprié dans Active Directory Domain Services (AD DS) pour que d'autres serveurs puissent se connecter à **CA-SVR1**.

## Exercice 2 : Déploiement d'une AC secondaire d'entreprise

### ► Tâche 1 : Installer et configurer AD CS sur LON-SVR1

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, sur **Gestionnaire de serveur**, puis sur **Ajouter des rôles et des fonctionnalités**.
2. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner rôles de serveur**, sélectionnez **Services de Certificats Active Directory**.
6. Quand l'**Assistant Ajout de rôles et de fonctionnalités** s'affiche, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Sur la page **Services de certificats Active Directory**, cliquez sur **Suivant**.
9. Sur la page **Sélectionner les services de rôle**, vérifiez que **Autorité de certification** est déjà sélectionné, puis sélectionnez **Inscription Web Autorité de certification**.
10. Quand l'**Assistant Ajout de rôles et de fonctionnalités** s'affiche, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
11. Sur la page **Rôle Serveur Web (IIS)**, cliquez sur **Suivant**.
12. Sur la page **Sélectionner les services du rôle**, cliquez sur **Suivant**.
13. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
14. Sur la page **Progression de l'installation**, après l'installation terminée, cliquez sur le texte **Configurer les services de certificats Active Directory** sur le serveur de destination.
15. Dans l'**Assistant Configuration AD CS**, sur la page **Identifiants**, cliquez sur **Suivant**.
16. Sur la page **Services de rôle**, sélectionnez à la fois **Autorité de certification** et **Inscription Web Autorité de certification**, puis cliquez sur **Suivant**.
17. Sur la page **Type d'installation**, sélectionnez **AC d'entreprise**, puis cliquez sur **Suivant**.
18. Sur la page **Type d'autorité de certification**, sélectionnez **AC secondaire**, puis cliquez sur **Suivant**.
19. Sur la page **Clé privée**, vérifiez que **Créer une nouvelle clé privée** est sélectionné, puis cliquez sur **Suivant**.
20. Sur la page **Chiffrement pour l'autorité de certification**, conservez les valeurs par défaut, puis cliquez sur **Suivant**.
21. Sur la page **Nom d'AC**, dans la zone **Nom commun pour cette AC**, saisissez **Adatum-IssuingCA**, puis cliquez sur **Suivant**.
22. Sur la page **Demande de certificat**, vérifiez que **Enregistrer une demande de certificat sur fichier dans la machine cible** est sélectionné, puis cliquez sur **Suivant**.
23. Sur la page **Base de données de l'autorité de certification**, cliquez sur **Suivant**.

24. Sur la page **Confirmation**, cliquez sur **Configurer**.
  25. Sur la page **Résultats**, ignorez les messages d'avertissement et cliquez sur **Fermer**.
  26. Sur la page **Progression de l'installation**, cliquez sur **Fermer**.
- **Tâche 2 : Installer un certificat d'autorité de certification subordonné**
1. Sur **LON-SVR1**, ouvrez une fenêtre **Explorateur de fichiers**, puis accédez à **Disque local (C:)**.
  2. Cliquez avec le bouton droit sur **RootCA.cer**, ensuite cliquez sur **Installer le certificat**.
  3. Sur la page **Assistant Importation de certificat**, cliquez sur **Ordinateur local** puis sur **Suivant**.
  4. Sur la page **Magasin de certificats**, cliquez sur **Placer tous les certificats dans le magasin suivant**, puis sur **Naviguer**.
  5. Sélectionnez **Autorités de certification racine de confiance**, cliquez sur **OK**, puis sur **Suivant** et **Terminer**.
  6. Lorsque la fenêtre **Assistant Importation de certificat** apparaît, cliquez sur **OK**.
  7. Dans la fenêtre **Explorateur de fichiers**, appuyez sur la touche Ctrl et cliquez sur les fichiers **AdatumRootCA.crl** et **CA-SVR1\_AdatumRootCA.crt**, cliquez avec le bouton droit sur les fichiers, puis cliquez sur **Copier**.
  8. Double-cliquez sur **inetpub**.
  9. Double-cliquez sur **wwwroot**.
  10. Créez un nouveau dossier, puis nommez-le **CertData**.
  11. Collez les deux fichiers copiés dans ce dossier.
  12. Basculez vers le **Disque local (C:)**.
  13. Cliquez avec le bouton droit sur le fichier **LON-SVR1.Adatum.com\_Adatum-LON-SVR1-CA.req**, puis cliquez sur **Copier**.
  14. Dans la barre d'adresse de l'Explorateur de fichiers, saisissez **\CA-SVR1\C\$**, puis appuyez sur Entrée.
  15. Dans la fenêtre **Explorateur de fichiers**, cliquez avec le bouton droit sur un espace vide, puis cliquez sur **Coller**. Assurez-vous que le fichier de demande est copié sur **CA-SVR1**.
  16. Basculez vers le serveur **CA-SVR1**.
  17. Dans la console **Autorité de certification** console, cliquez avec le bouton droit sur **AdatumRootCA**, pointez vers **Toutes les tâches**, puis cliquez sur **Soumettre nouvelle demande**.
  18. Dans la fenêtre **Ouvrir fichier de demande**, accédez à **Disque local (C:)**, cliquez sur le fichier **LON-SVR1.Adatum.com\_Adatum- LON-SVR1-CA.req**, puis cliquez sur **Ouvrir**.
  19. Dans la console **Autorité de certification**, cliquez sur le conteneur **Demandes en attente**. Cliquez avec le bouton droit sur **Requêtes en attente**, puis cliquez sur **Actualiser**.
  20. Dans le volet d'informations, cliquez avec le bouton droit sur la requête (avec ID 2), pointez sur **Toutes les tâches** et cliquez sur **Délivrer**.
  21. Dans la console **Autorité de certification**, cliquez sur le conteneur **Certificats délivrés**.
  22. Dans le volet d'informations, double-cliquez sur le certificat, cliquez sur l'onglet **Détails**, puis sur **Copier dans un fichier**.
  23. Dans l'**Assistant Exportation du certificat**, sur la page **Bienvenue**, cliquez sur **Suivant**.

24. Sur la page **Format de fichier d'exportation**, cliquez sur **Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)**, cliquez sur **Inclure tous les certificats dans le chemin d'accès de certification, si possible**, puis sur **Suivant**.
25. Sur la page **Fichier à exporter**, cliquez sur **Parcourir**.
26. Dans la zone de texte **Nom de fichier**, saisissez **\lon-svr1\C\$**, puis appuyez sur Entrée.
27. Dans la boîte **Nom de fichier**, saisissez **SubCA**, cliquez successivement sur **Enregistrer**, **Suivant** et **Terminer**, puis cliquez sur **OK** deux fois.
28. Basculez vers **LON-SVR1**.
29. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Autorité de certification**.
30. Dans la console **Autorité de certification**, cliquez avec le bouton droit sur **Adatum-IssuingCA**, pointez vers **Toutes les tâches**, puis cliquez sur **Installer un certificat d'autorité de certification**.
31. Allez sur **Disque local (C:)**, cliquez sur le fichier **SubCA.p7b**, puis cliquez sur **Ouvrir**.
32. Patientez 15-20 secondes, puis sur la barre d'outils, cliquez sur l'icône **verte** pour démarrer le service CA.
33. Assurez-vous que le CA démarre correctement.
34. Basculez vers **CA-SVR1**.
35. Arrêtez le serveur.

 **Remarque :** De ce point, vous pouvez mettre en toute sécurité l'AC racine hors connexion et utiliser simplement l'AC subordonnée d'entreprise.

#### ► Tâche 3 : Publier un certificat AC racine via la stratégie de groupe

1. Dans **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la **Console de gestion de stratégie de groupe**, développez **Forêt : Adatum.com**, **Domaines** et **Adatum.com**, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
3. Dans le nœud **Configuration de l'ordinateur**, développez successivement **Stratégies**, **Paramètres Windows**, **Paramètres Sécurité** et **Stratégies de clé publique**, cliquez avec le bouton droit sur **Autorités de certification racine de confiance**, cliquez sur **Importer**, puis cliquez sur **Suivant**.
4. Sur la page **Fichier à exporter**, cliquez sur **Parcourir**.
5. Dans la zone de texte **Nom de fichier**, saisissez **\lon-svr1\C\$** et appuyez sur Entrée.
6. Cliquez sur **RootCA.cer**, puis sur **Ouvrir**.
7. Cliquez deux fois sur **Suivant** puis cliquez sur **Terminer**.
8. Lorsque la fenêtre **Assistant Importation de certificat** apparaît, cliquez sur **OK**.

 **Remarque :** Il se peut que cette fenêtre n'apparaisse pas avant 15-20 secondes.

9. Fermez l'**Éditeur de gestion des stratégies de groupe** et la **Console de gestion des stratégies de groupe**.

**Résultats :** Une fois cet exercice terminé, vous aurez déployé et configuré une autorité de confiance d'entreprise. Vous aurez également un certificat d'autorité de certification subordonné émis par une AC racine installée sur **LON-SVR1**. Pour établir la confiance entre l'AC racine et les clients joints à un domaine, vous allez utiliser la stratégie de groupe pour déployer un certificat AC racine.

► **Tâche 4 : Préparer le module suivant**

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-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 **22742A-LON-SVR1**, **22742A-LON-DC2** et **22742A-CA-SVR1**.



## Module 9 : Déploiement et gestion des certificats

# Atelier pratique : Déploiement et utilisation de certificats

### Exercice 1 : Configuration des modèles de certificats

► Tâche 1 : Créer un nouveau modèle basé sur le modèle de serveur Web

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Autorité de certification**.
2. Dans la console **Autorité de certification**, développez **AdatumCA**, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
3. Dans la console **Modèles de certificats**, recherchez le modèle **Serveur Web** dans la liste, cliquez avec le bouton droit sur ce dernier, puis cliquez sur **Dupliquer modèle**.
4. Cliquez sur l'onglet **Général**, dans la zone de texte **Nom complet du modèle**, saisissez **Serveur Web de production**, puis saisissez **3** dans la zone de texte **Période de validité**.
5. Cliquez sur l'onglet **Traitement de la demande**, sélectionnez **Autoriser l'exportation de la clé privée**, puis cliquez sur **OK**. Réduisez la console **Modèles de certificats**.
6. Dans la console **Autorité de certification** sur **LON-DC1**, cliquez avec le bouton droit sur **Révocation du certificat**, sélectionnez **Toutes les tâches**, cliquez sur **Publier**, puis cliquez sur **OK**.

► Tâche 2 : Créer un nouveau modèle pour les utilisateurs qui inclut la connexion carte à puces

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Autorité de certification**.
2. Développez **AdatumCA**, puis cliquez avec le bouton droit sur **Modèles de certificats** et cliquez sur **Gérer**. Dans la console **Modèles de certificats**, cliquez avec le bouton droit sur le modèle de certificat **Utilisateur**, puis cliquez **Dupliquer Modèle**.
3. Dans la boîte de dialogue **Propriétés du Nouveau Modèle**, cliquez sur l'onglet **Général**, dans la zone de texte **Nom complet du modèle**, saisissez **Utilisateur adatum**.
4. Sous l'onglet **Nom Sujet**, désactivez les deux cases à cocher **Inclure le nom de compte de messagerie dans le nom du sujet** et **Nom E-mail**.
5. Sous l'onglet **Extensions**, cliquez sur **Stratégies d'application**, puis cliquez sur **Modifier**.
6. Dans la boîte de dialogue **Modifier l'extension des stratégies d'application**, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Ajouter une stratégie d'application**, sélectionnez **Ouverture de session par carte à puce**, puis cliquez sur **OK** deux fois.
8. Cliquez sur l'onglet **Modèles Obsolètes**, sur **Ajouter**, sur le modèle **Utilisateur**, puis sur **OK**.
9. Sous l'onglet **Sécurité**, cliquez sur **Utilisateurs authentifiés**. Sous **Autorisations pour les utilisateurs authentifiés**, cochez la case **Autoriser pour Lire, Écrire et Inscription automatique**, puis cliquez sur **OK**.
10. Fermer la console **Modèles de certificats**.

► **Tâche 3 : Configurer les modèles de sorte qu'ils peuvent être émis**

1. Sur **LON-DC1**, dans la console **Autorité de certification**, cliquez avec le bouton droit sur **Modèles de certificats**, pointez vers **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
2. Dans la fenêtre **Activer les modèles de certificats**, sélectionnez **Utilisateur Adatum** et **Serveur Web de production**, puis cliquez sur **OK**.

► **Tâche 4 : Incrire le certificat de serveur Web sur LON-SVR2**

1. Basculez vers **LON-SVR2**.
2. Cliquez sur **Démarrer**, puis cliquez sur l'icône **Windows PowerShell**.
3. À l'invite de commandes dans l'interface de ligne de commande Windows PowerShell, entrez **gpupdate/force**, puis appuyez sur Entrée.
4. Cliquez **Démarrer**, puis cliquez sur **Gestionnaire de serveur**. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur le **Gestionnaire des services d'information Internet (IIS)**.
5. Dans la console IIS, cliquez sur **LON-SVR2**, puis dans le volet central, double-cliquez sur **Certificats Serveur**.
6. Dans le volet **Actions**, cliquez sur **Créer un certificat de domaine**.
7. Sur la page **Propriétés nom différencié**, complétez les informations suivantes, puis cliquez sur **Suivant :**
  - Nom commun : **lon-svr2.adatum.com**
  - Organisation : **Adatum**
  - Unité d'organisation : **Research**
  - Ville/localité : **Seattle**
  - État/Province : **WA**
  - Pays/Région : **USA**
8. Sur la page **Autorité de certification en ligne**, cliquez sur **Sélectionner**, cliquez sur **AdatumCA**, puis cliquez sur **OK**.
9. Dans la zone de texte **Nom convivial**, entrez **lon-svr2**, puis cliquez sur **Terminer**.
10. Assurez-vous que le certificat apparaît dans la console **Certificats de serveur**.
11. Dans la console **IIS**, développez **LON-SVR2**, développez **Sites**, puis cliquez sur **Site Web par défaut**.
12. Dans le volet **Actions**, cliquez sur **Liaisons**.
13. Dans la fenêtre **Liaisons de sites**, sélectionnez **Ajouter**.
14. Dans la fenêtre **Ajouter la liaison de site**, sélectionnez **https** à partir de la liste déroulante **Entrer**. Dans la liste déroulante **certificat SSL**, cliquez sur **lon-svr2**, cliquez sur **OK**, puis cliquez sur **Fermer**.
15. Fermez le **Gestionnaire de services d'information Internet (IIS)**.
16. Basculez vers **LON-CL1**. Dans le champ de recherche **Cortana**, saisissez **Internet Explorer**. Puis cliquez sur **Internet Explorer** dans la recherche des résultats renvoyés.
17. Dans Internet Explorer, entrez **HTTPS://lon-svr2.adatum.com** dans la barre d'adresse, puis appuyez sur Entrée.
18. Assurez-vous que la page **Internet Information Services** s'ouvre et qu'aucune erreur de certificat ne s'affiche.

