

PRODUIT OFFICIEL DE FORMATION MICROSOFT

22412B

Configuration des services avancés  
de Windows Server® 2012

*Contenu d'accompagnement*

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

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

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

© 2013 Microsoft Corporation. Tous droits réservés.

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

Numéro de produit : 22412B

Numéro de référence : X18-86876

Date de publication : 3/2013

---

## **TERMES DU CONTRAT DE LICENCE MICROSOFT COURS MICROSOFT AVEC FORMATEUR**

---

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

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

---

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

### **1. DÉFINITIONS.**

- a. « Centre de Formation Agréé » désigne un Membre du Programme Microsoft IT Academy ou un Membre Microsoft Learning Competency, ou toute autre entité que Microsoft peut occasionnellement désigner.
- b. « Session de Formation Agréée » désigne le cours avec formateur utilisant le Cours Microsoft avec Formateur et mené par un Formateur ou un Centre de Formation Agréé.
- c. « Dispositif de la Classe » désigne un (1) ordinateur dédié et sécurisé qu'un Centre de Formation Agréé possède ou contrôle, qui se trouve dans les installations de formation d'un Centre de Formation Agréé et qui répond ou est supérieur au niveau matériel spécifié pour le Cours Microsoft avec Formateur concerné.
- d. « Utilisateur Final » désigne une personne qui est (i) dûment inscrite et participe à une Session de Formation Agréée ou à une Session de Formation Privée, (ii) un employé d'un membre MPN, ou (iii) un employé à temps plein de Microsoft.
- e. « Contenu Concédé sous Licence » désigne le contenu qui accompagne le présent contrat et qui peut inclure le Cours Microsoft avec Formateur ou le Contenu du Formateur.
- f. « Formateur Agréé Microsoft » ou « MCT » désigne une personne qui est (i) engagée pour donner une session de formation à des Utilisateurs Finaux au nom d'un Centre de Formation Agréé ou d'un Membre MPN, et (ii) actuellement Formateur Agréé Microsoft dans le cadre du Programme de Certification Microsoft.
- g. « Cours Microsoft avec Formateur » désigne le cours avec formateur Microsoft qui forme des professionnels de l'informatique et des développeurs aux technologies Microsoft. Un Cours Microsoft avec Formateur peut être labellisé cours MOC, Microsoft Dynamics ou Microsoft Business Group.
- h. « Membre du Programme Microsoft IT Academy » désigne un membre actif du Programme Microsoft IT Academy.
- i. « Membre Microsoft Learning Competency » désigne un membre actif du programme Microsoft Partner Network qui a actuellement le statut Learning Competency.

- j. « MOC » désigne le cours avec formateur « Produit de Formation Officiel Microsoft » appelé Cours Officiel Microsoft qui forme des professionnels de l'informatique et des développeurs aux technologies Microsoft.
- k. « Membre MPN » désigne un membre actif Silver ou Gold du programme Microsoft Partner Network.
- l. « Dispositif Personnel » désigne un (1) ordinateur, un dispositif, une station de travail ou un autre dispositif électronique numérique qui vous appartient ou que vous contrôlez et qui répond ou est supérieur au niveau matériel spécifié pour le Cours Microsoft avec Formateur concerné.
- m. « Session de Formation Privée » désigne les cours avec formateur fournis par des Membres MPN pour des clients d'entreprise en vue d'enseigner un objectif de formation prédéfini à l'aide d'un Cours Microsoft avec Formateur. Ces cours ne font l'objet d'aucune publicité ni promotion auprès du grand public et la participation aux cours est limitée aux employés ou sous-traitants du client d'entreprise.
- n. « Formateur » désigne (i) un formateur accrédité sur le plan académique et engagé par un Membre du Programme Microsoft IT Academy pour donner une Session de Formation Agréée et/ou (ii) un MCT.
- o. « Contenu du Formateur » désigne la version du formateur du Cours Microsoft avec Formateur et tout contenu supplémentaire uniquement conçu à l'usage du Formateur pour donner une session de formation en utilisant le Cours Microsoft avec Formateur. Le Contenu du Formateur peut inclure des présentations Microsoft PowerPoint, un guide de préparation du formateur, des documents de formation du formateur, des packs Microsoft One Note, un guide de préparation de la classe et un formulaire préliminaire de commentaires sur le cours. À des fins de clarification, le Contenu du Formateur ne contient aucun logiciel, disque dur virtuel ni machine virtuelle.

