Microsoft

PRODUIT OFFICIEL DE FORMATION MICROSOFT

# 22742A

# Identité avec Windows Server 2016

*Contenu d'accompagnement*

Numéro de produit : 22742A

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

      **pour autant que vous vous conformiez à ce qui suit :**
   iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,
   iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,
   v. vous veillerez à ce que chaque Utilisateur Final ayant reçu la version papier du Cours Microsoft avec

Formateur reçoive une copie du présent contrat et reconnaisse que son utilisation du Cours Microsoft avec Formateur sera soumises aux termes du présent accord, et ce avant de lui fournir ledit Cours Microsoft avec Formateur. Chacun devra confirmer son acceptation du présent contrat d'une manière opposable aux termes de la réglementation locale avant d'accéder au Cours Microsoft avec Formateur,

vi. vous veillerez à ce que chaque Formateur donnant une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,
vii. vous n'utiliserez que des Formateurs qualifiés qui ont une connaissance et une expérience approfondies de la technologie Microsoft qui est l'objet du Cours Microsoft avec Formateur donné pour toutes vos Sessions de Formation Agréées,
viii. vous ne donnerez qu'un maximum de 15 heures de formation par semaine pour chaque Session de Formation Agréée qui utilise un cours MOC, et
ix. vous reconnaissez que les Formateurs qui ne sont pas MCT n'auront pas accès à l'ensemble des ressources destinées au formateur du Cours Microsoft avec Formateur.

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

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

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

ix. vous ne donnerez accès au Cours Microsoft avec Formateur qu'aux Utilisateurs Finaux, et
x. vous ne donnerez accès au Contenu du Formateur qu'aux Formateurs.

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

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

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

e. **Si vous êtes un Formateur :**
i. Pour chaque licence que vous achetez, vous êtes autorisé à installer et utiliser une (1) copie du Contenu du Formateur sous la forme dans laquelle il vous a été fourni sur un (1) Dispositif

Personnel exclusivement pour préparer et donner une Session de Formation Agréée ou une Session de Formation Privée, et à installer une (1) copie supplémentaire sur un autre Dispositif Personnel comme copie de sauvegarde, utilisable uniquement pour réinstaller le Contenu du Formateur. Vous n'êtes pas autorisé à installer ou utiliser une copie du Contenu du Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas. Vous êtes également autorisé à imprimer une (1) copie du Contenu du Formateur uniquement pour préparer et assurer une Session de Formation Agréée ou une Session de Formation Privée.

ii. Vous pouvez personnaliser les parties écrites du Contenu du Formateur qui sont logiquement associées à la présentation d'une session de formation conformément à la version la plus récente du contrat MCT. Si vous choisissez d'exercer les droits qui précèdent, vous acceptez de vous conformer à ce qui suit : (i) les personnalisations ne peuvent être utilisées que pour donner des Sessions de Formation Agréées et des Sessions de Formation Privées, et (ii) toutes les personnalisations seront conformes au présent contrat. À des fins de clarté, toute utilisation de « *personnaliser* » ne fait référence qu'à la modification de l'ordre des diapositives et du contenu, et/ou à la non-utilisation de l'ensemble du contenu ou des diapositives, et ne signifie pas le changement ou la modification d'aucune diapositive ni d'aucun contenu.

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

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

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

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

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

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

b. **Commentaires.** Si vous acceptez de faire part à Microsoft de vos commentaires concernant le Contenu Concédé sous Licence, directement ou par l'intermédiaire de son représentant tiers, vous concédez à Microsoft, gratuitement, le droit d'utiliser, de partager et de commercialiser vos commentaires de

quelque manière et à quelque fin que ce soit. Vous concédez également à des tiers, à titre gratuit, tout droit de propriété sur leurs produits, technologies et services, nécessaires pour utiliser ou interfacer des parties spécifiques d'un logiciel, produit ou service Microsoft qui inclut les commentaires. Vous ne donnerez pas d'informations faisant l'objet d'une licence qui impose à Microsoft de concéder sous licence son logiciel, ses technologies ou produits à des tiers parce que nous y incluons vos commentaires. Ces droits survivent au présent contrat.

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

**4. CHAMP D'APPLICATION DE LA LICENCE.** Le Contenu Concédé sous Licence n'est pas vendu. Le présent contrat ne fait que vous conférer certains droits d'utilisation du Contenu Concédé sous Licence. Microsoft se réserve tous les autres droits. Sauf si la réglementation applicable vous confère d'autres droits, nonobstant la présente limitation, vous n'êtes autorisé à utiliser le Contenu Concédé sous Licence qu'en conformité avec les termes du présent contrat. Ce faisant, vous devez vous conformer aux restrictions techniques contenues dans le Contenu Concédé sous Licence qui ne vous permettent de l'utiliser que d'une certaine façon. Sauf stipulation expresse dans le présent contrat, vous n'êtes pas autorisé à :

- accéder au Contenu Concédé sous Licence ou à y autoriser l'accès à quiconque qui n'a pas acheté une licence valide du Contenu Concédé sous Licence,
- modifier, supprimer ou masquer les mentions de droits d'auteur ou autres notifications de protection (y compris les filigranes), marques ou identifications contenue dans le Contenu Concédé sous Licence,
- modifier ou créer une œuvre dérivée d'un Contenu Concédé sous Licence,
- présenter en public ou mettre à disposition de tiers le Contenu Concédé sous Licence à des fins d'accès ou d'utilisation,
- copier, imprimer, installer, vendre, publier, transmettre, prêter, adapter, réutiliser, lier ou publier, mettre à disposition ou distribuer le Contenu Concédé sous Licence à un tiers,
- contourner les restrictions techniques contenues dans Contenu Concédé sous Licence, ou
- reconstituer la logique, décompiler, supprimer ou contrecarrer des protections, ou désassembler le Contenu Concédé sous Licence, sauf dans la mesure où ces opérations seraient expressément permises par les termes du contrat de licence ou la réglementation applicable nonobstant la présente limitation.

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

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

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

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

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

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

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

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

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

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

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

    Cette limitation concerne :

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

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

Dernière mise à jour : septembre 2012.

# Module 1

## Installation et configuration de contrôleurs de domaine

### Sommaire :

Leçon 1

# Vue d’ensemble d’AD DS

## Sommaire :

## Questions et réponses

**Question :** Quels sont les deux principaux objectifs des UO ?

> **Réponse :** Les deux principaux objectifs des UO consistent à fournir un cadre pour la délégation de l'administration et fournir une structure qui permet un déploiement GPO ciblé.

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

> **Réponse :** Vous auriez déployé un arbre supplémentaire dans la forêt AD DS si vous aviez besoin de plus d'un espace de nom Domain Name System (DNS).

## Ressources

**Lectures supplémentaires :** pour plus d'informations sur les domaines et les forêts, consultez le site suivant : « Aperçu d'Active Directory Domain Services », à l'adresse http://aka.ms/M2lr5a

## Nouveautés d'AD DS dans Windows Server 2016

**Lectures supplémentaires :** pour plus d'informations sur la gestion de l'accès privilégié (PAM, Privileged Access Management), consultez : « Gestion de l'accès privilégié aux Services de domaine Active Directory (AD DS) » à l'adresse : http://aka.ms/Ibsyai

**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

**Lectures supplémentaires :** 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

**Lectures supplémentaires :** pour plus d'informations sur les nouvelles fonctionnalités d'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

## Démonstration : Utiliser le Centre d'administration Active Directory pour administrer et gérer AD DS

### Procédures de démonstration

### Naviguez 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. Cliquez sur **Adatum (local)**.
3. Cliquez sur **Contrôle d'accès dynamique**.
4. Cliquez sur **Recherche globale**.
5. Dans le volet de navigation, cliquez sur l'onglet **Arborescence**, puis développez le nœud **Adatum (local)** pour afficher les détails du domaine Adatum.com.

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

1. Dans le Centre d'administration Active Directory, cliquez sur **Vue d'ensemble**.
2. Dans la boîte de dialogue **Réinitialiser le mot de passe**, dans la zone **Nom d'utilisateur**, tapez **Adatum\David.**
3. Dans les zones **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa$$w0rd**.
4. Désactivez la case à cocher **L'utilisateur doit changer le mot de passe à la prochaine connexion**, puis cliquez sur **Appliquer**.
5. Dans la boîte de dialogue **Recherche générale**, dans la zone **Rechercher**, tapez **lon**, puis appuyez sur Entrée.

## Création d'un objet

1. Dans le centre d'administration Active Directory, dans l'arborescence du volet de navigation, développez **Adatum (local)**, puis cliquez sur le conteneur **Ordinateurs**.
2. Dans le volet **Tâches** dans la section **Ordinateurs**, cliquez sur **Nouveau**, puis sélectionnez **Ordinateur**.
3. Dans la boîte de dialogue **Créer un ordinateur**, fournissez les détails suivants, puis cliquez sur **OK** :
   - Nom de l'ordinateur : **LON-CL4**
   - Ordinateur (NetBIOS) : **LON-CL4**
4. Cliquez sur **OK**.

## 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'attribut**, puis vous verrez que tous les attributs de l'objet ordinateur sont disponibles ici.
4. Cliquez sur **Annuler** pour fermer la fenêtre **Propriétés LON-CL4**.

## Utiliser la visionneuse de l'Historique de Windows PowerShell

1. Dans le centre d'administration Active Directory, cliquez sur la barre d'outils de l'**historique Windows PowerShell** dans la partie inférieure de l'écran.
2. Voir les détails de l'applet de commande **New AD-Computer** qui a été utilisé pour exécuter la tâche la plus récente.
3. Sur **LON-DC1**, fermez toutes les fenêtres actives.

Leçon 2

# Vue d'ensemble des contrôleurs de domaine AD DS

## Sommaire :

## Questions et réponses

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

**Réponse :** Le placement de catalogue global affecte le temps nécessaire à un utilisateur pour se connecter. Par conséquent, vous devez soigneusement planifier le placement de catalogue global. Dans un environnement de domaine unique, chaque contrôleur de domaine doit héberger le catalogue global, parce que chaque contrôleur de domaine détient déjà une copie complète du domaine. Dans un scénario à plusieurs domaines, vous devez considérer les heures de connexion des utilisateurs, les dépendances de programme, la nécessité d'une haute disponibilité du catalogue global, et le trafic de réplication lors de la planification de placement du catalogue global.

**Question :** Dans une forêt à plusieurs domaines, une copie du catalogue global doit être enregistrée sur chaque contrôleur de domaine.

( ) Vrai

( ) Faux

**Réponse :**

( ) Vrai

(√) Faux

**Commentaire :**

Dans un seul domaine, 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.

## Ressources

## Transférer et prise des rôles

**Lectures supplémentaires :**

- Pour plus d'informations sur l'utilisation de Windows PowerShell pour le transfert ou la prise des rôles FSMO, reportez-vous à : « Move (Transferring or Seizing) FSMO Roles with AD-Powershell Command to Another Domain Controller » à l'adresse : http://aka.ms/Rn7kfi
- 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 prendre ou transférer des rôles FSMO vers un contrôleur de domaine » à l'adresse : http://aka.ms/Npye86

## Démonstration : Affichage des enregistrements SRV dans DNS

### Procédures de démonstration

### Afficher les enregistrements SRV dans DNS

1. Sur **LON-DC1**, connectez-vous avec le nom d'utilisateur **Adatum\Administrateur** et le mot de passe **Pa$$w0rd**.
2. Dans **Gestionnaire de serveur**, cliquez sur le menu **Outils**.
3. Dans la liste **Outils**, cliquez sur **DNS**.

4. Dans la fenêtre **Gestionnaire DNS**, dans le menu de l'arborescence, développez **LON-DC1 et Zones de recherche suivantes,** puis cliquez sur **Adatum.com**. Afficher les quatre sous-zones DNS suivantes :
   - **_msdcs**
   - **_sites**
   - **_tcp**
   - **_udp**
5. Développez **Adatum.com**, **_sites**, **Nom-Premier-Site-Par défaut** et **_tcp**, puis sélectionnez l'enregistrement suivant :
   - **_Emplacement Service Idap (SRV) [0] [100] [389] lon-dc1.adatum.com**
6. Si les étudiants ont une expertise et un intérêt suffisants, ouvrez **c:\windows\system32\config**, puis ouvrez le fichier **netlogon.dns** dans Microsoft Bloc-notes. Affichez tous les enregistrements de service (enregistrements SRV) que ce contrôleur de domaine enregistrera dans DNS.

Leçon 3

# Déploiement d’un contrôleur de domaine

## Sommaire :

## Questions et réponses

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

**Réponse :** Clonage

**Commentaire :** La façon la plus rapide de déployer plusieurs ordinateurs qui sont configurés de manière identique, en particulier lorsque qu'ils fonctionnent dans un environnement virtualisé tels que Hyper-V, consiste à les cloner. 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.

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

**Réponse :** Les deux principales considérations sont la restauration et les limites de l'ordinateur virtuel.

**Commentaire :**

- Restauration. Lorsqu'un système AD DS est restauré, il est possible de créer des nombres de séquences de mise à jour (USN) en double et puisque la réplication du contrôleur de domaine dépend d'USN, les nombres en double peuvent provoquer des problèmes. Pour éviter cela, Windows Server 2016 Active Directory a un identificateur nommé VM-Generation ID. VM-Generation ID peut détecter une restauration et il empêche le contrôleur de domaine virtualisé de répliquer des modifications sortantes tant que l'AD DS virtualisé n'a pas convergé avec les autres contrôleurs de domaine dans le domaine
- Limitations de l'ordinateur virtuel. Les ordinateurs virtuels Azure sont limités à 14 gigaoctets (Go) de mémoire vive (RAM) et une carte réseau. En outre, la fonction de point de contrôle n'est pas prise en charge

## Ressources

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

**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 : « AD DS Deployment Cmdlets in Windows PowerShell » à l'adresse : http://aka.ms/Lnxifx

## Installer un contrôleur de domaine en installant à partir de support

**Lectures supplémentaires :** 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

## Meilleures pratiques pour la virtualisation du contrôleur de domaine

**Lectures supplémentaires :** pour plus d'informations sur la virtualisation des contrôleurs de domaine, reportez-vous à : « Running Domain Controllers in Hyper-V » à : http://aka.ms/Tjjl9g

## Démonstration : Cloner un contrôleur de domaine

### Procédures de démonstration

### Préparer un contrôleur de domaine source à cloner

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'UO **Contrôleurs de domaine**.
3. Dans la liste de gestion, sélectionnez **LON-DC1** le cas échéant, puis dans le volet **Office**, dans la section **LON-DC1**, cliquez sur **Ajouter au groupe**.
4. Dans la boîte de dialogue **Sélectionner des groupes**, dans la zone **Entrer les noms des objets à sélectionner**, tapez **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. Dans le menu Démarrer, cliquez sur **Windows PowerShell**.
7. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée.

```
Get-ADDCCloningExcludedApplicationList
```

8. Vérifiez la liste des applications critiques. Dans la production, vous devez vérifier chaque application ou utiliser un contrôleur de domaine qui possède le moins d'applications installées par défaut. Tapez la commande suivante, puis appuyez sur Entrée.

```
Get-ADDCCloningExcludedApplicationList -GenerateXML
```

9. Tapez la commande suivante pour créer le fichier DCCloneConfig.xml, puis appuyez sur Entrée.

```
New-ADDCCloneConfigFile
```

10. Tapez la commande suivante pour arrêter LON-DC1, puis appuyez sur Entrée.

```
Stop-Computer
```

11. Patientez pendant que l'ordinateur virtuel s'arrête. Vous pouvez être invité à confirmer l'arrêt.

### Exporter l'ordinateur virtuel source

1. Sur l'ordinateur hôte, dans Microsoft Hyper-V Manager, dans le volet d'informations, sélectionnez l'ordinateur virtuel **22742A-LON-DC1**.
2. Dans le volet **Actions**, dans la section **22742A-LON-DC1**, cliquez sur **Exporter**.
3. Dans la boîte de dialogue **Exporter l'ordinateur virtuel**, allez à l'emplacement **D:\Program Files\Microsoft Learning\22742**, puis cliquez sur **Exporter**. Patientez pendant que l'exportation se termine.
4. Dans le volet **Actions**, dans la section **22742-LON-DC1**, cliquez sur **Démarrer**.

## Créer et démarrer le contrôleur de domaine cloné

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 Importation d'ordinateur virtuel, sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Localiser le dossier**, cliquez sur **Parcourir**, allez dans le dossier **D:\Program Files\Microsoft Learning\22742\22742A-LON-DC1**, cliquez sur **Sélectionner un dossier**, puis sur **Suivant**.
4. Sur la page **Sélectionner l'ordinateur virtuel**, sélectionnez **22742A-LON-DC1** (le cas échéant), puis cliquez sur **Suivant**.
5. Sur la page **Choisissez un 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**, activez la case à cocher **Stocker l'ordinateur virtuel dans un emplacement différent**. Pour chaque emplacement du dossier, spécifiez **D:\Program Files\Microsoft Learning\22742** comme chemin d'accès. Cliquez sur **Suivant**.
7. Sur la page **Choisir les dossiers pour stocker les disques durs virtuels**, indiquez le chemin d'accès **D:\Program Files\Microsoft Learning\22742**, puis cliquez sur **Suivant**.
8. Dans la page **Fin de l'Assistant Importation**, cliquez sur **Terminer**.
9. Dans la liste de gestion, identifiez et sélectionnez l'ordinateur virtuel nouvellement importé nommé **22742A-LON-DC1**, qui affiche l'**État Désactivé**. Dans la section basse du volet **Actions**, cliquez sur **Renommer**.
10. Tapez le nom **22742A-LON-DC3**, puis appuyez sur Entrée.
11. Dans le volet **Actions** dans la section **22742A-LON-DC3**, cliquez sur **Démarrer**, puis cliquez sur **Connecter** pour voir l'ordinateur virtuel démarrer.
12. Pendant le démarrage du serveur, vous pouvez voir le message **Le clonage du contrôleur de domaine est achevé à** x **%**.

# Contrôle des acquis et éléments à retenir

## 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 disposant d'une connexion WAN limitée ?

> **Réponse :** Vous utilisez l'option **Installation à partir du support**, car elle élimine la nécessité de copier l'intégralité de la base de données AD DS via la liaison WAN.

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

> **Réponse :** Pour promouvoir une installation Server Core de Windows Server 2016 au rôle de contrôleur de domaine, vous pouvez utiliser les outils suivants :
>
> - Le gestionnaire de serveur qui vous permet d'installer AD DS à distance
> - Windows PowerShell
> - La commande **dcpromo /unattend**, que vous exécutez sur le serveur exécutant l'installation minimale

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

> **Réponse :** Les réponses peuvent varier en fonction des besoins des stagiaires. Azure AD est conçu pour fournir l'identité et la gestion d'accès pour les applications Web. L'utilisation des ordinateurs virtuels IaaS Azure permet de déployer un contrôleur de domaine AD DS complet.

## Problèmes courants et conseils de dépannage

| Problème courant | Conseil pour la résolution du problème |
|---|---|
| Erreurs de syntaxe | Les erreurs de syntaxe résultent souvent de fautes de frappe ou de l'oubli d'un paramètre lors de la saisie d'applets de commande Windows PowerShell. Examinez la sortie de la console pour plus de détails sur les raisons de l'échec d'une commande particulière. |
| Problèmes préalables | Beaucoup d'erreurs irrécupérables sont directement liées à des erreurs trouvées par l'outil de vérification des conditions préalables. Assurez-vous d'examiner attentivement les résultats et de suivre les indications fournies. |
| Problèmes de configuration du réseau et de la forêt | Les problèmes de configuration réseau ou de configuration de la forêt AD DS pourraient empêcher la promotion de nouveaux contrôleurs de domaine. Utilisez les fichiers dcpromoui.log et dcpromo.log pour afficher les erreurs de promotion spécifiques ou le journal des événements pour les erreurs qui indiquent des problèmes de configuration. Vous pouvez également utiliser dcdiag.exe et repadmin.exe pour vérifier l'intégrité globale de la forêt. |

# Module 2

## Gestion d'objets dans AD DS

### Sommaire :

Leçon 1

# Gestion des comptes d’utilisateurs

## Sommaire :

## Questions et réponses

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

> **Réponse :** Ce système stocke et synchronise le profil utilisateur vers un partage réseau. Cela permet à l'utilisateur de se déplacer entre les ordinateurs et d'avoir toujours le même profil lors de son identification sur un nouvel ordinateur.

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

> **Réponse :** La désactivation d'un compte est un acte intentionnel fait par un administrateur pour empêcher l'utilisation d'un compte. Un verrouillage de compte ne peut être le résultat que d'un trop grand nombre d'échecs de connexion (en supposant que la stratégie de mot de passe configurée l'applique).

## Démonstration : Gestion des comptes d'utilisateurs

### Procédures de démonstration

### Créer un nouveau compte utilisateur

1. Sur **LON-DC1**, dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Dans le centre d'administration Active Directory, cliquez sur **Adatum (local)**, puis double-cliquez sur **Gestionnaires**.
3. Dans le volet **Actions**, cliquez sur **Nouveau**, puis sur **Utilisateur**.
4. Dans la boîte de dialogue **Créer un utilisateur**, dans le champ **Prénom**, entrez **Ventes**.
5. Dans le champ **Nom**, tapez **Gestionnaire**.
6. Dans la zone de texte d'**Ouverture de session UPN de l'utilisateur**, saisissez **Gestionnaire Ventes**.
7. Dans les champs **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **OK**.

### Supprimer un compte utilisateur

1. Cliquez le compte **Art Odum**.
2. Dans le volet d'**actions**, cliquez sur **Supprimer**
3. Dans la boîte de dialogue **Confirmer la Suppression**, cliquez sur **Oui**.

### Déplacer un compte utilisateur

1. Cliquez sur le compte Burton Bartels.
2. Dans le volet Actions, cliquez sur Déplacer...
3. Cliquez sur l'UO Développement, puis sur OK.
4. Dans le volet gauche, cliquez sur **Adatum (local)**.
5. Dans le volet de droite, double-cliquez sur l'UO **Développement** et veiller à ce que le compte Burton Bartels soit présent.

### Configurer les attributs de l'utilisateur

1. Double-cliquez sur le compte Burton Bartels.
2. Dans le volet de gauche, cliquez sur Organisation, puis modifiez le champ Département de Gestionnaires à Développement.
3. Cliquez Membre de dans le volet gauche.
4. Dans la section Membre de, cliquez sur Gestionnaires, puis sur Supprimer.

5. Cliquez sur Ajouter. Dans la boîte de dialogue Sélectionner des groupes, dans la zone Entrez les noms des objets à sélectionner (exemple) : fenêtre, tapez Développement, puis cliquez ensuite sur OK.
6. Cliquez sur OK pour fermer les propriétés de Burton Bartels.
7. Fermez le **Centre d'administration Active Directory**. Laissez le Gestionnaire de serveur ouvert pour la démonstration suivante.

## Démonstration : Utiliser des modèles pour gérer les comptes

### Procédures de démonstration

### Créer un modèle utilisateur

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Développez **Adatum.com**, puis cliquez sur l'UO **Ventes**.
3. Cliquez sur l'icône nouvelle utilisateur dans la barre d'outils.
4. Dans la boîte de dialogue **Nouvel objet - Utilisateur**, saisissez les informations suivantes, puis cliquez sur **Suivant** :
   - Prénom : **_ventes**
   - Nom : **modèle**
   - Nom de connexion d'utilisateur : **modèle des ventes**
5. Dans le champ **Mot de passe** et le champ **Entrer de nouveau le mot de passe**, tapez **Pa$$w0rd**.
6. Décochez la case **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**, cochez la case **Le mot de passe n'expire jamais**, cochez la case **Le compte est désactivé**, puis cliquez sur **Suivant**.
7. Cliquez sur **Terminer**.

### Configurer les propriétés du modèle

1. Double-cliquez sur le compte **modèle des ventes**.
2. Dans la boîte de dialogue **propriétés du modèle des ventes**, cliquez sur l'onglet **Membre de**, puis cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Sélectionner des groupes**, tapez **Ventes**, puis cliquez sur **OK**.
4. Cliquez sur l'onglet **Organisation**. Dans le champ **Département**, saisissez **Ventes**.
5. Dans la section **Gestionnaire**, cliquez sur **Modifier**. Dans la boîte de dialogue **Sélectionner l'utilisateur ou le contact**, tapez **Erin**, puis cliquez sur **Vérifier les noms**. Cliquez sur **OK**.
6. Cliquez sur l'onglet **Profil**. Dans la section **Profil de l'utilisateur**, dans le champ de **Script d'ouverture de session** tapez **\\lon-dc1\netlogon\logon.bat**, puis cliquez sur **OK**.

### Créer un nouvel utilisateur en copiant le modèle

1. Cliquez avec le bouton droit sur le compte **_ventes modèle**, puis cliquez sur **Copier**.
2. Dans la boîte de dialogue **Copier l'objet - Utilisateur**, tapez **Ventes** dans le champ **Prénom**. Tapez **Utilisateur** dans le champ **Nom**.
3. Tapez **vendeur** dans le champ **Nom Ouverture de session d'utilisateur**, puis cliquez sur **Suivant**.
4. Dans les champs **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa$$w0rd**.

5. Décochez **Le mot de passe n'expire jamais**, désactivez la case à cocher **Le compte est désactivé**, sélectionnez la case à cocher **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**, puis cliquez sur **Suivant**.
6. Cliquez sur **Terminer**.
7. Double-cliquez sur le compte **Vendeur** compte, puis cliquez sur l'onglet **Membre de**. Assurez-vous que l'utilisateur est un membre du groupe de vente.
8. Cliquez sur l'onglet **Organisation**. Veillez à ce que le Département soit Ventes et que le Gestionnaire soit Erin Bull.
9. Cliquez sur l'onglet **Profil**. Assurez-vous que le chemin du script d'ouverture de session est \\lon-dc1\netlogon\logon.bat. Cliquez sur **OK** pour fermer la boîte de dialogue**.**
10. Fermez la fenêtre **Utilisateurs et ordinateurs Active Directory**.

Leçon 2

# Gérer des groupes dans AD DS

## Sommaire :

# Démonstration : Gestion des groupes dans Windows Server

## Procédures de démonstration

### Créer un nouveau groupe et ajouter des membres

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Développez **Adatum (local)**, puis double-cliquez sur **Informatique**.
3. Dans la liste **Tâches**, sous **Informatique**, pointer vers **Nouveau**, puis cliquez sur **Groupe**.
4. Dans la boîte de dialogue **Créer un groupe**, dans le champ **Nom du groupe**, tapez **Gestionnaires informatiques**. Notez que par défaut, il s'agit d'un groupe de sécurité global.
5. Dans le volet gauche, cliquez sur **Membres**, puis sur **Ajouter**.
6. 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 **Aurore ; Julien**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
7. Cliquez sur **OK** pour fermer la fenêtre **Créer un groupe :** boîte de dialogue **Gestionnaires informatiques**.

### Ajouter un utilisateur au groupe

1. Cliquez avec le bouton droit sur l'utilisateur nommé **Maj Hojski**, puis cliquez sur **Ajouter au groupe**.
2. Dans la boîte de dialogue **Sélectionner des groupes**, dans **Entrez les noms des objets à sélectionner (exemples)**, tapez **Gestionnaires informatiques**.
3. Cliquez sur **Vérifier les noms**, puis sur **OK**.

### Modifier le type et l'étendue du groupe

1. Double-cliquez sur le groupe **Gestionnaires informatiques**.
2. Dans la fenêtre **Gestionnaires informatiques**, sous **Type de groupe**, cliquez sur **Distribution**. Lisez le message en surbrillance. Sous **Étendue du groupe**, cliquez sur **Universel**, puis cliquez sur **OK**.

### Configurez un gestionnaire pour le groupe

1. Double-cliquez sur le groupe **Gestionnaires informatiques**.
2. Dans la section **Géré par**, cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Sélectionner un utilisateur, un contact ou des groupes**, dans la zone **Entrer les noms des objets à sélectionner (exemples)**, tapez **Parsa**, cliquez sur **Vérifier les noms**, puis sur **OK**.
4. Sélectionnez la case à cocher en regard de **Le gestionnaire peut mettre à jour la liste des membres**.
5. Cliquez sur **OK** pour fermer les propriétés des gestionnaires informatiques.
6. Fermez le **Centre d'administration Active Directory**.

Leçon 3

# Gestion des objets ordinateur dans AD DS

## Sommaire :

## Questions et réponses

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

**Réponse :** En règle générale, ça provient d'un décalage de mot de passe entre l'ordinateur local et ce qui est stocké dans Active Directory.

Leçon 4

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

## Sommaire :

## Questions et réponses

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

> **Réponse :** L'environnement d'écriture de scripts intégré de Windows PowerShell fournit un environnement pour écrire, exécuter et tester des scripts Windows PowerShell. Ce système fournit la couleur de syntaxe, la saisie semi-automatique, le débogage visuel et une aide contextuelle, autant de fonctions qui ne sont pas disponibles dans la fenêtre classique de Windows PowerShell.

## Ressources

## Interrogation d'objets avec Windows PowerShell

 **Lectures supplémentaires :** pour plus d'informations, consultez about_ActiveDirectory_Filter : http://aka.ms/Kv5dy3

 **Lectures supplémentaires :** pour plus d'informations, reportez-vous à Comment utiliser les indicateurs UserAccountControl pour manipuler les propriétés du compte d'utilisateur : http://aka.ms/Mxt8a1

## Modification des objets avec Windows PowerShell

 **Lectures supplémentaires :** Pour plus d'informations, consultez Set-ADUser : http://aka.ms/K34c8d

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

### Procédures de démonstration

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Développez **Adatum.com**, puis cliquez sur l'UO **Recherche**.
3. Dans le volet d'informations, cliquez sur le haut de la colonne **Type** pour trier l'objet par type.
4. Cliquez sur le **premier objet Utilisateur** de la liste (cela devrait être **Arturs Prede**).
5. Faites défiler vers le bas de la liste, maintenez la touche **Majuscule**, puis cliquez sur le dernier objet utilisateur de la liste (cela devrait être Valérie Dupont).
6. Cliquez avec le bouton droit sur le bloc des objets sélectionnés, et cliquez sur **Propriétés**.
7. Dans la boîte de dialogue **Propriétés d'éléments multiples**, sélectionnez la case à côté de **Bureau**, dans le champ, saisissez **Winnipeg**, puis cliquez sur **OK**.
8. Double-cliquez sur l'un des objets utilisateur et notez que le champ **Bureau** va maintenant devenir **Winnipeg**.
9. Cliquez sur **Annuler**, puis fermez **Utilisateurs et ordinateurs Active Directory**.