**Résultats :** Une fois cet exercice terminé, vous aurez configuré les modèles de certificats.

## Exercice 2 : Incription et utilisation de certificats

► Tâche 1 : Configurer l’inscription automatique pour les utilisateurs

1. Dans **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Développez **Forêt : Adatum.com, Domaines et Adatum.com**, cliquez avec le bouton droit sur **Stratégie de domaine par défaut**, puis cliquez sur **Modifier**.
3. Développez successivement **Configuration utilisateur**, **Stratégies**, **Paramètres Windows** et **Paramètres de sécurité**, puis cliquez sur pour sélectionner **Stratégies de clé publique**.
4. Dans le volet **Détails**, double-cliquez sur **Client de services de certificats – Inscription automatique**.
5. Dans la liste déroulante **Modèle de configuration**, cliquez sur **Activé**, sélectionnez **Renouveler les certificats expirés, mettre à jour les certificats en attente, supprimer les certificats révoqués et Mettre à jour les certificats qui utilisent les modèles de certificats**, puis cliquez sur **OK** pour fermer la fenêtre des propriétés.
6. Dans le volet de droite, double-cliquez sur l’objet **Client de services de certificats - Stratégie d’inscription de certificats**.
7. Sous l’onglet **Stratégie d’inscription**, définissez le **Modèle de configuration** sur **Activé**, puis assurez-vous que la liste **Stratégie d’inscription de certificats** affiche la stratégie **Inscription Active Directory**. Vous devriez voir une coche à côté et l’état **Activé** devrait être affiché. Cliquez sur **OK** pour fermer la fenêtre.
8. Fermez la fenêtre **Éditeur de gestion des stratégies de groupe** et la console de **Gestion des stratégies de groupe**.

► Tâche 2 : Vérifier l’inscription automatique

1. Sur **LON-CL1**, cliquez sur **Démarrer**, entrez **PowerShell**, puis sur l’icône **Windows PowerShell**.
2. À l’invite de commandes Windows PowerShell, saisissez **gpupdate/force**, puis appuyez sur Entrée.
3. Après le rafraîchissement de la stratégie, saisissez **mmc.exe**, puis appuyez sur Entrée.
4. Dans **Console1**, cliquez sur **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**, cliquez sur **Certificats**, cliquez sur **Ajouter**, cliquez sur **Terminer**, puis cliquez sur **OK**.
5. Développez successivement **Certificats – Utilisateur actuel**, **Personnel**, puis cliquez sur **Certificats**.
6. Vérifiez qu’un certificat basé sur le modèle **Utilisateur Adatum** est délivré pour **Administrateur**. Pour vérifier le nom du modèle, faites défiler vers la droite dans la fenêtre de la console.
7. Fermez la **Console1** sans enregistrer les modifications.
8. Déconnectez-vous de **LON-CL1**.

► Tâche 3 : Configurer l’agent d’inscription pour les certificats de carte à puce

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis ouvrez **Autorité de certification**.
2. Dans la console **certsrv**, développez **AdatumCA**, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
3. Dans la console **Modèles de certificats**, double-cliquez sur **Agent d’inscription**.
4. Cliquez sur l’onglet **Sécurité**, puis sur **Ajouter**.

5. Dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, saisissez **Annie**, cliquez sur **Vérifier les noms** puis cliquez sur **OK**.
6. Sous l'onglet **Sécurité**, cliquez sur **Annie Conner**, cochez la case **Autoriser** pour autorisations **Lire, Écrire et Incrire**, puis cliquez sur **OK**.
7. Fermer la console **Modèles de certificats**.
8. Dans la console **certsrv**, cliquez avec le bouton droit sur **Modèles de certificats**, pointez vers **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
9. Dans la liste des modèles, cliquez sur **Agent d'inscription**, puis cliquez sur **OK**.
10. Basculez vers **LON-CL1**, puis connectez-vous en tant qu'**Adatum\Annie** avec le mot de passe **Pa55w.rd**.
11. Cliquez sur **Démarrer**, saisissez **Invite de commande**, puis appuyez sur Entrée. Dans la fenêtre **Invite de commandes**, saisissez **mmc.exe**, puis appuyez sur Entrée.
12. Dans la fenêtre **Console1**, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
13. Cliquez sur **Certificats**, cliquez sur **Ajouter**, puis cliquez sur **OK**.
14. Développez **Certificats - Utilisateur actuel**, développez **Personnel**, cliquez sur **Certificats**, cliquez avec le bouton droit sur **Certificats**, pointez vers **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.
15. Dans l'**Assistant Inscription de certificats**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
16. Sur la page **Sélectionner la stratégie d'inscription du certificat**, cliquez sur **Suivant**.
17. Sur la page **Demandeur des certificats**, cochez la case **Agent d'inscription**, cliquez sur **Incrire**, puis sur **Terminer**.
18. Déconnectez-vous de **LON-CL1**.
19. Basculez vers **LON-DC1**.
20. Dans la console **Autorité de certification**, cliquez avec le bouton droit sur **AdatumCA**, puis cliquez sur **Propriétés**.
21. Sous l'onglet **Agents d'inscription**, cliquez sur **Restreindre les agents d'inscription**.
22. Dans la fenêtre indépendante qui apparaît, cliquez sur **OK**.
23. Dans la section **Agents d'inscription**, cliquez sur **Ajouter**.
24. Dans le champ **Sélectionner Utilisateur, Ordinateur ou Groupe**, entrez **Annie**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
25. Sélectionnez **Tout le monde**, puis cliquez sur **Supprimer**.
26. Dans la section **Modèles de certificat**, cliquez sur **Ajouter**.
27. Dans la liste des modèles, sélectionnez **Utilisateur Adatum**, puis sur **OK**.
28. Dans la section **Modèles de certificat**, cliquez sur **<Tous>**, puis cliquez sur **Retirer**.
29. Dans la section **Autorisations**, cliquez sur **Ajouter**.
30. Dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs ou des groupes**, saisissez **Marketing**, cliquez sur **Vérifier les noms** puis cliquez sur **OK**.
31. Dans la section **Autorisations**, cliquez sur **Tout le monde**, cliquez sur **Supprimer**, puis sur **OK**.

► **Tâche 4 : Utiliser des certificats pour la signature numérique d'un document Microsoft Office**

1. Sur **LON-CL1**, connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur le bouton **Démarrer**, saisissez **Word 2016**, puis cliquez sur **Word 2016**.



**Remarque :** Si vous recevez une invite de **Assistant d'activation Microsoft Office**, cliquez sur **Fermer**. Si vous êtes invité à mettre à jour, sélectionnez **Me demander ultérieurement**, puis cliquez sur **Accepter**.

3. Cliquez sur **document vierge**, entrez du texte, puis enregistrez le document sur le bureau.
4. Sur la barre d'outils, cliquez sur **INSÉRER**, puis dans le volet **Texte**, dans la liste déroulante **Ligne de signature**, cliquez sur **Ligne de signature Microsoft Office**.
5. Dans la fenêtre **Configuration de signature**, saisissez votre nom dans la zone de texte **Signataire suggéré, Administrateur** dans la zone de texte **Titre du signataire suggéré** et **Administrateur@adatum.com** dans la zone de texte **Adresse e-mail du signataire suggéré**, puis cliquez sur **OK**.
6. Cliquez avec le bouton droit sur la ligne de signature dans le document, puis cliquez sur **Signer...**.
7. Dans la fenêtre **Signer**, cliquez sur **Modifier**.
8. Dans la liste **Certificat**, assurez-vous de disposer d'un certificat délivré pour **Administrateur**, puis cliquez sur **OK**.
9. Dans la zone de texte à droite de **X**, saisissez votre nom, cliquez sur **Signer**, puis cliquez sur **OK**. Outre la saisie de votre nom, vous pouvez également sélectionner une image. Cette image peut être votre signature manuscrite numérisée.
10. Assurez-vous que le document ne peut plus être modifié.



**Remarque :** Essayez de taper un texte dans le document.

11. Fermez Word 2016, puis enregistrez les modifications si vous recevez une invite.
12. Déconnectez-vous de **LON-CL1**.

**Résultats :** À la fin de cet exercice, les stagiaires auront implémenté l'inscription de certificats.

### Exercice 3 : Configuration et mise en œuvre de récupération de clés

► **Tâche 1 : Configurer l'autorité de certification (AC) pour émettre des certificats KRA**

1. Sur **LON-DC1**, dans la console **Autorité de certification**, développez le nœud **AdatumCA**, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
2. Dans le **volet d'informations**, cliquez avec le bouton droit sur le certificat **Agent de récupération de clé** et cliquez sur **Propriétés**.

3. Dans la boîte de dialogue **Propriétés Agent de récupération de clés**, cliquez sur l'onglet **Conditions d'émission**, puis désactivez la case à cocher **Approbation du gestionnaire de certificat de l'autorité de certification**.
4. Cliquez sur l'onglet **Sécurité**. Notez que les groupes d'Admins du domaine et Administrateurs de l'entreprise sont les seuls groupes qui ont l'autorisation d'**Inscrire**, puis cliquez sur **OK**.
5. Fermer la console **Modèles de certificats**.
6. Dans la console **Autorité de certification**, cliquez avec le bouton droit sur **Modèles de certificats**, pointez vers **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
7. Dans la boîte de dialogue **Activer les modèles de certificats**, cliquez sur le modèle **Agent de récupération de clé**, puis sur **OK**.
8. Fermez la console **Autorité de certification**.

#### ► Tâche 2 : Acquérir le certificat KRA

1. Sur **LON-DC1**, cliquez sur **Démarrer**, puis sur l'icône **Windows PowerShell**.
2. À l'invite de commandes Windows PowerShell, saisissez **mmc.exe**, puis appuyez sur Entrée.
3. Dans **Console1 - [Racine de la console]**, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
4. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **Certificats**, puis sur **Ajouter**.
5. Dans la boîte de dialogue **Composant logiciel enfichable Certificats**, sélectionnez **Mon compte d'utilisateur**, cliquez sur **Terminer**, puis sur **OK**.
6. Développez le nœud **Certificats - Utilisateur actuel**, cliquez avec le bouton droit sur **Personnel**, pointez vers **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.
7. Dans l'**Assistant Inscription de certificats**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner la stratégie d'inscription du certificat**, cliquez sur **Suivant**.
9. Sur la page **Demandeur des certificats**, cochez la case **Agent de récupération de clé**, cliquez sur **Inscrire**, puis sur **Terminer**.
10. Actualisez la console, puis consultez l'agent de récupération de clé (KRA) dans le magasin personnel ; faites défiler les propriétés du certificat et vérifiez que **Agent de récupération de clé Modèle de certificat** est présent.
11. Fermez la **Console1** sans enregistrer vos modifications.

#### ► Tâche 3 : Configurer l'AC pour autoriser la récupération de clé

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Autorité de certification**. Dans la console **Autorité de certification**, cliquez avec le bouton droit sur **AdatumCA**, puis cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés AdatumCA**, cliquez sur l'onglet **Agents de récupération**, puis sélectionnez **Archiver la clé**.
3. Sous **Certificats d'agent de récupération de clé**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Sélection agent de récupération de clé**, cliquez sur le certificat qui est à des fins KRA (il sera très probablement le dernier sur la liste), puis cliquez sur **OK** deux fois.
5. Lorsque vous êtes invité à redémarrer l'autorité de confiance, cliquez sur **Oui**.

► **Tâche 4 : Configurer un modèle personnalisé pour l'archivage de clés**

1. Sur **LON-DC1**, dans la console **Autorité de certification**, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
2. Dans la console **Modèles de certificats**, cliquez avec le bouton droit sur le certificat **Utilisateur**, puis cliquez sur **Duplicer modèle**.
3. Dans la boîte de dialogue **Propriétés** du Nouveau Modèle, sous l'onglet **Général**, dans la zone de texte **Nom complet du modèle**, saisissez **Archiver utilisateur**.
4. Sous l'onglet **Traitement de la demande**, cochez la case **Archiver la clé privée de chiffrement du sujet**.
5. Dans la fenêtre indépendante qui apparaît, cliquez sur **OK**.
6. Cliquez sur l'onglet **Nom Sujet**, désactivez les cases à cocher **Nom E-mail** et **Inclure le nom E-mail au nom du sujet**, puis cliquez sur **OK**.
7. Fermer la console **Modèles de certificats**.
8. Dans la console **Autorité de certification**, cliquez avec le bouton droit sur **Modèles de certificats**, pointez vers **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
9. Dans la boîte de dialogue **Activer les modèles de certificats**, cliquez sur le modèle **Archiver utilisateur**, puis sur **OK**.
10. Fermez la console **Autorité de certification**.

► **Tâche 5 : Vérifier la fonctionnalité d'archivage de clé**

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Mary** avec le mot de passe **Pa\$\$w0rd**.
2. Sur l'écran d'accueil, saisissez **mmc.exe**, puis appuyez sur Entrée. Si vous y êtes invité, cliquez sur **Oui** dans la fenêtre **Contrôle de compte d'utilisateur**.
3. Dans **Console1 - [Racine de la console]**, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
4. Dans la fenêtre **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **Certificats**, sur **Ajouter** et sur **OK**.
5. Développez le nœud **Certificats - Utilisateur actuel**, cliquez avec le bouton droit sur **Personnel**, pointez vers **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.
6. Dans l'**Assistant Inscription de certificats**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner la stratégie d'inscription du certificat**, cliquez sur **Suivant**.
8. Sur la page **Demander des certificats**, cochez la case **Archiver utilisateur**, cliquez sur **Inscrire**, puis sur **Terminer**.
9. Actualisez la console, puis consultez qu'un certificat est délivré à **Mary** basé sur le modèle de certificat **Archive utilisateur**.
10. Simulez la perte d'une clé privée par la suppression du certificat. Dans le volet central, cliquez avec le bouton droit sur le certificat que vous venez d'inscrire, sélectionnez **Supprimer**, puis cliquez sur **Oui** pour confirmer.
11. Basculez vers **LON-DC1**.
12. Ouvrez la console **Autorité de certification**, développez **AdatumCA**, puis cliquez sur le magasin **Certificats délivrés**.
13. Dans le volet **Détails**, double-cliquez sur un certificat avec **Nom demandeur** de **Adatum\Mary** et un nom **Modèle de certificat** de **Archive utilisateur**.