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

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

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

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

**pour autant que vous vous conformiez à ce qui suit :**

- iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,
- iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,
- v. vous veillerez à ce que chaque Utilisateur Final ayant reçu la version papier du Cours Microsoft avec Formateur reçoive une copie du présent contrat et reconnaisse que son utilisation du Cours Microsoft avec Formateur sera 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 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 interfacier 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](http://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

## Implémentation des services réseau avancés

### Table des matières :

Leçon 1: Configuration des fonctionnalités DHCP avancées	12
Leçon 2: Configuration des paramètres DNS avancés	14
Leçon 3: Implémentation de la réplique IPAM	17
Contrôle des acquis et éléments à retenir	20
Questions et réponses de contrôle des acquis de l'atelier pratique	22

## Leçon 1

# Configuration des fonctionnalités DHCP avancées

### Table des matières :

Démonstration

13

# Démonstration

## Démonstration : Configuration du basculement DHCP

### Procédure de démonstration

#### Configurer une relation de basculement DHCP

1. Connectez-vous à LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa\$\$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP** dans la liste déroulante. Notez que le serveur est autorisé, mais qu'aucune étendue n'est configurée.
3. Basculez vers LON-DC1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP** dans la liste déroulante.
4. Dans la console DHCP, développez **lon-dc1.adatum.com**, sélectionnez puis cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Configurer un basculement**.
5. Dans l'Assistant Configurer un basculement, cliquez sur **Suivant**.
6. Sur la page **Spécifier le serveur partenaire à utiliser pour le basculement**, dans le champ **Serveur partenaire**, entrez dans **172.16.0.21**, puis cliquez sur **Suivant**.
7. Sur la page **Créer une relation de basculement**, dans le champ **Nom de la relation**, entrez **Adatum**.
8. Dans le champ **Délai de transition maximal du client (MCLT)**, définissez les heures sur **zéro**, puis définissez les minutes sur **15**.
9. Vérifiez que le champ **Mode** est défini sur **Équilibrage de charge**.
10. Vérifiez que le champ **Pourcentage d'équilibrage de charge** est défini sur **50 %**.
11. Activez la case à cocher **Intervalle de basculement d'état**. Laissez la valeur par défaut de 60 minutes.
12. Dans le champ **Activer l'authentification du message Secret partagé**, saisissez **Pa\$\$w0rd**, puis cliquez sur **Suivant**.
13. Cliquez sur **Terminer**, puis sur **Fermer**.
14. Basculez vers LON-SVR1. Notez que le nœud IPv4 est actif.
15. Actualisez le nœud **IPv4**, développez le nœud **IPv4**, puis développez **Étendue [172.16.0.0.] Adatum**.
16. Cliquez sur **Pool d'adresses**, et notez que le pool d'adresses est configuré.
17. Cliquez sur **Options d'étendue**, et notez que les options d'étendue sont configurées.
18. Fermez la console DHCP sur LON-DC1 et LON-SVR1.
19. Rétablissez LON-SVR1.