# Démonstration : Exécution d'opérations en bloc avec Windows PowerShell

## Procédures de démonstration

### Créer un nouveau groupe global dans le département

1. Sur **LON-DC1**, clic-droit sur **Démarrer**, cliquez sur **Exécuter**, saisissez **PowerShell**, puis appuyez sur Entrée.
2. Dans la fenêtre **Administrateur** : Dans la fenêtre **Windows PowerShell**, saisissez la commande suivante, puis appuyez sur Entrée :

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

### Ajouter tous les utilisateurs dans le service informatique pour le groupe Support technique

- Dans la fenêtre **Administrateur** : Dans la fenêtre **Windows PowerShell**, saisissez la commande suivante, puis appuyez sur Entrée :

```
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**, saisissez la commande suivante, puis appuyez sur Entrée :

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

**Remarque :** notez cette commande filtre en utilisant des parenthèses plutôt que des guillemets et utilise l'applet de commande **Set-ADUser** plutôt qu'une boucle **foreach**.

### Créer une unité d'organisation

- Dans la fenêtre **Administrateur** : Dans la fenêtre **Windows PowerShell**, saisissez la commande suivante, puis appuyez sur Entrée :

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

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

1. Ouvrez l'Explorateur de fichiers, tapez **E:\Labfiles\Mod02** dans la barre d'adresse, puis appuyez sur Entrée.
2. Cliquez avec le bouton droit sur **DemoUsers.csv**, cliquez sur **Ouvrir avec**, puis cliquez sur **Bloc-notes**. Expliquez la structure du fichier aux étudiants.
3. Fermez le Bloc-notes.
4. Revenez à la fenêtre **Windows PowerShell**, puis tapez **cd E:\Labfiles\Mod02**.
5. Pour exécuter le script, tapez **.\DemoUsers.ps1**, puis appuyez sur Entrée.

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

1. Dans le Gestionnaire de serveur, cliquez sur **Outils** puis sur **Utilisateurs et ordinateurs Active Directory**.

2. S'assurez que l'UO Londres existe.
3. Cliquez sur l'UO **Londres**. Vérifier qu'il y a trois utilisateurs tels que définis dans le fichier .csv. Notez que les comptes des utilisateurs sont désactivés. En effet, aucun de mot de passe n'avait été fourni.
4. Cliquez sur l'UO **Informatique.** S'assurer que le groupe **Support technique** existe.
5. Double-cliquez sur le groupe **Support technique**, puis dans **Propriétés du support technique**, cliquez sur l'onglet **Membres**. Assurez-vous que les membres sont remplis avec les utilisateurs du département informatique, puis cliquez sur **Annuler**.
6. Cliquez l'UO **Recherche**, puis double-cliquez sur l'un des comptes d'utilisateurs.
7. Dans la page des propriétés de l'utilisateur, cliquez sur l'onglet **Adresse**. Assurez-vous que les champs d'adresse sont remplis comme prévu, puis cliquez sur **Annuler**.

Leçon 5

# Implémentation et gestion d'UO

## Sommaire :

## Questions et réponses

**Question :** Quel est l'avantage d'utiliser l'**Assistant Délégation de contrôle** ?

> **Réponse :** L'**Assistant Délégation de contrôle** peut simplifier la délégation de l'administration en attribuant des autorisations en fonction de la tâche sélectionnée.

## Démonstration : Délégation des autorisations administratives sur une unité d'organisation

### Procédures de démonstration

### Créer une unité d'organisation

1. Sur LON-DC1, dans Utilisateurs et ordinateurs Active Directory, cliquez sur **Adatum.com**.
2. Cliquez sur l'icône Nouvelle unité d'organisation sur la barre d'outils.
3. Dans la boîte de dialogue **Nouvel objet - Unité d'organisation**, saisissez **Ressources humaines** dans le champ **Nom**, puis cliquez sur **OK**.

### Utiliser l'Assistant Délégation de contrôle pour assigner une tâche

1. Clic-droit sur l'objet de domaine **Adatum.com**, puis cliquez sur **Délégation de contrôle**.
2. Dans l'**Assistant Délégation de contrôle**, cliquez sur **Suivant**.
3. Sur la page **Utilisateurs ou groupes**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs ou des groupes**, dans le champ **Entrez les noms des objets à sélectionner (exemples)**, saisissez **Support technique**, cliquez sur **Vérifier les noms**, ensuite sur **OK**, puis sur **Suivant**.
5. Sur la page **Tâches à déléguer**, sélectionnez les cases en regard de **Réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe à la prochaine ouverture de session** et **Joindre un ordinateur au domaine**, puis cliquez sur **Suivant**.
6. Cliquez sur **Terminer**.

### Attribuer au groupe de recherche le droit de modifier les adresses des utilisateurs et les titres de poste dans l'unité de recherche

1. Dans Utilisateurs et ordinateurs Active Directory, cliquez sur **Afficher**, puis cliquez sur **Fonctionnalités avancées**.
2. Cliquez avec le bouton droit sur l'UO **Recherche**, puis cliquez sur **propriétés**.
3. Cliquez sur l'onglet **Sécurité**, puis sur **Avancé** et enfin sur **Ajouter**.
4. Dans la fenêtre **Entrée d'autorisation pour la recherche**, cliquez sur **Sélectionner un principal**.
5. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs ou des groupes**, dans le champ **Entrez les noms des objets à sélectionner (exemple)**, tapez **Recherche.** Cliquez sur **Vérifier les noms**, puis sur **OK**.
6. Dans la zone de liste déroulante **S'applique à**, sélectionnez **Objets USER descendants**. (Indice : il est au bas de la liste.)
7. Dans la section **Propriétés**, faites défiler vers le bas, recherchez et sélectionnez la case à cocher en regard de **Écrire adresse personnelle**.
8. Faites défiler en davantage vers le bas, sélectionnez la case à cocher en regard de **Renseigner Poste**, Puis cliquez sur **OK**.
9. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de Recherche**.

# Révision du module et éléments à retenir

## Meilleures pratiques

Retenez les meilleures pratiques suivantes pour administrer AD DS :

- Évitez d'utiliser les groupes intégrés pour déléguer l'accès administratif à moins de comprendre quelles sont les autorisations octroyées par l'appartenance au groupe
- Créez des groupes administratifs spécialisés et leur affectez seulement les droits et autorisations requis pour exécuter les tâches assignées
- Développez des scripts Windows PowerShell pour effectuer les tâches répétitives
- Ne pas vous connectez avec votre compte administratif pour les activités quotidiennes. Ne l'utilisez que pour une tâche administrative

## Enjeux et scénarios du monde réel

De nombreuses organisations vont créer des comptes d'utilisateurs basés sur le poste plutôt qu'un utilisateur remplissant la fonction. Par exemple, l'organisation aura toujours une réceptionniste. Pour assurer la continuité, la personne qui remplit cette fonction utilise un compte générique appelé Réception. Ainsi, quand une nouvelle personneassume la fonction, il suffit de changer le mot de passe de l'utilisateur Réception. Applications, paramètres, documents, mails, etc. resteront compatibles.

## Outils

Le tableau suivant répertorie les outils référencés par ce module :

| 1. Outil | 2. Utilisé pour | 3. Emplacement |
|---|---|---|
| Windows PowerShell ; | Ligne de commande et script de toutes les tâches administratives. | Natif au système d'exploitation. |
| Centre d'administration Active Directory ; | Effectuer les tâches administratives quotidiennes dans AD DS. | Dans le Gestionnaire de serveur, sous **Outils** ou dans **Panneau de contrôle** dans **Outils d'administration**. |
| Utilisateurs et ordinateurs Active Directory ; | Exécuter les tâches administratives courantes dans AD DS. | Dans le Gestionnaire de serveur, sous **Outils** ou dans **Panneau de contrôle** dans **Outils d'administration**. |
| Assistant Délégation de contrôle ; | Assigner les autorisations afin d'effectuer des tâches administratives. | Clic droit sur une unité d'organisation dans Utilisateurs et ordinateurs Active Directory. |

## Problèmes courants et conseils de dépannage

| Problème courant | Conseil pour la résolution du problème |
|---|---|
| Les utilisateurs ne peuvent pas accéder aux ressources réseau. | Vérifier les appartenances aux groupes. Cherchez des groupes imbriqués qui sont à l'origine des conflits. |
| Vous avez affecté à un utilisateur des droits d'administration dans AD DS, mais il ne dispose pas des outils pour effectuer la tâche. | Vous devez télécharger et installer les outils d'administration de serveur distant pour Windows 10 et les installer sur le poste de travail de l'utilisateur pour lui fournir les outils administratifs nécessaires. |

# Questions et réponses sur les ateliers pratiques

## Atelier pratique A : Gestion des objets AD DS

## Questions et réponses

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

**Réponse :** Les utilisateurs et les autres rôles (groupes globaux) du même domaine sont des objets qui peuvent être membres de groupes globaux.

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

**Réponse :** Vous devez fournir les informations d'identification d'un utilisateur qui a la permission de joindre des ordinateurs au domaine. En règle générale, les informations d'identification d'un administrateur de domaine.

## Atelier pratique B : Administration AD DS

## Questions et réponses

**Question :** Pourquoi les utilisateurs créés par ce script sont activés ?

**Réponse :** Le script attribue un mot de passe pour les utilisateurs lors de leur création.

**Question :** Quel est l'état des comptes créés par de l'applet de commande **New-ADUser** ?

**Réponse :** Par défaut, ces comptes seront désactivés s'ils n'obtiennent pas de mots de passe au moment de la création.

# Module 3

## Gestion avancée de l'infrastructure AD DS

### Sommaire :

Leçon 1

# Présentation des déploiements AD DS avancés

## Sommaire :

## Questions et réponses

**Question :** Laquelle des propositions suivantes nécessite l'implémentation du déploiement de plusieurs forêts AD DS ?

( ) Exigences de l'isolement de sécurité

( ) Exigences de schéma

( ) Exigences de l'espace de noms DNS

( ) Fusions d'entreprises

( ) Exigences administratives distribuées

**Réponse :**

(√) Exigences de l'isolement de sécurité

(√) Exigences de schéma

( ) Exigences de l'espace de noms DNS

( ) Fusions d'entreprisess

( ) Exigences administratives distribuées

**Commentaire :**

L'isolement de sécurité et les exigences de schéma sont les seules exigences présentées dans les options susmentionnées qui nécessitent l'implémentation de plusieurs forêts. Les exigences d'espace de noms DNS et d'administration de distribution nécessitent plusieurs domaines, cependant les forêts séparées ne sont pas nécessaires, car une forêt unique peut avoir plusieurs espaces de noms et ne sont pas nécessaires à l'autonomie administrative. Dans un scénario de fusion d'entreprise, vous pourriez maintenir des forêts distinctes s'il n'y avait pas besoin de beaucoup de collaboration entre les organisations, mais ce ne serait pas nécessaire.

**Question :** Avant de déployer une réplique de contrôleur de domaine AD DS sur un ordinateur virtuel Azure, quelles propositions de la liste ci-dessous doivent être remplies ?

( ) 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 dont le cache en lecture et écriture est désactivé.

( ) 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 comme statique à l'aide de l'applet de commande Set-AzureStaticVNetIP.

**Réponse :**

( ) 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 dont le cache en lecture et écriture est désactivé.

(√) 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 comme statique à l'aide de l'applet de commande Set- AzureStaticVNetIP.

**Commentaire :**

Bien que nous recommandons de créer un site AD DS pour un contrôle plus rigoureux de la réplication, ceci n'est pas nécessaire. Vous devez toutefois créer un disque dur supplémentaire sur l'ordinateur virtuel Azure dans lequel la mise en cache est désactivée. Ce disque dur doit contenir le fichier NTDS.DIT et le dossier SYSVOL. Vous devez également avoir à disposition un réseau virtuel Azure correctement configuré et lui avoir attaché l'ordinateur virtuel. La création manuelle des enregistrements SRV dans Azure DNS est une réponse incorrecte, parce que cela est impossible. L'ordinateur virtuel doit également posséder une adresse IP statique configurée avant de déployer AD DS pour garantir que l'IP ne changera jamais si l'ordinateur virtuel est libéré en raison d'un arrêt ou d'actions réparation de service.

Leçon 2

# Déploiement d'un environnement AD DS distribué

## Sommaire :

## Questions et réponses

**Question :** Quel est le niveau fonctionnel minimum de domaine dans lequel vous devez déployer un contrôleur de domaine AD DS Windows Server 2016 ?

( ) Windows Server 2003

( ) Windows Server 2008

( ) Windows Server 2008 R2

( ) Windows Server 2012 R2

( ) Windows Server 2016

**Réponse :**

( ) Windows Server 2003

(√) Windows Server 2008

( ) Windows Server 2008 R2

( ) Windows Server 2012 R2

( ) Windows Server 2016

**Commentaire :**

Windows Server 2008 est le niveau fonctionnel de domaine minimum recommandé dans lequel vous devez déployer un contrôleur de domaine AD DS avec Windows Server 2016.
Windows Server 2003 n'est plus pris en charge. Bien que le domaine / les niveaux fonctionnels de Windows Server 2003 sont toujours pris en charge, vous devriez avoir les fonctionnalités de Windows Server 2008 afin d'assurer la réplication des dossiers SYSVOL qui se fait à l'aide de la réplication DFS et non plus à partir de la méthode FRS utilisée par Windows Server 2003 et les versions antérieures. Vous devez supprimer du domaine tous les contrôleurs de domaine fonctionnant toujours sur Windows Server 2003 avant d'introduire un contrôleur de domaine Windows Server 2016.

**Question :** Parmi les éléments suivants, lequel pouvez-vous utiliser pour optimiser la résolution de noms dans les espaces de noms DNS ?

( ) Redirecteurs conditionnels

( ) Sites AD DS

( ) Ordre de recherche des suffixes DNS

( ) Zones de stub DNS

( ) Serveurs de catalogue global

**Réponse :**

(√) Redirecteurs conditionnels

( ) Sites AD DS

(√) Ordre de recherche des suffixes DNS

(√) Zones de stub DNS

( ) Serveurs de catalogue global

**Commentaire :**

Les bonnes réponses sont redirecteurs conditionnels, zones de stub DNS et ordre de recherche des suffixes DNS. Les redirecteurs conditionnels et les zones de stub DNS vous permettent de créer des raccourcis de sorte que la résolution de nom n'ait pas à parcourir un arbre de domaine de haut en bas ou à traverser des forêts. En configurant un ordre de recherche des suffixes DNS, les clients n'ont pas besoin de recourir à la dévolution DNS pour résoudre les noms en une partie.

Les réponses incorrectes sont sites AD DS et serveurs de catalogue global. Bien que les sites AD DS puissent vous aider à optimiser la réplication des zones DNS intégrées à AD DS, ils ne rendent pas la résolution de noms intrinsèquement plus efficace. Les serveurs de catalogue global ne sont pas impliqués dans la résolution de noms DNS.

## Ressources

## Domaine des niveaux fonctionnels AD DS

 **Lectures supplémentaires :** Pour plus d'informations sur les caractéristiques de la version d'évaluation des fonctionnalités d'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, consultez : http://aka.ms/Ynmvma

## Migration vers Windows Server 2016 AD DS à partir d'une version précédente

 **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

## Démonstration : Installer un contrôleur de domaine dans un nouveau domaine dans une forêt existante

### Procédures de démonstration

### Installer les binaires d'AD DS sur TOR-DC1

1. Sur TOR-DC1, cliquez sur **Démarrer**, puis sur **Gestionnaire de serveur**. Dans le **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, vérifiez si **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. Sur la page **Pool de serveurs**, vérifiez que **TOR-DC1.Adatum.com** est en surbrillance, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs** cochez **Active Directory Domain Services** cliquez sur **Ajouter des fonctionnalités** puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités** cliquez sur **Suivant**
7. Sur la page **Services de domaine Active Directory**, examinez le message, puis cliquez sur **Suivant**.

8. Sur la page **Confirmer les sélections pour l'installation**, examinez le message, puis cliquez sur **Installer**. L'installation peut prendre plusieurs minutes.
9. Sur la page **Résultats**, cliquez sur **Promouvoir ce serveur en contrôleur de domaine**. L'assistant continue.

## 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

1. Sur la page **Configuration de déploiement**, sélectionnez l'option **Ajouter un nouveau domaine à une forêt existante**, puis en regard de **Sélectionner le type de domaine**, confirmez la sélection du **Domaine enfant**.
2. Dans le champ **Nom du domaine parent**, vérifiez que **Adatum.com** est listé.
3. Dans la zone **Nouveau nom de domaine**, tapez **NA**, puis cliquez sur **Suivant**.
4. Sur la page **Options du contrôleur de domaine** vérifiez que **Windows Server Technical Preview** est sélectionné comme **niveau fonctionnel du domaine**, que **Serveur du Système de Noms de Domaine (DNS)** est sélectionné, et que **Catalogue global (CG)** est sélectionné.
5. Dans les zones de texte **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)**, tapez **Pa$$w0rd** dans les deux zones, puis cliquez sur **Suivant**.
6. Dans la page **Options DNS**, cliquez sur **Suivant**.
7. Dans la page **Options supplémentaires**, cliquez sur **Suivant**. Dans la page **Chemins d'accès**, cliquez sur **Suivant**. Dans la page **Examiner les options**, cliquez sur **Suivant**. Dans la fenêtre **Confirmer les conditions préalables**, cliquez sur **Installer**.
8. Vérifiez les informations et autorisez TOR-DC1 à redémarrer en tant que contrôleur de domaine AD DS dans le nouveau domaine AD DS que vous avez créé dans la forêt AD DS.
9. Connectez-vous à TOR-DC1 comme **NA\Administrateur** avec le mot de passe **Pa$$w0rd** et vérifiez les outils AD DS pour confirmer l'installation du nouveau domaine.

Leçon 3

# Configuration des approbations AD DS

## Sommaire :

## Questions et réponses

**Question :** Parmi les éléments suivants, lequel doit être en place avant de pouvoir créer une approbation de forêt ?

( ) La résolution de noms entre les domaines racine dans chaque forêt

( ) Niveau fonctionnel de la forêt de Windows Server 2003 ou version ultérieure

( ) Niveau fonctionnel de la forêt de Windows Server 2008 ou version ultérieure

( ) Niveau fonctionnel de la forêt de Windows Server 2012 ou version ultérieure

( ) Les contrôleurs de domaine doivent être activés pour l'authentification sélective.

**Réponse :**

(√) La résolution de noms entre les domaines racine dans chaque forêt

(√) Niveau fonctionnel de la forêt de Windows Server 2003 ou version ultérieure

( ) Niveau fonctionnel de la forêt de Windows Server 2008 ou version ultérieure

( ) Niveau fonctionnel de la forêt de Windows Server 2012 ou version ultérieure

( ) Les contrôleurs de domaine doivent être activés pour l'authentification sélective.

**Commentaire :**

Afin de créer une approbation de forêt, vous devez avoir configuré la résolution de noms entre les domaines racines dans chaque forêt. En outre, pour chaque forêt, son niveau fonctionnel doit être Windows Server 2003 ou une version ultérieure.

**Question :** Quel paramètre de confiance AD DS vous permet de contrôler l'étendue de l'authentification des principaux de sécurité de confiance ?

( ) Routage de suffixes de noms

( ) Délégation Kerberos contrainte (KCD)

( ) Authentification sélective

( ) Filtrage des SID

( ) Historique SID

**Réponse :**

( ) Routage de suffixes de noms

( ) Délégation Kerberos contrainte (KCD)

(√) Authentification sélective

( ) Filtrage des SID

( ) Historique SID

**Commentaire :**

L'authentification sélective vous permet de gérer l'étendue de l'authentification des principaux de sécurité de confiance en permettant l'authentification de services uniquement sur des ordinateurs spécifiques.

# Ressources

## Configurer des paramètres avancés d'approbation AD DS

**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 sélective sur une approbation de forêt, reportez-vous à : http://aka.ms/Blp826
- Pour plus d'informations sur le routage de suffixe de noms, consultez : http://aka.ms/Egc6g7

## Démonstration : configurer une approbation de forêt

### Procédures de démonstration

### Configurer la résolution de noms DNS en utilisant un redirecteur conditionnel

1. Sur LON-DC1, dans le **Gestionnaire de serveur**, cliquez sur le menu **Outils** puis sur **DNS** dans la liste déroulante. Le **Gestionnaire DNS** s'ouvre.
2. Dans le **Gestionnaire DNS**, développez **LON-DC1**, cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez de nouveau sur **Nouveau redirecteur conditionnel**.
3. Dans la fenêtre **Nouveau redirecteur conditionnel**, dans la boîte **Domaine DNS**, saisissez **treyresearch.net**.
4. Dans **Adresse IP des serveurs maîtres :** zone de texte, tapez **172.16.10.10**. Cliquez sur l'espace libre, puis sur **OK**. (Si une erreur apparaît, ignorez-la.)
5. Fermez le **Gestionnaire DNS**.
6. Basculez vers **TREY-DC1** et répétez les étapes 1 à 5. Utilisez le nom de domaine **adatum.com** avec l'adresse IP **172.16.0.10**.

### Configurer une approbation de forêt sélective bidirectionnelle

1. Dans **LON-DC1**, dans le menu **Outils**, cliquez sur **Domaines et approbations Active Directory**.
2. Lorsque la fenêtre **Domaines et approbations Active Directory** s'ouvre, cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de : Adatum.com**, sur l'onglet **Approbations**, cliquez sur **Nouvelle approbation**.
4. Dans l'**Assistant Nouvelle approbation**, cliquez sur **Suivant**.
5. Sur la page **Nom d'approbation** dans la zone **Nom**, tapez **treyresearch.net**, puis cliquez sur **Suivant**.
6. Dans l'**Assistant Nouvelle approbation**, cliquez sur **Approbation de forêt**, puis cliquez sur **Suivant**.
7. Dans la page **Direction de l'approbation**, cliquez sur **Bidirectionnelle**, puis sur **Suivant**.
8. Dans la page **Sens de l'approbation**, cliquez sur **Ce domaine et le domaine spécifié**, puis sur **Suivant**.
9. Dans la zone de texte **Nom d'utilisateur**, saisissez **Administrateur**. Dans la zone de texte **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Suivant**.
10. Dans la page **Niveau d'authentification d'approbations sortantes - forêt locale**, cliquez sur **Authentification sélective**, puis cliquez sur **Suivant**.

11. Dans la page **Niveau d'authentification d'approbations sortantes - forêt spécifiée**, cliquez sur **Authentification sélective**, puis cliquez sur **Suivant**.
12. Dans la page **Fin de la sélection des approbations**, cliquez sur **Suivant**.
13. Dans la page **Fin de la création de l'approbation**, cliquez sur **Suivant**.
14. Dans la page **Confirmer l'approbation sortante**, cliquez sur **Oui, confirmer l'approbation sortante**, puis sur **Suivant**.
15. Dans la page **Confirmer l'approbation entrante**, cliquez sur **Oui, confirmer l'approbation entrante**, puis cliquez sur **Suivant**.
16. Sur la page **Fin de l'Assistant Nouvelle approbation**, cliquez sur **Terminer**.
17. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur **OK**.

# Révision du module et points importants à retenir

## Questions 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 son 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 avec 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. Le leadership 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 ? Discutez des objectifs à court terme et à long terme de l'intégration AD DS et comment les différentes exigences pourraient changer votre approche.

**Réponse : Objectifs à court terme**

- Créer une approbation de forêt entre les forêts AD DS adatum.com et treyresearch.net. Cela permettra l'authentification entre forêts et fournira aux employés de A. Datum et de Trey Research l'autorisation d'accès aux ressources des deux forêts.

### Objectifs à long terme

- Créer les nouveaux domaines enfant suivants dans adatum.com :
  - Europe.adatum.com
  - Na.adatum.com
  - Asia.adatum.com
- Vous devez planifier un effort de restructuration de forêt pour la forêt adatum.com :
  - Migrer les objets de domaine existants d'adatum.com dans europe.adatum.com. Laisser les objets de niveau forêt nécessaires dans le domaine adatum.com racine de la forêt.
  - Déplacer des objets du domaine na.treyresearch.net dans na.adatum.com.
  - Déplacer des objets du domaine asia.treyresearch.net dans asia.adatum.com

**Commentaire :**

Dans ce scénario, votre objectif à court terme est d'intégrer les environnements AD DS dès que possible afin que les employés des deux entreprises puissent collaborer immédiatement. La façon la plus rapide et la plus facile pour vous d'accomplir ceci serait de créer une approbation de forêt entre les deux forêts. Bien que cette approche pourrait fonctionner pour les besoins à court terme et à long terme de A. Datum, le leadership a exprimé que Trey Research fait partie de leur stratégie à long terme. En outre, ils ont manifesté le désir d'adopter un modèle opérationnel régional similaires à ce que Trey Research utilise déjà. Compte tenu de ces deux éléments d'information clés, votre plan à long terme pour AD DS devrait être de restructurer la forêt d'adatum.com et de créer des domaines enfant pour chaque région dans laquelle A. Datum opérera.

Si l'acquisition de Trey Research était simplement un objectif à court terme et la cession future de Trey Research est une possibilité probable, vous pouvez décider de mettre uniquement en œuvre une approbation de forêt afin de séparer Trey Research facilement à l'avenir.

Si un modèle opérationnel régional n'est pas obligatoire, vous pouvez décider de maintenir une forêt unique, un modèle de domaine unique et de migrer tous les objets treyresearch.net dans le domaine adatum.com racine de la forêt.

## Problèmes courants et conseils de dépannage

| Problème courant | Conseil pour la résolution du problème |
|---|---|
| Vous recevez des messages d'erreur tels que :<br>• Échec de la recherche DNS ;<br>• Serveur RPC indisponible ;<br>• Le domaine n'existe pas ;<br>• Le contrôleur de domaine est introuvable. | Habituellement, ces erreurs sont dues à un échec de recherche d'enregistrements DNS ou un pare-feu mal configuré. Veillez à ce qu'il y ait au moins deux serveurs DNS opérationnels disponibles sur le réseau. Assurez-vous que chaque ordinateur dispose d'au moins deux serveurs DNS configurés dans le réseau.<br>Vérifiez que les serveurs DNS sont en mesure de résoudre de manière satisfaisante les requêtes pour les enregistrements DNS en dehors de leur domaine DNS (par exemple, les adresses Internet). Utilisez divers outils de dépannage tels que nslookup, dnslint, DCdiag, netdiag, repadmin, replmon, et l'observateur d'événements. |
| L'utilisateur ne peut être authentifié pour accéder aux ressources sur un autre domaine AD DS ou Kerberos. | Utilisez la console **Domaines et approbations Active Directory**, (Domain.msc), ou l'outil en ligne de commande Netdom pour valider les relations d'approbation. Si nécessaire, réinitialisez le mot de passe d'approbation. Assurez-vous que les relations d'approbation sont configurées dans la bonne direction.<br>Vérifiez que tous les contrôleurs de domaine AD DS ont enregistré tous les enregistrements SRV corrects dans la base de données DNS. (Vous pouvez redémarrer le service Accès réseau sur un contrôleur de domaine AD DS pour le forcer à réenregistrer les enregistrements SRV dans la base de données DNS.) |

# Questions et réponses sur les ateliers pratiques

## Atelier pratique : Domaine et gestion des approbations dans AD DS

## Questions et réponses

**Question :** Lors de la création du lien de confiance entre Adatum.com et TreyResearch.net, des zones de stub DNS ont été créés pour permettre la résolution de nom entre les deux forêts. Quelle alternative auriez-vous pu utiliser à la place d'une zone de stub DNS ?

**Réponse :** Au lieu de créer des zones de stub DNS dans chaque forêt, vous auriez également pu avoir utilisé un redirecteur conditionnel. Un DNS secondaire aurait également accompli la résolution de noms requis, mais il entraînerait une réplication inutile.

**Question :** Lorsque vous créez une approbation de forêt, pourquoi voudriez-vous créer une approbation sélective au lieu d'une approbation totale ?

**Réponse :** En utilisant l'authentification sélective lors de la configuration d'une approbation, vous avez plus de contrôle sur les ressources auxquelles les utilisateurs du domaine / de la forêt approuvés sont autorisés à s'authentifier. Si vous n'utilisez l'authentification sélective, les utilisateurs de la forêt du domaine approuvée peuvent s'authentifier à toutes les ressources.

# Module 4

## Implémentation, administration des sites AD DS et réplication

### Sommaire :

Leçon 1

# Vue d’ensemble de la réplication AD DS

## Sommaire :

## Questions et réponses

**Question :** Pourquoi la réplication est importante dans le catalogue global ?

**Réponse :** La partition de configuration contient des informations de catalogue global qui sont répliquées sur tous les contrôleurs de domaine désignés comme serveurs de catalogue global.

## Comment fonctionne la réplication AD DS au sein d'un site ?

**Question :** Décrivez les circonstances qui se produisent lorsque vous créez manuellement un objet de connexion entre les contrôleurs de domaine dans un site.

**Réponse :** 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 supprimera 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.

Leçon 2

# Configurer les sites AD DS

## Sommaire :

## Questions et réponses

**Question :** Lequel des éléments suivants n'est pas à considérer pour la mise en œuvre des sites AD DS ?

( ) Réduction de l'utilisation de la bande passante entre les sites du réseau

( ) Application des paramètres de Stratégie de groupe à un seul endroit dans votre organisation

( ) Contrôler avec l'utilisation des ordinateurs clients du contrôleur de domaine pour l'authentification

( ) Création d'un site de sauvegarde pour la récupération d'urgence

( ) Contrôler l'accès aux applications et services pour un certain segment de votre réseau

**Réponse :**

( ) Réduction de l'utilisation de la bande passante entre les sites du réseau

( ) Application des paramètres de Stratégie de groupe à un seul endroit dans votre organisation

( ) Contrôler avec l'utilisation des ordinateurs clients du contrôleur de domaine pour l'authentification

(√) Création d'un site de sauvegarde pour la récupération d'urgence

( ) Contrôler l'accès aux applications et services pour un certain segment de votre réseau

## Ressources

## Comment les ordinateurs clients localisent les contrôleurs de domaine au sein des sites

**Lectures supplémentaires :** Pour plus d'informations, consultez Recherche d'un contrôleur de domaine dans le site le plus proche : http://aka.ms/Cjpzdd

## Démonstration : Configurer les sites AD DS

### Procédures de démonstration

1. Sur **LON-DC1**, cliquez sur **Démarrer**, puis cliquez sur **Gestionnaire de serveurs**.
2. Dans le **Gestionnaire de serveurs**, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
3. Dans la console **Sites et services Active Directory**, développez **Sites**, puis cliquez sur **Nom-Premier-Site-Par défaut**.
4. Clic-droit sur **Nom-Premier-Site-Par défaut**, cliquez sur **Renommer**, saisissez **LondonHQ**, puis appuyez sur Entrée.
5. Dans le volet de navigation, cliquez avec le bouton droit sur **Sites**, puis cliquez sur **Nouveau Site**.
6. Dans la boîte de dialogue **Nouvel objet - Site**, dans la zone de texte **Nom**, tapez **Toronto**.
7. Sélectionnez **DEFAULTIPSITELINK**, puis cliquez sur **OK**.
8. Dans la boîte de dialogue **Active Directory Domain Services,** cliquez sur **OK**.
9. Dans le volet de navigation, cliquez avec le bouton droit sur **Sous-réseaux**, puis cliquez sur **Nouveau sous-réseau**.
10. Dans la boîte de dialogue **Nouvel objet - Sous-réseau**, dans la zone de texte **Préfixe**, tapez **172.16.0.0/24**.
11. Sous **Sélectionner un objet de site pour ce préfixe**, cliquez sur **LondonHQ**, puis ensuite sur **OK**.

12. Dans le volet de navigation, cliquez avec le bouton droit sur **Sous-réseaux**, puis cliquez sur **Nouveau sous-réseau**.
13. Dans la boîte de dialogue **Nouvel objet - Sous-réseau**, dans la zone de texte **Préfixe**, tapez **172.16.1.0/24**.
14. Sous **Sélectionnez un objet de site pour ce préfixe**, cliquez sur **Toronto**, puis cliquez sur **OK**.
15. Dans le volet de navigation, développez **LondonHQ**, puis **Serveurs**.
16. Cliquez avec le bouton droit sur **TOR-DC1**, puis sur **Déplacer**.
17. Dans la boîte de dialogue **Déplacer un serveur**, sélectionnez **Toronto**, puis cliquez sur **OK**.
18. Dans le volet de navigation, développez **Toronto**, puis **Serveurs**.
19. Vérifiez que **TOR-DC1** est maintenant situé dans le site **Toronto**.

Leçon 3

# Configuration et surveillance de la réplication AD DS

## Sommaire :

## Questions et réponses

**Question :** La durée la plus courte de réplication que vous pouvez configurer avec la planification de la réplication de site est de 15 minutes.

( ) Vrai

( ) Faux

**Réponse :**

(√) Vrai

( ) Faux

## Ressources

## Outils pour le suivi et la gestion de la réplication

 **Lectures supplémentaires :** Pour plus d'informations, reportez-vous à Applets de commande d'administration AD DS dans Windows PowerShell : http://aka.ms/ltjgof

## Démonstration : Configuration de la réplication inter-sites AD DS

### Procédures de démonstration

1. Sur **TOR-DC1**, dans **Gestionnaire de serveurs**, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
2. Dans la console **Sites et services Active Directory**, développez **Sites**, puis **Transports inter-sites**.
3. Cliquez sur **IP**, clic-droit sur **DEFAULTIPSITELINK**, cliquez sur **Renommer**, saisissez **LON-TOR**, puis appuyez sur Entrée.
4. Cliquez avec le bouton droit sur **LON-TOR**, puis cliquez sur **Propriétés**. Expliquez les options **Coût**, **Réplication toutes les :** et **Modifier la planification**.
5. Dans la boîte de dialogue **Propriétés LON-TOR**, dans la zone de sélection numérique **Réplication toutes les**, configurez la valeur à **60** minutes.
6. Cliquez sur **Modifier la planification**.
7. Mettez en surbrillance la plage de **Lundi 12 heures** à **Vendredi 16 heures**, comme suit :
8. Cliquez sur la vignette **Lundi à 12h00**, appuyez et maintenez le bouton de la souris, puis faites glisser le curseur vers la vignette **Vendredi à 16:00**.
9. Cliquez sur **Réplication Non Disponible**, puis cliquez sur **OK**.
10. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés LON-TOR**.
    - Dans le volet de **navigation**, cliquez avec le bouton droit sur **IP**, puis sur **Propriétés**.
11. Dans la boîte de dialogue **Propriétés IP**, soulignez et expliquez l'option **Relier tous les liens de sites**.
12. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés IP**.

# Révision du module et points importants 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.
- Veillez à ce que tous les sites aient des sous-réseaux associés appropriés.
- Lorsque vous configurez les planifications de réplication pour la réplication inter-site, ne pas mettre en place de longs intervalles sans réplication.
- Évitez d'utiliser le protocole de transfert de courrier simple (SMTP) en tant que protocole pour la réplication.

## Questions de contrôle des acquis

**Question :** Dans une entreprise multisite, pourquoi est-il important que tous les sous-réseaux soient identifiés et associés à un site ?

**Réponse :** Vous pouvez renforcer l'efficacité du processus de localisation des contrôleurs de domaine et d'autres services en renvoyant les clients vers le site approprié en fonction de l'adresse IP du client et de la définition des sous-réseaux. Si un client possède une adresse IP qui n'appartient pas à un site, le client va interroger tous les contrôleurs de domaine du domaine. Cette stratégie n'est pas efficace. En fait, un seul client peut effectuer des actions contre les contrôleurs de domaine de différents sites, ce qui peut conduire à des résultats inattendus si ces changements ne sont pas encore répliqués. Par conséquent, il est essentiel que chaque client sache dans quel site il se trouve ; vous pouvez y parvenir en faisant en sorte que les contrôleurs de domaine puissent identifier l'emplacement du site d'un client.

**Question :** Quels sont les avantages et les inconvénients de la réduction de l'intervalle de réplication intersite ?

**Réponse :** La réduction de l'intervalle de réplication inter-site améliore la convergence. Les modifications apportées à un site se répliquent plus rapidement à d'autres sites. Il y a en fait peu d'inconvénients, voire aucun. Si l'on considère que les mêmes changements doivent se répliquer, que le délai d'attente à la reproduction soit de 15 minutes ou 3 heures, il s'agit essentiellement d'une question de minutage de réplication plutôt que de quantité de réplication. Cependant, dans certaines situations extrêmes, permettre à un plus petit nombre de changements de se produire plus fréquemment pourrait être moins judicieux que de permettre à un grand nombre de modifications de se répliquer moins fréquemment.

**Question :** Quelle est l'utilité d'un serveur tête de pont ?

**Réponse :** Un serveur tête de pont est responsable de toute les réplications dans et hors d'un site. Au lieu de répliquer tous les contrôleurs de domaine d'un site avec tous les contrôleurs de domaine dans un autre site, vous pouvez utiliser les serveurs tête de pont pour gérer la réplication inter-site. Toutefois, si un certain serveur tête de pont n'est pas spécifiquement nécessaire pour des raisons de performance ou d'autres facteurs, une meilleure pratique consiste à laisser le ISTG choisir les serveurs têtes de pont parmi le bassin de contrôleurs de domaine du site.

## Outils

Le tableau suivant répertorie les outils référencés par ce module.

| 1. Outil | 2. Utilisation | 3. Emplacement |
|---|---|---|
| Console **Sites et services Active Directory** | Crée des sites, des sous-réseaux, des liens de site, des pontages de lien de site, une réplication de force et relance le vérificateur de cohérence. | Outils **Gestionnaire de serveur** |
| **Repadmin.exe** | Indique l'état de la réplication sur chaque contrôleur de domaine, crée la topologie de réplication et la réplication de force, et affiche les niveaux de détail y compris les 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 de 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 basées 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 spécifié. | Windows PowerShell |
| **Get-ADReplicationSiteLink** | Un lien spécifique du site Active Directory ou un ensemble de liens de site selon un filtre spécifié. | 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 spécifié. | Windows PowerShell |
| **Get-ADReplicationSubnet** | Un sous-réseau Active Directory spécifique ou un ensemble de sous-réseaux Active Directory basé sur un filtre spécifié. | Windows PowerShell |

## 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 au sein de son site. | • Vérifiez si tous les enregistrements SRV pour le contrôleur de domaine sont présents dans le DNS.<br>• Vérifiez si le contrôleur de domaine a une adresse IP à partir du sous-réseau qui est associée à ce site.<br>• Vérifiez que le client est un membre de domaine et que le réglage de l'heure est correct. |
| La réplication entre les sites ne fonctionne pas. | • Vérifiez que la configuration des liens de site est correcte.<br>• Vérifiez la planification de réplication.<br>• Vérifiez si le pare-feu entre les sites autorise le trafic pour la réplication AD DS. Utilisez **repadmin /bind**. |
| La réplication entre deux contrôleurs de domaine dans le même site ne fonctionne pas. | • Vérifiez si les deux contrôleurs de domaine apparaissent dans un même site.<br>• Vérifiez si AD DS fonctionne correctement sur les contrôleurs de domaine.<br>• Vérifiez la communication de réseau et si le réglage de l'heure sur chaque serveur est valide. |

# Questions et réponses sur les laboratoires

## Atelier pratique : Mise en œuvre des sites AD DS et réplication

## Questions et réponses

**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** ?

> **Réponse :** Vous aurez à configurer ce nouveau contrôleur de domaine comme le serveur tête de pont préféré pour le site **LondonHQ**.

**Question :** Vous avez ajouté un nouveau contrôleur de domaine nommé **LON-DC2** au site **LondonHQ**. Quelles partitions AD DS seront modifiées en conséquence ?

> **Réponse :** Il est probable que toutes les partitions seront modifiées à l'exception de la partition de schéma. Vous ajoutez le nouveau contrôleur de domaine à la fois à la partition de domaine et à la partition de configuration pour garantir la configuration correcte de la réplication AD DS. Si vous utilisez DNS intégré à Active Directory, alors les enregistrements du contrôleur de domaine se mettront également à jour dans les partitions d'application de DNS.

**Question :** Dans le laboratoire, vous avez créé un lien de site distinct pour les sites **Toronto** et **Site de test**. Que pourriez-vous aussi avoir à faire pour veiller à ce que **LondonHQ** ne crée pas automatiquement un objet de connexion directement avec le site **TestSite** ?

> **Réponse :** Vous pourriez aussi avoir à désactiver automatiquement le lien du site pont afin de désactiver la transitivité du site entre **LondonHQ**, **Toronto** et **TestSite**.

# Module 5

## Mise en place d'une stratégie de groupe

### Sommaire :

Leçon 1

# Introduction d’une stratégie de groupe

## Sommaire :

## Questions et réponses

**Classez l'activité**

**Question :** Catégorisez 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 | Place |
| 6 | Groupe |
| 7 | Conteneur utilisateurs |
| 8 | Conteneur ordinateurs |

| Catégorie 1 | | Catégorie 2 |
|---|---|---|
| Peut relier les GPO à | | Ne peut pas relier les GPO à |
| | | |

**Réponse :**

| Catégorie 1 | | Catégorie 2 |
|---|---|---|
| Peut relier les GPO à | | Ne peut pas relier les GPO à |
| Domaine<br>Unité organisationnelle<br>Place | | Utilisateur<br>Ordinateur<br>Groupe<br>Conteneur Utilisateurs<br>Conteneur Ordinateurs |

# Démonstration : Exploration des outils et consoles de stratégie de groupe

## Procédure de démonstration

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Si nécessaire, basculez vers la fenêtre **Gestion des stratégies de groupe**.
3. Dans l'Éditeur de gestion des stratégies de groupe, dans le volet de navigation, développez **Forêt : Adatum.com**, développez **Domaines**, **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 **Nouvel objet GPO**, saisissez **Désactiver le Panneau** de configuration, puis cliquez sur **OK**.
6. Dans le volet d'informations, cliquez avec le bouton droit sur **Désactiver le panneau de configuration**, puis cliquez sur **Modifier**.
7. Dans l'Éditeur gestion de stratégie de groupe, dans le volet de navigation, sous **Configuration utilisateur**, développez **Politiques**, développez **Modèles d'administration**, puis cliquez sur **Panneau de contrôle**.
8. Dans le volet d'informations, double-cliquez sur Interdire l'accès au **Panneau de configuration et aux paramètres du PC**.
9. Dans la boîte de dialogue **Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC**, affichez les trois valeurs possibles pour une mise en **Modèles d'administration**, affichez la **Prise en charge sur** texte, puis affichez le texte **Aidez-moi**.
10. Cliquez sur **Activé**. Dans la zone de texte **Commentaire**, tapez **Activé** <*Date*> **par** <*votre nom*>. Remplacez la <*Date*> avec la date d'aujourd'hui et <*votre nom*> avec votre nom, puis cliquez sur **OK**.
11. Dans le volet de navigation, sous **Configuration utilisateur**, développez **Préférences** et affichez les différentes catégories sous **Politiques** et **Préférences**.
12. Fermez la fenêtre de **l'Éditeur de gestion des stratégies de groupe**.
13. Dans la fenêtre **Gestion des stratégies de groupe**, dans le volet de navigation, développez **Objets de stratégie de groupe**, puis cliquez sur **Désactiver le Panneau de contrôle**.
14. Dans le volet d'informations, affichez les onglets **Étendue**, **Détails** et **Paramètres**.
15. Dans le volet de navigation, cliquez avec le bouton droit sur le domaine **Adatum.com**, puis cliquez sur **Associer un GPO existant**.
16. Dans la boîte de dialogue **Sélectionner objet GPO**, cliquez sur **Désactiver le Panneau de configuration**, puis cliquez sur **OK**.
17. Dans le volet de navigation, cliquez sur **Adatum.com**.
18. Dans le volet d'informations, affichez les onglets **Objets de stratégie de groupe associés** et **Héritage des stratégies de groupe**.
19. Cliquez **Démarrer**, puis cliquez sur **Windows PowerShell**.
20. Dans la fenêtre **Administrateur** : Dans la fenêtre **Windows PowerShell**, saisissez la commande suivante, puis appuyez sur Entrée :