14. Cliquez sur l'onglet **Détails**, copiez le **Numéro de série**, puis cliquez sur **OK**. Vous pouvez soit copier le numéro en le sélectionnant et en appuyant sur Ctrl+C ou en le notant dans un document.

15. Cliquez sur le bouton **Démarrer**, puis cliquez sur l'icône **Windows PowerShell**.

16. À l'invite de commandes de Windows PowerShell, entrez la commande suivante, où <numéro de série> est le numéro de série que vous avez copié, puis appuyez sur Entrée :

```
Certutil -getkey <numéro de série> outputblob
```



**Remarque :** Si vous copiez et collez le numéro de série, supprimez les espaces entre les numéros ou joignez le numéro de série entre guillemets.

17. Vérifiez que le fichier **Outputblob** s'affiche maintenant dans le dossier **C:\Utilisateurs\Administrateur**.

18. Pour convertir le fichier **Outputblob** en fichier .pfx, sur l'invite de commandes Windows PowerShell, entrez la commande suivante et appuyez sur Entrée :

```
Certutil -recoverkey outputblob Mary.pfx
```

19. Lorsque vous êtes invité à entrer le nouveau mot de passe, saisissez **Pa55w.rd**, puis confirmez le mot de passe.

20. Après exécution de la commande, fermez Windows PowerShell.

21. Aller sur **C:\Utilisateurs\Administrateur**, puis vérifiez que **aidan.pfx**-la clé récupérée est créée.

22. Basculez vers **LON-CL1**.

23. Ouvrez l'**Explorateur de fichiers** puis accédez à **\LON-DC1.adatum.com\c\$**. À l'invite, connectez-vous en tant que **Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.

24. Allez sur **\ LON-DC1.adatum.com\c\$\utilisateurs\administrateur**.

25. Cliquez avec le bouton droit sur le fichier **mary.pfx**, puis sélectionnez **Copier**. Allez sur **C:\Utilisateurs\mary**. Dans le volet de navigation, cliquez avec le bouton droit, puis sélectionnez **Coller**.

26. Double-cliquez sur le fichier **Mary.pfx**.

27. Sur la page **Bienvenue dans l'Assistant Importation de certificat**, cliquez sur **Suivant**.

28. Sur la page **Fichier à importer**, cliquez sur **Suivant**.

29. Sur la page **Mot de passe**, saisissez le mot de passe **Pa55w.rd**, puis cliquez sur **Suivant**.

30. Sur la page **Magasin de certificats**, cliquez sur **Suivant**, puis sur **Terminer**, puis cliquez sur **OK**.

31. Dans la fenêtre **Console1**, développez le noeud **Certificats – Utilisateur actuel**, développez **Personnel**, puis cliquez sur **Certificats**.

32. Actualisez la console, puis vérifiez que le certificat Aidan est rétabli.

**Résultats :** À la fin de cet exercice, les stagiaires auront implémenté la récupération de clé.

► **Tâche 6 : Préparer le module suivant**

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour **22742A-LON-CL1**, **22742A-LON-SVR1** et **22742A-LON-SVR2**.



# Module 10 : Implémentation et administration de AD FS

## Atelier pratique : Implémentation de AD FS

### Exercice 1 : Configuration des conditions préalables pour les services AD FS

► Tâche 1 : Configurer les redirecteurs DNS

1. Sur **LON-DC1**, dans la fenêtre **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.
2. Dans le **Gestionnaire DNS**, développez **LON-DC1**, puis cliquez sur **Redirecteurs conditionnels**.
3. Cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez sur **Nouveau redirecteur conditionnel**.
4. Dans la fenêtre **Nouveau redirecteur conditionnel**, dans la boîte **Domaine DNS**, saisissez **Treyresearch.net**.
5. Dans la zone **Adresses IP des serveurs maîtres**, saisissez **172.16.10.10**, puis appuyez sur Entrée.
6. Cochez la case **stocker ce redirecteur conditionnel dans Active Directory, et le répliquer comme suit** : sélectionnez **Tous les serveurs DNS de cette forêt**, puis cliquez sur **OK**.
7. Fermez le **Gestionnaire DNS**.
8. Sur **TREY-DC1**, dans la fenêtre **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.
9. Dans le **Gestionnaire DNS**, développez **TREY-DC1**, puis cliquez sur **Redirecteurs conditionnels**.
10. Cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez sur **Nouveau redirecteur conditionnel**.
11. Dans la fenêtre **Nouveau redirecteur conditionnel**, dans la boîte **Domaine DNS**, saisissez **Adatum.com**.
12. Dans la zone **Adresses IP des serveurs maîtres**, saisissez **172.16.0.10**, puis appuyez sur Entrée.
13. Cochez la case **stocker ce redirecteur conditionnel dans Active Directory, et le répliquer comme suit** : sélectionnez **Tous les serveurs DNS de cette forêt**, puis cliquez sur **OK**.
14. Fermez le Gestionnaire DNS.



**Remarque :** Dans un environnement de production, il est probable que vous utilisez le DNS (Domain Name System) Internet au lieu des redirecteurs conditionnels.

► Tâche 2 : Configurer les approbations de certificats

1. Sur **LON-DC1**, ouvrez l'**Explorateur de fichiers**, allez sur **\TREY-DC1\CertEnroll**, puis copiez **TREY-DC1.TreyResearch.net\_TreyResearchCA.crt** sur **C:\**.
2. Fermez l'Explorateur de fichiers.
3. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
4. Dans **Gestion de stratégie de groupe**, développez **Forêt : Adatum.com**, développez les **Domaines**, développez **Adatum.com**, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
5. Dans **Éditeur de gestion des stratégies de groupe**, sous **Configuration ordinateur**, développez successivement **Stratégies, Paramètres Windows, Paramètres de sécurité, Stratégies de clé publique**, puis cliquez sur **Autorité de certification racine de confiance**.

6. Cliquez avec le bouton droit sur **Autorités de certification racine de confiance**, puis cliquez sur **Importer**.
7. Dans l'**Assistant importation de certificat**, sur la page **Bienvenue sur l'assistant d'importation de certificat**, cliquez sur **Suivant**.
8. Sur la page **Fichier à importer**, saisissez **C:\TREY-DC1.TreyResearch.net\_TreyResearchCA.crt**, puis cliquez sur **Suivant**.
9. Sur la page **Magasin de certificats**, cliquez sur **Placez tous les certificats dans le magasin suivant**, sélectionnez **Autorité de certification racine de confiance**, puis cliquez sur **Suivant**.
10. Sur la page **Assistant de fin d'importation de certificat**, cliquez sur **Terminer**, puis cliquez sur **OK** pour fermer le message de fin.
11. Fermez l'**Éditeur de gestion des stratégies de groupe**.
12. Fermez **Gestion de stratégie de groupe**.
13. Sur **TREY-DC1**, ouvrez l'**Explorateur de fichiers** puis accédez à **\LON-DC1\CertEnroll**.
14. Cliquez avec le bouton droit sur **LON-DC1.Adatum.com\_AdatumCA.crt**, ensuite cliquez sur **Installer le certificat**.
15. Dans **Assistant d'importation de certification**, sur la page **Bienvenue dans l'assistant d'importation de certification**, cliquez sur **Ordinateur local**, puis cliquez sur **Suivant**.
16. Sur la page **Magasin de certificats**, cliquez sur **Placer tous les certificats dans le magasin suivant**, puis sur **Parcourir**.
17. Dans la fenêtre **Sélectionner magasin de certificats**, cliquez sur **Autorités de certification racine de confiance**, puis sur **OK**.
18. Sur la page **Magasin de certificats**, cliquez sur **Suivant**.
19. Sur la page **Assistant de fin d'importation de certificat**, cliquez sur **Terminer**, puis sur **OK** pour fermer le message de fin.
20. Fermez l'Explorateur de fichiers.
21. Sur **LON-SVR1**, cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
22. À l'invite de commandes Windows PowerShell, saisissez **gpupdate**, puis appuyez sur Entrée.
23. Fermez Windows PowerShell.



**Remarque :** Si vous obtenez des certificats d'une autorité de certification de confiance (CA), vous n'avez pas à configurer un certificat de confiance entre les organisations.

#### ► Tâche 3 : Demander et installer un certificat pour le serveur Web

1. Sur **LON-SVR1**, ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire des services d'information Internet (IIS)**.
2. Dans **Microsoft Internet Information Services (IIS)**, cliquez sur **LON-SVR1 (adatum\Administrateur)**, puis double-cliquez sur **Certificats de serveur**.
3. Dans le volet **Actions**, cliquez sur **Créer un certificat de domaine**.
4. Dans l'**Assistant Crée un certificat**, sur la page **Propriétés du nom unique**, complétez les informations suivantes, puis cliquez sur **Suivant** :
  - Nom commun : **lon-svr1.adatum.com**

- Organisation : **A. Datum Corporation**
  - Unité d'organisation : **Research**
  - Ville/localité : **Londres**
  - État/Province : **Angleterre**
  - Pays/Région : **GB**
5. Sur la page **Autorité de certification en ligne**, cliquez sur **Sélectionner**.
  6. Sur la page **Sélectionner autorité de certification**, cliquez sur **AdatumCA**, puis cliquez sur **OK**.
  7. Sur la page **Autorité de certification en ligne**, dans la boîte **Nom convivial**, entrez **Certificat AdatumTestApp**, puis cliquez sur **Terminer**.
  8. Dans **Gestionnaire des services Internet**, développez **LON-SVR1 (ADATUM\Administrateur)**, développez **Sites**, cliquez sur **Site Web par défaut**, puis dans le volet **Actions**, cliquez sur **Liaisons**.
  9. Dans la fenêtre **Liaisons de sites**, cliquez sur **Ajouter**.
  10. Dans la fenêtre **Ajouter la liaison de site**, dans la liste **Type**, sélectionnez **https**.
  11. Dans la liste **Certificat SSL**, sélectionnez **Certificat AdatumTestApp**, puis cliquez sur **OK**.
  12. Dans la fenêtre **Liaisons de sites**, cliquez sur **Fermer**.
  13. Fermez le Gestionnaire IIS.

**Résultats :** Une fois cet exercice terminé, vous aurez activé la résolution DNS et les approbations de certificat entre les domaines. En outre, vous aurez activé un certificat SSL pour le site Web et validé son accès.

## Exercice 2 : Installation et configuration AD FS

### ► Tâche 1 : Créer un enregistrement DNS pour AD FS

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.
2. Dans le **Gestionnaire DNS**, développez **LON-DC1**, développez **Zones de recherche directes**, puis cliquez sur **Adatum.com**.
3. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
4. Dans la fenêtre **Nouvel hôte**, dans la zone **Nom**, saisissez **adfs**.
5. Dans le champ **Adresse IP**, saisissez **172.16.0.10**, puis cliquez sur **Ajouter un hôte**.
6. Dans la fenêtre **DNS**, cliquez sur **OK**.
7. Cliquez sur **Terminer**, puis cliquez sur **Gestionnaire de serveur**.

### ► Tâche 2 : Installer AD FS

1. Sur **LON-DC1**, cliquez sur **Démarrer**, cliquez avec le bouton droit sur **Windows PowerShell**, puis sur **Exécuter en tant qu'administrateur**.
2. À l'invite de commandes, entrez la commande suivante et appuyez sur Entrée :

```
Add-KdsRootKey -EffectiveTime((get-date).addhours(-10))
```

Cette commande crée la clé racine du Service de distribution de clés de groupe Microsoft pour générer le mot de passe du compte de service géré de groupe pour le compte qui sera utilisé plus tard dans cet atelier pratique. Vous devriez recevoir un identifiant global unique (GUID) en réponse à cette commande.

3. Cliquez sur **Démarrer**, cliquez sur **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**.
4. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Sélectionner un serveur du pool de serveurs**, puis cliquez sur **LON-DC1.Adatum.com** et sur **Suivant**.
7. Sur la page **Sélectionner des rôles de serveurs**, cochez la case **Services de fédération Active Directory (ADFS)**, puis cliquez sur **Suivant**.
8. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Sur la page **Services de fédération Active Directory (AD FS)**, cliquez sur **Suivant**.
10. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. Une fois l'installation terminée, cliquez sur **Fermer**.

#### ► Tâche 3 : Configurer AD FS

1. Sur **LON-DC1**, dans **Gestionnaire de serveur**, cliquez sur l'icône **Notifications**, puis cliquez sur **Configurez le service FS (Federation Service) sur ce serveur**.
2. Sur l'**Assistant Configuration des services de fédération Active Directory (AD FS)**, sur la page **Bienvenue**, cliquez sur **Créer le premier serveur de fédération dans une batterie de serveurs de fédération**, puis cliquez sur **Suivant**.
3. Sur la page **Se connecter aux services de domaine Active Directory**, cliquez sur **Suivant**, utilisez **Adatum\Administrateur** pour effectuer la configuration.
4. Sur la page **Spécifier les Propriétés du service**, dans la liste **Certificat SSL**, sélectionnez **adfs.adatum.com**.
5. Dans le champ **Nom complet du service de fédération**, saisissez **A. Datum Corporation**, puis cliquez sur **Suivant**.
6. Sur la page **Spécifier un compte de service**, cliquez sur **Créer un compte de service géré de groupe**.
7. Dans la zone **Nom du compte**, saisissez **ServiceADFS**, puis cliquez sur **Suivant**.
8. Sur la page **Spécifier une base de données de configuration**, cliquez sur **Créez une base de données sur ce serveur à l'aide de la base de données interne Windows**, puis cliquez sur **Suivant**.
9. Sur la page **Examiner les options**, cliquez sur **Suivant**.
10. Sur la page **Vérifications des conditions préalables**, cliquez sur **Configurer**.
11. Sur la page **Résultats**, cliquez sur **Fermer**.



**Remarque :** Le certificat adfs.adatum.com a été préconfiguré pour cette tâche. Dans votre propre environnement, vous devez obtenir ce certificat.

- Tâche 4 : Vérifier la fonctionnalité AD FS
- Sur **LON-CL1**, cliquez sur **Démarrer, Toutes les applications, Accessoires Windows et Internet Explorer**.
  - Dans Internet Explorer, dans la barre d'adresse, entrez **<https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml>**, puis appuyez sur Entrée.
  - Vérifiez que le fichier charge, puis fermez Internet Explorer.