## Leçon 2

# Configuration des paramètres DNS avancés

### Table des matières :

Démonstration

15

# Démonstration

## Démonstration : Configuration de DNSSEC

### Procédure de démonstration

#### Configurer DNSSEC

1. Connectez-vous à **LON-DC1** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa\$\$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS** dans la liste déroulante.
3. Dans DNS, développez successivement **LON-DC1** et **Zones de recherche directes**, puis cliquez avec le bouton droit sur **Adatum.com**.
4. Dans le menu, cliquez sur **DNSSEC>Signer la zone**.
5. Dans l'Assistant Signature de zone, cliquez sur **Suivant**.
6. Cliquez sur **Personnalisez les paramètres de signature de zone**, puis sur **Suivant**.
7. Sur la page **Maître des clés**, cliquez sur **Le serveur DNS LON-DC1 est le maître des clés**. Cliquez sur **Suivant**.
8. Sur la page **Clé KSK**, cliquez sur **Suivant**.
9. Sur la page **Clé KSK**, cliquez sur **Ajouter**.
10. Sur la page **Nouvelle clé KSK**, cliquez sur **OK**.
11. Sur la page **Clé KSK**, cliquez sur **Suivant**.
12. Sur la page **Clé ZSK**, cliquez sur **Suivant**.
13. Sur la page **Clé ZSK**, cliquez sur **Ajouter**.
14. Sur la page **Nouvelle clé ZSK**, cliquez sur **OK**.
15. Sur la page **Clé ZSK**, cliquez sur **Suivant**.
16. Sur la page **Next Secure (NSEC)**, cliquez sur **Suivant**.
17. Sur la page **Ancre d'approbation**, activez la case à cocher **Activer la distribution des ancres d'approbation pour cette zone**, puis cliquez sur **Suivant**.
18. Sur la page **Paramètres de signature et d'interrogation**, cliquez sur **Suivant**.
19. Sur la page **Extensions de sécurité DNS (DNSSEC)**, cliquez sur **Suivant**, puis sur **Terminer**.
20. Dans le Gestionnaire DNS, développez successivement **Points d'approbation** et **com**, puis cliquez sur **Adatum**. Assurez-vous que les enregistrements de ressource de DNSKEY existent, et que leur état est valide.
21. Dans le Gestionnaire de serveur, cliquez sur **Outils** puis, dans la liste déroulante, cliquez sur **Gestion des stratégies de groupe**.
22. Dans la Console de gestion des stratégies de groupe (GPMC), développez successivement **Forêt : Adatum.com**, développez **Domaines**, développez **Adatum.com**, cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.

23. Dans l'Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, développez successivement **Stratégies** et **Paramètres Windows**, puis cliquez sur le dossier **Stratégie de résolution de noms**.
24. Dans la section Créer des règles, dans le champ **Suffixe**, tapez **Adatum.com** pour appliquer la règle au suffixe de l'espace de noms.
25. Activez la case à cocher **Activer DNSSEC dans cette règle**.
26. Activez la case à cocher **Demander aux clients DNS de vérifier que les données de nom et d'adresse ont été validées par le serveur DNS**, puis cliquez sur **Créer**.
27. Fermez toutes les fenêtres.

## Leçon 3

# Implémentation de la réplication IPAM

### Table des matières :

Démonstration	18
---------------	----

# Démonstration

## Démonstration : Installation et configuration du système IPAM

### Procédure de démonstration

#### Installer les services IPAM

1. Connectez-vous à **LON-SVR2** en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa\$\$wOrd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, activez la case à cocher **Serveur de gestion des adresses IP (IPAM)**.
8. Dans la fenêtre contextuelle **Ajouter les fonctionnalités requises pour Serveur de gestion des adresses IP (IPAM) ?**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Quand l'Assistant Ajout de rôles et de fonctionnalités a terminé, fermez l'Assistant.

#### Configurer les services IPAM

1. Dans le volet de navigation Gestionnaire de serveur, cliquez sur **IPAM**.
2. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Se connecter au serveur IPAM**. Cliquez sur **LON-SVR2.Adatum.com**, puis cliquez sur **OK**.
3. Cliquez sur **Configurer le serveur IPAM**.
4. Dans l'Assistant Approvisionnement IPAM, cliquez sur **Suivant**.
5. Sur la page **Sélectionner la méthode d'approvisionnement**, vérifiez que l'option **Basée sur une stratégie de groupe** est sélectionnée, dans la zone **Préfixe du nom d'objet de stratégie de groupe**, saisissez **IPAM**, puis cliquez sur **Suivant**.
6. Sur la page **Confirmer les paramètres**, cliquez sur **Appliquer**. La configuration prendra quelques instants.
7. Une fois la configuration terminée, cliquez sur **Fermer**.
8. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Configurer la découverte de serveurs**.
9. Dans la boîte de dialogue **Configurer la découverte de serveur**, cliquez sur **Ajouter** pour ajouter le domaine **atum.com**, puis cliquez sur **OK**.
10. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Démarrer la découverte de serveurs**. Le processus de découverte peut durer 5 à 10 minutes. La barre jaune indique quand la découverte est terminée.

11. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Sélectionner ou ajouter des serveurs à gérer et vérifier l'accès IPAM**. Notez que l'état de l'accès IPAM est bloqué. Faites défiler l'écran jusqu'au volet Détails, et notez le rapport d'état. Le serveur IPAM n'a pas encore obtenu l'autorisation de gérer LON-DC1 par l'intermédiaire de la stratégie de groupe.
12. Dans la barre des tâches, cliquez avec le bouton droit sur l'icône Windows PowerShell, puis cliquez sur **Exécuter en tant qu'administrateur**.
13. Sur invitation de Windows PowerShell® saisissez la commande suivante et appuyez sur Entrée :

```
Invoke-IPAMGpoProvisioning -Domain Adatum.com -GpoPrefixName IPAM -IPAMServerFqdn LON-SVR2.adatum.com -DelegatedGpoUser Administrateur
```

14. Quand vous êtes invité à confirmer l'action, saisissez **O**, puis appuyez sur Entrée. Cette commande demande quelques minutes pour s'exécuter.
15. Fermez Windows PowerShell.
16. Basculez vers Gestionnaire de serveur. Dans le volet d'informations sur IPv4, cliquez avec le bouton droit sur **LON-DC1**, puis cliquez sur **Modifier le serveur**.
17. Dans la boîte de dialogue **Ajouter ou modifier un serveur**, définissez le champ **État de gérabilité** sur **Géré**, puis cliquez sur **OK**.
18. Basculez vers **LON-DC1**.
19. Dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
20. À l'invite de Windows PowerShell, saisissez **Gpupdate /force** et appuyez sur Entrée.
21. Fermez Windows PowerShell.
22. Retournez sur LON-SVR2 et, dans le Gestionnaire de serveur, cliquez avec le bouton droit sur LON-DC1, puis cliquez sur **Actualiser l'état de l'accès serveur**. Le processus de découverte peut durer 5 à 10 minutes. La barre jaune indique quand la découverte est terminée. Une fois la découverte terminée, actualisez IPv4 en cliquant sur l'icône **Actualiser**. La modification de l'état peut prendre jusqu'à 5 minutes.
23. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Récupérer les données des serveurs gérés**. L'exécution de cette action prendra quelques minutes.

## Contrôle des acquis et éléments à retenir

### Méthode conseillée

- Implémentez le basculement DHCP pour vous assurer que les ordinateurs clients peuvent continuer à recevoir les informations de configuration IP en cas de défaillance du serveur.
- Assurez-vous qu'au moins deux serveurs DNS hébergent chaque zone.
- Utilisez IPAM pour contrôler la distribution d'adresses IP et les affectations d'adresses statiques.

### Questions de contrôle des acquis

**Question :** Quel est l'un des inconvénients liés à l'utilisation d'IPAM ?

**Réponse :** Si vous utilisez IPAM, vous ne pouvez pas gérer les périphériques réseau compatibles avec DHCP (tels que les passerelles et les protocoles WAP de la console de gestion IPAM).

### Problèmes réels et scénarios

Certains clients réseau reçoivent une configuration DHCP incorrecte. Quel outil devriez-vous utiliser pour commencer le processus de résolution des problèmes ?

**Réponse :** Certains clients réseau reçoivent une configuration DHCP incorrecte. Quel outil devriez-vous utiliser pour commencer le processus de résolution des problèmes ?

Quelles sont les causes possibles des configurations incorrectes ?

**Réponse :** Un serveur DHCP non autorisé pourrait être présent sur le réseau. Recherchez la présence de passerelles, telles que des modems câbles ou des systèmes Private Branch Exchange (PBX), sur lesquelles un composant DHCP est activé. Il est également possible que quelqu'un ait configuré manuellement l'adresse IP sur le client.

### Outils

Outil	Utilisation	Emplacement
Dnscmd	Configurer tous les aspects de gestion de DNS	%systemroot%\System32\dnscmd.exe
Console DHCP	Contrôler tous les aspects de gestion de DHCP d'une interface utilisateur	%systemroot%\System32\dhcpcmgmt.msc
Console DNS	Contrôler tous les aspects de gestion de DNS d'une interface utilisateur	%systemroot%\System32\dnsmgmt.msc
Console de gestion des services Internet (IPAM)	Contrôler tous les aspects de gestion d'IPAM	Gestionnaire de serveur

## Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Les utilisateurs ne peuvent plus accéder au site Web d'un fournisseur auquel ils ont déjà pu accéder.	L'adresse IP du site Web a peut-être changé, mais le verrouillage de cache DNS ne met pas à jour l'adresse IP en mémoire cache pour ce nom de domaine complet parce que la durée de vie de l'enregistrement n'a pas encore expiré. Vous devez vider le cache sur le serveur DNS manuellement.
Les serveurs gérés ne peuvent pas se connecter au serveur IPAM.	Vérifiez que le service de base de données interne Windows et le service d'activation des processus Windows s'exécutent sur le serveur IPAM.