```
gpupdate
```

21. Vérifiez que les paramètres de l'ordinateur et de l'utilisateur ont été mis à jour avec succès.

22. À l'invite de commande Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
gpresult / r
```

23. Dans la sortie de la commande, dans la section des **Paramètres utilisateur**, dans la liste **GPO appliqués**, vérifiez que le GPO **Désactiver le Panneau de configuration** est répertorié.
24. Fermez la fenêtre **Windows PowerShell**.

Leçon 2

# Mise en œuvre et administration des GPO

## Sommaire :

## Questions et réponses

**Question :** Quels sont les groupes AD DS dont les membres peuvent des GPO par défaut ? (Sélectionnez trois réponses)

( ) Administrateurs du domaine

( ) Opérateurs de compte

( ) Administrateurs de l'entreprise

( ) Administrateurs de GPO

( ) Propriétaires créateurs de la stratégie de groupe

**Réponse :**

(√) Administrateurs du domaine

( ) Opérateurs de compte

(√) Administrateurs de l'entreprise

( ) Administrateurs de GPO

(√) Propriétaires créateurs de la stratégie de groupe

**Commentaire :**

Le groupe Administrateurs de GPO n'existe pas. Les groupes Administrateurs du domaine et Administrateurs de l'entreprise peuvent effectuer toutes les tâches administratives dans le domaine, y compris créer des GPO. Les propriétaires créateurs de la stratégie de groupe constituent le seul groupe auquel vous pouvez ajouter des utilisateurs si vous souhaitez qu'ils puissent créer des GPO sans obtenir des droits d'administration sur le domaine ou la forêt. Les opérateurs de compte n'ont aucune autorisation par rapport à la stratégie de groupe. Ils ne peuvent que gérer les utilisateurs, les ordinateurs et les groupes dans AD DS.

## Démonstration : Délégation de l'administration de la stratégie de groupe

### Procédure de démonstration

### Faire d'Aurore un administrateur local sur LON-SVR1

1. Basculez vers **LON-DC1**.
2. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
3. Dans la fenêtre **Explorateur de fichiers**, dans le volet de navigation, développez **AllFiles (E:)**, développez **Labfiles**, puis cliquez sur **Mod05**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur le fichier **Set-LocalAdmin.ps1**, puis cliquez sur **Exécuter avec PowerShell**. Tapez **O**, si vous y êtes invité, puis appuyez sur Entrée.

### Vérifier les autorisations des utilisateurs avant délégation

1. Basculez vers **LON-SVR1**.
2. Connectez-vous en tant qu'**Adatum\Aurore** avec le mot de passe **Pa$$w0rd**.
3. Dans le **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
4. Dans l'**Assistant Ajouter des rôles et des fonctionnalités**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.

7. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner des fonctionnalités**, activez la case à cocher **Gestion des stratégies de groupe**, puis cliquez sur **Suivant**.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Une fois l'installation terminée, cliquez sur **Fermer**.
11. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
12. Si nécessaire, basculez vers la fenêtre **Gestion des stratégies de groupe**.
13. Dans **Gestion de stratégie de groupe**, développez **Forêt : Adatum.com**, développez **Domaines**, **Adatum.com**, puis cliquez sur **Objets de stratégie de groupe (GPO)**.
14. Cliquez avec le bouton droit sur **Objets de stratégie de groupe (GPO)**. Vous remarquerez que l'élément **Nouveau** est grisé parce qu'Aurore ne dispose pas des autorisations pour créer des GPO.
15. Dans le volet de navigation, cliquez avec le bouton droit sur le domaine **Adatum.com**. Vous remarquerez que l'élément de menu **Associer un GPO existant** est grisée parce qu'Aurore ne dispose pas des autorisations pour lier les GPO au domaine.
16. Dans le volet de navigation, cliquez avec le bouton droit sur l'UO **IT**, puis notez cet élément de menu **Associer un GPO existant** est grisé parce qu'Aurore ne dispose pas non plus des autorisations pour relier les GPO à l'UO **IT**.
17. Cliquez **Démarrer**, puis cliquez sur **Windows PowerShell**.
18. Dans la fenêtre **Windows PowerShell**, saisissez la commande suivante et appuyez sur Entrée :

```
GPResult / r
```

19. Dans la sortie de la commande, vous remarquerez que seuls les paramètres **Utilisateur** sont affichés parce qu'Aurore n'est pas autorisée à voir les résultats de stratégie de groupe pour les paramètres de l'ordinateur.

## Déléguer des autorisations

1. Sur **LON-DC1**, basculez vers la fenêtre **Gestion des stratégies de groupe**.
2. Dans **Gestion des stratégies de groupe**, Dans le volet de navigation, cliquez sur le conteneur **Objets de stratégie de groupe**, puis dans le volet d'informations, cliquez sur l'onglet **Délégation**.
3. Cliquez sur **Ajouter**. Dans la boîte de dialogue **Sélectionner un utilisateur**, **un ordinateur ou un groupe**, tapez **Aurore**, cliquez sur **Vérifier** les noms, puis cliquez sur **OK**..
4. Dans le volet de navigation, cliquez sur l'UO **IT**, puis dans le volet d'informations, cliquez sur l'onglet **Délégation**.
5. Dans la liste déroulante **Autorisation**, **Lien GPO** est sélectionné, puis cliquez sur **Ajouter**.
6. Dans boîte de dialogue **Sélectionnez Utilisateur, Ordinateur ou Groupe**, tapez **Aurore**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
7. Dans la boîte de dialogue **Ajouter un utilisateur** ou un groupe, cliquez sur **OK**.
8. Dans le volet de navigation, cliquez sur le domaine **Adatum.com**, puis dans le volet d'informations, cliquez sur l'onglet **Délégation**.
9. Dans la liste déroulante **Autorisation**, sélectionnez **Lire les données des résultats de stratégie de groupe**, puis cliquez sur **Ajouter**.

10. Dans la boîte de dialogue **Sélectionner un utilisateur, un ordinateur ou un groupe**, tapez **Utilisateurs authentifiés**, cliquez sur **Vérifier les noms**, puis sur **OK**.
11. Dans la boîte de dialogue **Ajouter un utilisateur ou un groupe**, cliquez sur **OK**.

## Vérifier les autorisations après la délégation

1. Basculez vers **LON-SVR1**.
2. Basculez vers la **Gestion des stratégies de groupe**.
3. Dans la fenêtre **Gestion des stratégies de groupe**, cliquez, puis cliquez avec le bouton droit sur le domaine **Adatum.com**, puis cliquez sur **Actualiser**.
4. Dans le volet de navigation, cliquez avec le bouton droit sur **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
5. Dans la boîte de dialogue **Nouvel objet GPO**, dans la zone de texte **Nom**, tapez **GPO d'Aurore**, puis cliquez sur **OK**.
6. Dans le volet de navigation, faites un clic droit sur **Adatum.com**. Vous remarquerez que **Associer un GPO existant** est encore grisé.
7. Dans le volet de navigation, cliquez avec le bouton droit sur **IT**, puis cliquez sur **Associer un GPO existant**.
8. Dans la boîte de dialogue **Sélectionner un objet** de stratégie de groupe, cliquez sur **GPO d'Aurore**, puis cliquez sur **OK**.
9. Basculez vers la fenêtre **Windows PowerShell**.
10. Dans la fenêtre **Windows PowerShell**, entrez la commande suivante et appuyez sur Entrée.

```
GPResult /r
```

11. Dans la sortie de la commande, notez que les deux paramètres **Ordinateur** et l'**Utilisateur** sont affichés.

Leçon 3

# Cadre et traitement de la stratégie de groupe

## Sommaire :

## Questions et réponses

**Question :** Il est possible de relier plus d'un filtre WMI à un GPO.

( ) Vrai

( ) Faux

**Réponse :**

( ) Vrai

(√) Faux

**Commentaire :**

Même s'il vous est impossible de relier plus d'un filtre WMI à un GPO, vous pouvez créer des filtres WMI avancés qui incluent plus d'une requête WMI.

**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.)

( ) Filtres WMI

( ) Filtrage de la sécurité

( ) Bloquer l'héritage

( ) Police

( ) Traitement en boucle

**Réponse :**

(√) Filtres WMI

(√) Filtrage de la sécurité

(√) Bloquer l'héritage

(√) Police

(√) Traitement en boucle

**Commentaire :**

Toutes les options sont des options viables pour changer la façon dont la stratégie de groupe est normalement appliquée. Vous devez utiliser les différentes options avec parcimonie, car le dépannage devient plus difficile lorsque vous utilisez ces options.

## Démonstration : Lier des GPO

### Procédure de démonstration

### Créer et éditer deux GPO

1. Sur **LON-DC1**, si nécessaire, ouvrez **Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
3. Dans la fenêtre **Gestion de stratégie de groupe**, développez **Forêt : Adatum.com**, **Domaines** et **Adatum.com**, cliquez avec le bouton droit sur le conteneur **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
4. Dans la boîte de dialogue **Nouvel objet GPO**, saisissez **Supprimer la commande Exécuter** dans la zone de texte **Nom**, puis validez avec **OK**.

5. Dans la fenêtre **Gestion des stratégies de groupe**, cliquez avec le bouton droit sur le conteneur **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
6. Dans la boîte de dialogue **Nouvel objet GPO**, saisissez **Ne pas supprimer la commande Exécuter** dans la zone de texte **Nom**, puis cliquez sur **OK**.
7. Développez **Objets de stratégie de groupe**, cliquez avec le bouton droit sur le GPO **Supprimer la commande Exécuter**, puis cliquez sur **Modifier**.
8. Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, sous **Configuration utilisateur**, développez **Stratégies** puis **Modèles d'administration**, cliquez sur le **menu Démarrer et la Barre des tâches**, puis double-cliquez sur **Supprimer le menu Exécuter du menu Démarrer**.
9. Dans la fenêtre **Supprimer le menu Exécuter du menu Démarrer**, cliquez sur **Activé**, puis sur **OK**.
10. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.
11. Dans **Objets de stratégie de groupe**, cliquez avec le bouton droit sur le GPO Ne pas **supprimer la commande Exécuter**, puis cliquez sur **Modifier**.
12. Dans la fenêtre **Éditeur de gestion des stratégies de groupe**, sous **Configuration utilisateur**, développez **Stratégies**, développez **Modèles d'administration**, cliquez sur menu **Démarrer et Barre des tâches**, puis double-cliquez sur **Supprimer le menu Exécuter du menu Démarrer**.
13. Dans la fenêtre **Supprimer le menu Exécuter du menu Démarrer**, cliquez sur **Désactivé**, puis cliquez sur **OK**. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.

## Lier les GPO à des emplacements différents

1. Dans la fenêtre **Gestion des stratégies de groupe**, cliquez avec le bouton droit sur le nœud de domaine **Adatum.com** dans le volet de navigation, puis cliquez sur **Associer un GPO existant**.
2. Dans la fenêtre **Sélectionner un GPO**, cliquez sur **Supprimer la commande Exécuter**, puis cliquez sur **OK**. Maintenant le GPO **Supprimer la commande Exécuter** est lié au domaine Adatum.com.
3. Cliquez et faites glisser le GPO **Ne pas supprimer la commande Exécuter** au-dessus de l'unité d'organisation **Informatique.**
4. Dans la fenêtre **Gestion des stratégies de groupe**, cliquez sur **OK** pour associer le GPO.
5. Cliquez sur l'unité d'organisation **Informatique** dans le volet de navigation, puis cliquez sur l'onglet **Héritage de stratégie de groupe** dans le volet d'informations. L'onglet **Héritage de stratégie de groupe** montre l'ordre de priorité pour les GPO.

## Désactiver un lien GPO

- Dans le volet de gauche, cliquez avec le bouton droit sur le lien **Supprimer la commande Exécuter** qui est répertorié sous **Adatum.com**, puis cliquez sur **Lien activé** pour désactiver la case à cocher. Actualisez le volet **Héritage des stratégies de groupe** pour l'UO technologie de l'information (**IT**), puis notez les résultats dans le volet d'informations. Le GPO **Supprimer la commande Exécuter** n'est plus répertorié.

## Supprimer un lien GPO

1. Dans le volet de gauche, développez l'UO **IT**, cliquez avec le bouton droit sur le lien **Ne pas supprimer la commande Exécuter**, puis cliquez sur **Effacer**. Cliquez sur **OK** dans la fenêtre indépendante.
2. Cliquez sur l'UO **IT** dans le volet gauche, puis cliquez sur l'onglet **Héritage des stratégies de groupe** dans le volet d'informations. Vérifiez la suppression de **Ne pas supprimer la commande Exécuter** et l'absence des GPO **Supprimer la commande Exécuter**.

3. Dans le volet de gauche, cliquez avec le bouton droit sur le GPO **Supprimer la commande Exécuter** qui est répertorié sous **Adatum.com**, puis cliquez sur **Lien activé** pour réactiver le lien. Actualisez la fenêtre **Héritage des stratégies de groupe** pour l'UO **IT**, puis notez les résultats dans le volet de droite.
4. Fermez **Gestion de stratégie de groupe**.

## Démonstration : Filtrage de l'application de la stratégie de groupe

### Procédure de démonstration

### Créer un GPO et le relier à l'unité d'organisation Service informatique

1. Sur **LON-DC1**, dans le **Gestionnaire de serveurs**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la fenêtre **Gestion de stratégie de groupe**, développez **Forêt : Adatum.com**, développez successivement **Domaines**, **Adatum.com**, puis cliquez sur l'unité d'organisation **Informatique**.
3. Cliquez avec le bouton droit sur **Informatique**, puis cliquez sur **Créer un GPO dans ce domaine et le lier ici**.
4. Dans la fenêtre **Nouvel objet GPO**, saisissez **Supprimer le menu Aide** dans la zone de texte **Nom**, puis cliquez sur **OK**.
5. Dans la fenêtre **Gestion des stratégies de groupe**, développez **Objets de stratégie de groupe**, cliquez avec le bouton droit sur le GPO **Supprimer le menu Aide**, puis cliquez sur **Modifier**.
6. Dans la fenêtre **Éditeur de gestion des stratégies de groupe**, sous **Configuration utilisateur**, développez **Stratégies**, développez **Modèles d'administration**, cliquez sur **Menu Démarrer et Barre des tâches**, puis double-cliquez sur **Supprimer le menu Aide à partir du menu Démarrer**.
7. Dans la fenêtre **Supprimer le menu Exécuter du menu Démarrer**, cliquez sur **Activé**, puis cliquez sur **OK**.
8. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.

### Filtrer l'application de stratégie de groupe en utilisant le filtrage de groupe de sécurité

1. Développez **IT**, puis cliquez sur le lien GPO **Supprimer le menu Aide**.
2. Dans la boîte de message **GPMC**, cliquez sur **OK**.
3. Dans le volet d'informations, sous **Filtrage de sécurité**, cliquez sur **Utilisateurs authentifiés**, puis cliquez sur **Supprimer**.
4. Dans la boîte de dialogue de confirmation, cliquez sur **OK**.
5. Dans le volet d'informations, sous **Sécurité Filtrage**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Sélectionner des utilisateurs**, des ordinateurs ou des groupes, dans la zone de texte **Entrer les noms des objets à sélectionner (exemples) :** entrez **Aurore Dupont** et cliquez ensuite sur **OK**.