**Résultats :** Une fois cet exercice terminé, vous aurez installé et configuré AD FS. Vous devez également avoir vérifié le bon fonctionnement en affichant le contenu du fichier **FederationMetadata.xml**.

### Exercice 3 : Configuration d'une application interne pour AD FS

► Tâche 1 : Configurer l'approbation de fournisseur de revendications Active Directory

- Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion AD FS**.
- Dans la console **Gestion AD FS**, cliquez sur **Approbations de fournisseur de revendications**.
- Dans la liste **Approbations de fournisseur de revendications**, cliquez avec le bouton droit sur **Active Directory**, puis cliquez sur **Modifier les règles de revendication**.
- Dans la fenêtre **Modifier les règles de revendication pour Active Directory**, sous l'onglet Règles de transformation d'acceptation, cliquez sur **Ajouter une règle**.
- Dans l'**Ajout de règle de revendication de transformation**, sur la page **Sélectionner un modèle de règle**, dans la liste **Modèle de règle de revendication**, sélectionnez **Envoyer les attributs LDAP en tant que revendications**, puis cliquez sur **Suivant**.
- Sur la page **Configurer la règle**, dans le champ **Nom de la règle de revendication**, saisissez **Règle d'attributs LDAP sortants**.
- Dans la liste **Magasin d'attributs**, sélectionnez **Active Directory**.
- Dans la section **Mappage des attributs LDAP aux types de revendications sortantes**, sélectionnez les valeurs suivantes pour l'**Attribut LDAP** et le **Type de revendication sortante**, puis cliquez sur **Terminer** :
  - Adresses électroniques : **Adresse électronique**
  - Nom d'utilisateur principal : **UPN**
  - Nom complet : **Nom**
- Dans la fenêtre **Modifier les règles de revendication pour Active Directory**, cliquez sur **OK**.

► Tâche 2 : Configurer l'application pour qu'elle se fie aux revendications entrantes

- Sur **LON-SVR1**, ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilitaire Windows Identity Foundation Federation**.
- Sur la page **Bienvenue dans l'Assistant Utilitaire Fédération**, dans la zone **Lieu de configuration de l'application**, entrez **C:\inetpub\wwwroot\AdatumTestApp\web.config** pour l'emplacement du fichier échantillon **web.config**.
- Dans le champ **URI d'application**, saisissez **<https://lon-svr1.adatum.com/AdatumTestApp/>** pour indiquer le chemin d'accès à l'application de l'échantillon qui se fie aux revendications entrantes à partir du serveur de fédération, puis cliquez sur **Suivant**.

4. Sur la page **Service de jeton de sécurité**, cliquez sur **Utilisez un STS existants** puis dans la boîte **STS WS-Emplacement document métadonnées Fédération**, entrez <https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml>. Cliquez sur **Suivant**.
5. Sur la page **Erreur de validation de la chaîne de certificat de signature STS**, cliquez sur **Désactiver la validation de la chaîne de certificat**, puis cliquez sur **Suivant**.
6. Sur la page **Chiffrement de jetons de sécurité**, cliquez sur **Aucun chiffrement**, puis sur **Suivant**.
7. Sur la page **Revendications proposées**, examinez les revendications proposées par le serveur de fédération, puis cliquez sur **Suivant**.
8. Sur la page **Résumé**, passez en revue les modifications qui seront apportées à l'application de l'échantillon par l'**Assistant de l'utilitaire de fédération**, faites défiler les éléments pour comprendre ce que chaque élément est en train de faire, puis cliquez sur **Terminer**.
9. Dans la fenêtre **Réussite**, cliquez sur **OK**.

► **Tâche 3 : Configurer une approbation de partie de confiance pour l'application en charge des revendications**

1. Dans **LON-DC1**, dans la console **AD FS**, cliquez sur **Approbations de partie de confiance**.
2. Dans le volet **Actions**, cliquez sur **Ajouter une approbation de partie de confiance**.
3. Dans l'**Assistant Ajouter une approbation de partie de confiance**, sur la page **Bienvenue**, cliquez sur **Démarrer**.
4. Sur la page **Sélectionner une source de données**, cliquez sur **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confiance**.
5. Dans la zone **Adresse des métadonnées de fédération (nom d'hôte ou URL)**, entrez <https://lon-srv1.adatum.com/adatumtestapp/>, puis cliquez sur **Suivant**. Cela télécharge les métadonnées configurées dans la tâche précédente.
6. Sur la page **Entrer le nom complet**, dans la zone de texte **Afficher le nom**, saisissez **A. Datum Corporation Test App**, puis cliquez sur **Suivant**.
7. Sur la page **Sélectionner une stratégie de contrôle d'accès**, cliquez sur **Autoriser tout le monde**, puis sur **Suivant**.
8. Sur la page **Prêt à ajouter l'approbation**, vérifiez les paramètres qui dépendent de la partie de confiance, puis cliquez sur **Suivant**.
9. Sur la page **Terminer**, cliquez sur **Fermer**.

► **Tâche 4 : Configurer des règles de revendication pour l'approbation de partie de confiance**

1. Sur **LON-DC1**, dans la console **AD FS Management**, dans la liste des **Approbations de partie de confiance**, cliquez sur **A. Datum Corporation Test App**, puis sélectionnez **Modifier la stratégie d'émission d'approbation**.
2. Dans la fenêtre **Modifier la stratégie d'émission de revendication pour A. Datum Corporation Test App**, dans l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
3. Dans la zone de texte **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
4. Dans la zone de texte **Nom de la règle de revendication**, saisissez **Passer le nom de compte Windows**.

5. Dans la liste **Type de revendication entrante**, cliquez sur **nom de compte Windows**, puis cliquez sur **Terminer**.
6. Dans l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
7. Dans la zone de texte **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
8. Dans la zone de texte **Nom de la règle de revendication**, saisissez **Passer l'adresse e-mail**.
9. Dans la liste **Type de revendication entrante**, cliquez sur **Adresse e-mail**, puis sur **Terminer**.
10. Dans l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
11. Dans la zone de texte **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
12. Dans la zone de texte **Nom de la règle de revendication**, saisissez **Passer l'UPN**.
13. Dans la liste **Type de revendication entrante**, cliquez sur **UPN**, puis sur **Terminer**.
14. Dans l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
15. Dans la boîte de dialogue **modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
16. Dans la zone de texte **Nom de la règle de revendication**, saisissez **Passer le nom**.
17. Dans la liste **Type de revendication entrante**, cliquez sur **Nom**, puis sur **Terminer**.
18. Dans l'onglet **Règles de transformation d'émission**, cliquez sur **OK**.

► **Tâche 5 : Tester l'accès de l'application en charge des revendications**

1. Sur **LON-CL1**, ouvrez **Internet Explorer**.
2. Dans Internet Explorer, dans la barre d'adresse, entrez **<https://lon-svr1.adatum.com/AdatumTestApp/>**, puis appuyez sur Entrée.



**Remarque :** Il est essentiel d'utiliser la barre oblique de fin (/) dans l'URL pour l'étape 2.

3. Dans la fenêtre **Sécurité Windows**, connectez-vous en tant qu'**Adatum\Adam** avec le mot de passe **Pa55w.rd**.
4. Vérifiez les informations de réclamation affichées par l'application.
5. Fermez Internet Explorer.

► **Tâche 6 : Configurer Internet Explorer pour passer automatiquement des informations d'identification locales à l'application**

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, saisissez **Options Internet**, puis cliquez sur **Options Internet**.
2. Dans la fenêtre **Propriétés Internet**, sous l'onglet **Sécurité**, cliquez sur **intranet local**, puis sur **Sites**.
3. Dans la fenêtre **Intranet local**, cliquez sur **Avancé**.
4. Dans la fenêtre **intranet local**, dans la boîte **Ajouter ce site à la zone**, saisissez **<https://adfs.adatum.com>**, puis cliquez sur **Ajouter**.
5. Dans la boîte **Ajouter ce site à la zone**, saisissez **<https://lon-svr1.adatum.com>**, cliquez **Ajouter**, puis cliquez sur **Fermer**.

6. Dans la fenêtre **Intranet local**, cliquez sur **OK**.
7. Dans la fenêtre **Propriétés Internet**, cliquez sur **OK**.
8. Sur **LON-CL1**, ouvrez **Internet Explorer**.
9. Dans Internet Explorer, dans la barre d'adresse, entrez **https://lon-svr1.adatum.com/AdatumTestApp/**, puis appuyez sur Entrée.



**Remarque :** Il est essentiel d'utiliser la barre oblique de fin (/) dans l'URL pour l'étape 9.

10. Notez que vous n'êtes pas invité à entrer des informations d'identification.
11. Vérifiez les informations de réclamation affichées par l'application.
12. Fermez Internet Explorer.

**Résultats :** Une fois cet exercice terminé, vous aurez configuré AD FS pour prendre en charge l'authentification pour une application.

## Exercice 4 : Configuration AD FS pour partenaires commerciaux fédérés

### ► Tâche 1 : Créer un enregistrement DNS pour AD FS à Trey Research

1. Sur **TREY-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.
2. Dans le **Gestionnaire DNS**, développez **TREY-DC1** et **Zones de recherche directes**, puis cliquez sur **TreyResearch.net**.
3. Cliquez avec le bouton droit sur **TreyResearch.net**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
4. Dans la fenêtre **Nouvel hôte**, dans la zone **Nom**, saisissez **adfs**.
5. Dans le champ **Adresse IP**, saisissez **172.16.10.10**, puis cliquez sur **Ajouter un hôte**.
6. Dans la fenêtre **DNS**, cliquez sur **OK**.
7. Cliquez sur **Terminer**, puis fermez le Gestionnaire DNS.

### ► Tâche 2 : Créer un certificat à Trey Research

1. Sur **TREY-DC1**, ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire des services d'information Internet (IIS)**.
2. Dans le Gestionnaire IIS, cliquez sur **TREY-DC1 (TREYRESEARCH\Administrateur)**, puis double-cliquez sur **Certificats de serveur**.
3. Dans le volet **Actions**, cliquez sur **Créer un certificat de domaine**.
4. Dans la fenêtre **Créer un certificat**, sur la page **Propriétés nom différencié**, complétez les informations suivantes, puis cliquez sur **Suivant** :
  - Nom commun : **adfs.TreyResearch.net**
  - Organisation : **recherche**
  - Unité d'organisation : **Recherche**
  - Ville/localité : **Londres**

- État/Province : **Angleterre**
  - Pays/Région : **GB**
5. Sur la page **Autorité de certification en ligne**, cliquez sur **Sélectionner**.
  6. Dans la fenêtre **Sélectionner autorité de certification**, cliquez sur **TreyResearchCA**, puis cliquez sur **OK**.
  7. Sur la page **Autorité de certification en ligne**, dans la boîte **Nom amical**, entrez **adfs.TreyResearch.net**, puis cliquez sur **Terminer**.
  8. Fermez le Gestionnaire IIS.
- **Tâche 3 : Installer AD FS pour Trey Research**
1. Sur **TREY-DC1**, cliquez sur **Démarrer**, cliquez avec le bouton droit sur **Windows PowerShell**, puis sur **Exécuter en tant qu' administrateur**.
  2. À l'invite de commandes, entrez la commande suivante et appuyez sur Entrée :
- ```
Add-KdsRootKey -EffectiveTime ((get-date) .addhours (-10))
```
- Cette commande crée la clé racine du Service de distribution de clés de groupe pour générer les mots de passe gMSA pour le compte qui sera utilisé plus tard dans cet atelier pratique. Vous devriez recevoir un identificateur global unique (GUID) en réponse à cette commande.
3. Cliquez sur **Démarrer**, cliquez sur **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**.
 4. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
 5. Sur la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
 6. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Sélectionner un serveur du pool de serveurs**, puis cliquez sur **TREY-DC1.TreyResearch.net** et sur **Suivant**.
 7. Sur la page **Sélectionner des rôles de serveurs**, cochez la case **Services de domaine Active Directory**, puis cliquez sur **Suivant**.
 8. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
 9. Sur la page **Services de fédération Active Directory (AD FS)**, cliquez sur **Suivant**.
 10. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
 11. Une fois l'installation terminée, cliquez sur **Fermer**.

► Tâche 4 : Configurer AD FS pour Trey Research

1. Sur **TREY-DC1**, dans **Gestionnaire de serveur**, cliquez sur l'icône **Notifications**, puis cliquez sur **Configurez le service FS (Federation Service) sur ce serveur**.
2. Sur l'**Assistant Configuration des services de fédération Active Directory (AD FS)**, sur la page **Bienvenue**, cliquez sur **Créer le premier serveur de fédération dans une batterie de serveurs de fédération**, puis cliquez sur **Suivant**.
3. Sur la page **Se connecter aux services de domaine Active Directory**, cliquez sur **Suivant**, utilisez **TreyResearch\Administrateur** pour effectuer la configuration.
4. Sur la page **Spécifier les Propriétés du service**, dans la liste **Certificat SSL**, sélectionnez **adfs.treystudy.net**.
5. Dans le champ **Nom complet du service de fédération**, saisissez **Trey Research**, puis cliquez sur **Suivant**.
6. Sur la page **Spécifier un compte de service**, cliquez sur **Créer un compte de service géré de groupe**.
7. Dans la zone **Nom du compte**, saisissez **ServiceADFS**, puis cliquez sur **Suivant**.
8. Sur la page **Spécifier une base de données de configuration**, cliquez sur **Créez une base de données sur ce serveur à l'aide de la base de données interne Windows**, puis cliquez sur **Suivant**.
9. Sur la page **Examiner les options**, cliquez sur **Suivant**.
10. Sur la page **Vérifications des conditions préalables**, cliquez sur **Configurer**.
11. Sur la page **Résultats**, cliquez sur **Fermer**.