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique : Implémentation des services réseau avancés

**Question :** Les ordinateurs clients cesseront-ils immédiatement de communiquer sur le réseau s'il n'y a aucun serveur DHCP en fonctionnement ?

**Réponse :** Non, les ordinateurs clients continueront à fonctionner normalement sur le réseau jusqu'à ce que le bail de leur adresse IP expire.

**Question :** Quelle est la taille du pool de sockets DNS par défaut ?

**Réponse :** La taille par défaut du pool de sockets DNS est de 2 500.

**Question :** Quelle valeur le verrouillage de cache DNS utilise-t-il pour déterminer quand mettre une adresse IP à jour dans le cache DNS ?

**Réponse :** La valeur est déterminée par la durée de vie de l'enregistrement d'adresse à compter du début de l'enregistrement de ressource SOA.

# Module 2

## Implémentation des services de fichiers avancés

### Table des matières :

Leçon 1: Configuration du stockage iSCSI	24
Leçon 2: Configuration de la fonctionnalité BranchCache	28
Leçon 3: Optimisation de l'utilisation du stockage	31
Contrôle des acquis et éléments à retenir	35
Questions et réponses de contrôle des acquis de l'atelier pratique	38

## Leçon 1

# Configuration du stockage iSCSI

### Table des matières :

Questions et réponses	25
Documentation supplémentaire	25
Démonstration	25

## Questions et réponses

### Qu'est-ce qu'iSCSI ?

**Question :** Pouvez-vous utiliser le réseau TCP/IP interne de votre organisation pour fournir une communication iSCSI ?

**Réponse :** Oui, vous pouvez. Il est toutefois conseillé d'avoir un réseau TCP/IP dédié à la communication iSCSI, afin qu'un autre trafic réseau n'interfère pas avec la communication iSCSI et que celle-ci n'interfère pas avec le trafic réseau.

### Serveur cible iSCSI et initiateur iSCSI

**Question :** Quand devez-vous penser à implémenter le démarrage sans disque sur les cibles iSCSI ?

**Réponse :** La réponse varie selon l'expérience, mais vous pouvez surtout y penser pour implémenter des technologies de virtualisation telles que VDI (Virtual Desktop Infrastructure) dans votre organisation.

## Documentation supplémentaire

### Serveur cible iSCSI et initiateur iSCSI



**Documentation supplémentaire :** Pour plus d'informations sur l'introduction des cibles iSCSI dans Windows Server 2012, reportez-vous à :

<http://go.microsoft.com/fwlink/?LinkId=270038>

(Certains de ces sites adressées dans ce cours sont en anglais.)

## Démonstration

### Démonstration : Configuration d'une cible iSCSI

#### Procédure de démonstration

#### Ajouter le service de rôle de serveur cible iSCSI

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Gérer** puis sur **Ajouter des rôles et fonctionnalités**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, développez **Service de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, activez la case à cocher **Serveur cible iSCSI**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
8. Une fois l'installation terminée, cliquez sur **Fermer**.

## Créer deux disques virtuels iSCSI et une cible iSCSI

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez dans le volet de navigation sur **Services de fichiers et de stockage**.
2. Dans le volet Services de fichiers et de stockage, cliquez sur **iSCSI**.
3. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES** puis, dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
4. Dans l'Assistant Nouveau disque virtuel iSCSI, sur la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur le lecteur **C**, puis sur **Suivant**.
5. Sur la page **Indiquer le nom du disque dur virtuel iSCSI**, saisissez **iSCSIDisk1**, puis cliquez sur **Suivant**.
6. Sur la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la case **Taille**, saisissez **5**, assurez-vous que **Go** est sélectionné dans zone de liste déroulante, puis cliquez sur **Suivant**.
7. Sur la page **Affecter la cible iSCSI**, cliquez sur **Nouvelle cible iSCSI**, puis cliquez sur **Suivant**.
8. Sur la page **Indiquer le nom de la cible**, dans la zone **Nom**, saisissez **LON-SVR2**, puis cliquez sur **Suivant**.
9. Sur la page **Indiquer les serveurs d'accès**, cliquez sur **Ajouter**.
10. Dans la boîte de dialogue **Sélectionnez une méthode pour identifier l'initiateur**, cliquez sur **Entrer une valeur pour le type sélectionné**, dans la zone de liste déroulante **Type**, cliquez sur **Adresse IP**, dans le champ **Valeur**, saisissez **172.16.0.22**, puis cliquez sur **OK**.
11. Sur la page **Indiquer les serveurs d'accès**, cliquez sur **Suivant**.
12. Sur la page **Activer l'authentification**, cliquez sur **Suivant**.
13. Sur la page **Confirmer les sélections**, cliquez sur **Créer**.
14. Sur la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.
15. Dans le volet DISQUES VIRTUELS iSCSI, cliquez sur **TÂCHES** puis, dans la zone de liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
16. Dans l'Assistant Nouveau disque virtuel iSCSI, sur la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur le lecteur **C**, puis sur **Suivant**.
17. Sur la page **Indiquer le nom du disque dur virtuel iSCSI**, saisissez **iSCSIDisk2**, puis cliquez sur **Suivant**.
18. Sur la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la case **Taille**, saisissez **5**, assurez-vous que **Go** est sélectionné dans zone de liste déroulante, puis cliquez sur **Suivant**.
19. Sur la page **Affecter la cible iSCSI**, cliquez sur **lon-svr2**, puis cliquez sur **Suivant**.
20. Sur la page **Confirmer les sélections**, cliquez sur **Créer**.
21. Sur la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.