### Filtrer l'application de stratégie de groupe en utilisant le filtrage WMI

1. Dans la fenêtre **Gestion des stratégies de groupe**, cliquez avec le bouton droit sur **Filtres WMI**, puis cliquez sur **Nouveau**.
2. Dans la boîte de dialogue **Nouveau filtre WMI**, dans la zone de texte **Nom**, tapez **Filtre Version OS**.
3. Dans le volet **Requêtes**, cliquez sur **Ajouter**.

4. Dans la boîte de dialogue **Requête WMI**, dans la zone de texte **Requête**, tapez la requête suivante, puis cliquez sur **OK** :

```
Sélectionner * dans Win32_OperatingSystem où l'on trouve des versions comme « 6.% »
```

5. Si une boîte de dialogue **Avertissement** s'ouvre, cliquez sur **OK**.
6. Dans la boîte de dialogue **Nouveau filtre WMI**, cliquez sur **Enregistrer**.
7. Cliquez avec le bouton droit sur le dossier **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
8. Dans la fenêtre **Nouvel objet GPO**, saisissez **Mises à jour des logiciels** dans la zone de texte **Nom**, puis cliquez sur **OK**.
9. Développez **Objets de stratégie de groupe**, puis cliquez sur le GPO **Mises à jour des logiciels**.
10. Dans le volet d'informations, sous **filtrage WMI**, dans la liste **Ce GPO est associé au filtre WMI suivant**, sélectionnez **Filtre de version SE**.
11. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.
12. Fermez la **Gestion des stratégies de groupe**.

Leçon 4

# Résolution de problèmes de l'application des GPO

## Sommaire :

## Ressources

## Examen des journaux d'événements de stratégie de groupe

**Lectures supplémentaires :** Pour télécharger le journal de stratégie de groupe, aller à : http://aka.ms/E8oi7g

## Démonstration : Exécution d'une analyse par simulation avec l'Assistant Modélisation de stratégie de groupe

### Procédure de démonstration

### Utiliser GPResult.exe pour créer un rapport

1. Dans **LON-DC1**, cliquez sur **Démarrer**, saisissez **cmd**, puis appuyez sur Entrée.
2. Dans la fenêtre **Administrateur : C:\Windows\System32\cmd.exe**, saisissez **cd** \, puis appuyez sur Entrée.
3. Entrez la commande suivante, puis appuyez sur Entrée :

```
GPResult / r
```

4. Examinez le résultat dans la fenêtre **Invite de commandes**.
5. Entrez la commande suivante, puis appuyez sur Entrée :

```
GPResult /h results.html
```

6. Fermez la fenêtre d'**invite de commandes**.
7. Cliquez sur **Démarrer**, sur **Toutes les applis**, sur **Accessoires Windows** et enfin sur **Internet Explorer**.
8. Dans la fenêtre **Internet Explorer**, appuyez sur la touche **Alt**, cliquez sur Fichier, puis cliquez sur **Ouvrir**.
9. Dans la boîte de dialogue **Nouvel** objet GPO, dans la zone de texte **Ouvrir**, tapez **C:\results.html**, puis cliquez sur **OK**.
10. Dans le message d'avertissement, cliquez sur **Autoriser le contenu bloqué**.
11. Vérifiez les résultats du rapport.
12. Fermez Microsoft Internet Explorer.

### Utiliser l'Assistant de rapports de stratégie de groupe pour créer un rapport

1. Ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la fenêtre **Gestion des stratégies de groupe**, dans le volet de navigation, faites un clic droit sur **Résultats de la stratégie de groupe**, puis cliquez sur **Assistant Résultats de stratégie de groupe**.
3. Dans l'**Assistant Résultats de stratégie de groupe**, cliquez sur **Suivant**.
4. Sur la page **Sélection de l'ordinateur**, cliquez sur **Suivant**.
5. Sur la page **Sélection de l'utilisateur**, cliquez sur **Suivant**.
6. Sur la page **Aperçu des sélections**, cliquez sur **Suivant**.
7. Sur la page **Fin de l'Assistant Résultats de stratégie de groupe**, cliquez sur **Terminer**.

8. Examinez les résultats de stratégie de groupe.
9. Développez **Résultats de la stratégie de groupe**, cliquez avec le bouton droit sur **Administrateur sur LON-DC1**, puis cliquez sur **Enregistrer le rapport**.
10. Dans la boîte de dialogue **Enregistrer le rapport GPO**, cliquez sur **Bureau**, puis sur **Enregistrer**.

### Utiliser l'Assistant Modélisation de stratégie de groupe pour créer un rapport

1. Cliquez avec le bouton droit sur **Modélisation de stratégie de groupe**, puis cliquez sur l'**Assistant Modélisation de stratégie de groupe**.
2. Dans l'**Assistant Modélisation de stratégie de groupe**, cliquez sur **Suivant**.
3. Sur la page **Sélection du contrôleur de domaine**, cliquez sur **Suivant**.
4. Sur la page **Sélection d'un utilisateur et d'un ordinateur**, sous **Informations de l'utilisateur**, cliquez sur **Utilisateur**, puis cliquez sur **Parcourir**.
5. Dans la boîte de dialogue **Sélectionner un utilisateur**, dans la zone de texte **Entrer les noms des objets à sélectionner (exemples)**, entrez **Aurore** et cliquez ensuite sur **OK**.
6. Sous **Informations sur l'ordinateur**, vérifiez que l'option **Conteneur** est sélectionnée, puis cliquez sur **Parcourir**.
7. Sur la boîte de dialogue **Choisir un conteneur d'ordinateur**, développez **Adatum**, cliquez sur **Informatique**, puis cliquez sur **OK**.
8. Sur la page **Sélection de l'utilisateur et de l'ordinateur**, cliquez sur **Suivant**.
9. Sur la page **Options de simulation avancées**, cliquez sur **Suivant**.
10. Sur la page **Remplacer les chemins Active Directory**, cliquez 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**.
16. Sur la page **Fin de l'Assistant Modélisation de stratégie de groupe**, cliquez sur **Terminer**.
17. Examinez le rapport.
18. Fermez toutes les fenêtres actives.

# Contrôle des acquis et éléments à retenir

## 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 ?

> **Réponse :** Les autorisations de sécurité pourraient être un problème. Si certains utilisateurs ne disposent pas de l'accès en lecture au dossier **Scripts**, ils ne peuvent pas appliquer la politique. En outre, le filtrage de sécurité sur un GPO pourrait être à l'origine de ce problème.

**Question :** Quels sont les paramètres GPO appliqués à l'ensemble des liaisons lentes par défaut ?

> **Réponse :** Le traitement de la politique d'enregistrement et de la politique de sécurité s'appliquent même lorsqu'une liaison lente est détectée. Vous ne pouvez pas modifier ce paramètre.

**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 ?

> **Réponse :** Définissez le lien à appliquer au niveau du domaine et utiliser le filtrage de groupe de sécurité pour refuser l'autorisation Appliquer la stratégie de groupe au groupe des gestionnaires.

## 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. | • Vérifiez le filtrage de sécurité sur l'objet de stratégie de groupe.<br>• Vérifiez les filtres WMI sur l'objet de stratégie de groupe. |
| Les paramètres de stratégie de groupe nécessitent parfois deux redémarrages avant de s'appliquer. | Activez le paramètre **Toujours attendre le réseau au démarrage et politique d'ouverture de session.** |

# Questions et réponses sur les ateliers pratiques

## Atelier pratique A : Implémentation d'une infrastructure de stratégie de groupe

### Questions et réponses

**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 bénéficiez-vous en utilisant le filtrage de groupe de sécurité plutôt que les liens GPO pour gérer l'étendue d'un GPO ?

**Réponse :** Le problème fondamental de compter sur les UO pour parcourir l'application des GPO est qu'une unité d'organisation est une structure fixe et rigide au sein de AD DS ; un seul utilisateur ou ordinateur ne peut exister qu'au sein d'une seule unité d'organisation. Alors que les organisations deviennent plus grandes et plus complexes, il devient difficile de faire entrer les exigences de configuration dans une relation directe avec toute structure de conteneur. Avec les groupes de sécurité, un utilisateur ou un ordinateur peut exister sur autant de groupes que nécessaire, vous pouvez les ajouter ou les supprimer facilement sans nuire à la sécurité ou à la gestion du compte de l'utilisateur ou de l'ordinateur.

**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.

**Réponse :** Il y a très peu de scénarios dans lesquels vous pouvez garantir que tous les paramètres d'un GPO devront toujours être appliqués à tous les utilisateurs et ordinateurs dans son étendue. En ayant un groupe d'exemption, vous êtes toujours en mesure de répondre aux situations dans lesquelles un utilisateur ou un ordinateur doit être exclu. Cela peut aussi aider à la compatibilité de dépannage et lors de problèmes de fonctionnalité. Parfois, les paramètres spécifiques de GPO peuvent interférer avec la fonctionnalité d'une application. Pour tester si l'application fonctionne sur une nouvelle installation du système d'exploitation Windows, vous pourriez avoir besoin d'exclure temporairement l'utilisateur ou l'ordinateur de l'étendue des GPO.

**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 ?

**Réponse :** Les réponses varient. Les scénarios pourraient inclure : dans les chambres et les kiosques, sur les ordinateurs virtuels (VDI), et dans d'autres environnements standards.

## Atelier pratique B : Dépannage de l'infrastructure de stratégie de groupe

### Questions et réponses

**Question :** Dans quelles situations avez-vous utilisé les rapports RSoP pour résoudre l'application de stratégie de groupe dans votre organisation ?

**Réponse :** Les réponses peuvent varier en fonction de l'expérience des stagiaires et des situations. Les réponses possibles peuvent inclure :

- Un problème de stratégie de groupe résolu où un GPO n'a pas appliqué en raison du filtrage de sécurité.
- Avoir résolu un problème de stratégie de groupe où une extension côté client a pris 20 secondes pour s'appliquer en raison d'un problème Domain Name System (DNS).
- Avoir localisé un paramètre de GPO qui a été configuré dans le mauvais GPO.

- Avoir localisé un problème de stratégie de groupe où des paramètres d'utilisateur incorrects ont été appliqués à cause du traitement en boucle.

**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 ?

**Réponse :** Les réponses peuvent varier en fonction de l'expérience des stagiaires et des situations. Les réponses possibles peuvent inclure :

- Avoir réussi à configurer correctement la stratégie de groupe en fonction des simulations de modélisation de stratégie de groupe.
- Avoir testé le résultat de l'ajout d'un utilisateur à un groupe de sécurité.
- Avoir testé le résultat du déplacement d'un utilisateur vers une autre UO.
- Avoir testé le résultat de la configuration de traitement en boucle pour un ordinateur.

# Module 6

## Gestion des paramètres de l'utilisateur avec la stratégie de groupe

### Sommaire :

Leçon 1

# Mise en œuvre des modèles d'administration

## Sommaire :

## Questions et réponses

**Question :** Quelles sont les sections disponibles dans le nœud **Modèles d'administration** sous le nœud **Configuration utilisateur** ? (Choisissez toutes les réponses applicables.)

( ) Bureau

( ) Composants Windows

( ) Serveur

( ) Système

( ) Panneau de configuration

**Réponse :**

(√) Bureau

(√) Composants Windows

( ) Serveur

(√) Système

(√) Panneau de configuration

**Commentaire :**

Certaines des sections affichent dans **Modèles d'administration** à la fois dans les sections de l'ordinateur et de l'utilisateur d'un GPO. La section bureau ne se trouve que dans la section utilisateur tandis que la section serveur ne se trouve que dans la section ordinateur. Les composants Windows, le système et le panneau de contrôle sont à la fois sur l'ordinateur et dans les sections utilisateur d'un GPO, bien que les paramètres que vous pouvez configurer dans ces sections ne sont pas les mêmes.

**Question :** Vous pouvez créer le magasin central à travers la GPMC.

( ) Vrai

( ) Faux

**Réponse :**

( ) Vrai

(√) Faux

**Commentaire :**

Pour créer le magasin central, vous devez créer manuellement le dossier **PolicyDefinitions** dans SYSVOL, puis copier à la fois les fichiers .admx et .adml dans le dossier **PolicyDefinitions**.

## Discussion : Utilisations pratiques des modèles d'administration

**Question :** Comment assurez-vous la sécurité du poste de travail actuellement ?

**Réponse :** Les réponses varient.

**Question :** Quel est le degré actuel d'accès des utilisateurs à des fonctionnalités d'administration ?

**Réponse :** Les réponses varient.

**Question :** Quels paramètres de stratégie de groupe trouvez-vous utiles pour votre organisation ?

**Réponse :** Les réponses varient.

# Ressources

## Importation des modèles de sécurité

**Lectures supplémentaires :** Pour plus d'informations, reportez-vous à Security Compliance Manager (SCM) : http://aka.ms/Ypdcmd

## Gestion des modèles d'administration

**Lectures supplémentaires : Pour** plus d'informations, consultez ADMX Migrator : http://aka.ms/Ny5p5c

**Lectures supplémentaires :** Pour plus d'informations, reportez-vous aux fichiers de modèles d'administration Office 2016 (ADMX / ADML) et à l'Outil de personnalisation Office : http://aka.ms/Nknzlx

## Démonstration : Configuration des paramètres avec les modèles d'administration

### Éapes de démonstration

### Configurer un paramètre de stratégie de modèles d'administration

1. Basculez vers **LON-DC1**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
3. Dans le volet de navigation, développez **Forêt : Adatum.com**, développez **Domaines**, développez **Adatum.com**, puis cliquez sur le conteneur **Objets de stratégie de groupe**.
4. Clic-droit sur le conteneur **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
5. Dans la boîte de dialogue **Nouveau GPO**, dans le champ **Nom**, tapez **GPO1**, puis cliquez sur **OK**.
6. Dans le volet d'informations, cliquez avec le bouton droit sur **GPO1**, puis cliquez sur **Modifier**.
7. Dans la fenêtre **Éditeur de gestion des stratégies de groupe**, dans le volet de navigation, développez **Configuration utilisateur**, développez **Stratégies**, développez **Modèles d'administration**, puis cliquez sur **Système**.
8. Dans le volet d'informations, double-cliquez sur **Désactiver l'accès à l'invite de commandes**.
9. Dans la boîte de dialogue **Désactiver l'accès à l'invite de commandes**, affichez les trois valeurs possibles, puis cliquez sur **Annuler**.

### Filtrer les paramètres de la stratégie des modèles administratifs

1. Cliquez avec le bouton droit sur **Modèles d'administration**, puis cliquez sur **Options de filtre**.
2. Cochez la case **Activer les filtres par mots clés**.
3. Dans la zone de texte **Filtrer par mot(s)**, saisissez **écran de veille**.
4. Dans le menu déroulant à côté de la zone de texte, sélectionnez **Tout**, puis cliquez sur **OK**.
5. Faites remarquer que les paramètres de stratégie des modèles d'administration filtrent pour afficher uniquement ceux qui contiennent les mots **écran de veille**. Prenez quelques instants pour examiner les paramètres que vous avez trouvés. Expliquez que les paramètres peuvent apparaître sans écran de veille dans le titre, parce que l'écran de veille peut également apparaître dans le texte d'aide.

6. Dans l'arborescence de la console, sous **Configuration utilisateur**, cliquez avec le bouton droit sur **Modèles d'administration**, puis cliquez sur **Options de filtre**.
7. Cochez la case **Activer les filtres par mots clés**.
8. Dans la liste déroulante **Configuré**, activez la case à cocher **Oui**, puis cliquez sur **OK**. Faites remarquer que maintenant les paramètres de stratégie des modèles d'administration filtrent pour montrer uniquement ceux qui ont été configurés pour être activés ou désactivés. Aucun paramètre n'a été configuré.
9. Dans l'arborescence de la console, sous **Configuration utilisateur**, faites un clic droit sur **Modèles d'administration**, puis désactivez l'option **Filtre activé**.

## Ajouter des commentaires à un paramètre de stratégie

1. Dans l'arborescence de la console, sous **Configuration utilisateur**, développez **Stratégies**, développez **Modèles d'administration**, développez **Panneau de contrôle**, puis cliquez sur **Personnalisation**.
2. Dans le volet d'informations, double-cliquez sur le paramètre de stratégie **Activer l'écran de veille**.
3. Dans la section **Commentaire**, tapez **Stratégie de sécurité informatique d'entreprise mise en œuvre avec cette stratégie en combinaison avec Protéger l'écran de veille avec un mot de passe**. Cliquez sur **Activé** pour activer la stratégie, puis cliquez sur **OK**.
4. Double-cliquez sur le paramètre de stratégie **Protéger l'écran de veille avec un mot de passe**, puis cliquez sur **Activée**.
5. Dans la section **Commentaire**, tapez **Stratégie de sécurité informatique d'Entreprise mise en œuvre avec cette stratégie en combinaison avec Activer l'écran de veille**, puis cliquez sur **OK**.

## Ajouter des commentaires à un GPO

1. Dans l'**Éditeur de gestion des stratégies de groupe**, dans l'arborescence de la console, cliquez avec le bouton droit sur le nœud racine **GPO1 [LON-DC1.ADATUM.COM]**, puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **Commentaire**.
3. Tapez Politiques standards d'entreprise Adatum. **Les paramètres sont étendus à tous les utilisateurs et ordinateurs du domaine. Personne responsable de ce GPO : *Votre nom***.
4. Faites remarquer que ce commentaire s'affiche sur l'onglet **Détails** du GPO dans la **console de gestion des stratégies de groupe**, puis cliquez sur **OK**.
5. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.

## Créer un nouveau GPO en copiant un GPO existant

1. Dans la GPMC, dans le volet de navigation, cliquez sur le conteneur **Objets de stratégie de groupe**, cliquez avec le bouton droit sur **GPO1**, puis cliquez sur **Copier**.
2. Cliquez avec le bouton droit sur le conteneur **Objets de stratégie de groupe**, cliquez sur **Coller**, puis cliquez sur **OK** deux fois.

## Créer un nouveau GPO par l'importation des paramètres qui ont été exportés d'un autre GPO

1. Dans la GPMC, dans le volet de navigation, cliquez sur le conteneur **Objets de stratégie de groupe**, cliquez avec le bouton droit sur **GPO1**, puis cliquez sur **Sauvegarder**.
2. Dans la zone **Emplacement**, entrez **adfswap.adatum.com**, puis cliquez sur **Sauvegarder**.
3. Une fois la sauvegarde terminée, cliquez sur **Fermer**.

4. Dans le GPMC, dans le volet de navigation, cliquez avec le bouton droit sur le conteneur **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
5. Dans la zone **Nom**, saisissez **Importer ADATUM**, puis cliquez sur **OK**.
6. Dans la GPMC, dans le volet de navigation, faites un clic droit sur **Importer ADATUM**, puis cliquez sur **Importer les paramètres**.
7. Dans l'**Assistant Importation de paramètres**, cliquez trois fois sur **Suivant**.
8. Sélectionnez **GPO1**, puis cliquez sur **Suivant** deux fois.
9. Cliquez sur **Terminer**, puis sur **OK**.
10. Fermez le GPMC.

Leçon 2

# Configuration de la redirection de dossiers, de l'installation de logiciel et des scripts

## Sommaire :

## Questions et réponses

**Question :** Lequel des dossiers suivants pouvez-vous rediriger en utilisant la redirection de dossiers ? (Choisissez toutes les réponses applicables.)

( ) Documents

( ) Favoris

( ) AppData (Itinérance)

( ) AppData (Local)

( ) Fichiers de programme

**Réponse :**

(√) Documents

(√) Favoris

(√) AppData (Itinérance)

( ) AppData (Local)

( ) Fichiers de programme

**Commentaire :**

Vous pouvez rediriger **Documents**, **Favoris** et **AppData (Itinérance)**. Trois répertoires existent dans le répertoire AppData de l'utilisateur : **Local**, **LocalLow** et **Roaming**. Vous ne pouvez rediriger **Itinérance** qu'en utilisant la redirection de dossiers. Vous ne pouvez pas rediriger **Fichiers de programme**. Ce dossier doit être situé sur le disque dur local.

**Classez l'activité**

**Question :** Catégorisez chaque élément dans la catégorie appropriée. Indiquez votre réponse en écrivant le numéro de catégorie à droite de chaque élément.

| 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 |
| | | | | |

**Réponse :**

| Catégorie 1 | | Catégorie 2 | | Catégorie 3 |
|---|---|---|---|---|
| **Configuration utilisateur** | | **Configuration ordinateur** | | **Configuration utilisateur et Configuration de l'ordinateur** |
| **Scripts d'ouverture de session**<br>**Scripts de déconnexion**<br>**Redirection de dossiers**<br>**Publier logiciel** | | **Scripts de démarrage**<br>**Scripts d'arrêt** | | **Attribuer logiciel** |

## Paramètres pour la configuration de la redirection de dossiers

**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 ?

> **Réponse : Créer un dossier pour chaque utilisateur sous le chemin racine**. Cette manipulation crée un dossier **Documents** auquel seul l'utilisateur a accès.

## Démonstration : Configuration de la redirection de dossiers

### Procédure de démonstration

### Créer un dossier partagé

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 sur l'onglet **Accueil**, cliquez sur **Nouveau dossier**.

4. Dans la zone de texte **Nom**, tapez **Redir** et appuyez sur Entrée.
5. Faites un clic droit sur le dossier **Redirection**, cliquez sur **Partager avec**, puis sur **Personnes spécifiques**.
6. Dans la boîte de dialogue **Partage de fichiers,** cliquez sur la flèche déroulante, sélectionnez **Tous publics**, puis sur **Ajouter.**
7. Pour le groupe Tout le monde, cliquez sur la flèche déroulante **Niveau d'autorisation**, puis sur **Lecture/écriture**.
8. Cliquez sur **Partager**, puis sur **Terminer**.
9. Fermez la fenêtre **Disque local (C:)**.

## Créer un GPO pour rediriger le dossier Documents

1. Dans le Gestionnaire de serveur, cliquez sur **Outils** puis sur **Gestion des stratégies de groupe**.
2. Dans le volet de navigation, cliquez avec le bouton droit sur le domaine **Adatum.com**, puis cliquez sur **Créer un objet GPO dans ce domaine et le lier ici**.
3. Dans la fenêtre de dialogue **Nouvel objet GPO**, dans la zone **Nom**, tapez **Redirection du dossier**, puis cliquez sur **OK**.
4. Dans le volet de navigation, cliquez avec le bouton droit sur **Redirection de dossiers**, puis cliquez sur **Modifier**.
5. Dans la fenêtre **Éditeur de gestion de la stratégie de groupe**, sous **Configuration utilisateur**, développez **Stratégies**, développez **Paramètres Windows**, puis développez **Redirection de dossiers**.
6. Cliquez avec le bouton droit sur **Documents**, puis cliquez sur **Propriétés**.
7. Dans la boîte de dialogue **Propriétés du document**, sur l'onglet **Cible**, cliquez sur la flèche déroulante **Paramètre**, puis **sélectionnez Redirection basique du dossier de tout le monde au même endroit**.
8. Assurez-vous que la boîte **Emplacement du dossier cible** soit réglée sur **Créer un dossier pour chaque utilisateur sous le chemin racine**.
9. Dans la zone de texte **Chemin racine**, entrez **\\LON-DC1\Redir**, puis cliquez sur **OK**.
10. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
11. Fermez l'Éditeur de gestion des stratégies de groupe.

## Tester la redirection de dossiers

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Invite de commandes**.
3. Dans la fenêtre d'invite de commandes, entrez la commande suivante et appuyez sur Entrée :

```
Gpupdate / force
```

4. Dans la fenêtre d'invite de commandes PowerShell, tapez la commande suivante et appuyez sur Entrée :

```
Y
```

5. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
6. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.

7. Dans le volet de navigation, dans la section **Accès rapide**, cliquez avec le bouton droit sur **Documents**, puis cliquez sur **Propriétés**.
8. Vérifiez que dans l'onglet **Général**, le champ Emplacement a une valeur de **\\LON-dc1\redir\Administrateur**.
9. Si cela échoue, répétez les étapes 2 à 7, puis vérifiez la redirection une fois de plus.
10. Déconnectez-vous de **LON-CL1**.

## Démonstration : Configuration des scripts avec des objets de stratégie de groupe

### Procédure de démonstration

### Créer un script d'ouverture de session pour afficher un message

1. Dans **LON-DC1**, cliquez sur **Démarrer**, saisissez **Bloc-notes**, puis cliquez sur **Bloc-notes**.
2. Dans le Bloc-notes, tapez la commande suivante, puis appuyez sur Entrée :

```
Msgbox "Ceci est le script"
```

3. Cliquez sur le menu **Fichier,** puis sur **Enregistrer sous**.
4. Dans la boîte de dialogue **Enregistrer** sous, dans la zone de texte **Nom du fichier**, entrez **Logon.vbs**.
5. Dans la liste **Sauvegarder comme type**, sélectionnez **Tous les fichiers (*.*)**.
6. Dans le volet de navigation, cliquez sur **Bureau**, puis sur **Enregistrer**.
7. Fermez le **Bloc-notes**.
8. Sur le bureau, cliquez avec le bouton droit sur le fichier **Logon.vbs**, puis cliquez sur **Copier**.

### Créer et lier un GPO pour utiliser le script

1. Ouvrez le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion de la stratégie de groupe**.
2. Développez **Forêt: Adatum.com**, puis développez **Domaines**.
3. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Créer un objet GPO dans ce domaine et le lier ici**.
4. Dans la boîte de dialogue **Nouvel objet GPO**, dans la zone de texte **Nom**, tapez **Scripts d'ouverture de session de l'utilisateur**, puis cliquez sur **OK**.
5. Développez **Adatum.com**, cliquez avec le bouton droit sur le GPO **Scripts d'ouverture de session de l'utilisateur**, puis cliquez sur **Modifier**.
6. Dans la fenêtre **Éditeur de gestion de la stratégie de groupe**, sous **Configuration utilisateur**, développez **Stratégies**, développez **Paramètres Windows**, puis développez **Scripts (d'ouverture de session/de déconnexion)**.
7. Dans le volet d'informations, double-cliquez sur **Ouverture** de session.
8. Dans la boîte de dialogue **Propriétés : ouverture de session**, cliquez sur **Afficher les fichiers**.
9. Dans le volet d'informations, cliquez avec le bouton droit sur un espace vide, puis cliquez sur **Coller**.
10. Fermez la fenêtre **Se connecter**.
11. Dans la boîte de dialogue **Propriétés : ouverture de session**, cliquez sur **Ajouter**.
12. Dans la boîte de dialogue **Ajout d'un script**, cliquez sur **Parcourir**.

13. Cliquez sur le script **Logon.vbs**, puis sur **Ouvrir**.
14. Cliquez sur **OK** deux fois pour fermer toutes les boîtes de dialogue.
15. Fermez la fenêtre **Éditeur de gestion des stratégies de groupe** et la **Console de gestion des stratégies de groupe**.

### Se connecter à un ordinateur client et tester les résultats

1. Sur **LON-CL1**, déconnectez-vous et connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
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. Si nécessaire, dans la fenêtre de l'invite de commandes, entrez la commande suivante et appuyez sur **Entrée** :

```
0
```

5. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Miranda** avec le mot de passe **Pa$$w0rd**.
6. Vérifiez que le script est exécuté, affichant le message que vous avez configuré dans le GPO plus tôt.

**Remarque :** Cela peut prendre jusqu'à dix minutes pour s'afficher. Si le message ne s'affiche pas, redémarrez **LON-CL1** et répétez l'étape un à cinq.

7. Déconnectez-vous de **LON-CL1**.

Leçon 3

# Configuration des préférences de stratégie de groupe

## Sommaire :

## Questions et réponses

**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)

( ) Internet Explorer

( ) Raccourcis

( ) Registre

( ) Options d'alimentation

( ) Options de dossier

**Réponse :**

(√) Internet Explorer

(√) Raccourcis

(√) Registre

( ) Options d'alimentation

( ) Options de dossier

**Commentaire :**

Vous pouvez utiliser les paramètres d'Internet Explorer dans les préférences de stratégie de groupe pour configurer Microsoft Internet Explorer. Les raccourcis peuvent créer des favoris que les utilisateurs peuvent ouvrir dans Internet Explorer. Vous pouvez utiliser le Registre pour configurer les paramètres basés sur le Registre d'Internet Explorer. Vous ne pouvez pas utiliser Options d'alimentation ou Options des dossiers pour configurer Internet Explorer.

**Question :** Vous pouvez utiliser un ciblage au niveau des articles pour limiter les préférences de stratégie de groupe en fonction de la forêt AD DS à laquelle appartient l'utilisateur.

( ) Vrai

( ) Faux

**Réponse :**

( ) Vrai

(√) Faux

**Commentaire :**

Une stratégie de groupe ne peut pas traverser les forêts. Vous pouvez utiliser des domaines, sites, groupes de sécurité et des unités organisationnelles dans le ciblage au niveau de l'élément.

**Question :** Dans quels scénarios avez-vous utilisé les préférences de stratégie de groupe et le ciblage au niveau élément ?

**Réponse :** Les réponses peuvent varier. Outre les réponses des stagiaires, partagez vos propres expériences avec le reste de la classe.