► Tâche 5 : Configurer une approbation de fournisseur de revendications pour le serveur Trey Research AD FS

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion AD FS**.
2. Dans la console de **Gestion AD FS**, cliquez sur **Approbations de partie de confiance**.
3. Dans le volet **Actions**, cliquez sur **Ajouter des approbations de partie de confiance**.
4. Dans l'**Assistant Ajout d'approbation de partie de confiance**, sur la page **Bienvenue**, cliquez sur **Démarrer**.
5. Sur la page **Sélectionner une source de données**, cliquez sur **Importer les données publiées en ligne ou sur un réseau local concernant le fournisseur de revendications**.
6. Dans la zone **Adresse des métadonnées de fédération (nom d'hôte ou URL)**, saisissez **https://adfs.treystudy.net**, puis cliquez sur **Suivant**.
7. Sur la page **Entrer le nom complet**, dans la zone de texte **Afficher le nom**, saisissez **Trey Research**, puis cliquez sur **Suivant**.
8. Sur la page **Prêt à ajouter l'approbation**, vérifiez les paramètres qui dépendent de la partie de confiance, puis cliquez sur **Suivant** pour enregistrer la configuration.
9. Sur la page **Terminer**, cliquez sur **Fermer**.
10. Dans la liste des **Approbations de parties de confiance de fournisseur**, cliquez avec le bouton droit sur **Trey Research**, puis cliquez sur **Modifier les règles de demande**.
11. Dans la fenêtre **Modifier les règles de confiance pour Active Directory**, sous l'onglet **Règles de transformation d'acceptation**, cliquez sur **Ajouter une règle**.

12. Dans l'**Ajout de règle de revendication de transformation**, sur la page **Sélectionner un modèle de règle**, dans la liste **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
 13. Sur la page **Configurer la règle**, dans la zone de texte **Nom de la règle de revendication**, saisissez **Passer le nom de compte Windows**.
 14. Dans la liste **Type de revendication entrante**, sélectionnez **Nom de compte Windows**.
 15. Sélectionnez **Passer toutes les valeurs de revendication**, puis cliquez sur **Terminer**.
 16. Dans la boîte de dialogue **Gestion AD FS**, cliquez sur **Oui** pour approuver l'avertissement.
 17. Dans la fenêtre **Modifier les règles de revendication pour Trey Research**, cliquez sur **OK**, puis fermez la console de **Gestion AD FS**.
- **Tâche 6 : Configurer une approbation de partie de confiance pour l'application A. Datum Corporation.**
1. Sur **TREY-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion AD FS**.
 2. Dans la console de **Gestion AD FS**, cliquez sur **Approbations de partie de confiance**.
 3. Dans le volet **Actions**, cliquez sur **Ajouter une approbation de partie de confiance**.
 4. Dans l'**Assistant Ajouter une approbation de partie de confiance**, sur la page **Bienvenue**, cliquez sur **Démarrer**.
 5. Sur la page **Sélectionner une source de données**, cliquez sur **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confiance**.
 6. Dans la zone **Adresse des métadonnées de fédération (nom d'hôte ou URL)**, saisissez **adfs.adatum.com**, puis cliquez sur **Suivant**.
 7. Sur la page **Entrer le nom complet**, dans la zone de texte **Afficher le nom**, saisissez **A. Datum Corporation**, puis cliquez sur **Suivant**.
 8. Sur la page **Sélectionner une stratégie de contrôle d'accès**, cliquez sur **Autoriser tout le monde**, puis sur **Suivant**.
 9. Sur la page **Prêt à ajouter l'approbation**, vérifiez les paramètres qui dépendent de la partie de confiance, puis cliquez sur **Suivant** pour enregistrer la configuration.
 10. Sur la page **Terminer**, cochez la case **Configurer la stratégie d'émission des approbations pour cette application**, puis cliquez sur **Fermer**.
 11. Dans la fenêtre **Modifier la stratégie d'émission de revendication pour A. Datum Corporation**, dans l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
 12. Dans l'**Assistant Ajout de règle de revendication de transformation**, sur la page **Sélectionner un modèle de règle**, dans la zone **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une approbation entrante**, puis cliquez sur **Suivant**.
 13. Sur la page **Configurer la règle**, dans la zone de texte **Nom de la règle de revendication**, saisissez **Passer le nom de compte Windows**.
 14. Dans la liste **Type de revendication entrante**, sélectionnez **Nom de compte Windows**.
 15. Cliquez sur **Passer toutes les valeurs de revendication**, puis sur **Terminer** et sur **OK**.
 16. Dans la fenêtre **Modifier la stratégie d'émission de revendication pour A. Datum Corporation**, cliquez sur **OK**.
 17. Fermez la console de **Gestion AD FS**.

► Tâche 7 : Vérifier l'accès au site Web

1. Sur **TREY-DC1**, dans Internet Explorer, ouvrez **Options Internet**, sélectionnez **Confidentialité**, puis sélectionnez **Sites**.
2. Sur la page **Actions de confidentialité par site**, dans la zone de texte **Adresse du site Web**, saisissez **adatum.com**, cliquez sur **Autoriser**, cliquez sur **OK** pour fermer la page **Actions de confidentialité par site**, puis cliquez sur **OK** pour fermer la fenêtre **Options Internet**.
3. Dans Internet Explorer, dans la barre d'adresse, entrez **https://lon-svr1.adatum.com/adatumtestapp/**, puis appuyez sur Entrée.
4. Sur la page **A. Datum Corporation**, cliquez sur **Trey Research**.
5. Dans la boîte de dialogue **Sécurité de Windows**, connectez-vous en tant que **TreyResearch\Cindy** avec le mot de passe **Pa55w.rd**.
6. Après le chargement de l'application, fermez Internet Explorer.
7. Ouvrez **Internet Explorer**.
8. Dans Internet Explorer, dans la barre d'adresse, entrez **https://lon-svr1.adatum.com/adatumtestapp/**, puis appuyez sur Entrée.
9. Dans la boîte de dialogue **Sécurité de Windows**, connectez-vous en tant que **TreyResearch\Cindy** avec le mot de passe **Pa55w.rd**.
10. Fermez Internet Explorer.



Remarque : Vous n'êtes pas invité à un domaine d'accueil lors du deuxième accès.

Après qu'un utilisateur sélectionne un domaine d'accueil et qu'une autorité de domaine authentifie l'utilisateur, le serveur de fédération de la partie de confiance émet un cookie **_LSRealm**. La durée de vie par défaut de ce cookie est de 30 jours. Par conséquent, pour vous connecter à plusieurs reprises, vous devez supprimer ce cookie après chaque tentative de connexion pour revenir à un état de bon fonctionnement.

► Tâche 8 : Configurer les règles de revendication d'autorisation d'émission pour autoriser l'accès uniquement à des groupes spécifiques

1. Sur **TREY-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion AD FS**.
2. Dans la console de **Gestion AD FS**, cliquez sur **Approbations de partie de confiance**.
3. Cliquez avec le bouton droit sur **A. Datum Corporation**, puis cliquez sur **Modifier stratégie d'émission de confiance**.
4. Dans la fenêtre **Modifier la stratégie d'émission de revendication pour A. Datum Corporation**, sous l'onglet **Règles de transformation d'émission**, cliquez sur **Supprimer une règle** puis sur **Oui**.
5. Cliquez sur **Ajouter une règle**.
6. Dans la zone de texte **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
7. Dans la zone de texte **Nom de la règle de revendication**, saisissez **Autoriser membres de production**.
8. Sur le **Type d'approbation entrante**, sélectionnez **Groupe**.
9. Cliquez sur **Passer uniquement une valeur de revendication spécifique**, puis dans la valeur de revendication entrante, saisissez **Treyresearch-Production**.

10. Cliquez sur **Terminer**, puis sur **OK**.
 11. Dans la console de **Gestion AD FS**, cliquez sur **Approbations de fournisseur de revendications**, cliquez avec le bouton droit sur **Active Directory**, puis cliquez sur **Modifier les règles de revendication**.
 12. Dans la fenêtre **Modifier les règles de revendication pour Active Directory**, cliquez sur **Ajouter une règle**.
 13. Dans l'**Assistant Ajout de règle de revendication de transformation**, sur la page **Sélectionner un modèle de règle**, dans la boîte **Modèle de règle de revendication**, sélectionnez **Envoyer l'appartenance à un groupe en tant que revendication**, puis cliquez sur **Suivant**.
 14. Sur la page **Configurer la règle**, dans le champ **Nom de la règle de revendication**, saisissez **Revendication de groupe de production**.
 15. Pour définir le **Groupe de l'utilisateur**, cliquez sur **Parcourir**, entrez **Production**, puis cliquez sur **OK**.
 16. Dans la zone **Type de revendication entrante**, sélectionnez **Groupe**.
 17. Dans la zone **Valeur de revendication sortante**, entrez **TreyResearch-Production**, puis cliquez sur **Terminer**.
 18. Dans la fenêtre **Modifier les règles de revendication pour Active Directory**, cliquez sur **OK**.
 19. Fermez la console de **Gestion AD FS**.
- **Tâche 9 : Vérifier l'accès au site Web avec les restrictions de groupe**
1. Sur **TREY-DC1**, dans Internet Explorer, ouvrez **Options Internet**, sélectionnez **Confidentialité**, puis sélectionnez **Sites**.
 2. Sur la page **Actions de confidentialité par site**, dans la zone de texte **Adresse du site Web**, saisissez **adatum.com**, cliquez sur **Autoriser**, cliquez sur **OK** pour fermer la page **Actions de confidentialité par site**, puis cliquez sur **OK** pour fermer la fenêtre **Options Internet**.
 3. Dans l'Explorateur de fichiers, dans la barre d'adresse, cliquez sur **<https://lon-svr1.adatum.com/adatumtestapp/>**.
 4. Dans la boîte de dialogue **Sécurité de Windows**, connectez-vous en tant que **TreyResearch\Ben** avec le mot de passe **Pa55w.rd**.
 5. Vérifiez que vous pouvez accéder à l'application parce que Ben est un membre du groupe **TreyResearch\Production**.
 6. Fermez Internet Explorer.

Résultats : Une fois cet exercice terminé, vous aurez configuré un accès à une application prenant en charge les réclamations dans une organisation partenaire.

► **Tâche 10 : Préparer le module suivant**

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.

4. Répétez les étapes 2 et 3 pour **22742A-LON-DC2**, **22742A-LON-SVR1**, **22742A-TREY-DC1** et **22742A-LON-CL1**.

Module 11 : Mise en œuvre et administration AD RMS

Atelier pratique : Implémentation d'une infrastructure AD RMS

Exercice 1 : Installation et configuration d'AD RMS

► Tâche 1 : Configurer le compte de service AD RMS et DNS

1. Connectez-vous à **LON-DC1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
3. Sélectionnez et cliquez avec le bouton droit sur **Adatum (local)**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
4. Dans la boîte de dialogue **Créer Unité organisationnelle**, dans la zone de texte **Nom**, entrez **Comptes service**, puis cliquez sur **OK**.
5. Cliquez avec le bouton droit sur l'Unité organisationnelle (UO) **Comptes service**, cliquez sur **Nouveau**, puis sur **Utilisateur**.
6. Dans la boîte de dialogue **Créer un utilisateur**, fournissez les détails suivants, puis cliquez sur **OK** :
 - Prénom : **ADRMSSVC**
 - Ouverture de la session UPN de l'utilisateur : **ADRMSSVC**
 - Ouverture du nom de compte d'utilisateur Gustave : **Adatum\ADRMSSVC**
 - Mot de passe : **Pa55w.rd**.
 - Confirmer le mot de passe : **Pa55w.rd**.
 - Le mot de passe n'expire jamais : **Activé** (Vous devez cliquer sur Autres options de mot de passe pour pouvoir sélectionner cette option)
 - L'utilisateur ne peut pas modifier le mot de passe : **Activé**
7. Cliquez avec le bouton droit sur le conteneur **Utilisateurs**, cliquez sur **Nouveau**, puis sur **Groupe**.
8. Dans la boîte de dialogue **Créer un groupe**, fournissez les détails suivants, puis cliquez sur **OK** :
 - Nom du groupe : **ADRMS_SuperUsers**
 - E-mail : **ADRMS_SuperUsers@adatum.com**
9. Cliquez avec le bouton droit sur le conteneur **Utilisateurs**, cliquez sur **Nouveau**, puis sur **Groupe**.
10. Dans la boîte de dialogue **Créer un groupe**, fournissez les détails suivants, puis cliquez sur **OK** :
 - Nom du groupe : **Cadres**
 - E-mail : **executives@adatum.com**
11. Double-cliquez sur l'UO **Managers**, puis Ctrl+clic sur les utilisateurs suivants:
 - **Aidan Norman**
 - **Holly Spencer**
12. Dans le volet **Tâches**, cliquez sur **Ajouter au groupe**.
13. Dans la boîte de dialogue **Sélectionner des groupes**, tapez **Cadres**, puis cliquez sur **OK**.

14. Fermez le **Centre d'administration Active Directory**.
15. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.
16. Dans la console du **Gestionnaire DNS**, développez **LON-DC1**, puis développez **Zones de recherche directes**.
17. Sélectionnez puis cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
18. Dans la boîte de dialogue **Nouvel hôte**, fournissez les informations suivantes, puis cliquez sur **Ajouter un hôte** :
 - Nom : **adrms**
 - Adresse IP : **172.16.0.21**
19. Cliquez sur **OK**, puis sur **Fin**.



Remarque : Ceci est l'adresse de **LON-SVR1**, où vous allez installer AD RMS.

20. Fermez la console **Gestionnaire DNS**.

► **Tâche 2 : Installer et configurer le rôle serveur AD RMS**

1. Connectez-vous à **LON-SVR1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, cliquez sur **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Suivant**.
4. Sur la page **Sélectionnez les rôles du serveur**, cliquez sur **Services ADRMS**.
5. Dans la boîte de dialogue **Assistant Ajouter des rôles et fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**, cliquez sur **Suivant** six fois, cliquez sur **Installer**, puis quand l'installation est terminée, cliquez sur **Fermer**.
6. Dans **Gestionnaire de serveur**, cliquez sur le nœud **Services AD RMS**.
7. À côté de **Configuration requise pour les services de gestion des droits Active Directory à LON-SVR1**, cliquez sur **Autres....**
8. Sur la page **Tous les détails des tâches et toutes les notifications des serveurs**, cliquez sur **Effectuer une configuration supplémentaire**.
9. Sur la page **AD RMS**, dans la boîte de dialogue **Configuration AD RMS** : fenêtre **LON-SVR1.adatum.com**, cliquez sur **Suivant**.
10. Sur la page **Cluster AD RMS**, cliquez sur **Créer un cluster racine AD RMS**, puis cliquez sur **Suivant**.
11. Sur la page **Base de données de configuration**, cliquez sur **Utiliser la base de données interne Windows sur ce serveur**, puis cliquez sur **Suivant**.
12. Sur la page **Compte de service**, cliquez sur **Spécifier**.
13. Dans la boîte de dialogue **Sécurité de Windows**, entrez les informations suivantes, cliquez sur **OK**, puis sur **Suivant** :
 - Nom d'utilisateur : **ADRMSSVC**
 - Mot de passe : **Pa55w.rd**.



Remarque : Si vous obtenez une erreur lorsque vous essayez d'utiliser le compte de service ADRMSSVC, forcez la réPLICATION entre **LON-DC1** et **LON-DC2**, puis essayez à nouveau d'effectuer cette étape.

14. Sur la page **Mode de chiffrement**, cliquez sur **Mode de chiffrement 2**, puis cliquez sur **Suivant**.
15. Sur la page **Cluster de la clé de stockage**, cliquez sur **Utiliser le stockage de clé géré de manière centralisée d'AD RMS**, puis cliquez sur **Suivant**.
16. Sur la page **Mot de passe de la clé de cluster**, tapez **Pa55w.rd** à deux reprises, puis cliquez sur **Suivant**.
17. Sur la page **Site Web de cluster**, vérifiez que **Site Web par défaut** est sélectionné, puis cliquez sur **Suivant**.
18. Sur la page **Adresse Cluster**, complétez les informations suivantes, puis cliquez sur **Suivant** :
 - Type de connexion : **Utilisez une connexion non chiffrée (http://)**
 - Nom de domaine complet : **adrms.adatum.com**
 - Port : **80**



Remarque : Cet atelier pratique utilise le port 80 pour plus de commodité. Dans les environnements de production, vous devrez aider à protéger les Services AD RMS (Active Directory Rights Management Services) en utilisant une connexion cryptée.

19. Sur la page **Certificat de licence**, saisissez **AdatumADRMS**, puis cliquez sur **Suivant**.
20. Sur la page **Enregistrement SCP**, cliquez sur **Enregistrer le SCP maintenant**, puis cliquez sur **Suivant**.
21. Sur la page de **Confirmation**, cliquez sur **Installer**, puis cliquez sur **Fermer**.
22. Dans le **Gestionnaire de serveur**, cliquez sur le menu **Outils**, puis cliquez sur le **Gestionnaire des services d'information Internet (IIS)**.
23. Dans la console **Internet Information Services (IIS)**, développez **LON-SVR1\Sites\Site Web par défaut**, puis cliquez sur **_wmcs**.
24. Sous le noeud **/_wmcs**, double-cliquez sur **Authentification**, cliquez sur **Authentification anonyme** puis dans le volet **Actions**, cliquez sur **Activer**.
25. Dans le volet **Connexions**, développez **_wmcs**, puis cliquez sur **Licensing**.
26. Sous le noeud **/_wmcs/licensing**, double-cliquez sur **Authentification**, cliquez sur **Authentification anonyme** puis dans le volet **Actions**, cliquez sur **Activer**.



Remarque : Vous n'activerez pas l'authentification anonyme dans un environnement de production. Ceci est juste pour rendre la configuration plus facile dans l'exercice.

27. Ouvrez l'écran d'accueil, cliquez sur **Administrateur**, puis cliquez sur **Se déconnecter**.



Remarque : Vous devez vous déconnecter avant de pouvoir gérer AD RMS.

► Tâche 3 : Configurer le groupe de super utilisateurs AD RMS.

1. Connectez-vous à **LON-SVR1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Ouvrir le **Gestionnaire de serveurs**, cliquez sur **Outils**, puis sur **Services AD RMS (Active Directory Rights Management Services)**.
3. Dans la console **AD RMS**, développez le nœud **LON-SVR1 (local)**, puis cliquez sur **Stratégies de sécurité**.
4. Dans la zone **Stratégies de sécurité**, sous **Super utilisateurs**, cliquez sur **Modifier les paramètres de super-utilisateur**.
5. Dans le volet **Actions**, cliquez sur **Activer les super utilisateurs**.
6. Dans la zone **Super utilisateurs**, cliquez sur **Modifier groupe de super-utilisateur**.
7. Dans la fenêtre de dialogue **Super utilisateurs**, dans la zone **Groupe super utilisateur**, tapez **ADRMS_SuperUsers@adatum.com**, puis cliquez sur **OK**.

Résultats : À la fin de cet exercice, vous devez avoir installé et configuré AD RMS.

Exercice 2 : Configuration des modèles AD RMS

► Tâche 1 : Configurer un nouveau modèle de stratégie de droits

1. Assurez-vous que vous êtes connecté à **LON-SVR1**.
2. Dans la console **AD RMS**, cliquez sur le nœud **Modèles de stratégie de droits**.
3. Dans le volet **Actions**, cliquez sur **Créer un modèle de stratégie de droits distribué**.
4. Dans l'assistant **Créer un modèle de stratégie de droits distribué**, sur la page **Ajouter des informations d'identification** du modèle, cliquez sur **Ajouter**.
5. Sur la page **Ajouter de nouvelles informations d'identification du modèle**, fournissez les informations suivantes, cliquez sur **Ajouter**, puis cliquez sur **Suivant** :
 - Langage : **Anglais (États-Unis)**
 - Nom : **LectureSeule**
 - Description : **Accès en lecture seule. Pas de copie ni d'impression.**
6. Sur la page **Ajouter des droits d'utilisateur**, cliquez sur **Ajouter**.
7. Sur la page **Ajouter un utilisateur ou un groupe**, saisissez **executives@adatum.com**, puis cliquez sur **OK**.
8. Quand **executives@adatum.com** est sélectionné, sous **Droits**, cliquez sur **Afficher**. Vérifiez que **Octroyer le contrôle total au propriétaire (auteur) sans date d'expiration** est sélectionné, puis cliquez sur **Suivant**.
9. Sur la page **Spécifier stratégie d'expiration**, sélectionnez les paramètres suivants, puis cliquez sur **Suivant** :
 - Expiration du contenu : **Expire après la durée suivante (en jours) : 7**
 - Expiration de la licence d'utilisation : **Expire après la durée suivante (en jours) : 7**

10. Sur la page **Spécifier la stratégie étendue**, cliquez sur **Demander une nouvelle licence d'utilisation à chaque accès au contenu (désactiver la mise en cache côté client)**, puis cliquez sur **Suivant**.

11. Sur la page **Spécifier la stratégie de révocation**, cliquez sur **Terminer**.

► **Tâche 2 : Configurer la distribution de modèle relative à la stratégie des droits**

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
2. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
New-Item c:\rmstemplates -ItemType Directory
```

3. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
New-SmbShare -Name RMSTEMPLATES -Path c:\rmstemplates -FullAccess ADATUM\ADRMSSVC
```

4. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
New-Item c:\docshare -ItemType Directory
```

5. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
New-SmbShare -Name docshare -Path c:\docshare -FullAccess "Tout le monde"
```

6. Entrez **Exit**, puis appuyez sur Entrée pour quitter Windows PowerShell.

7. Passez à la console **AD RMS**, cliquez sur le noeud **Modèles de stratégie de droits**, puis dans la zone **Modèles de stratégie de droits distribués**, cliquez sur **Modifier l'emplacement du fichier de modèles de stratégies de droits distribués**.

8. Dans la boîte de dialogue **Modèles de stratégie de droits**, cliquez sur **Activer exportation**.

9. Dans la boîte **Spécifier emplacement du fichier des modèles (UNC)**, entrez **\LON-SVR1\RMSTEMPLATES**, puis cliquez sur **OK**.

10. Dans la barre des tâches, cliquez sur **Explorateur de fichiers**.

11. Accédez au dossier **C:\rmstemplates**, puis vérifiez que **ReadOnly.xml** est présent.

12. Fermez les fenêtres de l'**Explorateur de fichiers**.

► **Tâche 3 : Configurer une stratégie d'exclusion**

1. Sur **LON-SVR1**, dans la console **AD RMS**, cliquez sur le noeud **Stratégies d'exclusion**, puis cliquez sur **Gérer la liste d'exclusions d'applications**.

2. Dans le volet **Actions**, cliquez sur **Activer l'exclusion d'applications**.

3. Dans le volet **Actions**, cliquez sur **Exclude l'application**.

4. Dans la boîte de dialogue **Exclude l'application**, saisissez les informations suivantes, puis cliquez sur **Terminer** :

- Nom de fichier d'application : **Powerpnt.exe**
- Version minimale : **14.0.0.0**
- Version maximale : **16.0.0.0**

5. Fermez la console **AD RMS**.

Résultats : À la fin de cet exercice, vous devez avoir configuré les modèles AD RMS.

Exercice 3 : Utilisation AD RMS sur les clients

► Tâche 1 : Créer un document protégé par des droits

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Aidan** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, tapez **Internet**, puis cliquez sur **Internet Explorer**. Dans la fenêtre **Internet Explorer**, cliquez avec le bouton droit sur la barre d'outils, cliquez sur la **barre de menus**, cliquez sur **Outils**, puis sélectionnez **Options Internet**.
3. Dans la boîte de dialogue **Options Internet**, cliquez sur **Sécurité**, cliquez sur **Intranet local**, cliquez sur **Sites**, cliquez sur **Avancé**, puis sous **Ajouter ce site à la zone**, saisissez **http://adrms.adatum.com**. Cliquez sur **Ajouter**, cliquez sur **Fermer**, puis cliquez sur **OK** deux fois.

 **Remarque :** Notez que vous avez ajouté adrms.adatum.com aux sites intranet locaux pour atteindre une authentification unique lors de la connexion aux serveurs AD RMS.

4. Fermez Internet Explorer.
5. Sur le menu **Démarrer**, entrez **Word**, puis dans la zone de résultats, cliquez sur **Word 2016**. Dans la boîte de dialogue **Premières choses d'abord**, sélectionnez l'option **Demander moi plus tard**, puis cliquez sur **Accepter**. Si la fenêtre **Bienvenue sur votre nouvel Office** apparaît, fermez-la.
6. Dans l'application Microsoft Word 2016, cliquez sur **Document vierge**.
7. Dans le document Word, tapez le texte suivant : **Ce document est seulement pour les cadres et il ne devrait pas être modifié**. Cliquez sur **Fichier**, cliquez sur **Protéger le document**, cliquez sur **Accès restreint**, puis cliquez sur **Lecture seule**.

 **Remarque :** Si le modèle **Lecture seule** n'apparaît pas, vous devrez peut-être d'abord cliquer sur **Se connecter aux serveurs de gestion des droits et obtenir des modèles**.

8. Sélectionnez **Enregistrer**, puis cliquez sur **Parcourir**.
9. Dans la boîte de dialogue **Enregistrer sous**, enregistrez le document sur **\LON-SVR1\DocShare** sous le nom **Cadres seulement.docx**.
10. Fermez Word 2016.
11. Cliquez sur le menu **Démarrer**, cliquez sur l'icône **Aidan Norman**, puis cliquez sur **Déconnecter**.

► Tâche 2 : Vérifier l'accès interne au contenu AD RMS protégé en tant qu'utilisateur autorisé

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Holly** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, tapez **Internet**, puis cliquez sur **Internet Explorer**. Dans la fenêtre **Internet Explorer**, cliquez avec le bouton droit sur la barre d'outils, cliquez sur **la barre de menus**, cliquez sur **Outils**, puis sélectionnez **Options Internet**.

3. Dans **Options Internet**, cliquez sur **Sécurité**, cliquez sur **Intranet local**, cliquez sur **Sites**, cliquez sur **Avancé**, puis sous **Ajouter ce site à la zone**, saisissez **http://adrms.adatum.com**. Cliquez sur **Ajouter**, cliquez sur **Fermer**, puis cliquez sur **OK** deux fois.
 4. Fermez Internet Explorer.
 5. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
 6. Dans la fenêtre de l'**Explorateur de fichiers**, accédez à **\\\lon-svr1\docshare**.
 7. Dans le dossier **DocShare**, double-cliquez sur le document **Cadres Seulement**.
 8. Lorsque le document s'ouvre, vérifiez qu'il n'est pas possible de modifier ou d'enregistrer le document. Dans la fenêtre **Premières choses d'abord** dans Word, sélectionnez l'option **Demandez moi plus tard**, puis cliquez sur **Accepter**. Si la fenêtre **Bienvenue sur votre nouvel Office** apparaît, fermez-la.
 9. Sélectionnez une ligne de texte dans le document, faites-y un clic droit, puis vérifiez que vous ne pouvez pas faire de modifications.
 10. Cliquez sur **Voir Autorisations**, examinez les autorisations, puis cliquez sur **OK**. Vous pouvez voir que Holly a seulement l'autorisation Voir. Elle est membre du groupe Cadres et peut accéder au contenu.
 11. Fermez Word 2016.
 12. Ouvrez l'écran d'accueil, cliquez sur l'icône **Holly Spencer**, puis cliquez sur **Se déconnecter**.
- **Tâche 3 : Ouvrir un document protégé par des droits comme un utilisateur non autorisé**
1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Harry** avec le mot de passe **Pa55w.rd**.
 2. Cliquez sur **Démarrer**, tapez **Internet**, puis cliquez sur **Internet Explorer**. Dans la fenêtre **Internet Explorer**, cliquez avec le bouton droit sur la barre d'outils, cliquez sur **la barre de menus**, cliquez sur **Outils**, puis sélectionnez **Options Internet**.
 3. Dans **Options Internet**, cliquez sur **Sécurité**, cliquez sur **Intranet local**, cliquez sur **Sites**, cliquez sur **Avancé**, puis sous **Ajouter ce site à la zone**, saisissez **http://adrms.adatum.com**. Cliquez sur **Ajouter**, cliquez sur **Fermer**, puis cliquez sur **OK** deux fois.
 4. Fermez Internet Explorer.
 5. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
 6. Dans la fenêtre de l'**Explorateur de fichiers**, accédez à **\\\lon-svr1\docshare**.
 7. Dans le dossier **DocShare** dossier, double-cliquez sur le document **Cadres Seulement**, puis cliquez sur **OK** dans la fenêtre **Microsoft Office**.
 8. Vérifiez qu'Harry ne peut pas ouvrir le document. Notez qu'Harry ne peut pas ouvrir le document parce que le document est protégé par un modèle RMS qui ne permet qu'au groupe Cadres d'afficher le document. Cliquez sur **OK** dans la fenêtre **Microsoft Word**.
 9. Fermez Word 2016.
 10. Ouvrez l'écran d'accueil, cliquez sur l'icône **Harry Lawrence**, puis cliquez sur **Se déconnecter**.

► **Tâche 4 : Préparer le module suivant**

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour ce faire, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.

2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-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 **22742A-LON-SVR1**, **22742A-LON-DC2** et **22742A-LON-CL1**.

Résultats : Après avoir terminé cet exercice, vous devriez avoir vérifié que le déploiement AD RMS est réussi.