## Démonstration : Configuration des préférences de stratégie de groupe

### Procédure de démonstration

### Créer une imprimante avec les préférences de stratégie de groupe

1. Sur **LON-DC1**, cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Panneau de configuration**.

2. Dans le Panneau de configuration, cliquez sur **Afficher les périphériques et imprimantes**.
3. Cliquez sur **Ajouter une imprimante**.
4. Dans la boîte de dialogue **Ajouter un périphérique**, cliquez sur **L'imprimante que je veux n'est pas listée**.
5. Dans la boîte de dialogue **Ajouter une imprimante**, sélectionnez **Ajouter une imprimante locale ou réseau avec des paramètres manuels, puis cliquez sur Suivant**.
6. Sur la page **Choisir un port d'imprimante**, cliquez sur **Suivant**.
7. Sur la page **Installer le pilote d'imprimante**, cliquez sur **Suivant**.
8. Sur la page **Entrer un nom d'imprimante**, dans la zone de texte **Nom de l'imprimante**, tapez **Brother**, puis cliquez sur **Suivant**.
9. Sur la page **Partage d'imprimantes**, cliquez sur **Suivant**.
10. Sur la page **Vous avez ajouté Brother avec succès**, cliquez sur **Terminer**.
11. Fermez le Panneau de configuration.
12. Si nécessaire, basculez vers le **Gestionnaire de serveur**.
13. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
14. Dans le volet de navigation, développez **Forêt : Adatum.com**, développez successivement **Domaines**, **Adatum.com**, puis cliquez sur le domaine **Adatum.com**.
15. Cliquez avec le bouton droit sur le domaine **Adatum.com**, puis cliquez sur **Créer un objet GPO dans ce domaine et le lier ici**.
16. Dans la boîte de dialogue **Nouvel objet GPO**, saisissez **Préférences des stratégies** de groupe, puis cliquez sur **OK**.
17. Dans le volet de navigation, cliquez avec le bouton droit sur **Préférences des stratégies** de groupe, puis cliquez sur **Modifier**.
18. Dans l'**Éditeur de gestion des stratégies de groupe**, développez **Configuration utilisateur**, développez **Préférences**, développez **Paramètres du panneau de configuration**, cliquez avec le bouton droit sur **Imprimantes**, survolez **Nouveau**, puis cliquez sur **Imprimante** partagée.
19. Dans la boîte de dialogue **Nouvelles propriétés de l'imprimante partagée**, dans la zone de texte **Chemin partagé**, tapez **\\LON-DC1\Brother**.
20. Cochez la case **Régler cette imprimante comme imprimante par défaut**.

## Cibler la préférence

1. Dans l'onglet **Commun**, activez la case à cocher **ciblage de niveau des articles**, puis cliquez sur **Ciblage**.
2. Dans la boîte de dialogue **Éditeur de ciblage**, cliquez sur **Nouvel article**, puis cliquez sur **Plage d'adresses IP**.
3. Dans la zone de texte **entre**, tapez **172.16.0.50**, dans la zone de texte **et**, tapez **172.16.0.99**, puis cliquez sur **OK** deux fois.

## Configurer un plan d'alimentation avec les préférences de stratégie de groupe

1. Dans l'éditeur de gestion des stratégies de groupe, développez **Configuration de l'ordinateur**, développez **Préférences**, développez **Paramètres du panneau de configuration**, puis cliquez sur **Options d'alimentation**.

2. Cliquez avec le bouton droit sur **Options d'alimentation**, sélectionnez **Nouveau**, puis cliquez sur **Plan d'alimentation (au moins Windows 7)**.
3. Dans la boîte de dialogue **Nouvelles propriétés du plan d'alimentation (au moins) de Windows 7**, cliquez sur la liste déroulante **Équilibré**, puis tapez **Plan d'alimentation Adatum**.
4. Cochez la case **Définir comme le plan d'alimentation actif**.

### Cibler la préférence

1. Dans l'onglet **Commun**, activez la case à cocher **ciblage de niveau des articles**, puis cliquez sur **Ciblage**.
2. Dans la boîte de dialogue **Éditeur de ciblage**, cliquez sur **Nouvel article**, puis cliquez sur **Système d'exploitation**.
3. Dans la liste **Produit**, sélectionnez **Windows 10**, puis cliquez sur **OK** deux fois.
4. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.

### Tester les préférences

1. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
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. Dans la fenêtre d'invite de commandes PowerShell, tapez la commande suivante et appuyez sur Entrée :

```
0
```

5. Connectez-vous à **LON-CL1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
6. Cliquez avec le bouton droit sur **Démarrer**, puis sur **Panneau de configuration**.
7. Cliquez sur **Matériel et son**, puis cliquez **Périphériques et imprimantes**.
8. Vérifier la présence de l'imprimante **Brother sur LON-DC1**.
9. Cliquez sur la flèche retour, puis sur **Options d'alimentation**.
10. Vérifiez que le **Plan d'alimentation Adatum** est présent et qu'il est le plan d'alimentation actif.

# Contrôle des acquis et éléments à retenir

## Méthodes conseillées

### 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.

## Questions de contrôle des acquis

**Question :** Pourquoi certains paramètres de stratégie de groupe nécessitent-ils deux signatures avant de prendre effet ?

> **Réponse :** Les utilisateurs se connectent généralement avec les informations d'identification mises en cache, ce qui peut empêcher la stratégie de groupe de les appliquer à la session en cours. Les paramètres prennent effet à la prochaine connexion.

**Question :** Quel est l'avantage d'utiliser un magasin central ?

> **Réponse :** Un magasin central est un dossier unique dans SYSVOL qui contient tous les fichiers .admx et .adml nécessaires à l'administration de la stratégie de groupe. Après avoir configuré le magasin central, l'éditeur de gestion des stratégies de groupe le reconnaît, puis charge tous les modèles d'administration à partir du magasin central au lieu de les charger à partir de la machine locale.

**Question :** Quelle est la principale différence entre les paramètres de stratégie de groupe et les préférences de stratégie de groupe ?

> **Réponse :** Les paramètres de stratégie de groupe appliquent certains paramètres du côté client et ils désactivent les interfaces client pour la modification. Toutefois, les préférences de stratégie de groupe fournissent des paramètres et elles permettent aux clients de les modifier.

## 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. | Le problème est très probablement lié aux autorisations. La stratégie de groupe crée les sous-répertoires nommés pour les utilisateurs, mais les utilisateurs n'ont pas suffisamment d'autorisations pour créer les dossiers redirigés qui sont à l'intérieur. |
| Vous avez des ordinateurs Windows 7 et Windows 10. Après avoir configuré plusieurs paramètres dans les modèles d'administration d'un GPO, les utilisateurs des systèmes d'exploitation Windows 7 indiquent que certains paramètres s'appliquent et que d'autres ne s'appliquent pas. | Tous les nouveaux paramètres ne s'appliquent pas aux anciens systèmes d'exploitation tels que Windows 7. Vérifiez le paramètre lui-même pour voir à quels systèmes d'exploitation il s'applique. |
| Les préférences de stratégie de groupe ne s'appliquent pas. | Vérifiez les paramètres de préférence pour le ciblage de niveau des articles ou une configuration incorrecte. |

# Questions et réponses sur les ateliers pratiques

## Atelier pratique : Gestion des paramètres de l'utilisateur avec la stratégie de groupe

## Questions et réponses

**Question :** Quelles sont les options que vous pouvez utiliser pour séparer les dossiers redirigés des utilisateurs vers des serveurs différents ?

> **Réponse :** Vous pouvez utiliser le paramètre **Avancé** dans Redirection de dossiers pour choisir différents dossiers partagés sur des serveurs différents pour des groupes de sécurité différents.

**Question :** Pouvez-vous nommer deux méthodes que vous pouvez utiliser pour attribuer un GPO à des objets sélectionnés au sein d'une UO ?

> **Réponse :** Vous pouvez utiliser les filtres Windows Management Instrumentation (WMI) pour définir un critère d'application de stratégie de groupe, tel que la machine est un ordinateur portable ou non, ou quelle version du système d'exploitation est installé. Vous pouvez également utiliser des autorisations sur le GPO lui-même pour autoriser ou refuser les paramètres GPO aux utilisateurs ou ordinateurs.

**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 ?

> **Réponse :** Vous pouvez utiliser un ciblage de niveau des articles pour appliquer la préférence aux ordinateurs portables. Ensuite, la préférence est appliquée si le profil matériel de l'ordinateur l'identifie comme un ordinateur portable.

# Module 7

## Sécurisation des services de domaine Active Directory

### Sommaire :

Leçon 1

# Sécurisation des contrôleurs de domaine

## Sommaire :

## Questions et réponses

**Question :** Comment pouvez-vous garantir une sécurité supplémentaire pour les disques durs dans les contrôleurs de domaine ?

> **Réponse :** Pour fournir un niveau supplémentaire de sécurité, pensez à utiliser le chiffrement de lecteur BitLocker pour crypter les disques durs du contrôleur de domaine.

## Démonstration : Configuration d'une stratégie de réplication de mot de passe

### Procédure de démonstration

### Organiser l'installation déléguée d'un RODC

1. Sur **LON-DC1**, 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** tapez **Munich**, sélectionnez l'objet du lien de sites **DEFAULTIPSITELINK**, puis validez avec **OK**.
4. Dans la boîte de message **Active Directory Domain Services**, 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 de détails, double-cliquez sur l'unité d'organisation (UO) **Contrôleurs de domaine.**
7. Dans le volet **Tâches**, dans la section **Contrôleurs de domaine**, cliquez sur **Pré-créer un compte de contrôleur de domaine en lecture seule**.
8. Dans l'**Assistant d'installation Active Directory Domain Services**, sur la page **Bienvenue dans l'assistant d'installation Active Directory Domain Services**, cliquez sur **Suivant**.
9. Sur la page **Identification Réseau**, cliquez sur **Suivant**.
10. Sur la page **Spécifier le nom de l'ordinateur**, tapez le nom d'ordinateur comme **MUC-RODC1**, puis cliquez sur **Suivant**.
11. Sur la page **Sélectionner un site**, cliquez sur **Munich**, puis sur **Suivant**.
12. Sur la page **Options supplémentaires du contrôleur de domaine**, acceptez les paramètres par défaut, activez les cases à cocher **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 Ordinateur**, dans le champ **Entrer les noms des objets à sélectionner**, tapez **Bill**, puis cliquez sur **Vérifier les noms**.
15. Vérifiez que Bill Norman 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 **Aperçu des sélections**, vérifiez vos paramètres, puis cliquez sur **Suivant**.
18. Sur le page **Fin de l'Assistant d'installation Active Directory Domain Services**, cliquez sur **Terminer**.

## Voir la stratégie de réplication de mot de passe d'un RODC

1. Dans **Centre d'administration Active Directory**, dans UO **Contrôleurs de domaine**, sélectionnez **MUC-RODC1**.
2. Dans le volet **Tâches**, dans la section **MUC-RODC1**, cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés MUC-DC1 (Désactivé)**, faites défiler vers le bas jusqu'à **Extensions**, puis cliquez sur l'onglet **Stratégie de réplication de mot de passe**.
4. Passez en revue les groupes par défaut, les utilisateurs et les ordinateurs dans la Stratégie de réplication de mot de passe.
5. Laissez la boîte de dialogue ouverte.

## Configurer une stratégie de réplication de mot de passe propre à un RODC

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**, tapez le nom du groupe **Groupe de réplication de mot de passe RODC autorisé par Munich**, puis validez avec **OK**.
5. Double-cliquez sur **Groupe Munich réplication de mot de passe autorisée RODC**, cliquez sur l'onglet **Membres** et puis cliquez **Ajouter**.
6. Dans la boîte de dialogue **Sélectionner des utilisateurs**, **des contacts, des ordinateurs, des comptes de service ou des groupes**, dans la zone de texte **Entrez les noms des objets à sélectionner**, entrez **Ana** et cliquez ensuite sur **Vérifier les noms**.
7. Dans la boîte de dialogue **Plusieurs noms trouvés**, sélectionnez **Ana Cantrell** et puis clique **D'accord**.
8. Dans la boîte de dialogue **Sélectionner Utilisateurs, Contacts, Ordinateurs, les comptes de service ou Groupes**, cliquez sur **OK**, puis dans la **Propriétés du Groupe Munich réplication de mot de passe autorisée RODC** boîte de dialogue, cliquez sur **D'accord**.
9. Fermez la fenêtre **Utilisateurs et ordinateurs Active Directory**.
10. Lancez le **Centre d'administration Active Directory**, puis ouvrez **Propriétés MUC-RODC1**. Dans la section **Extensions**, dans l'onglet **Stratégie de réplication de mot de passe**, cliquez sur **Ajouter**.
11. Dans la boîte de dialogue **Ajouter des groupes, des utilisateurs et des ordinateurs**, sélectionnez l'option **Autoriser les mots de passe pour le compte à répliquer à ce RODC**, puis validez avec OK..
12. Dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, dans la zone de texte **Entrer les noms des objets à sélectionner**, entrez **Munich**, cliquez sur **Vérifier les noms**, puis sur **OK**.
13. Dans la boîte de dialogue **MUC-RODC1 (Désactivé)**, cliquez sur **OK**.

## Vérifier la stratégie de mots de passe qui en résulte

1. Dans le **Centre d'administration Active Directory**, dans le volet **Tâches**, dans la section **MUC-RODC1**, cliquez sur **Propriétés**.
2. Dans la boîte de dialogue **Propriétés MUC-RODC1 (désactivé)**, dans la section **Extensions**, dans l'onglet **Stratégie de réplication de mot de passe**, cliquez sur **Avancée**.

**Remarque :** La boîte de dialogue **Stratégie de réplication de mot de passe avancée pour MUC-RODC1** affiche tous les comptes avec des mots de passe qui sont stockés dans ce RODC.

3. Dans la liste déroulante **Afficher les utilisateurs et les ordinateurs qui répondent aux critères suivants**, cliquez sur **Comptes qui ont été authentifiés à ce contrôleur de domaine en lecture seule**, puis dites aux étudiants que cette page ne montre que les comptes qui ont les autorisations nécessaires et que le RODC a authentifiés.
4. Dans l'onglet **Stratégie résultantes**, cliquez sur **Ajouter**, puis dans la boîte de dialogue **Sélectionner Utilisateurs ou ordinateurs**, dans le champ **Entrez le nom de l'objet pour sélectionner**, tapez **Ana**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
5. Notez qu'Ana a un **Paramètre résultant d'Autoriser**.
6. Fermer ou annuler toutes les boîtes de dialogue.

Leçon 2

# Implémentation de la sécurité du compte

## Sommaire :

## Questions et réponses

**Question :** Quelle technologie vous permet d'utiliser la fonctionnalité biométrique pour vous connecter à des périphériques Windows ?

> **Réponse :** Windows Hello est une nouvelle technologie présente dans Windows 10 et Windows 10 Mobile qui vous permet de vous authentifier grâce à votre empreinte digitale, un scan de l'iris ou d'autres données biométriques.

## Ressources

## Options de sécurité du compte dans Windows Server 2016

 **Lectures supplémentaires :** Pour plus d'informations sur la protection des informations d'identification et la gestion, consultez le site suivant : http://aka.ms/R5bfid

## Démonstration : Configuration des stratégies de compte de domaine

### Procédure de démonstration

### Configurer une stratégie de mots de passe basée sur le domaine

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la **Console de gestion de stratégie de groupe**, développez **Forêt** : **Adatum.com\Domains\Adatum.com\Group Policy Objects**, cliquez avec le bouton droit sur **Stratégie de domaine par défaut**, puis cliquez sur **Modifier**.
3. Dans la fenêtre **Éditeur de gestion des stratégies de groupe**, dans le volet de navigation, sous **Configuration ordinateur**, développez **Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de compte**, double-cliquez sur **Stratégie de mot de passe**, puis double-cliquez sur **Appliquer l'historique des mots de passe**.
4. Dans la boîte de dialogue **Propriétés de l'application de l'histoire de mot de passe**, dans le champ **Conserver l'historique du mot de passe pendant**, saisissez **20**, cliquez sur **OK**, puis double-cliquez sur **Durée de vie maximale du mot de passe**.
5. Dans la boîte de dialogue **Propriétés de la durée de vie maximale du mot de passe**, dans le champ **Le mot de passe expirera dans**, saisissez **45**, validez avec **OK**, puis double-cliquez sur **Durée de vie minimale du mot de passe**.
6. Dans la boîte de dialogue **Propriétés de l'âge minimum de mot de passe**, assurez-vous que le **Mot de passe peut être modifié après** que le champ soit **1**, validez avec **OK**, puis double-cliquez sur **longueur du mot de passe minimum**.
7. Dans la boîte de dialogue **Propriétés de longueur de mot de passe minimum**, dans le champ **Mot de passe doit être au moins**, type **10**, validez avec **OK**, puis double-cliquez sur **Mot de passe doit répondre aux exigences de complexité**.
8. Dans la boîte de dialogue **Propriétés-Mot de passe doit répondre aux exigences de complexité**, cliquez sur **Activé**, puis sur **OK**.
9. Ne fermez pas la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.

### Configurer une stratégie de verrouillage du compte

1. Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, dans le volet de navigation, cliquez sur **Stratégie de verrouillage du compte**, puis double-cliquez sur **Durée de verrouillage du compte**.
2. Dans la boîte de dialogue **Propriétés de la durée de verrouillage du compte**, cliquez sur **Définir ce paramètre de stratégie**, dans le champ **Minutes**, tapez **30**, puis cliquez sur **OK**.
3. Dans la boîte de dialogue **Changements des valeurs suggérées**, notez les valeurs suggérées, y compris la configuration automatique du **Seuil de verrouillage du compte**, cliquez sur **OK**, puis double-cliquez sur **Réinitialiser le compteur de verrouillage du compte après**.
4. Dans la boîte de dialogue **Propriétés de Réinitialisation du compteur de verrouillage du compte après**, dans le champ **Réinitialiser le compteur de verrouillage du compte après**, tapez **15**, puis cliquez sur **OK**.
5. Fermez la fenêtre **Éditeur de gestion des stratégies de groupe** et la **Console de gestion des stratégies de groupe**.

## Démonstration : Configuration d'une stratégie de mots de passe fine

### Procédure de démonstration

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Dans le **Centre d'administration Active Directory**, dans le volet de navigation, cliquez sur **Adatum (local)**.
3. Dans le volet d'informations, double-cliquez sur l'unité d'organisation **Gestionnaires**.
4. Dans le volet d'informations, repérez et cliquez avec le bouton droit sur le groupe **Gestionnaires**, puis cliquez sur **Propriétés**.

   **Remarque :** Assurez-vous d'ouvrir la boîte de dialogue **Propriétés** pour le groupe des gestionnaires et non des gestionnaires UO.

5. Dans la boîte de dialogue **Gestionnaires**, sous **Étendue** du groupe, cliquez sur **Global**, puis cliquez sur **OK**.
6. Dans le **Centre d'administration Active Directory**, dans le volet de navigation, cliquez sur **Adatum (local)**.
7. Dans le volet d'informations, double-cliquez sur **Conteneur système**.
8. Dans le volet d'informations, cliquez-droit sur le Classe d'**Classe d'objets PSC**, cliquez sur **Nouveau**, puis sur **Paramètres de mot de passe**.
9. Dans la fenêtre **Créer les paramètres de mot de passe**, procédez comme suit :
   a. Dans le champ **Nom**, saisissez **GestionnairesPSO**.
   b. Dans le champ **Priorité**, saisissez **10**.
   c. Cochez la case **Appliquer la longueur minimale du mot de passe**, puis dans le champ **longueur du mot de passe minimum (caractères)**, tapez **15**.
   d. Cochez la case **Appliquer l'historique du mot de passe**, puis dans le champ **Nombre de mots de passe conservés**, tapez **20**.

e. Sélectionnez le **Mot de passe doit répondre aux exigences de complexité** activez la case à cocher.

f. Cochez la case **Appliquer la durée de vie minimale du mot de passe**, puis dans le champ **Utilisateur ne peut pas changer le mot de passe pendant (jours) 1**.

g. Cochez la case **Appliquer la durée de vie minimale du mot de passe**, puis dans le type de champ **Utilisateur doit changer le mot de passe après (jours) 30**.

h. Cochez la case **Appliquer la stratégie de verrouillage du compte**.

i. Dans le champ **Nombre de tentatives de connexion autorisées**, tapez **3**.

j. Dans le champ **Réinitialiser l'échec des tentatives d'ouverture de session compte** tapez **30**, puis cliquez sur **Jusqu'à ce qu'un administrateur déverrouille manuellement le compte**.

10. Dans la section **S'applique directement à**, cliquez sur **Ajouter**.
11. Dans la zone de texte **Entrez le nom de l'objet à sélectionner**, tapez **Adatum\Gestionnaires**, cliquez sur **Vérifier les noms** puis validez avec OK.
12. Dans les **Paramètres de création de mot de passe : ManagersPSO**, cliquez sur **OK**.
13. Fermez le **Centre d'administration Active Directory**.

Leçon 3

# Mise en œuvre d'authentification d'audit

## Sommaire :

## Questions et réponses

**Question :** Lorsqu'un utilisateur se connecte à un contrôleur de domaine, un événement d'ouverture de session est généré.

( ) Vrai

( ) Faux

**Réponse :**

( ) Vrai

(√) Faux

**Commentaire :**

Lorsqu'un utilisateur se connecte à un contrôleur de domaine, un événement de compte d'ouverture de session et non un événement d'ouverture de session, est généré.

## Démonstration : Configuration des stratégies de vérification liées à l'authentification

### Procédure de démonstration

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur le menu **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 Contrôleurs 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 locales**, puis cliquez sur **Stratégie d'audit**.
5. Dans le volet de détails, double-cliquez sur **Événements de compte d'ouverture de session d'audit**, puis expliquez les options de configuration suivantes :
   - Si vous activez la case à cocher **Définir ces paramètres de stratégie**, la stratégie est appliquée.
   - Si vous sélectionnez **Succès**, seuls audits de succès sont enregistrés.
   - Si vous sélectionnez **Échec**, seuls audits d'échec sont enregistrés.

   Si plusieurs stratégies contiennent le paramètre et qu'il est défini différemment, les options de réussite et d'échec s'appliquent selon la dernière stratégie appliquée qui définit ces paramètres. Si une stratégie définit les audits des succès et qu'une autre définit les audits des échecs, ils ne se confondent pas.
6. Sur l'onglet **Expliquer**, affichez l'explication et discutez-en. Cliquez sur **Annuler** pour fermer la boite de dialogue **Propriétés des événements de compte d'ouverture de session d'audit**.
7. Répétez les étapes cinq et six avec la stratégie **Événements d'ouverture de session d'audit**.
8. Dans la fenêtre **Éditeur de gestion des stratégies de groupe**, dans le volet de navigation, développez **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Audit avancé\Configuration de la stratégie\Stratégies d'audit**, puis cliquez sur **Stratégie d'audit**.

9. Dans la stratégie **Stratégies d'audit**, affichez les dix catégories principales, puis cliquez **sur compte d'ouverture de session**.
10. Affichez les quatre sous-catégories, puis double-cliquez sur **Service d'authentification Audit Kerberos**.
11. Montrer que la sous-catégorie a les mêmes paramètres que dans la **Stratégie d'audit de compte d'ouverture de session d'audit**, puis expliquez qu'ils sont maintenant à un niveau plus détaillé et qu'ils permettent une vérification plus sélective.
12. Sélectionnez **Configurer les événements d'audit suivants**, sélectionnez **Succès**, sélectionnez **Échec**, puis cliquez sur **Appliquer**.
13. Sur l'onglet **Expliquer**, affichez l'explication, les paramètres par défaut, le volume d'audit prévu et discutez-en.
14. Pour fermer la boîte de dialogue **Propriétés des services d'authentification Audit Kerberos**, cliquez sur **OK**.

## Démonstration : Affichage des événements d'ouverture de session

### Procédure de démonstration

1. Sur **LON-DC1**, sur l'écran d'accueil, tapez **cmd**, puis cliquez sur **Invite de commandes**.
2. Tapez **gpupdate /force** et appuyez sur Entrée.
3. Patientez jusqu'à ce que la stratégie ait été mise à jour.
4. Basculez vers l'écran Démarrer. Dans le coin supérieur droit, cliquez sur **Administrateur**, puis sur **Se déconnecter**.
5. Sur **LON-DC1**, essayez de vous connecter en tant **Adatum\Aidan** avec mot de passe **123456**.
6. Vous recevez un message indiquant que le nom d'utilisateur ou le mot de passe est incorrect. Cliquez sur **OK**.
7. Connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
8. Patientez jusqu'à ce que l'ouverture de session soit terminée et que le **Gestionnaire de serveur** ait commencé.
9. Dans le **Gestionnaire de serveurs**, cliquez sur **Outils**, puis sur **Observateur d'événements**.
10. Dans l'Observateur d'événements, dans le volet de navigation, développez **Journaux Windows**, puis cliquez sur **Sécurité**.
11. Dans le volet d'informations, recherchez l'**ID d'événement 4771**, puis montrez que cet événement est un événement d'échec de l'audit. Double-cliquez sur l'**événement d'échec de l'audit**. Montrez que cet événement a été enregistré lorsque Adatum\Aidan a essayé de se connecter avec le mot de passe erroné. Cliquez sur **Fermer**.
12. Localisez l'événement avec l'**ID d'événement 4768**. Montrez que ceci est un événement de succès de l'audit. Double-cliquez sur **Événement de succès** de l'audit. Montrez que cet événement a été enregistré lorsque Adatum\Administrateur s'est connecté avec succès. Cliquez sur **Fermer**.
13. Fermez l'Observateur d'événements.

Leçon 4

# Configuration des comptes de services administrés (MSA)

## Sommaire :

## Questions et réponses

**Question :** En quoi les MSA de groupe différent-ils des MSA standards ?

> **Réponse :** Les MSA de groupe vous permettent d'étendre les capacités des MSA standards sur plus d'un serveur dans votre domaine.

## Démonstration : Configuration des MSA de groupe

### Procédure de démonstration

### Créer la racine principale KDS pour le domaine

1. Sur **LON-DC1**, à partir du **Gestionnaire de serveur**, cliquez sur **Outils** et ouvrir la console **Module Active Directory pour Windows PowerShell**.
2. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours (-10))
```

### Créer et associer un MSA

1. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée.

```
Nouvelle-ADServiceAccount -Name SampleApp_SVR1 -DNSHostname LON-DC1.Adatum.com -
PrincipalsAllowedToRetrieveManagedPassword LON-SVR1 $
```

2. À l'invite de commandes, tapez la commande suivanteet appuyez sur Entrée :

```
Add-ADComputerServiceAccount -identity LON-SVR1 -ServiceAccount SampleApp_SVR1
```

3. À l'invite de commandes, tapez la commande suivanteet appuyez sur Entrée :

```
Get-ADServiceAccount -Filter *
```

4. Vérifiez que le compte de service **SampleApp_SVR1** est répertorié.

### Installer un MSA

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, cliquez sur **Gestionnaire de serveur**. Ensuite, à partir du menu **Outils**, ouvrez la console **Module Active Directory pour Windows PowerShell**.
2. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
Install-ADServiceAccount -Identity SampleApp_SVR1
```

3. Dans le **Gestionnaire de serveur**, cliquez sur la barre d'outils **Menu**, sur **Outils** puis sur **Services**.
4. Dans la console **Services**, cliquez avec le bouton droit sur **Service de partage de données** puis cliquez sur **Propriétés**.

> **Remarque :** Cette démonstration utilise le service de partage de données comme exemple. Dans un environnement de production, vous pouvez utiliser le service auquel le MSA doit être assigné.

5. Dans la boîte de dialogue **Propriétés du service de partage de données (ordinateur local)**, cliquez sur l'onglet **Se connecter**.
6. Sur l'onglet **Se connecter**, cliquez sur **Ce compte**, puis tapez **Adatum\SampleApp_SVR1$**.

7. Effacer le mot de passe à la fois pour les boîtes **Mot de passe et Confirmer le mot de passe**, puis cliquez sur **OK**.
8. Cliquez **OK** à toutes les invites.

# Contrôle des acquis et éléments à retenir

## Questions de contrôle des acquis

**Question :** Pourquoi la sécurité physique est-elle si importante, en particulier pour les contrôleurs de domaine AD DS ?

**Réponse :** Les contrôleurs de domaine AD DS stockent toutes les informations sur tous les utilisateurs, les ordinateurs, les groupes et tous les autres objets dans le domaine. Si une personne accède physiquement au serveur ou son disque dur, cette personne peut contourner les mesures de sécurité facilement et récupérer toutes ces informations. Cette personne peut alors utiliser l'information pour attaquer votre réseau, ou pourrait modifier votre contrôleur de domaine et le remettre dans le réseau avec une intention malveillante.

**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 ?

**Réponse :** Si vous voulez activer l'audit, il est très important que vous configuriez les mêmes paramètres d'audit pour tous les serveurs pertinents sur lesquels l'événement est susceptible de se produire. Si vous souhaitez configurer l'audit pour l'authentification de domaine ou des modifications dans AD DS, configurez ces paramètres dans la stratégie des contrôleurs de domaine par défaut ou d'un GPO qui est lié à l'unité d'organisation des contrôleurs de domaine.

**Question :** Votre organisation vous oblige à assurer la maintenance d'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 du compte. Que devez-vous prendre en considération ?

**Réponse :** Les paramètres de verrouillage du compte ne sont pas seulement une fonction de sécurité. Ils fournissent également aux attaquants une interface DoS facilement accessible. Si Outlook Web Access est accessible à partir de l'Internet, vous devez configurer des protocoles ou des services supplémentaires pour garantir que seuls les utilisateurs de votre domaine sont en mesure d'entrer leurs informations d'identification d'ouverture de session. Les autres utilisateurs ne doivent pas être autorisés à utiliser le site pour entrer des mots de passe erronés et verrouiller les comptes d'utilisateur valides.

## Outils

Le tableau suivant répertorie les outils référencés par ce module.

| 1. Outil | 2. Utilisation | 3. 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 |

| 1. Outil | 2. Utilisation | 3. Emplacement |
|---|---|---|
| Gpupdate.exe | Mise à jour manuelle des GPO des machines locales. | Ligne de commande |

## 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. | Vérifiez que vous avez défini la **Vérification : Paramètre de stratégie Obliger les paramètres de sous-catégorie de stratégie d'audit (Windows Vista ou version ultérieure) à remplacer les paramètres de catégorie** de stratégie d'audit sous **Configuration ordinateur\Stratégies \Paramètres Windows\Paramètres de sécurité \Stratégies locales\Options de sécurité**. |
| Vous avez configuré la vérification du compte d'ouverture de session ou des changements des services de répertoire. Maintenant, vous pouvez les tester, mais vous ne trouvez pas les événements dans le journal des événements de votre serveur. | Si vous avez plusieurs contrôleurs de domaine, vous avez besoin de regarder le journal de sécurité de chaque contrôleur de domaine. En outre, assurez-vous que la stratégie d'audit est configurée pour chaque contrôleur de domaine. |

# Questions et réponses de l'atelier pratique

## Atelier pratique : Sécurisation AD DS

## Questions et réponses

**Question :** Dans l'atelier pratique, 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 disponibles pour vous aider à atteindre la solution ?