Module 12 : Mise en œuvre de la synchronisation AD DS avec Microsoft Azure AD

Atelier pratique : Configuration de la synchronisation des annuaires

Exercice 1 : Préparation de la synchronisation des annuaires

► Tâche 1 : Créer un compte Microsoft

D'autres tâches dans cet exercice exigent que vous ayez un compte Microsoft actif auquel aucun abonnement Microsoft Azure n'est assigné. Si vous ne voulez pas utiliser votre compte Microsoft privé, si vous n'en avez pas, ou si vous avez déjà un abonnement à Azure, veuillez suivre les étapes de cette tâche pour créer un nouveau compte Microsoft.

1. Sur **LON-CL1**, cliquez sur **Démarrer** et sur **Toutes les applications**, étendez **Accessoires Windows**, puis cliquez sur **Internet Explorer**.
2. Dans la barre d'adresses, saisissez **www.live.com**, puis appuyez sur Entrée.
3. Au bas de la page, cherchez le texte « **Pas de compte ?** », puis cliquez sur le lien **Créer un compte !**.
4. Sur la page **Créer un compte**, remplissez les champs requis avec les données appropriées. Dans la zone de texte **Nom d'utilisateur**, tapez une nouvelle adresse de messagerie dans le domaine Outlook.com.



Remarque : Assurez-vous d'avoir écrit le nom d'utilisateur que vous avez choisi. Par exemple, vous pouvez choisir un nom d'utilisateur dans le format *Vosinitiales-date@outlook.com*, comme DJ-060815@outlook.com. Utilisez **Pa55w.rd1** comme mot de passe. Nous recommandons que vous saisissez votre adresse de messagerie professionnelle dans la zone de texte **Adresse de messagerie alternative**.

5. Après avoir rempli tous les champs, au bas de la page, cliquez sur **Créer un compte**.
6. Assurez-vous que votre boîte de réception Outlook.com s'ouvre dans une fenêtre de navigateur Web.
7. Si la page **Bienvenue dans votre nouvelle boîte de réception** apparaît, cliquez sur **Atteindre la boîte de réception**.
8. Si la fenêtre **Même adresse, boîte de réception intelligente** apparaît, cliquez sur l'icône **Fermer** pour afficher la boîte de réception.
9. Lorsque vous avez terminé, fermez Internet Explorer.

► Tâche 2 : Créer un abonnement d'évaluation Azure.

1. Sur **LON-CL1**, ouvrez **Internet Explorer**.
2. Dans la barre d'adresses au bas de la page, tapez **http://aka.ms/cu92vo**, puis appuyez sur Entrée.
3. Lorsque la page apparaît, sélectionnez votre pays/région dans la liste déroulante, tapez le n° de document que vous avez reçu de votre instructeur, puis cliquez sur **Soumettre**. Si votre pays/région ne figure pas sur la liste, sélectionnez **États-Unis**.
4. Sur la page suivante, cliquez sur **se connecter**.
5. Sur la page **Azure**, connectez-vous avec votre compte Microsoft que vous avez créé lors de la tâche précédente.



Remarque : Vous pouvez choisir d'utiliser votre compte Microsoft personnel ou celui créé plus tôt dans le cadre du laboratoire. La page **Se connecter** peut ne pas demander un mot de passe si vous avez encore un onglet ouvert dans la boîte de réception de votre compte.

6. Sur la page **Microsoft Azure**, vérifiez vos coordonnées, puis cliquez sur **Soumettre**.
7. Sur la page **Azure passe**, cliquez sur **Activer**. Un nouvel onglet s'ouvrira dans le navigateur Internet Explorer.
8. Sur la page **S'inscrire**, inscrivez votre numéro de téléphone, cliquez sur **Je suis d'accord avec le contrat d'abonnement, les détails de l'offre et la déclaration de confidentialité**, puis cliquez sur **S'inscrire**.
9. Attendez quelques minutes jusqu'à ce que votre abonnement Azure ait été créé.
10. Cliquez **Commencer à gérer mon service**, puis vérifiez qu'un nouveau portail classique Azure s'ouvre. Vous pouvez cliquer sur le portail pour voir les options offertes, mais n'apportez pas de modifications.
11. Fermez la fenêtre du navigateur.

► Tâche 3 : Créer un client Azure AD

1. Sur **LON-CL1**, ouvrez **Internet Explorer** et accédez à <https://manage.windowsazure.com>.
2. Si vous y êtes invité sur la page **Microsoft Azure**, tapez le compte Microsoft qui est associé à votre abonnement Azure (le même compte que vous avez utilisé pour créer votre abonnement d'essai Azure dans la tâche précédente), puis cliquez sur **Continuer**.
3. Sur la page **Se connecter**, connectez-vous avec le compte Microsoft qui est associé à votre abonnement Azure.
4. Si la page **VISITE DE WINDOWS AZURE** apparaît, fermez-la. Si la fenêtre **Le nouveau portail Azure est disponible!** apparaît, fermez-la.
5. Dans le volet de navigation de gauche, cliquez sur **ACTIVE DIRECTORY**, cliquez sur **NOUVEAU**, cliquez sur **ANNUAIRE**, puis cliquez sur **CRÉATION PERSONNALISÉE**.
6. Dans la boîte de dialogue **Ajout d'un annuaire**, configurez les paramètres suivants, puis cliquez sur **Terminé** (l'icône signe de vérification) :
 - ANNUAIRE : **Créer un nouvel annuaire**
 - NOM **Adatum**
 - NOM DE DOMAINE : Pour créer le nom de domaine, utilisez vos initiales, avec Adatum et des nombres aléatoires (par exemple, « DDA datum111 ») ; si vous recevez un message **Déjà utilisé par un autre annuaire**, changez les numéros jusqu'à ce que vous receviez un signe de vérification vert.



Remarque : À partir de ce moment dans le cadre du cours, vous devez utiliser ce nom lorsque vous voyez la variable *votrenomdedomaine* lors des laboratoires.

- PAYS OU RÉGION : **États-Unis**
7. Laissez le portail Azure Classic ouvert et attendez qu'une nouvelle instance de répertoire soit créée.

Résultats : À la fin de cet exercice, vous devez avoir créé le client Azure AD.

Exercice 2 : Configuration de la synchronisation des annuaires

► **Tâche 1 : Configurer le compte de synchronisation et ajouter un domaine à Azure**

1. Sur votre machine hôte, sur l'écran Démarrer, cliquez sur **Internet Explorer**.
2. Dans la barre d'adresses, tapez <https://manage.windowsazure.com>, puis appuyez sur Entrée.
3. Sur la page **Microsoft Azure**, cliquez sur **Utiliser un autre compte**.
4. Sur la page **Microsoft Azure**, saisissez votre compte Microsoft qui est associé à votre abonnement Azure, puis cliquez sur **Continuer**.
5. Connectez-vous à Azure en utilisant le compte Microsoft qui est associé à votre abonnement d'évaluation. Il s'agit du compte que vous aviez utilisé dans l'exercice 1 pour créer votre abonnement Azure.
6. Dans le portail classique Azure, cliquez sur l'instance d'annuaire **Adatum**.
7. Cliquez sur l'onglet **UTILISATEURS**, puis cliquez sur **AJOUTER UN UTILISATEUR**.
8. Dans la liste **TYPE D'UTILISATEUR**, cliquez sur **Nouvel utilisateur dans votre organisation**.
9. Dans la zone de texte **NOM D'UTILISATEUR**, saisissez **Sync**.



Remarque : Notez le nom complet de l'utilisateur. Il s'agit du **NOM D'UTILISATEUR** ainsi que le suffixe qui apparaît à droite du signe (@), tel que Sync@votredomaine.onmicrosoft.com.

10. Cliquez sur **Suivant**.
11. Sur la page **profil utilisateur**, dans la zone de texte de **NOM D'AFFICHAGE**, saisissez **SYNC**.
12. Dans la liste **RÔLE**, cliquez sur **Administrateur général**.
13. Dans la zone de texte **AUTRE ADRESSE DE MESSAGERIE**, saisissez votre propre adresse e-mail, puis cliquez sur **Suivant**.
14. Cliquez sur **Créer**.
15. Notez le mot de passe temporaire qui s'affiche.
16. Cliquez sur **Terminé**.
17. Fermez Internet Explorer, puis rouvrez-le.
18. Dans la barre d'adresses, tapez <https://manage.windowsazure.com>, puis appuyez sur Entrée.
19. Cliquez sur **Utiliser un autre compte**.
20. Saisissez le nom d'utilisateur pour l'utilisateur **SYNC** que vous avez enregistré précédemment. Il s'agira de **SYNC@votredomaine.onmicrosoft.com**. Cliquez sur **Continuer**.
21. Saisissez le mot de passe temporaire que vous avez noté lors de la création de votre compte de synchronisation, puis cliquez sur **Se connecter**.
22. Lorsque vous êtes invité, saisissez votre ancien mot de passe que vous avez saisi à l'étape 21, dans la zone de texte **Ancien mot de passe**, puis dans les zones de texte **Nouveau mot de passe** et **Confirmer le mot de passe**, saisissez **Pa55w.rd**, puis cliquez sur **Mettre à jour le mot de passe et se connecter**.
23. Si vous êtes invité à vous connecter de nouveau sur le portail, utilisez les informations d'identification du compte **SYNC** et le mot de passe **Pa55w.rd**. Vous recevrez un message stipulant qu'aucun abonnement n'est trouvé.
24. Fermez et rouvrez Internet Explorer.

25. Dans la barre d'adresses, tapez <https://manage.windowsazure.com>, puis appuyez sur Entrée.
26. Connectez-vous à Azure en utilisant le compte Microsoft qui est associé à votre abonnement d'évaluation. Le compte doit figurer dans la liste.
27. Dans le portail classique Azure, cliquez sur **Adatum**. La page **COMMENCER** est chargée.
28. Cliquez sur **Ajouter un domaine**.
29. Dans l'assistant **AJOUTER UN DOMAINE**, dans la zone de texte **NOM DE DOMAINE**, tapez **Adatum.com**, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
30. Sur la page **Vérifier Adatum.com**, cliquez sur **Terminé** (l'icône **signe de vérification**).
31. Réduisez la fenêtre **Internet Explorer**.

► **Tâche 2 : Installer et configurer Azure AD Connect**

1. Sur **LON-SVR1**, connectez-vous en tant que **Adatum\Administrateur**.
2. Ouvrez **Internet Explorer**, puis recherchez <http://www.microsoft.com/EN-US/download/details.aspx?id=47594>.
3. Sur la page **Microsoft Azure Active Directory Connect**, cliquez sur **Télécharger**, puis cliquez sur **Exécuter**.



Remarque : Si vous rencontrez des problèmes avec le démarrage du téléchargement, ajoutez le site Web <https://download.microsoft.com> à vos sites **de confiance**.

4. Dans l'assistant Microsoft Azure Active Directory Connect, sur la page **Bienvenue sur Azure AD Connect**, activez la case à cocher **Je suis d'accord avec les termes de la licence et avis de confidentialité**, puis cliquez sur **Continuer**.
5. Sur la page **Configuration rapide**, cliquez sur **Utiliser la configuration rapide**.
6. Sur la page **Connexion à Azure AD**, dans la zone de texte **NOM D'UTILISATEUR**, saisissez le nom de compte utilisateur **SYNC**. Dans la zone de texte **MOT DE PASSE**, tapez **Pa55w.rd**, puis cliquez sur **Suivant**.
7. Sur la page **Connexion à Azure AD**, dans la zone de texte **NOM D'UTILISATEUR**, saisissez **Adatum\administrateur**. Dans la zone **MOT DE PASSE**, tapez **Pa55w.rd**, puis cliquez sur **Suivant**.
8. Sur la page **Configuration de la connexion à Azure AD**, activez la case à cocher à côté de **Continuer sans aucun domaine vérifié**, puis cliquez sur **Suivant**.
9. Cliquez **Installer**. Lorsque l'installation est terminée, cliquez sur **Quitter**.
10. À ce moment, la synchronisation des objets de vos services de domaine Active Directory locaux (AD DS) et Microsoft Azure Active Directory (Azure AD) commence. Vous devez attendre environ 10 minutes pour que ce processus se termine.
11. Fermez la fenêtre Internet Explorer sur **LON-SVR1**.

► **Tâche 3 : Vérifier la synchronisation initiale et gérer les paramètres**

1. Basculez vers **Internet Explorer** sur votre machine hôte. Le portail classique Azure devrait être ouvert.
2. Sur la page **annuaire**, cliquez sur l'onglet **UTILISATEURS**.
3. Vérifiez que vous pouvez voir les comptes d'utilisateurs de vos AD DS locaux. Vous devriez être en mesure de voir tous les utilisateurs de votre domaine adatum.com local.

4. Sur **LON-SVR1**, cliquez sur **Démarrer**, puis cliquez sur **Toutes les applications**. Développez **Azure AD Connect**, puis cliquez sur **Service de synchronisation**.
5. Dans la fenêtre **Synchronization Service Manager** sur **LON-SVR1**, cliquez sur l'onglet **Opérations**.
6. Assurez-vous que vous voyez les tâches **Exporter, synchronisation complèteet importation complète**.
7. Veillez à ce que toutes les tâches aient une heure et une date dans les colonnes **Heure de début** et **Heure de fin**. En outre, veillez à ce que toutes les tâches soient classées sous succès dans la colonne **Statut**.
8. Fermez le Synchronization Service Manager.
9. Sur **LON-SVR1**, ouvrez **Windows PowerShell**.
10. Dans la fenêtre **Administrateur** : fenêtre Windows PowerShell, saisissez la commande suivante, puis appuyez sur Entrée

```
Get-ADSyncScheduler
```



Remarque : Si cette commande renvoie une erreur, redémarrez l'ordinateur **LON-SVR1** et répétez l'étape 10.

11. Vérifiez les résultats. Veillez à ce que la valeur **AllowedSyncCycleInterval** et la valeur **CurrentlyEffectiveSyncCycleInterval** soient réglées à **30 minutes**.
 12. Dans la fenêtre **Administrateur** : **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :
- ```
Set-ADSyncScheduler -CustomizedSyncCycleInterval 01:00:00
```
13. Dans la fenêtre **Administrateur** : **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :
- ```
Start-ADSyncSyncCycle -PolicyType Delta
```
14. Attendez environ deux minutes.
 15. Dans la fenêtre **Administrateur** : **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :
- ```
Get-ADSyncScheduler
```
16. Veillez à ce que la nouvelle valeur soit appliquée à la variable **CurrentlyEffectiveSyncCycleInterval**.
  17. Fermez la fenêtre **Windows PowerShell**.