**Réponse :** il se peut que vous ayez créé un PSO avec des paramètres spécifiques pour tous les utilisateurs, configurés avec une très haute priorité et liés au groupe de sécurité Utilisateurs du domaine. L'avantage est qu'il n'y a qu'une seule interface pour la gestion des stratégies de mot de passe de domaine et les paramètres par défaut pour les comptes locaux sur les membres du domaine peuvent être réglés différemment à travers l'ensemble du domaine.

**Question :** Dans l'atelier pratique, pour le PSO administratif, vous utilisiez la priorité d'une valeur de 10. Pourquoi faire cela ?

**Réponse :** Le PSO administratif est très restrictif, de sorte que la priorité devrait être faible. Cependant, il peut y avoir des groupes d'administrateurs à l'avenir avec des paramètres plus restrictifs, comme un sous-ensemble des administrateurs pour accéder aux données de ressources humaines ou des comptes de services pour lesquels vous pourrez vouloir imposer plus des mots de passe plus longs avec des droits administratifs qui changent moins fréquemment. Pour toutes ces raisons, l'utilisation d'une valeur de 10 permet un certain espace pour la mise en œuvre des PSO qui sont plus précis.

# Module 8

## Déploiement et gestion AD CS

### Sommaire :

Leçon 1

# Déploiement des AC

## Sommaire :

## Questions et réponses

**Question :** Lesquelles des options suivantes décrivent les avantages du déploiement d'une AC d'entreprise au lieu d'une AC autonome ?

( ) 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 mise hors ligne pour éviter un compromis.

( ) Peut utiliser des modèles pour émettre des certificats basés sur les données dans AD DS.

**Réponse :**

(√) 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 mise hors ligne pour éviter un compromis.

(√) Peut utiliser des modèles pour émettre des certificats basés sur les données dans AD DS.

**Commentaire :**

Les avantages d'une AC d'entreprise sont que vous pouvez profiter de multiples façons de vous inscrire à des certificats, y compris pour une inscription automatique à l'aide de modèles de certificats. Les AC d'entreprise permettent également l'approbation ou le refus automatique des demandes fondées sur des stratégies d'émission. Une AC d'entreprise, cependant, nécessite AD DS et doit être maintenue en ligne pour faciliter l'inscription du certificat.

**Question :** Lesquelles des options suivantes sont des raisons pour déployer plusieurs AC secondaires ?

( ) Vous voulez segmenter l'émission de certificats selon des politiques d'utilisation uniques.

( ) Vous avez plusieurs domaines dans votre environnement AD DS et chaque domaine exige sa propre autorité de certification secondaire.

( ) Vous voulez segmenter l'émission de certificats selon la division organisationnelle ou d'une région géographique.

( ) Vous voulez plusieurs AC subordonnées pour la haute disponibilité et l'équilibrage de charge des demandes.

( ) Vous avez besoin de publier des modèles de certificat multiples et chaque modèle nécessite sa propre autorité de certification secondaire.

**Réponse :**

(√) Vous voulez segmenter l'émission de certificats selon des politiques d'utilisation uniques.

( ) Vous avez plusieurs domaines dans votre environnement AD DS et chaque domaine exige sa propre autorité de certification secondaire.

(√) Vous voulez segmenter l'émission de certificats selon la division organisationnelle ou d'une région géographique.

(√) Vous voulez plusieurs AC subordonnées pour la haute disponibilité et l'équilibrage de charge des demandes.

( ) Vous avez besoin de publier des modèles de certificat multiples et chaque modèle nécessite sa propre autorité de certification secondaire.

**Commentaire :**

Vous pouvez déployer plusieurs AC pour les politiques uniques d'utilisation, les divisions organisationnelles ou les régions géographiques. En outre, vous pouvez déployer plusieurs AC pour assurer la haute disponibilité pour l'équilibrage de charge des demandes.

Les AC subordonnées multiples ne sont pas nécessaires dans un environnement multi-domaine AD DS, bien que vous pourriez utiliser cette approche si vos domaines AD DS s'alignent déjà aux divisions organisationnelles ou aux régions géographiques. Les AC subordonnées multiples ne sont pas nécessaires si vous avez besoin de publier différents modèles de certificats, car une AC peut être configurée pour délivrer des certificats de plus d'un modèle.

# Démonstration : Déploiement d'une AC racine d'entreprise

## Étapes de la démonstration

## Déployer une AC racine d'entreprise

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, puis cliquez sur **Gestionnaire de serveur**.
2. 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**.
7. Dans **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
8. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Sur la page **Services de certificats Active Directory**, cliquez sur **Suivant**.
10. Sur la page **Sélectionner les services** de rôle, vérifiez que l'**Autorité de certification** est sélectionnée, puis cliquez sur **Suivant**.
11. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
12. Sur la page **Progression de l'installation** après la fin de l'installation, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination.**
13. Dans l'assistant de **Configuration AD CS**, sur la page **Informations d'identification**, cliquez sur **Suivant**.
14. Sur la page **Services de rôle**, sélectionnez **Autorité de certification**, puis cliquez sur **Suivant**.
15. Sur la page **Type d'installation**, sélectionnez **Enterprise AC**, puis cliquez sur **Suivant**.
16. Sur la page **Type d'AC**, sélectionnez l'option **AC Racine**, puis cliquez sur **Suivant**.
17. Sur la page **Clé privée**, vérifiez que **Créer une nouvelle clé privée** est sélectionné, puis cliquez sur **Suivant**.
18. Sur la page **Cryptographie pour AC**, conservez les sélections par défaut pour le fournisseur de services cryptographiques (CSP) et l'algorithme de hachage, mais définissez la longueur clé de **4096**, puis cliquez sur **Suivant**.

19. Sur la page **Nom d'AC**, dans la zone **Nom habituel pour cette AC**, tapez **ACracineAdatum**, puis cliquez sur **Suivant**.
20. Sur la page **Période de validité**, cliquez sur **Suivant**.
21. Sur la page **Base de données AC**, cliquez sur **Suivant**.
22. Sur la page **Confirmation**, cliquez sur **Configurer**.
23. Sur la page **Résultats**, cliquez sur **Fermer**.
24. Sur la page **Progression de l'installation**, cliquez sur **Fermer**.

Leçon 2

# Administration des AC

## Sommaire :

## Questions et réponses

**Question :** Lesquelles des options suivantes sont des affirmations exactes concernant l'administration basée sur les rôles de votre déploiement AD CS ?

( ) 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 autorisations 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 qui se basent sur les besoins spécifiques de votre organisation.

( ) Le principal de sécurité des utilisateurs authentifiés peut s'inscrire pour un certificat publié sur un AC.

**Réponse :**

( ) 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 autorisations 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 qui se basent sur les besoins spécifiques de votre organisation.

( ) Le principal de sécurité des utilisateurs authentifiés peut s'inscrire pour un certificat publié sur un AC.

**Commentaire :**

L'administration basée sur les rôles dans AD CS est un concept, non une fonctionnalité qui est automatiquement installée ; par conséquent, vous devez créer manuellement des groupes de rôles. Après avoir créé un groupe de rôles, vous pouvez lui affecter une ou plusieurs des autorisations d'AC suivantes : Gérer AC, émettre et gérer des certificats, lire, demander des certificats. Vous pouvez personnaliser les rôles en fonction des besoins de votre organisation, y compris la restriction de l'autorisation des certificats d'émission et de gestion à un modèle spécifique ou un ensemble de modèles. Le principal de sécurité des utilisateurs authentifiés peut demander un certificat, mais le modèle de certificat contrôle la capacité à s'inscrire et non la AC elle-même.

**Question :** Lesquelles des affirmations suivantes sont correctes par rapport à l'extension AIA et CDP d'une AC ?

( ) Chaque extension nécessite un minimum de deux URL valides et accessibles pour la validation du certificat pour fonctionner correctement.

( ) Vous pouvez publier manuellement en mode hors connexion des certificats d'AC et des LCR autonomes sur un environnement AD DS.

( ) L'ordre dans lequel vous spécifiez les URL AIA et CDP n'est pas important, puisque le moteur de certificat-chaînage dicte automatiquement les emplacements en fonction de la connexion la plus rapide.

( ) Pour faciliter la validation du certificat pour les clients externes, vous devez publier les URL externes AIA et CDP en utilisant HTTP via un serveur Windows Server 2016 Web Application Proxy.

( ) Si vous utilisez une AC d'entreprise, la validation du certificat interne fonctionne sans aucune configuration supplémentaire.

**Réponse :**

( ) Chaque extension nécessite un minimum de deux URL valides et accessibles pour la validation du certificat pour fonctionner correctement.

(√) Vous pouvez publier manuellement en mode hors connexion des certificats d'AC et des LCR autonomes sur un environnement AD DS.

( ) L'ordre dans lequel vous spécifiez les URL AIA et CDP n'est pas important, puisque le moteur de certificat-chaînage dicte automatiquement les emplacements en fonction de la connexion la plus rapide.

(√) Pour faciliter la validation du certificat pour les clients externes, vous devez publier les URL externes AIA et CDP en utilisant HTTP via un serveur Windows Server 2016 Web Application Proxy.

(√) Si vous utilisez une AC d'entreprise, la validation du certificat interne fonctionne sans aucune configuration supplémentaire.

**Commentaire :**

Pour que la validation du certificat fonctionne, les extensions AIA et CDP doivent contenir au minimum un URL valide et accessible. Pour les AC hors ligne et autonomes, vous pouvez publier manuellement le certificat de l'AC et la liste de révocation de certificats dans AD DS. L'ordre des URL AIA et CDP est important, car le moteur de certificat-chaînage les cherche séquentiellement. Vous devez placer les URL les plus susceptibles d'être disponibles en haut de l'ordre d'URL. Afin de faciliter la validation du certificat pour les clients externes, vous pouvez publier les URL AIA et CDP en utilisant HTTP via un serveur Web 2016 Windows Application Proxy ou une tierce solution de proxy inverse. Si vous utilisez une AC d'entreprise, la validation du certificat fonctionne automatiquement pour les clients internes, mais peut exiger une configuration supplémentaire dans d'autres scénarios.

## Ressources

## Gestion des AC

**Lectures complémentaires :** Pour plus d'informations, veuillez consulter :

- « Déploiement d'applets de commandes AD DS dans Windows PowerShell » http://aka.ms/Giih2g à l'adresse :
- « Déploiement d'applets de commandes AD DS dans Windows PowerShell » http://aka.ms/Dekm5i à l'adresse :

## Démonstration : Configuration des propriétés de l'AC

### Étapes de la démonstration

1. Sur **LON-SVR1**, ouvrez le **Gestionnaire de serveur,** cliquez sur **Outils**, puis sur **Autorité de certification**.
2. Dans la console Certsrv, cliquez avec le bouton droit sur **ACracineAdatum**, puis sélectionnez **Propriétés**.
3. Dans l'onglet **Général**, cliquez sur **Voir le certificat**. Lorsque la fenêtre de certificat s'ouvre, examinez les données dans les onglets **Général**, **Détails** et **Chemin de certification**, puis cliquez sur **OK**.

4. Dans l'onglet **Module de stratégie**, cliquez sur **Propriétés**. Passez en revue les paramètres disponibles pour le module de stratégie par défaut, puis cliquez sur **OK**.
5. Sur l'onglet **Module de sortie**, cliquez sur **Propriétés**. Affichez les Paramètres de publication disponibles dans le module de Sortie par défaut, puis cliquez sur **OK**.
6. Dans l'onglet **Extensions**, examinez les options disponibles pour les extensions CDP et AIA sous la liste déroulante **Sélectionner l'extension**.
7. Dans l'onglet **Sécurité**, examinez les options disponibles dans la liste de contrôle d'accès (ACL) et examinez les autorisations par défaut.
8. Dans l'onglet **Gestionnaires de certificats**, examinez les options et expliquez comment limiter les entités de sécurité à des modèles de certificats spécifiques, puis cliquez sur **Annuler**.
9. Fermez la console Certsrv.

Leçon 3

# Dépannage et maintien des AC

## Sommaire :

## Questions et réponses

**Question :** Laquelle des questions suivantes pourrait empêcher l'inscription automatique de fonctionner correctement dans AD CS ?

( ) 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.

( ) Le modèle de certificat n'est pas publié sur une AC.

( ) L'URL AIA est configuré correctement dans l'onglet Extensions de l'AC.

**Réponse :**

(√) 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.

(√) Le modèle de certificat n'est pas publié sur une AC.

( ) L'URL AIA est configuré correctement dans l'onglet Extensions de l'AC.

**Commentaire :**

La succession d'un objet de stratégie de groupe est un problème commun qui peut empêcher l'inscription automatique. Les utilisateurs et les ordinateurs doivent être dans une organisation AD DS où vous avez lié les paramètres requis GPO et où vous n'avez pas bloqué la succession de la stratégie. En outre, les AC doivent être des AC d'entreprise pour que l'inscription automatique fonctionne correctement, car les clients utilisent AD DS pour déterminer les AC disponibles et les modèles. Vous devez publier des modèles sur une AC d'entreprise et l'utilisateur ou l'ordinateur doit disposer des autorisations d'inscription automatique configurées sur le modèle. Un URL AIA ou CDP invalide configuré sur l'AC n'empêche pas l'inscription automatique, mais il peut empêcher la validation correcte du certificat lorsqu'il est utilisé par une application ou un service client.

**Question :** Lesquelles des affirmations suivantes sont exactes au sujet de l'outil PKIView ?

( ) PKIView affiche tous vos AC d'entreprise et leur état de santé actuel.

( ) Vous pouvez utiliser PKIView pour ajouter manuellement les 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 Répondeur en ligne de l'AD CS.

**Réponse :**

(√) PKIView montre l'ensemble de vos AC d'entreprise et de leur état de santé actuel.

( ) Vous pouvez utiliser PKIView pour ajouter manuellement les 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 Répondeur en ligne de l'AD CS.

**Commentaire :**

Vous pouvez utiliser PKIView pour voir l'ensemble de vos AC d'entreprise et leur état de santé actuel, mais il ne peut pas afficher l'état d'une autorité de certification autonome Vous avez configuré l'inscription automatique pour les utilisateurs et les ordinateurs via la stratégie de groupe et non pas à travers l'outil PKIView. PKIView vous permet d'évaluer l'état de CDP et AIA pour chaque emplacement défini sur chaque AC, ainsi que le statut du service de rôle Répondeur en ligne de l'AD CS, si vous l'avez déployé.

# Contrôle des acquis et éléments à retenir

## Méthodes conseillées

- Lors du déploiement d'une infrastructure d'AC, déployez une AC 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.
- Fournissez plus d'un emplacement pour l'AIA et la liste de révocation de certificats.

## Questions de contrôle des acquis

**Question :** Quelles sont les raisons pour lesquelles une organisation utiliserait une PKI ?

**Réponse :** Certaines des raisons expliquant l'utilisation d'une PKI comprennent l'amélioration de la sécurité, l'augmentation du contrôle d'identité et signature numérique du code.

**Question :** Pourquoi voudriez-vous déployer une stratégie personnalisée et des modules de sortie ?

**Réponse :** Si vous avez une demande supplémentaire pour la gestion des certificats, tels que la Gestion de certificats MIM, vous devez installer des modules de stratégie et de sortie personnalisés afin de pouvoir intégrer votre application avec AC.

## Outils

- Console d'administration de l'AC
- Utilitaire de ligne de commande Certutil
- Interface de ligne de commande Windows PowerShell
- Pkiview.msc
- Gestionnaire de serveur

## Problèmes courants et conseils de dépannage

| 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 générer une chaîne de certificats et la validation du certificat pourrait échouer. | Utilisez le composant logiciel enfichable de l'autorité de certification pour configurer l'extension AIA afin d'inclure le nom du certificat suffixe dans chaque emplacement. |
| L'AC n'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 liste de révocation de certificats pour vérifier l'état de révocation d'un certificat et la validation du certificat pourrait échouer. | Utilisez le composant logiciel enfichable de l'autorité de certification pour configurer l'extension CDP et pour spécifier l'emplacement du réseau de la liste de révocation de certificats. |

# Questions et réponses sur les ateliers pratiques

## Atelier pratique : Déploiement et configuration d'une hiérarchie AC à deux niveaux

## Questions et réponses

**Question :** Pourquoi n'est-il pas recommandé d'installer seulement une AC racine d'entreprise ?

> **Réponse :** Pour des raisons de sécurité, une autorité de certification racine doit être mise hors ligne et ne devrait pas avoir accès au réseau. Étant donné que l'AC racine d'entreprise ne peut pas être déconnectée, vous ne pouvez pas fournir une protection maximale pour sa clé et son identité.

**Question :** Quelles sont les raisons pour lesquelles une organisation utiliserait une AC racine d'entreprise ?

> **Réponse :** Si une organisation veut utiliser une seule AC et veut utiliser les modèles de certificats et l'inscription automatique, une AC racine d'entreprise est le seul choix.

# Module 9

## Déploiement et gestion de certificats

### Sommaire :

Leçon 1

# Déploiement et gestion des modèles de certificats

## Sommaire :

## Questions et réponses

**Question :** Lesquels des énoncés suivants sont vrais en ce qui concerne les modèles de certificats de version 2 dans AD CS ? (Choisissez toutes les réponses applicables.)

( ) Les modèles version 2 prennent en charge l'inscription automatique.

( ) Vous pouvez modifier uniquement l'onglet Sécurité sur un modèle de 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 sur Windows Server 2008 et Windows Vista ou sur des systèmes d'exploitation plus récents.

( ) Les modèles version 2 sont uniquement pris en charge sur Windows Server 2012 et Windows 8 ou sur des systèmes d'exploitation plus récents.

**Réponse :**

(√) Les modèles version 2 prennent en charge l'inscription automatique.

( ) Vous pouvez modifier uniquement l'onglet Sécurité sur un modèle de 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 sur Windows Server 2008 et Windows Vista ou sur des systèmes d'exploitation plus récents.

( ) Les modèles version 2 sont uniquement pris en charge sur Windows Server 2012 et Windows 8 ou sur des systèmes d'exploitation plus récents.

**Commentaire :**

Un aspect important des modèles de version 2 est qu'ils prennent en charge l'inscription automatique par les utilisateurs et les ordinateurs AD DS. Contrairement aux modèles de version 1, vous pouvez modifier tous les aspects d'un modèle de version 2. Pour passer à un modèle de version 2, vous pouvez dupliquer un modèle de version 1. Les modèles de version 2 sont pris en charge sur Windows Server 2003 Enterprise Edition, Windows Server 2008 Enterprise et Windows Server 2008 R2 et versions ultérieures. Les modèles de version 2 sont entièrement pris en charge tant que l'AC exécute Windows Server 2008 ou des versions ultérieures.

**Question :** Vous êtes l'administrateur AD DS pour A. Datum Corporation. Plusieurs utilisateurs dans votre environnement AD DS se sont inscrits automatiquement pour un certificat d'utilisateur. Vous voulez raccourcir la période de validité du certificat d'utilisateur et vous 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.)

( ) Dupliquer le modèle existant et fournir un nouveau nom de modèle. Modifier de 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 d'utilisateur émis à partir du modèle existant.

( ) Modifier le nouveau modèle afin qu'il remplace le modèle existant. Publier le nouveau modèle.

**Réponse :**

(√) Dupliquer le modèle existant et fournir un nouveau nom de modèle. Modifier de 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 d'utilisateur émis à partir du modèle existant.

(√) Modifier le nouveau modèle afin qu'il remplace le modèle existant. Publier le nouveau modèle.

**Commentaire :**

Dans cette situation, vous devez dupliquer le modèle existant, en fournissant un nouveau nom de modèle et une nouvelle période de validité. En outre, vous devez mettre à jour le nouveau modèle afin qu'il remplace le modèle précédent. Après avoir publié le nouveau modèle à une AC d'entreprise, les utilisateurs qui s'étaient inscrits automatiquement contre le modèle précédent s'inscriront automatiquement à nouveau pour le nouveau modèle. Une fois que les nouveaux certificats avec la période de validité correcte auront remplacé les certificats émis antérieurement, vous devrez révoquer tous les certificats d'utilisateur à partir du modèle existant de sorte qu'ils ne peuvent plus être utilisés.

Si vous modifiez la période de validité du modèle existant, les nouvelles inscriptions contre le modèle auront les bons réglages, mais les certificats émis antérieurement contiendront encore la période de validité non désirée. La modification des paramètres d'inscription automatique sur le modèle existant n'est pas nécessaire et ne produirait pas l'effet désiré.

## Démonstration : Modification et autorisation d'un modèle de certificat

### Procédure de démonstration

1. Sur **LON-DC1**, dans le **Gestionnaire de serveurs**, cliquez sur **Outils**, puis sur **Autorité de certification**.
2. Dans la console **Autorité de certification**, développez le nœud **AdatumCA**, clic-droit sur **Modèles de certificats**, puis cliquez sur **Gérer**.
3. Passez en revue la liste des modèles par défaut. Examinez les modèles et leurs propriétés.
4. Dans le **volet d'informations**, double-cliquez sur **IPSec**.
5. Dans la boîte de dialogue **Propriétés IPsec**, cliquez sur les onglets, puis notez ce que vous pouvez modifier sur chacun. Notez que dans l'onglet **Sécurité**, vous pouvez définir des autorisations pour l'inscription. Cliquez sur **Annuler** pour fermer le modèle.
6. Dans la **Console Modèles de certificats**, dans le **voletd'informations**, faites clic-droit sur le modèle de certificat **Échange Utilisateur**, puis cliquez sur **Dupliquer le modèle**.
7. Dans la boîte de dialogue **Propriétés du nouveau modèle**, révisez les options dans l'onglet **Compatibilité**.
8. Cliquez sur l'onglet **Général**, puis dans la zone de texte **Modèle Afficher un nom**, tapez **Échange Utilisateur Test1**.
9. Cliquez sur l'onglet **Modèles remplacés**, puis cliquez sur **Ajouter.**
10. Cliquez sur le modèle **Changer d'utilisateur**, puis cliquez sur **OK**.
11. Cliquez sur l'onglet **Sécurité**, puis sur **Utilisateurs authentifiés.**
12. Sous le nœud **Autorisations pour les utilisateurs authentifiés**, cochez les cases **Autoriser** à la fois **pourInscrire** et **Inscription** automatique, puis cliquez sur **OK**.
13. Fermer la console **Modèles de certificats**.
14. 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 émettre**.

15. Dans la boîte de dialogue **Activer les modèles de certificats**, cliquez sur le certificat **Échange Utilisateur Test1**, puis sur **OK**.

Leçon 2

# Gestion du déploiement, de la révocation et de la récupération de certificats

## Sommaire :

## Questions et réponses

**Question :** Lorsque vous révoquez un certificat, où est publiée l'empreinte du certificat ?

( ) Point de distribution de la liste de révocation de certificats (CDP)

( ) Accès aux informations sur l'Autorité (AIA)

( ) Liste de révocation des certificats (CRL)

( ) AD DS

( ) Le service de répondeur en ligne

**Réponse :**

( ) Point de distribution de la liste de révocation de certificats (CDP)

( ) Accès aux informations sur l'Autorité (AIA)

(√) Liste de révocation des certificats (CRL)

( ) AD DS

( ) Le service de répondeur en ligne

**Commentaire :**

Lorsque vous révoquez un certificat, l'empreinte du certificat est publiée à la liste de révocation de certificats (LRC). Un point de distribution de LRC (CDP) est l'emplacement de l'URL où la LRC est stockée. L'accès aux informations de l'autorité (AIA) est l'URL où le certificat de l'AC est situé. AD DS est un emplacement valide pour un CDP, mais les certificats révoqués ne sont pas directement publiés sur l'AD DS. Un service de Répondeur en ligne valide l'état d'un certificat spécifique à l'aide d'une copie locale de la LCR, mais les certificats révoqués ne sont pas publiés directement à un service de Répondeur en ligne.

**Question :** Lesquelles des mesures suivantes devez vous effectuer pour configurer l'archivage principal sur une AC AD CS ? (Choisissez toutes les réponses applicables.)

( ) 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 nécessaires pour l'archivage des clés

**Réponse :**

(√) 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 nécessaires pour l'archivage des clés

**Commentaire :**

Pour configurer l'archivage de clés, vous devez :

1. Configurer le certificat KRA afin que seuls les utilisateurs de confiance peuvent inscrire un certificat.
2. Inscrire un utilisateur de confiance au certificat KRA.

3. Configurer un agent de récupération sur l'autorité de certification via le certificat KRA.
4. Configurer les modèles de certificats souhaités pour l'archivage de clé.

Il est inutile de publier la clé publique KRA en utilisant la stratégie de groupe.

## Démonstration : Configuration d'un AC pour l'rchivage principal

### Étapes de la démonstration

1. Sur **LON-DC1**, dans le **Gestionnaire de serveurs**, cliquez sur **Outils**, puis sur **Autorité de certification**. Dans la console **Autorité de certification**, développez le nœud **AdatumCA**, clic 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**, désactivez la case à cocher **Approbation du gestionnaire de certificats de l'AC**, puis cliquez sur l'onglet **sécurité**. Vérifiez que les groupes Administrateurs du domaine et Administrateurs de l'entreprise sont les seuls groupes qui ont **l'autorisation** d'Inscrire, puis cliquez sur **OK**.
4. Fermer la console **Modèles de certificats**.
5. 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 émettre**.
6. Dans la boîte de dialogue **Activer les modèles de certificats**, cliquez sur le modèle **Agent de récupération de clé**, puis sur **OK**.
7. Cliquez sur **Démarrer**, puis cliquez sur l'icône **Windows PowerShell**.
8. À l'invite de commandes Windows PowerShell, tapez **mmc.exe**, puis appuyez sur Entrée.
9. Dans **Console1 - [Racine de la console]**, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
10. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **Certificats**, puis sur **Ajouter**.
11. Dans la boîte de dialogue **Composant logiciel enfichable Certificats**, sélectionnez **Mon compte d'utilisateur**, cliquez sur **Terminer**, puis sur **OK**.
12. 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**.
13. Dans **l'Assistant Inscription de certificats**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
14. Sur la page **Sélectionner la stratégie d'inscription du certificat**, cliquez sur **Suivant**.
15. Sur la page **Demander des certificats**, cochez la case **Agent de récupération de clé**, cliquez sur **Inscrire**, puis sur **Terminer**.
16. Actualisez la console, puis affichez la KRA dans le magasin personnel ; c'est-à-dire, parcourez les propriétés du certificat et vérifiez que le modèle de certificat avec le but visé **Agent de récupération de clé** est présent.
17. Fermez la **Console1** sans enregistrer les modifications.
18. Retournez à la console **Autorité de certification**, cliquez avec le bouton droit sur **AdatumCA**, puis cliquez sur **Propriétés**.

19. Dans la boîte de dialogue **Propriétés AdatumCA**, cliquez sur l'onglet **Agents de récupération**, puis sélectionnez **Archiver la clé**.
20. Sous certificats d'agent de récupération de clé, cliquez sur **Ajouter**.
21. Dans la boîte de dialogue Sélection de l'**Agent de récupération de clé**, cliquez sur le certificat qui est le but KRA (le plus probable sera le dernier sur la liste publiée à l'**Administrateur**), puis cliquez sur **OK** deux fois.
22. Lorsque vous êtes invité à redémarrer l'AC, cliquez sur **Oui**.

Leçon 3

# Utilisation de certificats dans un contexte commercial

## Sommaire :

## Questions et réponses

**Question :** Lesquelles des affirmations suivantes sont correctes au sujet de l'utilisation de certificats dans un environnement commercial ? (Choisissez toutes les réponses applicables.)

( ) 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.

**Réponse :**

(√) 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.

**Commentaire :**

Les certificats peuvent être utilisés pour crypter le trafic HTTP, pour signer numériquement et / ou crypter des documents et des e-mails et pour l'authentification client / serveur. Les documents signés numériquement sont invalidés si les contenus sont modifiés. Pour envoyer un e-mail crypté à un destinataire externe, vous pouvez utiliser soit un certificat interne ou publiquement émis tant que vous avez accès à la clé publique du destinataire. Les fichiers cryptés avec EFS peuvent être lus par l'individu qui a crypté le fichier et par tous les utilisateurs explicitement désignés pour le partage EFS. Si la clé privée du cryptage individuel est perdue ou supprimée, un agent de récupération de données peut accéder au fichier ou un agent de récupération de clé peut être utilisé pour récupérer la clé privée si l'archivage de clés a été préalablement configuré sur le modèle de certificat EFS et l'AC émettrice.

**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. Parmi les étapes suivantes, lesquelles sont nécessaires ?

( ) Activer un agent de récupération de clé.

( ) Activer un agent de récupération de données.

( ) Publier le modèle de certificat d'utilisateur et configurer les groupes souhaités des utilisateurs pour l'inscription automatique.

( ) Activer EFS sur les ordinateurs de domaine AD DS en utilisant la stratégie de groupe.

( ) Mettre à jour tous les ordinateurs du domaine AD DS vers Windows Server 2016 ou Windows 10.

**Réponse :**

( ) Activer un agent de récupération de clé.

( ) Activer un agent de récupération de données.

(√) Publier le modèle de certificat d'utilisateur et configurer les groupes souhaités des utilisateurs pour l'inscription automatique.

( ) Activer EFS sur les ordinateurs de domaine AD DS en utilisant la stratégie de groupe.

( ) Mettre à jour tous les ordinateurs du domaine AD DS vers Windows Server 2016 ou Windows 10.

**Commentaire :**

Pour activer la signature numérique et le cryptage, vous ne devriez avoir besoin de publier le modèle de certificat d'utilisateur et de le configurer pour l'inscription automatique. Bien que l'utilisation d'un agent de récupération de clé et d'un agent de récupération de données soit la meilleure pratique, ceux-ci ne sont pas nécessaires pour permettre les signatures numériques et le cryptage. Vous ne devez activer EFS sur les ordinateurs de domaine AD DS, vous ne devez pas non plus mettre à jour tous les ordinateurs AD DS de domaine vers Windows Server 2016 ou Windows 10.