**Résultats :** Après avoir terminé cet exercice, vous devriez avoir installé Azure AD Connect avec des paramètres personnalisés, terminé la synchronisation d'annuaires pour Azure AD et vérifié que la synchronisation est réussie.

## Exercice 3 : Gestion des utilisateurs et des groupes Active Directory

### ► Tâche 1 : Ajouter de nouveaux objets dans AD DS

1. Basculez vers **LON-DC1**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
3. Dans le volet de navigation, développez **Adatum.com**, cliquez avec le bouton droit sur **Sales**, puis cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Nouvel objet - utilisateur**, dans la zone de texte **Nom d'utilisateur**, entrez votre nom.
5. Dans la zone de texte **Ouverture de session de l'utilisateur**, entrez **votre prénom**, puis cliquez sur **Suivant**.
6. Dans les boîtes **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa55w.rd**, puis désactivez la case à cocher **L'utilisateur devra changer le mot de passe**.
7. Cliquez sur **Suivant**, cliquez sur **Terminer**, puis cliquez sur **Sales**.
8. Cliquez avec le bouton droit sur votre compte d'utilisateur, puis cliquez sur **Ajouter à un groupe**.
9. Dans la boîte de dialogue **Sélection des groupes**, dans la zone **Entrer le nom de l'objet à sélectionner (exemples)**, saisissez **Sales**, puis cliquez sur **OK**.
10. Dans la boîte de dialogue **Services de domaine Active Directory**, cliquez sur **OK**.

### ► Tâche 2 : Vérifier la synchronisation des nouveaux objets USER

1. Sur **LON-SVR1**, cliquez droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (Admin)**.
2. Dans la fenêtre **Administrateur : Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :

```
Start-ADSyncSyncCycle -PolicyType Delta
```
3. Attendez environ 4 minutes. Ne fermez pas l'**Administrateur : Windows PowerShell**. Cependant, vous pouvez la réduire.
4. Basculez vers **Internet Explorer** sur votre machine hôte, où vous avez ouvert le portail classique Azure.
5. Actualisez la page Web, cliquez sur **UTILISATEURS**, puis vérifiez la présence du compte d'utilisateur que vous venez d'ajouter.
6. Cliquez sur **GROUPES**, puis cliquez sur **Ventes**.
7. Assurez-vous que votre compte a également été ajouté au groupe **Ventes**.
8. Réduisez la fenêtre **Internet Explorer**.

**Résultats :** Après avoir terminé cet exercice, vous devriez avoir identifié la façon dont la gestion des comptes d'utilisateur et de groupe a changé avec la synchronisation d'annuaire.

► **Tâche 3 : Préparer le module suivant**

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour rétablir **22742A-LON-DC2**, **22742A-LON-SVR1** et **22742A-LON-CL1**.



## Module 13 : Surveillance, gestion et récupération AD DS

### Atelier pratique : Récupération d'objets dans AD DS

#### Exercice 1 : Sauvegarde et restauration de système de domaine Active Directory (AD DS)

##### ► Tâche 1 : Installer la fonction de sauvegarde Windows Server

1. Basculez vers **LON-DC1**.
2. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
3. Dans l'**Assistant Ajouter des rôles et des fonctionnalités**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner les fonctionnalités**, dans la liste **Fonctionnalités**, activez la case à cocher **Sauvegarde Windows Server**, puis cliquez sur **Suivant**.
8. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
9. Une fois l'installation terminée, cliquez sur **Fermer**.

##### ► Tâche 2 : Créer une sauvegarde planifiée

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Sauvegarde Windows Server**.
2. Dans Sauvegarde Windows Server, cliquez sur **Sauvegarde locale**, puis sur **Planification de la sauvegarde**.
3. Dans l'**assistant Planification de sauvegarde**, sur la page **Mise en route**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner la configuration de la sauvegarde**, cliquez sur **Personnalisation**, puis sur **Suivant**.
5. Sur la page **Sélectionner les éléments à sauvegarder**, cliquez sur **Ajouter des éléments**.
6. Dans la boîte de dialogue **Sélectionner les éléments**, sélectionnez **Récupération complète**, cliquez sur **OK**, puis sur **Suivant**.
7. Sur la page **Indiquer la fréquence de sauvegarde**, cliquez sur **Tous les jours**.
8. Dans la liste **Sélectionnez une heure**, sélectionnez **12 : 00**, puis cliquez sur **Suivant**.
9. Sur la page **Spécifier le type de destination** cliquez sur **Sauvegarder vers un disque dur dédié aux sauvegardes (recommandé)**, puis sur **Suivant**.
10. Sur la page **Sélectionner le disque de destination**, cliquez sur **Afficher tous les disques disponibles**.
11. Dans la boîte de dialogue **Afficher tous les disques disponibles**, cochez la case **Disque 1** puis cliquez sur **OK**.
12. Sur la page **Sélectionner le disque de destination**, activez la case à cocher **Disque 1**, puis cliquez sur **Suivant**.

13. Quand la boîte de dialogue **Sauvegarde de Windows Server** apparaît vous informant de la suppression de toutes les données sur le disque, cliquez sur **Oui** pour continuer.



**Remarque :** Vous annulez le processus à l'étape suivante pour éviter le formatage du lecteur E.

14. Sur la page **Confirmation**, cliquez sur **Annuler** pour empêcher le formatage du lecteur E.

► **Tâche 3 : Réaliser une sauvegarde interactive**

1. Dans le volet **Actions**, cliquez sur **Sauvegarde unique**.
2. Sur la page **Options de sauvegarde**, vérifiez que **Autres options** est sélectionné, puis cliquez sur **Suivant**.
3. Sur la page **Sélectionner la configuration de la sauvegarde**, cliquez sur **Personnalisation**, puis sur **Suivant**.
4. Sur la page **Sélectionner les éléments à sauvegarder**, cliquez sur **Ajouter des éléments**.
5. Dans la boîte de dialogue **Sélectionner les éléments**, cliquez sur **État du système**, puis sur **OK**.
6. Cliquez sur **Paramètres avancés**, puis sur l'onglet **Paramètres VSS**.
7. Cliquez sur **Sauvegarde complète VSS**, sur **OK**, puis sur **suivant**.
8. Sur la page **Sélectionner le type de destination**, cliquez sur **Suivant**.
9. Sur la page **Sélectionner la destination de la sauvegarde**, cliquez sur **Suivant**.
10. Sur l'écran **Confirmation**, sélectionner **Sauvegarde**, puis cliquez sur **Fermer**.



**Remarque :** La sauvegarde prend environ 10 à 15 minutes. Une fois la sauvegarde terminée, fermez la fenêtre sauvegarde Windows Server.

► **Tâche 4 : Supprimer une unité d'organisation (UO)**



**Remarque :** Patientez pendant que la sauvegarde se termine avant de continuer.

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans la barre de **menus**, cliquez sur **Affichage Fonctionnalités avancées**, puis sur **Paramètres d'affichage de compatibilité**.
3. Dans l'arborescence de la console, développez **Adatum.com**, puis cliquez sur **l'UO Research**.
4. Cliquez avec le bouton droit sur **Recherche**, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de recherche**, sur l'onglet **Objet**, désactivez la case à cocher **Protéger l'objet d'une suppression accidentelle**, puis cliquez sur **OK**.
6. Dans le volet de navigation, cliquez avec le bouton droit sur **Research**, puis sur **Supprimer**.
7. Quand un message de confirmation apparaît, cliquez sur **Oui**.
8. Quand un message d'avertissement apparaît, cliquez sur **Oui**.
9. Patientez pendant que le script se termine.

10. Vérifiez que l'unité d'organisation de la recherche a été supprimée.

UTILISATION RÉSERVÉE À L'INSTRUCTEUR MCT UNIQUEMENT

► **Tâche 5 : Redémarrer dans le mode restauration des services d'annuaire (DSRM)**

1. Sur **LON-DC1**, cliquez sur **Démarrer**, cliquez avec le bouton droit sur **Windows PowerShell**, puis cliquez sur **Exécuter en tant qu'administrateur**.
2. Dans l'interface de ligne de commande Windows PowerShell®, tapez la commande suivante, puis appuyez sur Entrée :

```
bcdedit /set safeboot dsrepair
```

3. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
shutdown /t 0 /r
```

► **Tâche 6 : Restaurer les données d'état du système**

1. Connectez-vous à **LON-DC1** en tant qu'**.\Administrateur** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, puis cliquez avec le bouton droit sur **Windows PowerShell**, puis cliquez sur **Exécuter en tant qu'administrateur**.
3. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
wbadmin get versions -backuptarget:E: -machine:LON-DC1
```

4. Notez l'identifiant de la version qui est renvoyée.
5. À l'invite de commandes, tapez la commande suivante, quand la *version* est le nombre que vous avez enregistré à l'étape précédente, puis appuyez sur Entrée :

```
wbadmin start systemstaterecovery -version:<version> -backuptarget:E: -machine:LON-DC1
```

Par exemple :

```
wbadmin start systemstaterecovery -version:01/22/2011-10:37 -backuptarget:E: -machine:LON-DC1
```

6. Tapez **O**, puis appuyez sur Entrée.
7. Tapez **O**, puis appuyez sur Entrée.



**Remarque :** La restauration prend environ 30 à 35 minutes. En fonction de la machine hôte, cela peut durer jusqu'à une heure.

8. Lorsque vous êtes invité à redémarrer, tapez **O**, puis appuyez sur Entrée.

► **Tâche 7 : Marquer des données restaurées comme faisant autorité**

1. Connectez-vous à **LON-DC1** en tant qu'**.Administrateur** avec le mot de passe **Pa55w.rd**.
2. Lorsque vous êtes invité, appuyez sur Entrée.
3. Cliquez sur **Démarrer**, puis cliquez avec le bouton droit sur **Windows PowerShell**, sélectionnez **Plus**, puis cliquez sur **Exécuter en tant qu'administrateur**.
4. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
ntdsutil.exe
```

5. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
activate instance ntds
```

6. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
authoritative restore
```

7. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
restore subtree "ou=Research,dc=adatum,dc=com"
```

8. Dans la fenêtre de confirmation de la boîte de messages qui apparaît, cliquez sur **Oui**.

9. Tapez **Quit**, puis appuyez sur Entrée.

10. Tapez **Quit**, puis appuyez sur Entrée.

11. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
bcdedit / deletevalue safeboot
```

12. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
shutdown /t 0 /r
```

► **Tâche 8 : Vérifier que les données ont été restaurées**

1. Patientez pendant que **LON-DC1** redémarre.
2. Connectez-vous à **LON-DC1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa\$\$w0rd**.
3. Basculez vers Server Manager et, à partir du menu **Outils**, lancez **Utilisateurs et ordinateurs Active Directory**.
4. Dans l'arborescence de la console, développez **Adatum.com**, puis vérifiez que la **Recherche** UO est restaurée. Notez que vous pouvez avoir à forcer une réplication de site dans Sites et services Active Directory pour voir immédiatement le changement.

**Résultats :** Une fois cet exercice terminé, vous devriez avoir effectué une sauvegarde interactive et une restauration faisant autorité de AD DS avec succès.

## Exercice 2 : Récupération d'objets dans AD DS

► **Tâche 1 : Vérifier les exigences pour la corbeille Active Directory**

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Domaines et approbations Active Directory**.
2. Dans la console Domaines et approbations Active Directory, cliquez avec le bouton droit sur **Domaines et approbations Active Directory**, puis cliquez sur **Augmenter le niveau fonctionnel de forêt**.
3. Confirmez que la valeur du **Niveau fonctionnel de la forêt actuel** est Windows Server 2012 R2, puis cliquez sur **Annuler**.
4. Fermez la console Utilisateurs et ordinateurs Active Directory.

► **Tâche 2 : Activer la fonctionnalité Corbeille de Active Directory**

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
2. Développez **Sites**, développez **Nom-Premier-Site-Par-défaut**, **Serveurs** et **LON-DC1**, puis cliquez sur **Paramètres NTDS**.
3. Cliquez avec le bouton droit sur <**Généré automatiquement**>, sur **Répliquer maintenant**, puis sur **OK**.
4. Déroulez le menu **LON-DC2**, puis cliquez sur **Paramètres NTDS**.
5. Cliquez avec le bouton droit sur <**Généré automatiquement**>, sur **Répliquer maintenant**, puis sur **OK**.
6. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Module Active Directory pour Windows PowerShell**.
7. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=adatum,DC=com' -Scope ForestOrConfigurationSet -Target 'adatum.com'
```

8. Tapez **O**, puis appuyez sur Entrée.
9. À l'invite de la commande, fermez la fenêtre **Windows PowerShell**.
10. Répétez les étapes 1 à 5 pour resynchroniser le domaine.

► **Tâche 3 : Supprimer les objets pour simuler la suppression accidentelle**

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Accédez à l'unité d'organisation **Sales**.
3. Cliquez avec le bouton droit sur **Sales**, puis sur **Supprimer**.
4. Dans la fenêtre de confirmation, cliquez sur **OK**.
5. Fermez la fenêtre Utilisateurs et ordinateurs Active Directory.

► **Tâche 4 : Effectuer la restauration de l'objet avec le module Active Directory pour Windows PowerShell**

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Module Active Directory pour Windows PowerShell**.
2. Tapez la commande suivante, puis appuyez sur Entrée :

```
Get-ADObject -Filter {displayName -eq "Abbie Parsons"} -IncludeDeletedObjects | Restore-ADObject
```

3. Fermez la fenêtre **Windows PowerShell**.

► **Tâche 5 : Vérifier la restauration de l'objet**

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Assurez-vous que **Abbie Parsons** existe dans l'unité d'organisation **Sales**.

**Résultats :** Après l'exercice terminé, vous devez avoir activé et testé la fonctionnalité Corbeille de Active Directory avec succès.

#### ► Tâche 6 : Se préparer pour la fin du cours

Une fois l'atelier pratique terminé, rétablissez l'état initial des ordinateurs virtuels. Pour cela, procédez comme suit :

1. Sur l'ordinateur hôte, démarrez le **Gestionnaire Hyper-V**.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton droit sur **22742A-LON-DC1**, puis cliquez sur **Rétablissement**.
3. Dans la boîte de dialogue **Rétablissement l'ordinateur virtuel**, cliquez sur **Rétablissement**.
4. Répétez les étapes 2 et 3 pour rétablir **22742A-LON-DC2**.