## Démonstration : Signature d'un document numérique

### Procédure de démonstration

1. Sur **LON-CL1**, ouvre l'interface de ligne de commande **Windows PowerShell**.
2. À l'invite de commandes **Windows PowerShell**, tapez **mmc.exe**, puis appuyez sur Entrée.
3. Dans la fenêtre **Console1 - [Racine de la console]**, cliquez sur le menu **Fichier**, puis sélectionnez **Ajouter/Supprimer un composant logiciel enfichable**.
4. Sélectionnez **Certificats**, cliquez sur **Ajouter**, sélectionnez **Mon compte d'utilisateur**, puis sur **Terminer** et **OK**.
5. Développez le nœud **Certificats - Utilisateur actuel**, cliquez avec le bouton droit sur **Personnel**, sélectionnez **Toutes les** tâches, puis cliquez sur **Demander un nouveau certificat**.
6. Dans **Assistant Inscription de certificat**, cliquez sur **Suivant** deux fois.
7. Sur la page **certificat d'inscription**, dans la liste des modèles disponibles, sélectionnez **Utilisateur**, cliquez sur **Inscrire**, puis cliquez sur **Terminer**.
8. Fermez la fenêtre **Console1 - [Console Root]** sans enregistrer les modifications.
9. Ouvrez Word 2016.

**Remarque :** Si l'**Assistant Activation Microsoft Office** apparaît, cliquez sur **Fermer**. Cliquez sur **Demandez-moi plus tard**, puis cliquez sur **Accepter**.

10. Dans un document vierge, tapez du texte, puis enregistrez le fichier sur le bureau.
11. 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**.
12. 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**.
13. Faites un clic droit sur la ligne de signature dans le document, puis cliquez sur **Signer**.
14. Dans la fenêtre **Signer**, cliquez sur **Modifier**.

15. Dans la liste **Certificats**, sélectionnez le certificat mentionnant la date d'aujourd'hui, puis cliquez sur **OK**.
16. Dans la zone de texte à droite du X, tapez votre nom, cliquez sur **Signer**, puis cliquez sur **OK**.

**Remarque :** Assurez-vous d'expliquer aux étudiants que, outre la saisie de votre nom, vous pouvez sélectionner une image à la place. Cette image peut être votre signature manuscrite numérisée.

17. Assurez-vous que le document ne peut plus être modifié.
18. Fermez Word 2016, puis enregistrez les modifications lorsque vous y êtes invité.
19. Restez connecté pour la prochaine démonstration.

## Démonstration : Crypter un fichier avec EFS (Encrypting File System)

### Procédure de démonstration

1. Sur **LON-CL1**, cliquez droit sur le document Word que vous avez enregistré sur le bureau dans la démonstration précédente, puis cliquez sur **Propriétés**.
2. Dans l'onglet **Général** de la boîte de dialogue **Propriétés**, cliquez sur **Avancé**, cliquez sur **Crypter le contenu pour sécuriser les données**, puis cliquez sur **OK** deux fois.
3. Dans la fenêtre d'invite, sélectionnez **Crypter le fichier uniquement**, puis cliquez sur **OK**.
4. Déplacez le document que vous avez crypté vers le dossier **C:\Users\Public\Documents publics**.
5. Déconnectez-vous de **LON-CL1**.
6. Connectez-vous en tant qu'**Adatum\Philippe** avec le mot de passe **Pa$$w0rd**.
7. Ouvrez l'Explorateur de fichiers, puis allez à **C:\\Users\Public\Public Documents**.
8. Tentez d'ouvrir le document crypté.
9. Vérifiez que vous ne pouvez pas ouvrir le document.
10. Déconnectez-vous de **LON-CL1**.

Leçon 4

# Mise en œuvre et gestion des cartes à puce

## Sommaire :

## Questions et réponses

**Question :** Lesquels des énoncés suivants sont exacts en ce qui concerne les cartes à puce ?

( ) Les cartes à puce offrent une option pour l'authentification multifactorielle.

( ) Les cartes à puce ne peuvent pas être utilisées pour une connexion interactive.

( ) Les cartes à puce contiennent un certificat et une clé privée qui sont accessibles à l'aide d'un code PIN seulement.

( ) Les cartes à puce offrent une sécurité renforcée au-delà d'un mot de passe.

( ) Les cartes à puce peuvent être utilisées uniquement pour la signature et le cryptage numériques.

**Réponse :**

(√) Les cartes à puce offrent une option pour l'authentification multifactorielle.

( ) Les cartes à puce ne peuvent pas être utilisées pour une connexion interactive.

(√) Les cartes à puce contiennent un certificat et une clé privée qui sont accessibles à l'aide d'un code PIN seulement.

(√) Les cartes à puce offrent une sécurité renforcée au-delà d'un mot de passe.

( ) Les cartes à puce peuvent être utilisées uniquement pour la signature et le cryptage numériques.

**Commentaire :**

Les cartes à puce fournissent une option pour l'authentification multifactorielle : les utilisateurs doivent avoir la carte à puce en leur possession physique et doivent en outre connaître leur PIN. En entrant le code PIN, les certificats et les clés privées stockées sur la carte à puce deviennent disponibles pour l'authentification, la signature numérique et le cryptage. L'utilisation de cartes à puce pour une connexion interactive offre une sécurité renforcée au-delà d'un mot de passe.

**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 ?

( ) Publication

( ) Révocation

( ) Renouvellement

( ) Blocage et déblocage

( ) Suspension

**Réponse :**

(√) Publication

(√) Révocation

(√) Renouvellement

(√) Blocage et déblocage

(√) Suspension

**Commentaire :**

Toutes les réponses ci-dessus sont des processus corrects que vous devriez inclure dans votre plan de gestion des certificats. Certains des processus peuvent être réalisés à l'aide d'utilitaires intégrés ; cependant, pour des raisons de complexité, nous vous recommandons de mettre en œuvre une solution dédiée pour la carte à puce et la gestion des certificats, tels que MIM.

# Contrôle des acquis et éléments à retenir

## Méthodes conseillées

- Lors du remplacement de vieux modèles de certificats, utilisez des modèles de remplacement.
- Archivez toujours les certificats qui sont utilisés à des fins de cryptage.
- 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 code PIN régulièrement.
- Si vous utilisez des cartes à puce, mettez en œuvre une solution de gestion de carte à puce.

## Questions de contrôle des acquis

**Question :** Listez les conditions requises pour utiliser l'inscription automatique pour les certificats.

> **Réponse :** Pour utiliser l'inscription automatique pour les certificats, vous devez avoir une AC d'entreprise et vous devez configurer les options de stratégie de groupe. En outre, vous devez activer l'inscription automatique pour les modèles de certificats souhaités et vous devez configurer les Objets de stratégie de groupe.

**Question :** Comment les cartes à puce virtuelles fonctionnent-elles ?

> **Réponse :** Les cartes à puce virtuelles émulent les fonctionnalités des cartes à puce traditionnelles, mais au lieu d'exiger l'achat de matériel supplémentaire, elles utilisent la technologie que les utilisateurs possèdent déjà et qu'ils ont probablement avec eux en tout temps.

## 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 comme plateforme pour la PKI. Les certificats seront utilisés principalement pour EFS, pour la signature numérique et pour les serveurs Web. Comme les documents à chiffrer 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-elle choisir ?
- Quel type de certificats Contoso devrait-elle utiliser pour EFS et la signature numérique ?
- Quel type de certificats Contoso devrait-elle utiliser pour un site Web ?
- Comment Contoso peut-elle faire en sorte que les données EFS cryptées 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**

## 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. | Assurez-vous que vous avez configuré correctement les autorisations de lecture et d'inscription sur le modèle. |
| L'inscription automatique ne fonctionne pas. | Assurez-vous que vous avez configuré les options d'inscription automatique dans la stratégie de groupe et que vous avez attribué les autorisations Lecture, Inscription et Inscription automatique au groupe approprié des utilisateurs ou des ordinateurs. |
| L'utilisateur qui a crypté un fichier ne peut pas le décrypter. | Assurez-vous que l'utilisateur possède la clé privée de la paire de clés. En outre, veillez à ce que le certificat n'ait pas expiré. Si une clé privée est perdue ou si un certificat a expiré, utilisez KRA ou DRA. |

# Questions et réponses sur les ateliers pratiques

## Atelier pratique : Déploiement et utilisation de certificats

## Questions et réponses

**Question :** Que devez-vous faire pour récupérer les clés privées ?

**Réponse :** Pour récupérer les clés privées, vous devez configurer une AC pour archiver les clés privées pour les modèles spécifiques et vous devez délivrer un certificat KRA.

**Question :** Quel est l'avantage d'utiliser un agent d'inscription restreint ?

**Réponse :** L'Agent d'inscription vous permet de limiter les autorisations pour les utilisateurs qui sont désignés comme agents d'inscription pour s'inscrire pour des certificats de cartes à puce au nom d'autres utilisateurs.

# Module 10

## Implémentation et administration d'AD FS

### Sommaire :

Leçon 1

# Vue d’ensemble d’AD FS

## Sommaire :

## Questions et réponses

**Question :** Une approbation fédérée est la même chose qu'une approbation de forêt que les organisations peuvent configurer entre forêts AD DS.

( ) Vrai

( ) Faux

**Réponse :**

( ) Vrai

(√) Faux

**Commentaire :**

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-feu pour permettre la fédération.

Leçon 2

# Exigences et planification AD FS

## Sommaire :

## Questions et réponses

**Question :** Dans Windows Server 2016, la fonctionnalité du proxy du serveur de fédération fait partie du rôle Proxy d'application Web.

( ) Vrai

( ) Faux

**Réponse :**

(√) Vrai

( ) Faux

**Commentaire :**

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 fournit une mesure de sécurité supplémentaire pour les connexions à partir de l'Internet vers le serveur de fédération. Dans Windows Server 2016, la fonctionnalité du proxy du serveur de fédération fait partie du Proxy d'application Web.

## Démonstration : Installation du rôle serveur AD FS

### Étapes de démonstration

### Installer AD FS

1. Sur **LON-DC1**, cliquez sur Démarrer, effectuez un clic droit sur **Windows PowerShell**, puis cliquez sur **Exécuter comme administrateur**.
2. À l'invite de commandes, tapez 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 les mots de passe du compte de service administré de groupe (gMSA, group Managed Service Account) 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. Sur **LON-DC1**, in Gestionnaire de serveur, **Gérer**, and puis **Ajouter des rôles et fonctionnalités**.
4. Dans **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 sur **Suivant**.
6. Sur la page **Sélectionner le serveur de destination**, cliquez sur **LON-DC1.Adatum.com**, puis sur **Suivant**.
7. Sur la page **Sélectionner des rôles de serveurs,** cochez la case **Active Directory Domain Services,** 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. Attendez la fin de l'installation puis cliquez sur **Fermer**.

## Ajouter 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**, puis **Zones de recherche directes**, et cliquez ensuite sur **Adatum.com**.
3. Effectuer un clic droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
4. Dans la fenêtre **Nouvel hôte**, dans la case **Nom**, tapez **adfs**.
5. Dans le champ **Adresse IP**, tapez **172.16.0.10**, puis cliquez sur **Ajouter un hôte**.
6. Dans la fenêtre **DNS**, cliquez sur **OK**, puis sur **Terminé**.
7. Fermez le Gestionnaire DNS.

## Configurez 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 **Assistant Configuration des services de fédération Active Directory (AD FS)**, sur la page **Accueil**, cliquez sur **Créer le premier serveur de fédération dans une batterie de serveurs de fédération**, puis sur **Suivant**.
3. Sur la page **Se connecter aux services de domaine Active Directory** cliquez sur **Suivant** utilisez **Adatum\Administrateur** pour effectuez la configuration.
4. Sur la page **Spécifier les propriétés du service**, dans la boîte de dialogue **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 **Créer une base de données sur ce serveur à l'aide de la base de données interne Windows**, puis sur **Suivant**.
9. Dans 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**.

Leçon 3

# Déploiement et configuration AD FS

## Sommaire :

## Questions et réponses

**Question :** Que sont les règles de revendication ? Dans quel but pouvez-vous utiliser des règles de revendication ?

**Réponse :** Les règles de revendication définissent comment les serveurs AD FS envoient et consomment les revendications. Les règles de réclamation définissent la logique métier qui est appliquée aux réclamations que les fournisseurs de revendications fournissent et que les parties utilisatrices acceptent. Vous pouvez utiliser les règles de réclamation 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.

## Ressources

## Comment fonctionne la découverte du domaine de base

 **Lectures complémentaires :** Pour en savoir plus sur *RelayState*, voir « Prise en charge du fournisseur d'identité initié RelayState » sur : http://aka.ms/Df8hqs

## Démonstration : Configuration d'approbations de fournisseur de revendications et de partie de confiance

### Étapes de démonstration

### Configurer une approbation de fournisseur de revendications

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion AD FS**.
2. Dans la console **Gestion AD FS** cliquez sur **Approbations de fournisseur de revendications**.
3. Faites un clic droit sur **Active Directory** puis cliquez sur **Modifier les règles de réclamation**.
4. Dans la fenêtre **Modifier les règles de revendication pour Active Directory**, sur l'onglet **Règles de transformation d'acceptation**, cliquez sur **Ajouter une règle**.
5. Dans **Assistant Ajout de règle de revendicationsur** la page **Sélectionner un modèle de règle** dans la liste **Modèle de règle de revendication**, cliquez sur **Envoyer Attributs LDAP** en tant que revendicationspuis sur **Suivant**.
6. Sur la page **Configurer la règle**, dans le champ **Nom de la règle de revendication**, **saisissez Règle des attributs LDAP sortants**.
7. Dans la liste **magasin d'attributs**, cliquez sur **Active Directory**.
8. Dans la section **Cartographie des attributs LDAP à des types de revendications sortantes**, sélectionnez les valeurs suivantes pour le **Attribut LDAP** et le **Type de revendication sortant** :
   - Adresses électroniques : **Adresse électronique**
   - Nom d'utilisateur principal : **UPN**
9. Cliquez sur **Terminer**, puis sur **OK**.

## Configurer une application Windows Identity Foundation (WIF) pour AD FS

1. Sur **LON-SVR1**, ouvrez le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Utilitaire de fédération Windows Identity Foundation**.
2. Sur la page **Bienvenue dans l'Assistant Utilitaire de fédération**, dans la case **Emplacement de configuration de l'application**, saisissez **C:\inetpub\wwwroot\AdatumTestApp\web.config** pour l'emplacement de l'exemple de fichier **Web.config**.
3. 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 fiera aux revendications entrantes à partir du serveur de fédération, puis cliquez sur **Suivant**.
4. Sur la page **Service d'émission de jeton de sécurité**, cliquez sur **Utiliser un STS existants**, puis dans la case **Emplacement du document des métadonnées de fédération-WS STS**, saisissez **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 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**.

## Configurer une approbation de partie de confiance

1. Sur **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 **Sélectionnez la source de données**, cliquez sur **Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confiance**.
5. Dans la case **Adresse des métadonnées de fédération (nom d'hôte ou URL)**, saisissez **https://lon-svr1.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 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**.
9. Sur la page **Terminer**, cliquez sur **Fermer**.
10. Sur la liste des approbations de parties de confiance, cliquez sur **A. Datum Corporation Test App**, puis sélectionnez **Modifier la stratégie d'émission de revendication**.
11. Dans la fenêtre **Éditer 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**.

12. Dans la boîte de dialogue **modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
13. Dans la zone de texte **Nom de la règle de revendication**, saisissez **Passez par le nom de compte Windows**.
14. Dans la liste **Type de revendication entrante**, cliquez sur **nom de compte Windows**, puis cliquez sur **Terminer**.
15. Dans l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
16. Dans la boîte de dialogue **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
17. Dans la zone de texte **Nom de la règle de revendication**, saisissez **Passez par l'adresse e-mail**.
18. Dans la liste **Type de revendication entrante**, cliquez sur **Adresse e-mail**, puis cliquez sur **Terminer**.
19. Dans l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
20. Dans la boîte de dialogue **Modèle de règle de revendication**, **sélectionnez Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
21. Dans la zone de texte **Nom de la règle de revendication**, saisissez **Passez par UPN**.
22. Dans la liste **Type de revendication entrante**, cliquez sur **UPN**, puis cliquez sur **Terminer**.
23. Dans l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
24. Dans la boîte de dialogue **Modèle de règle de revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
25. Dans la zone de texte **Nom de la règle de revendication**, saisissez **Passez par le nom**.
26. Dans la liste **Type de revendication entrante**, cliquez sur **Nom**, puis cliquez sur **Terminer**.
27. Dans l'onglet **Règles de transformation d'émission**, cliquez sur **OK**.

## Démonstration : configuration des règles de revendication

### Étapes de démonstration

1. Sur **LON-DC1**, dans Gestionnaire AD FS, sélectionnez **Approbation de parties de confiancecliquez** avec le bouton droit sur **A. Datum Corporation Test Apppuis Modifier stratégie émission revendication**.
2. Dans la fenêtre **Éditer 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 boîte de dialogue **Modèle de règle de Revendication**, sélectionnez **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
4. Dans la boîte de dialogue **Nom de la règle de revendication**, tapez **Envoyer la Règle du nom de groupe**.
5. Dans la liste **Type de revendication entrante**, cliquez sur **Groupe**, puis cliquez sur **Terminer**.
6. Cliquez sur **OK**.
7. Cliquez avec le bouton droit sur **A. Datum Corporation Test App**, and puis sur **Modifier stratégie contrôle d'accès**.
8. Dans **Modifier stratégie contrôle d'accès pour A. Datum Corporation Test App** sur l'onglet **stratégie contrôle d'accès**, cliquez **Autoriser règle groupe spécifique**.
9. En dessous de **Stratégie**, cliquez le lien **<paramétrer>**.

10. Cliquez sur **Ajouter**, puis dans la boîte **Sélectionner les groupes**, tapez **Recherche** puis cliquez sur **OK**. Cliquez sur **OK** à nouveau pour fermer la case **Sélectionner les groupes.**
11. Cliquez sur **OK** pour fermer la boîte de dialogue Stratégie de contrôle d'accès.
12. Faites un clic-droit sur **A. Datum Corporation Test App**, puis cliquez sur **Éditer la stratégie d'émission de revendication**
13. Sur l'onglet **Règles de transformation d'émission**, cliquez sur **Passez par UPN** puis cliquez sur **Modifier la règle**.
14. Dans la liste **Type de revendication entrante**, vérifiez que **UPN** est sélectionné.
15. Sélectionnez **Passez à travers seulement une valeur spécifique de réclamation**.
16. Dans la zone **Valeur de réclamation entrante**, tapez **@ adatum.com**.
17. Cliquez sur **Voir la langue de la règle**.
18. Cliquez sur **OK**, puis à nouveau sur **OK**.
19. Dans la fenêtre **Modifier la stratégie de revendication d'émission pour A. Datum Corporation Test App**, cliquez sur **OK**.

Leçon 4

# Vue d’ensemble du Proxy d’application Web

## Sommaire :

## Questions et réponses

**Question :** Lequel des énoncés suivants concernant la configuration du Proxy d'application Web est correct ? (Choisissez toutes les réponses applicables.)

( ) Pour installer le Proxy d'application Web, vous devez avoir implémenté AD FS dans votre organisation.

( ) Pour installer le Proxy d'application Web, vous n'avez pas eu à implémenter AD FS dans votre organisation.

( ) Pour chaque application que vous publiez, vous devez configurer un URL externe et un 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.

**Réponse :**

(√) Pour installer le Proxy d'application Web, vous devez avoir implémenté AD FS dans votre organisation.

( ) Pour installer le Proxy d'application Web, vous n'avez pas eu à implémenter AD FS dans votre organisation.

(√) Pour chaque application que vous publiez, vous devez configurer un URL externe et un 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.

**Commentaire :**

L'option 4 est incorrecte. Le certificat doit contenir le nom d'hôte de l'URL externe.

L'option 2 est incorrecte. Pour installer le Proxy d'application Web, AD FS doit déjà être mis en œuvre dans votre organisation.

## Ressources

## Scénarios pour l'utilisation du Proxy d'application Web

**Lectures complémentaires :** Pour plus d'informations sur la configuration d'un site Web pour utiliser IWA et la délégation Kerberos contrainte, voir « Configurer un site pour utiliser l'authentification Windows intégrée » à l'adresse : http ://aka.ms/Nbsbll

**Lectures supplémentaires :** Pour plus d'informations sur la configuration de l'authentification Kerberos pour les serveurs Exchange d'équilibrage de charge, voir « Configuration de l'authentification Kerberos pour les serveurs d'accès au client à charge équilibrée » à : http://aka.ms/Nd2avi

**Lectures supplémentaires :** Pour plus d'informations sur la publication RD Gateway via le proxy d'application Web, reportez-vous à la publication d'applications avec SharePoint, Exchange et DGR : http://aka.ms/C7f0wn

# Démonstration : Installation et configuration du Proxy d'application Web

## Étapes de démonstration

### Installer le proxy d'application Web

1. Sur **LON-SVR2**, dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
2. Dans **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**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité,** puis sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, cliquez sur **LON-SVR2.Adatum.com**, puis sur **Suivant**.
5. Dans la page **Sélectionnez des rôles de serveurs**, activez la case à cocher **Accès à distance**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Sur la page **Accès à distance**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner les services du rôle**, sélectionnez **Proxy d'application Web**.
9. Dans la boîte de dialogue **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**.
10. Sur la page **Sélectionner les services du rôle**, cliquez sur **Suivant**.
11. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
12. Sur la page **Progression de l'installation**, cliquez sur **Fermer**.

### Exportez le certificat adfs.adatum.com à partir de LON-DC1

1. Sur **LON-DC1**, sur l'écran d'accueil, tapez **mmc**, puis appuyez sur Entrée.
2. Dans la console de gestion Microsoft Management Console, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
3. Dans la fenêtre **Ajouter ou supprimer des composants logiciels enfichables**, dans la colonne **Composants logiciels enfichables disponibles**, double-cliquez sur **Certificats**.
4. Dans la fenêtre **Composant logiciel enfichable Certificats**, cliquez sur **Compte d'ordinateur**, puis sur **Suivant**.
5. Dans la fenêtre **Sélectionner un ordinateur**, cliquez sur **Ordinateur local (l'ordinateur sur lequel cette console est en cours d'exécution)**, puis cliquez sur **Terminer**.
6. Dans la fenêtre **Ajouter/supprimer des composants logiciels enfichables**, cliquez sur **OK**.
7. Dans Microsoft Console de gestion, développez **Certificats (ordinateur local)** et **Personnel**, puis cliquez sur **Certificats**.
8. Cliquez avec le bouton droit sur **adfs.adatum.com**, pointez sur **Toutes les tâches**, puis cliquez sur **Exporter**.
9. Dans l'**Assistant Exportation du certificat**, cliquez sur **Suivant**.
10. Dans la page **Exporter la clé privée**, cliquez sur **Oui, exporter la clé privée**, puis sur **Suivant**.
11. Sur la page **Exporter le format du fichier**, cliquez sur **Suivant**.

12. Sur la page **Sécurité**, cochez la case la **Mot de passe**.
13. Dans la zone de texte **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Suivant**.
14. Sur la page **Fichier à exporter**, dans la zone **Nom du fichier**, tapez **\C:\adfs.pfx**, puis cliquez sur **Suivant**.
15. Sur la page **Fin de l'Assistant Exportation de certificat**, cliquez sur **Terminer**, puis sur **OK** pour fermer le message de réussite.
16. Fermer la Console de gestion Microsoft et ne pas enregistrer les modifications.

## Importez le certificat adfs.adatum.com sur LON-SVR2

1. Sur **LON-SVR2**, sur l'écran d'accueil, tapez **mmc**, puis appuyez sur Entrée.
2. Dans la console de gestion Microsoft Management Console, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
3. Dans la fenêtre **Ajouter ou supprimer des composants logiciels enfichables**, dans la colonne **Composants logiciels enfichables disponibles**, double-cliquez sur **Certificats**.
4. Dans la fenêtre **Composant logiciel enfichable Certificats**, cliquez sur **Compte d'ordinateur**, puis sur **Suivant**.
5. Dans la fenêtre **Sélectionner un ordinateur**, cliquez sur **Ordinateur local (l'ordinateur sur lequel cette console est en cours d'exécution)**, puis cliquez sur **Terminer**.
6. Dans la fenêtre **Ajouter ou supprimer des composants logiciels enfichables**, cliquez sur **OK**.
7. Dans la Console de gestion Microsoft, développez **Certificats (ordinateur local)**, puis cliquez sur **Personnel**.
8. Cliquez avec le bouton droit sur **Personnel**, pointez sur **Toutes les tâches**, puis cliquez sur **Importer**.
9. Dans la fenêtre **Assistant Importation de certificat**, cliquez sur **Suivant**.
10. Sur la page **Fichier à importer**, dans la zone **Nom du fichier**, tapez **\\LON-DC1\c$\adfs.pfx**, puis cliquez sur **Suivant**.
11. Sur la page **Protection de la clé privéedans** la zone **Mot de passe**, tapez **Pa$$w0rd**.
12. Sélectionnez la case **Marquer cette clé comme exportable. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement**, puis cliquez sur **Suivant**.
13. Sur la page **Magasin de certificats**, cliquez sur **Placer tous les certificats dans le magasin suivant**.
14. Dans la zone **Magasin de certificats**, saisissez **Personnel**, puis cliquez sur **Suivant**.
15. Sur la page **Fin de l'Assistant Exportation de certificat**, cliquez sur **Terminer**.
16. Cliquez sur **OK** pour effacer le message de confirmation.
17. Fermez la Console de gestion Microsoft, et n'enregistrez pas les modifications.

## Configurer le Proxy d'application Web

1. Sur **LON-SVR2** dans Gestionnaire de serveur, cliquez sur l'icône **Notifications** puis cliquez sur **Ouvrir l'Assistant du Proxy d'application Web**.
2. Dans **Assistant Configuration du proxy d'application Web**, sur la page **Bienvenue**, cliquez sur **Suivant**.
3. Sur la page **Serveur de fédération**, saisissez les informations suivantes, puis cliquez sur **Suivant** :
    - Nom du service de fédération : **adfs.adatum.com**

- Nom d'utilisateur : **Adatum\Administrateur ;**
- Mot de passe : **Pa$$w0rd ;**

4. Sur la page **Certificats de proxy AD FS**, dans la boîte de dialogue **Sélectionner un certificat à utiliser par le proxy AD FS**, sélectionnez **adfs.adatum.com**, puis cliquez sur **Suivant**.
5. Sur la page **Confirmation**, cliquez sur **Configurer**.
6. Sur la page **Résultats**, cliquez sur **Fermer**.

# Contrôle des acquis et éléments à retenir

## Meilleures pratiques

Dans les versions antérieures d'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 ?

> **Réponse :** Vous avez besoin d'un seul certificat d'une autorité de certification tierce, car le seul certificat AD FS qui doit être digne de confiance est le certificat de communication de service. Vous pouvez laisser les certificats de signature de jeton et de déchiffrement de jeton comme auto-signés.

**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 disponibles.

Pendant l'installation d'AD FS, vous avez choisi d'utiliser WID. Pouvez-vous utiliser cette base de données dans une configuration à haute disponibilité ?

> **Réponse :** Oui, vous pouvez utiliser la Base de données interne Windows (IFD) pour supporter jusqu'à cinq serveurs AD FS. Le premier serveur AD FS est le serveur principal, où tous les changements de configuration ont lieu. Les changements dans le serveur principal sont répliqués sur les autres serveurs AD FS.

# Questions et réponses sur les ateliers pratiques

## Atelier pratique : Implémentation d'AD FS

## Questions et réponses

**Question :** Pourquoi est-il important de configurer adfs.adatum.com pour l'utiliser comme nom d'hôte pour le service AD FS ?

**Réponse :** Si vous utilisez le nom d'hôte d'un serveur existant pour le serveur AD FS, vous ne pourrez pas ajouter de serveurs supplémentaires à votre batterie de serveurs. Tous les serveurs de la batterie de serveurs doivent partager le même nom d'hôte pour fournir des services AD FS. Les serveurs proxy AD FS utilisent également le nom d'hôte pour AD FS.

**Question :** Comment pouvez-vous vérifier si AD FS fonctionne correctement ?

**Réponse :** Si vous pouvez accéder avec succès à **https://hostname/federationmetadata/2007-06/federationmetadata.xml** sur le serveur AD FS, cela signifie que AD FS fonctionne correctement.

# Module 11

## Mise en œuvre et administration de AD RMS

### Sommaire :

Leçon 1

# Vue d’ensemble de AD RMS

## Sommaire :

## Questions et réponses

**Question :** Quand un utilisateur reçoit-il un certificat de compte de droits ?

> **Réponse :** Un certificat de compte de droits est délivré la première fois qu'un utilisateur tente d'accéder au contenu protégé par les services AD RMS ou d'effectuer une tâche de AD RMS, comme la création d'un document protégé.

**Question :** Azure RMS est déployé localement sur un serveur.

( ) Vrai

( ) Faux

> **Réponse :**
>
> ( ) Vrai
>
> (√) Faux
>
> **Commentaire :**
>
> Azure RMS est un service cloud et vous ne devez pas le déployer localement.

## Ressources

## Qu'est-ce qu'Azure RMS ?

**Liens de référence :** Pour télécharger l'application de partage RMS gratuite depuis Microsoft, rendez-vous sur : http://aka.ms/v1s1xd

## Comparaison de AD RMS, Azure RMS et Azure RMS pour Office 365

**Lectures complémentaires :** Pour plus d'informations, reportez-vous à Comparaison de Azure Rights Management et de AD RMS : http://aka.ms/sndlw0

Leçon 2

# Déploiement et gestion d'une infrastructure AD RMS

## Sommaire :

## Questions et réponses

**Question :** Pour mettre en œuvre un cluster AD RMS, quels composants sont nécessaires ?

( ) Office

( ) Un compte de service

( ) Une base de données

( ) AD FS

( ) Un certificat SSL (Secure Sockets Layer)

**Réponse :**

( ) Office

(√) Un compte de service

(√) Une base de données

( ) AD FS

( ) Un certificat SSL (Secure Sockets Layer)

**Commentaire :**

Vous devez avoir un compte de service créé pour mettre en œuvre AD RMS ainsi qu'une une base de données disponible, soit comme base de données WID ou SQL Server.

**Question :** Lorsque vous décidez de supprimer votre cluster AD RMS de AD DS, que devez-vous faire en premier ?

**Réponse :** Avant de retirer un serveur AD RMS, vous devez désaffecter ce serveur.

## Ressources

## Surveillance de AD RMS

**Lectures complémentaires :** Pour plus d'informations, consultez les Scénarios de surveillance : http://aka.ms/Pyumg7

## Démonstration : Installation du premier serveur d'un cluster AD RMS

### Étapes de démonstration

### Configurer un compte de service

1. Sur **LON-DC1**, dans **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Sélectionnez et cliquez avec le bouton droit sur **Adatum (local)**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
3. Dans la boîte de dialogue **Créer Unité d'organisation**, dans la case **Nom**, tapez **Comptes de service**, cliquez sur **OK**, faites un clic droit sur **Comptes de service** Unité d'organisation (OU), déplacez le pointeur sur **Nouveau**, puis cliquez sur **Utilisateur**.
4. 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**

- **Utilisateur SamNomdecompte Ouverture de session** : **Adatum\ADRMSSVC**
- Mot de passe : **Pa$$w0rd**
- Confirmer le mot de passe : **Pa$$w0rd**
- Le mot de passe n'expire jamais : **Activé** (Vous devez cliquer sur **Autres options de mot de passe** pour pouvoir sélectionner cette case)
- L'utilisateur ne peut pas modifier le mot de passe : **Activé**

## Préparation du système DNS (Domain Name System)

1. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.
2. Dans la console du **Gestionnaire DNS**, développez **LON-DC1**, puis **Zones de recherche directes**.
3. Sélectionnez puis cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
4. Dans la boîte de dialogue **Nouvel hôte**, tapez les informations suivantes, puis cliquez sur **Ajouter un hôte** :
   - Nom : **adrms**
   - Adresse IP : **172.16.0.21**

Cliquez sur **OK**, puis sur **Terminé**.

5. Fermez la console **Gestionnaire DNS**.

## Installation du rôle AD RMS

1. Connectez-vous à **LON-SVR1** en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur Démarrer, puis sur **Gestionnaire de serveur**.
3. Dans le **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
4. Dans l'**Assistant Ajouter des rôles et fonctionnalités**, cliquez trois fois sur **Suivant**.
5. Sur la page **Rôles du serveur**, cliquez sur **Services AD RMS (Active Directory Rights Management Services)**.
6. Dans la boîte de dialogue de l'**Assistant Ajout de rôle et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**, ensuitesix fois sur **Suivant**, puis sur **Installer**, et enfin sur **Fermer**.

## Configurer AD RMS

1. Sur **LON-SVR1**, dans **Gestionnaire de serveur**, cliquez sur le nœud **AD RMS**.
2. À côté de **Configuration requise pour les Active Directory Rights Management Services de LON-SVR1**, cliquez sur **Plus**.
3. Sur la page **Tous les détails et notifications des tâches de serveurs**, cliquez sur **Effectuer une configuration supplémentaire**.
4. Sur la page **AD RMS**, dans la boîte de dialogue **Configuration AD RMS** : **LON-SVR1.adatum.com**, cliquez sur **Suivant**.
5. Sur la page **Cluster AD RMS**, cliquez sur **Créer un cluster racine AD RMS**, puis sur **Suivant**.
6. Sur la page **Base de données de configuration**, cliquez sur **Utiliser la base de données interne Windows sur ce serveur**, puis cliquez sur **Suivant**.
7. Sur la page **Compte de service**, cliquez sur **Spécifier**.

8. 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 : **Pa$$w0rd**

   **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.

9. Sur la page **Mode de chiffrement**, cliquez sur **Mode de chiffrement 2**, puis sur **Suivant**.
10. Sur la page **Stockage de clé de cluster**, cliquez sur **Utiliser le stockage de clé géré de manière centralisée de AD RMS**, puis sur **Suivant**.
11. Sur la page **Mot de passe de la clé de cluster**, tapez **Pa$$w0rd** à deux reprises, puis cliquez sur **Suivant**.
12. Sur la page **Site Web de cluster**, vérifiez que **Site Web par défaut est sélectionné**, puis cliquez sur **Suivant**.
13. Sur la page **Adresse du 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**
14. Sur la page **Certificat de licence**, tapez **AdatumADRMS**, puis cliquez sur **Suivant**.
15. Sur la page **Inscription du SCP**, cliquez sur **Inscrire le SCP maintenant**, puis sur **Suivant**.
16. Sur la page **Confirmation**, cliquez sur **Installer**, puis une fois l'installation terminée, sur **Fermer**.
17. Dans le Menu Démarrer, cliquez sur **Administrateur**, puis sur **Se déconnecter**.

**Remarque :** Vous devez vous déconnecter avant de pouvoir gérer AD RMS.

Leçon 3

# Configurer la protection de contenu AD RMS

## Sommaire :

## Questions et réponses

**Question :** Quels types d'autorisations un groupe de super utilisateurs possède-t-il ?

> **Réponse :** Les membres du groupe de super utilisateurs ont tous les droits du propriétaire dans toutes les licences d'utilisation délivrés par le cluster AD RMS sur lequel le groupe de super utilisateurs est configuré.

## Ressources

## Quelles sont les stratégies d'exclusion ?

 **Lectures complémentaires :** Pour plus d'informations, reportez-vous +q Activation des stratégies d'exclusion : http://aka.ms/Lnwbcr

## Démonstration : Création d'un modèle de stratégie de droits

### Étapes de démonstration

1. Sur **LON-SVR1**, ouvrez **Gestionnaire de serveur,** cliquez sur **Outils**, puis sur **Active Directory Rights Management Services.**
2. Dans la console **AD RMS**, cliquez sur le nœud **LON-SVR1\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**, entrez les informations suivantes, cliquez sur **Ajouter**, puis 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**, tapez **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 la stratégie d'expiration**, choisissez 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)**, ensuite sur **Suivant**, puis sur **Terminer**.

# Démonstration : Création d'une stratégie d'exclusion pour une application

## Étapes de démonstration

1. Sur **LON-SVR1**, dans la console **AD RMS**, cliquez sur le nœud **Stratégies d'exclusion**, puis cliquez sur **Gérer la liste d'exclusion d'applications**.
2. Dans le volet **Actions**, cliquez sur **Activer l'exclusion d'applications**.
3. Dans le volet **Actions**, cliquez sur **Exclure l'application**.
4. Dans la boîte de dialogue **Exclure l'application**, tapez les informations suivantes, puis cliquez sur **Terminer** :
   - Nom du fichier d'application : **Powerpnt.exe**
   - Version minimale : **14.0.0.0**
   - Version maximale : **16.0.0.0**

# Contrôle des acquis et éléments à retenir

## Méthodes conseillées

- Avant de déployer AD RMS, vous devez analyser les impératifs professionnels de votre organisation et créer les modèles nécessaires. Vous devez 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 ont besoin.
- Contrôlez 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.

## 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 ?

**Réponse :** Vous pouvez protéger la connexion entre les clients et le serveur AD RMS avec SSL.

**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 ?

**Réponse :** Utilisez un compte Microsoft pour fournir des CCR aux entrepreneurs non affiliés.

**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 ?

**Réponse :** Vous devez configurer l'exclusion d'applications pour PowerPoint.

# Questions et réponses de l'atelier pratique

## Atelier pratique : Mise en œuvre d'une infrastructure AD RMS

## Questions et réponses

**Question :** Quelles mesures pouvez-vous prendre pour vous assurer que vous pouvez utiliser les services IRM avec le rôle AD RMS ?

**Réponse :** Vous devez configurer un certificat de serveur pour le serveur AD RMS avant de déployer AD RMS.

# Module 12

## Mise en œuvre de la synchronisation AD DS avec Microsoft Azure AD

### Sommaire :

Leçon 1

# Planification et préparation à la synchronisation de répertoires

## Sommaire :

## Questions et réponses

**Question :** Lorsque vous mettez en œuvre la synchronisation des répertoires, les comptes et groupes d'utilisateurs sont transférés de votre AD DS local vers Azure AD.

( ) Vrai

( ) Faux

**Réponse :**

( ) Vrai

(√) Faux

**Commentaire :**

La synchronisation des répertoires ne déplace pas d'objet. Elle copie des objets à partir des AD DS locaux avec un sous-ensemble de leurs attributs, et elle crée de nouveaux objets dans Azure AD.

## Ressources

## Planification de la synchronisation des répertoires

 **Lectures complémentaires :** Pour plus d'informations, reportez-vous au Guide des considérations relatives à la conception d'identités hybrides Azure : http://aka.ms/ibuqek

## Prérequis et préparation à la synchronisation d'annuaire

 **Lectures complémentaires :** Pour plus d'informations, reportez-vous à Vous recevez une erreur dans un rapport de synchronisation d'annuaire « Cette entreprise a dépassé le nombre d'objets qui peuvent être synchronisés » : http://aka.ms/r4x1q4

Leçon 2

# Mise en œuvre de synchronisation des répertoires par le biais d'Azure AD Connect

## Sommaire :

## Questions et réponses

**Question :** Lorsque vous mettez en place la synchronisation entre AD DS et Azure AD, où maîtrisez-vous les objets AD DS ?

> **Réponse :** Si 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 que les utilisateurs et ordinateurs Active Directory ou Windows PowerShell—La source d'autorité est l'AD DS local.

## Ressources

## Synchronisation personnalisée d'Azure AD Connect

**Lectures complémentaires :** Pour plus d'informations, reportez-vous à la section « Configuration d'un ID de connexion alternatif » sur : http://aka.ms/nqh5gc

## Fonctionnalités de contrôle d'Azure AD Connect

**Lectures complémentaires :** Pour plus d'informations, reportez-vous à Contrôler vos services locaux d'infrastructure d'identité et de synchronisation dans le cloud : http://aka.ms/dqaaps

## Démonstration : Installer et configurer Azure AD Connect

### Procédure de démonstration

1. Sur LON-SVR1, connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
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**.
4. Cliquez sur **Exécuter**. Patientez quelques minutes, jusqu'à la fin du téléchargement.

   **Remarque :** Si vous rencontrez des problèmes avec le démarrage du téléchargement, ajoutez le site Web https://download.microsoft.com à vos sites de confiance.

5. Dans l'assistant Microsoft Azure Active Directory Connect, sur la page **Bienvenue sur Azure AD Connect**, sélectionnez la case à cocher **Je suis d'accord avec les termes de la licence et avis de confidentialité**, puis cliquez sur **Continuer**.
6. Sur la page **Configuration rapide**, cliquez sur **Personnaliser**.
7. Sur la page **Installer les composants requis**, révisez les options disponibles, mais sans effectuer de changements, puis cliquez sur **Installer**.
8. Sur la page **Connexion utilisateur**, sélectionnez **Synchronisation de mot de passe**, puis cliquez sur **Suivant**.
9. Sur la page **Connectez-vous à Azure AD**, dans les zones de texte **NOM D'UTILISATEUR** et **MOT DE PASSE**, tapez **SYNC@votredomaine.onmicrosoft.com** pour le nom d'utilisateur du compte, tapez le mot de passe **Pa$$w0rd**, puis cliquez sur **Suivant**. L'établissement de la connexion peut prendre quelques minutes.

10. Sur la page **Connectez vos répertoires**, dans la zone de texte **NOM D'UTILISATEUR**, tapez ***Adatum*\administrateur**, puis dans la zone de texte **MOT DE PASSE**, tapez **Pa$$w0rd**. Cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
11. Sur la page **Configuration de connexion AD Azure**, sélectionnez la case à cocher à côté de **Continuer sans tous les domaines vérifiés**, puis cliquez sur **Suivant.**
12. Sur la page **Filtrage du domaine ou de l'UO**, cliquez sur **Suivant.**
13. Sur la page **Identification unique de vos utilisateurs**, passez en revue les options disponibles et expliquez-les, mais n'effectuez aucun changement.
14. Cliquez sur **Suivant**.
15. Sur la page **Filtrer les utilisateurs et les dispositifs**, cliquez sur **Synchroniser sélectionné**. Dans la zone de texte **GROUPE**, tapez **Recherche**, puis cliquez sur **Résoudre**. Assurez-vous qu'une coche verte apparaît lorsque vous cliquez sur **Résoudre**.
16. Cliquez sur **Suivant**.
17. Sur la page **Caractéristiques optionnelles**, sélectionnez **Écriture différée de mot de passe**, expliquez les autres options aux étudiants, puis cliquez sur **Suivant**.
18. Sur la page **Prêt pour la configuration**, cliquez sur **Installer**, puis à la fin de l'installation, cliquez sur **Sortie**.
19. La synchronisation des objets à partir de votre AD DS local et Azure AD doit commencer. Vous devez patienter environ 5 minutes pour que ce processus se termine.
20. Ouvrez Internet Explorer sur votre ordinateur hôte, puis ouvrez le portail classique Azure pour accéder à **https://manage.windowsazure.com**.
21. Connectez-vous à Azure en utilisant le compte Microsoft qui est associé à votre abonnement d'essai. Dans le portail classique Azure, cliquez sur le répertoire **Adatum**.
22. Sur la page **adatum**, cliquez sur l'onglet **UTILISATEURS**.

    **Remarque :** Vérifiez que vous pouvez voir les comptes d'utilisateurs depuis vos AD DS locaux. Vous devez être en mesure de voir les utilisateurs de la Recherche à partir de votre domaine local adatum.com.

23. Réduisez Internet Explorer sur votre ordinateur hôte.
24. Sur l'ordinateur **LON-SVR1**, cliquez sur le bouton **Démarrer**, puis tapez **Synchronisation**.
25. Dans le volet de recherche, cliquez sur **Service de synchronisation**.
26. Dans la fenêtre **Gestionnaire de service de synchronisation sur LON-SVR1**, cliquez sur l'onglet **Opérations**.
27. Assurez-vous que vous voyez les tâches **Exportation, Synchronisation delta**, etImportation delta. Assurez-vous que toutes les tâches disposent de l'heure et de la date du jour dans les colonnes **Heure de début** et **Heure de fin**. En outre, assurez-vous que les tâches les plus récentes sont classées sous **succès** dans la colonne **Statut**.
28. Fermez le Gestionnaire de service de synchronisation.

Leçon 3

# Gestion des identités par le biais de la synchronisation des répertoires

## Sommaire :

## Questions et réponses

**Question :** Si vous voulez disposer de l'authentification unique pour les services cloud et locaux, que vous faut-il déployer ? Sélectionnez toutes les réponses appropriées.

( ) Azure AD Connect Health

( ) AD FS

( ) Azure AD Connect

( ) Microsoft Office 365

( ) Azure AD

**Réponse :**

( ) Azure AD Connect Health

(√) AD FS

(√) Azure AD Connect

( ) Microsoft Office 365

( ) Azure AD

**Question :** 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.

( ) Vrai

( ) Faux

**Réponse :**

( ) Vrai

(√) Faux

**Commentaire :**

L'AD DS local effectue l'authentification, puis transmet cette information à Azure AD. Le mot de passe pour Azure AD n'est pas utilisé. Cependant, les comptes dans les deux services d'annuaire doivent correspondre. Par conséquent, il est nécessaire que vous utilisiez Azure AD Connect et AD FS.

## Ressources

## Modification de la synchronisation des répertoires

**Lectures complémentaires :** Pour plus d'informations, reportez-vous à « Azure AD Connect sync : Configurer le filtrage » sur : http://aka.ms/au8smo

## Contrôle de la synchronisation des répertoires

**Lectures complémentaires :** Pour plus d'informations, reportez-vous à « Applets de commande Active Directory » à l'adresse : http://aka.ms/pfsm1x

## Résolution des problèmes liés à la synchronisation des répertoires

**Lectures complémentaires :** Pour plus d'informations, reportez-vous à « Intégrer vos identités locales avec Azure Active Directory » à l'adresse : http://aka.ms/cdm2kk

**Lectures supplémentaires :** Pour plus d'informations, reportez-vous à « Comment faire pour résoudre les erreurs d'installation de l'outil Azure Active Directory Sync et les erreurs de l'Assistant de configuration » à l'adresse : http://aka.ms/bz5cjw

# Contrôle des acquis et éléments à retenir

## Méthodes conseillées

- 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 par le biais d'au moins deux méthodes d'authentification.
- Pensez à utiliser les fonctionnalités de réécriture.
- Implémentez Azure AD Connect Health si vous disposez d'un compte Azure AD Premium.

## Enjeux et cas dans le monde réel

La synchronisation des répertoires étant le lien entre vos objets AD DS locaux et les services dans Azure AD, faites attention lorsque vous modifiez Azure AD Connect ou le Gestionnaire de service de synchronisation après le déploiement de production. Par exemple, une erreur mineure dans le filtrage peut 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 dans le Gestionnaire de service de synchronisation 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(s) de contrôle des acquis

**Question :** Quelle fonctionnalité devez-vous configurer de sorte que les objets se synchronisent d'Azure AD à votre AD DS local ?

> **Réponse :** Vous devez déployer des fonctionnalités d'écriture différée. Actuellement, vous pouvez utiliser l'écriture différée de mot de passe, l'écriture différée de groupes et l'écriture différée des dispositifs.

## 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 |
| Azure AD Connect Health | Contrôle 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 |

## Problèmes courants et conseils pour leur résolution

| Problème courant | Conseil pour la résolution du problème |
|---|---|
| Le filtrage de synchronisation d'annuaire ne fonctionne plus. | Il est important d'être sur la version la plus récente de l'outil de synchronisation des répertoires. Toutefois, lors de la mise à niveau vers une nouvelle version de l'outil, tous les filtres existants et d'autres personnalisations d'agent de gestion ne seront pas importés automatiquement dans la nouvelle installation. Si vous effectuez une mise à niveau pour obtenir une version plus récente de la synchronisation des répertoires, vous devez toujours réappliquer manuellement les configurations de filtrage après la mise à niveau, mais avant de lancer le premier cycle de synchronisation. |
| Après avoir installé Azure AD Connect, vous pouvez recevoir une invite avec le message d'erreur suivant lorsque vous ouvrez le Gestionnaire de service de synchronisation : **Impossible de se connecter au Service de synchronisation**. | Ajoutez le compte d'utilisateur de domaine Azure AD Connect approprié au groupe ADSyncAdministrateurs, déconnectez-vous, puis connectez-vous à nouveau. Le compte d'utilisateur de domaine que vous utilisez pour vous connecter lors de l'installation d'Azure AD Connect est automatiquement ajouté au groupe, mais vous aurez toujours besoin de vous déconnecter et de vous reconnecter avant de pouvoir ouvrir le Gestionnaire de service de synchronisation. |

# Questions et réponses sur les ateliers pratiques

## Atelier pratique : Configuration de la synchronisation des répertoires

## Questions et réponses

**Question :** Que devez-vous faire avant de commencer à configurer Azure AD Connect ?

**Réponse :** Vous devez créer un compte de synchronisation dans Azure AD, puis ajouter votre nom de domaine au locataire d'AD Azure.

**Question :** Quel applet de commande devez-vous utiliser pour modifier le calendrier de synchronisation pour Azure AD Connect ?

**Réponse :** Vous devez utiliser l'applet **Set-ADSyncScheduler** sur l'ordinateur sur lequel vous installez Azure AD Connect.

# Module 13

## Surveillance, gestion et récupération d'AD DS

### Sommaire :

Leçon 1

# Suivre AD DS

## Sommaire :

## Ressources

## Vue d'ensemble des outils de suivi

**Lectures complémentaires :** Pour plus d'informations, reportez-vous à «Utilisation de PowerShell pour recueillir des données de performance » à l'adresse : http://aka.ms/F8mxnr

## Démonstration : Suivre AD DS

### Procédures de démonstration

### Configurer l'analyseur de performances pour contrôler AD DS

1. Basculez vers **LON-DC1**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Analyseur de performances.**
3. Sous le nœud Outils de surveillance, cliquez sur Analyseur de performances.
4. Cliquez sur le bouton **Ajouter** ; le **Signe plus** (**+**) vert sur la barre d'outils pour ajouter des objets et des compteurs.
5. Dans la boîte de dialogue **Ajouter des compteurs**, dans la liste **Compteurs disponibles,** développez l'objet **Services d'annuaire**.
6. Cliquez sur le compteur **Nb total d'octets DRA entrants/s.** puis cliquez sur **Ajouter**.
7. Répétez l'étape précédente (étape 6) pour ajouter les compteurs suivants :
   - **DirectoryServices\DRA Outbound Bytes Total/sec**
   - **DirectoryServices\DS Threads In Use**
   - **DirectoryServices\DS Directory Reads/sec**
   - **DirectoryServices\DS Directory Writes/sec**
   - **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**
8. Cliquez sur **OK**, puis attendez quelques instants.
9. Dans la liste des compteurs en dessous du graphique, sélectionnez **Recherches DS Directory par sec**.
10. Dans la barre d'outils, cliquez sur **Surligner**. Le compteur sélectionné est mis en évidence, ce qui permet de voir plus facilement la performance de ce compteur.
11. Sur la barre d'outils, cliquez sur **Surligner** pour désactiver le surlignage.

### Créer un ensemble des collecteurs de données

1. Dans l'arborescence de la console, déroulez les menus **Performance**, **Outils de suivi**, puis cliquez sur **Suivi des performances**. Cliquez avec le bouton droit sur **Suivi des performances**, pointez sur **Nouveau**, puis cliquez sur **Ensemble des collecteurs de données**.
2. Dans la boîte de dialogue **Créer un nouvel ensemble des collecteurs de données**, dans la zone de texte **Nom**, tapez **Personnalisée AJOUTE compteurs de performance**, puis cliquez sur **Suivant**.

3. Notez le premier répertoire par défaut dans lequel l'ensemble des collecteurs de données sera enregistré, cliquez sur **Suivant**, puis sur **Terminer**.

### Démarrer l'ensemble des collecteurs de données

1. Dans l'arborescence de la console, développez **Ensembles de collecteurs de données**, développez **Définis par l'utilisateur** puis cliquez sur **Définis par l'utilisateur**.
2. Cliquez avec le bouton droit sur **Compteurs de performances ADDS personnalisés** puis cliquez sur **Démarrer**. Faites remarquer que le nœud **Compteurs de performances ADDS personnalisés** est automatiquement sélectionné.

**Remarque :** 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.

3. Dans l'arborescence de la console, cliquez avec le bouton droit sur l'ensemble des collecteurs de données **Personnalisée AJOUTE compteurs de performance**, puis cliquez sur **Arrêter**.

### Analyser les données obtenues dans un rapport

1. Dans l'arborescence de la console, développez **Rapports** puis **Définis par l'utilisateur**, et enfin **Compteurs de performance ADDS personnalisés** puis cliquez sur **Journal de Moniteur système.blg**.
2. Vérifiez que le graphique des compteurs de performances du journal s'affiche.

Leçon 2

# Gestion de la base de données Active Directory

## Sommaire :

# Démonstration : Gestion de la base de données

## Procédures de démonstration

### Arrêter AD DS

1. Si besoin, sur **LON-DC1**, dans la barre des tâches, cliquez sur l'icône **Gestionnaire de serveur**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Services**.
3. Dans la console **Services**, cliquez avec le bouton droit sur **Services de domaine Active Directory**, puis cliquez sur **Arrêter**.
4. Dans la boîte de dialogue **Arrêter les autres services**, cliquez sur **Arrêter**.

### Effectuer une défragmentation hors ligne de la base de données Active Directory

1. Sur **LON-DC1**, cliquez sur Démarrer, puis sur **Windows PowerShell**.
2. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Ntdsutil.exe
```

3. Sur **NtdsUtil.exe :** tapez la commande suivante, puis appuyez sur Entrée :

```
activer instance NTDS
```

4. Sur **NtdsUtil.exe :** tapez la commande suivante, puis appuyez sur Entrée :

```
fichiers
```

5. À l'invite **Maintenance de fichier :** tapez la commande suivante, puis appuyez sur Entrée :

```
compacter sur C:\
```

### **Vérifiez l'intégrité de la base de données** Active Directory en mode hors ligne

1. À l'invite **Maintenance de fichier :** tapez la commande suivante, puis appuyez sur Entrée :

```
Intégrité
```

2. À l'invite **Maintenance de fichier :** tapez la commande suivante, puis appuyez sur Entrée :

```
quitter
```

3. À l'invite **NtdsUtil.exe :** tapez la commande suivante et appuyez sur Entrée :

```
quitter
```

4. Fermez la fenêtre **Windows PowerShell**.

### Démarrer AD DS

1. Dans la barre des tâches, cliquez sur l'icône de **Gestionnaire de serveur.**
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Services**.
3. Dans la console **Services**, cliquez avec le bouton droit sur **Services de domaine Active Directory**, puis sur **Démarrer**.
4. Vérifiez que la colonne État pour les services de domaine Active Directory est répertoriée comme Exécution en cours.

Leçon 3

# Sauvegarde d'Active Directory, options de récupération pour AD DS et autres solutions d'identité et d'accès

## Sommaire :

# Démonstration : Implémentation de la Corbeille d'Active Directory

## Procédures de démonstration

### Activer la Corbeille d'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**, développez **Serveurs**, développez **LON-DC1**, puis cliquez sur **Paramètres NTDS**.
3. Cliquez avec le bouton droit sur **<Généré automatiquement>**, cliquez sur **Répliquer maintenant**, puis cliquez sur **OK**.
4. Déroulez le menu **LON-DC2**, puis cliquez sur **Paramètres NTDS**.
5. Cliquez avec le bouton droit sur **<Généré automatiquement>**, cliquez sur **Répliquer maintenant**, puis cliquez sur **OK**.
6. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory.**
7. Cliquez **Adatum (local)**.
8. Dans le volet des tâches, cliquez sur **Activer le recyclage de la Corbeille**. Dans la boîte de message d'avertissement, cliquez sur **OK**, puis cliquez sur **OK** à nouveau pour actualiser le message du Centre d'administration Active Directory.
9. Appuyez sur le **F5** clé pour actualiser le Centre d'administration Active Directory.

### Créer, puis supprimer les comptes d'essai

1. Dans le Centre d'administration Active Directory, double-cliquez sur l'unité d'organisation **Recherche** (UO).
2. Dans le volet **Tâche**, cliquez sur **Nouveau**, puis cliquez sur **Utilisateur**.
3. Dans la rubrique Compte, saisissez les informations suivantes, puis cliquez sur **OK** :
   - Nom complet : **Test1**
   - Ouverture de la session UPN de l'utilisateur : **Test1**
   - Mot de passe : **Pa$$w0rd**
   - Confirmez le mot de passe : **Pa$$w0rd**
4. Répétez les étapes précédentes pour créer un second utilisateur, **Test2**.
5. Dans la case **Comptes**, sélectionnez à la fois **Test1** et **Test2**, cliquez-avec le bouton droit sur la sélection, puis cliquez sur **Effacer**.
6. À l'invite de confirmation, cliquez sur **Oui**.

### Restaurer les comptes supprimés

1. Dans le Centre d'administration Active Directory, cliquez sur **Adatum (local)**, puis double-cliquez sur **Objets supprimés**.
2. Cliquez avec le bouton droit sur **Test1**, puis sur **Restaurer**.
3. Cliquez avec le bouton droit sur **Test2**, puis sur **Restaurer vers**.
4. Dans la fenêtre **Restaurer vers**, cliquez sur l'UO **IT**, puis sur **OK**.
5. Assurez-vous que Test1 est maintenant situé dans l'UO Rechercher, et que Test2 est dans l'UO technologies de l'information (IT).

# Contrôle des acquis et éléments à retenir

## Meilleures pratiques

- Sauvegardez vos contrôleurs de domaine régulièrement.
- Envisagez la récupération de la base de données AD DS comme l'un de vos scénarios de restauration pour les contrôleurs de domaine.
- Activez la corbeille d'Active Directory pour faciliter la récupération des objets supprimés.
- Utilisez l'AD DS redémarrable lors de l'exécution des tâches de maintenance de base de données.

## Question de contrôle des acquis

**Question :** Quel type de restauration pouvez-vous effectuer avec AD DS ?

**Réponse :** Vous pouvez effectuer une restauration faisant autorité, une restauration ne faisant pas autorité, et la restauration d'objets simples avec Corbeille Active Directory.

# Questions et réponses sur les ateliers pratiques

## Atelier pratique : Récupération d'objets dans AD DS

## Questions et réponses

**Question :** Lorsque vous restaurez un utilisateur supprimé ou une unité organisationnelle avec des objets utilisateur à l'aide de la restauration faisant autorité, les objets sont-ils exactement les mêmes qu'avant ? Quels attributs pourraient ne pas être les mêmes ?

**Réponse :** Les réponses peuvent varier, mais la question est destinée à encadrer une discussion à propos de l'appartenance au groupe. L'appartenance à un groupe d'un utilisateur n'est pas un attribut de l'objet utilisateur, mais plutôt de l'objet de groupe. Lorsque vous restaurez autoritairement un utilisateur, vous ne restaurez pas l'adhésion de l'utilisateur dans les groupes. L'utilisateur a été supprimé de l'attribut des membres du groupe quand il a été supprimé. Par conséquent, l'utilisateur restauré ne sera pas un membre d'un groupe autre que le groupe principal de l'utilisateur. Pour restaurer les appartenances aux groupes, vous devez également penser à une restauration autoritaire des groupes. Cela n'est pas toujours souhaitable, lorsque vous restaurez autoritairement groupes, vous ramenez leur appartenance à la date à laquelle la sauvegarde a été effectuée.

**Question :** Pendant l'atelier pratique, serait-il possible de restaurer ces objets supprimés s'ils ont été supprimés avant que la corbeille d'Active Directory soit activée ?

**Réponse :** Oui, mais seulement comme des objets de désactivation sans la plupart des attributs, ou en utilisant une restauration autoritaire d'AD DS.