## Démonstration : Connexion au stockage iSCSI

### Procédure de démonstration

#### Procédure de préparation

Avant de commencer cette démonstration, effectuez les étapes suivantes :

1. Sur l'ordinateur hôte, cliquez sur l'icône **Gestionnaire Hyper-V** sur la barre des tâches.
2. Dans la console Gestionnaire Hyper-V, cliquez avec le bouton droit sur **22412B-LON-SVR2**, puis cliquez sur **Paramètres**.
3. Dans le volet de gauche de la fenêtre **Paramètres pour 22412B-LON-SVR2**, assurez-vous que les deux cartes réseau héritées sont connectées à **Private Network**.
4. Si l'état d'une carte réseau héritée est défini sur **Non connecté**, cliquez sur **Carte réseau héritée** puis, dans la liste déroulante **Network** du volet de droite, sélectionnez **Private Network** et cliquez sur **OK**.

#### Se connecter à la cible iSCSI

1. Sur LON-SVR2, dans le Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur **Initiateur iSCSI**.
2. Dans la boîte de message **Microsoft iSCSI**, cliquez sur **Oui**.
3. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, dans l'onglet **Cibles**, saisissez **LON-DC1**, puis cliquez sur **Connexion rapide**.
4. Dans la fenêtre Connexion rapide, dans la section **Cibles découvertes**, cliquez sur **iqn.1991-05.com.microsoft:lon-dc1-lon-svr2-target**, puis sur **Terminer**.
5. Dans la boîte de dialogue **Propriétés de : Initiateur iSCSI**, cliquez sur **OK** pour fermer la boîte de dialogue.

#### Vérifier la présence du disque iSCSI

1. Sur LON-SVR2, dans le menu **Outils** du Gestionnaire de serveur, cliquez sur **Gestion de l'ordinateur**.
2. Dans la console Gestion de l'ordinateur, sous **Stockage**, cliquez sur **Gestion des disques**. Notez que les nouveaux disques sont ajoutés. Ils sont toutefois tous hors connexion et non formatés pour le moment.
3. Fermez la console Gestion de l'ordinateur.



**Remarque :** Laissez les ordinateurs allumés car vous en aurez besoin pour la démonstration suivante.

## Leçon 2

# Configuration de la fonctionnalité BranchCache

### Table des matières :

Démonstration

29

# Démonstration

## Démonstration : Configuration de la fonctionnalité BranchCache

### Procédure de démonstration

#### Ajouter BranchCache pour le service de rôle Fichiers réseau

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, développez **Service de fichiers et de stockage (Installé)**, développez **Services de stockage (Installé)**, activez la case à cocher **BranchCache pour fichiers réseau**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
8. Une fois l'installation terminée, cliquez sur **Fermer**.

#### Activez BranchCache pour le serveur

1. Sur LON-DC1, cliquez sur l'écran Accueil.
2. Sur l'écran Accueil, saisissez **gpedit.msc**, puis appuyez sur ENTRÉE.
3. Développez **Configuration ordinateur**, développez **Modèles d'administration**, développez **Réseau**, cliquez sur **Serveur Lanman** et double-cliquez sur **Publication de hachages pour BranchCache**.
4. Dans la boîte de dialogue **Publication de hachages pour BranchCache**, cliquez sur **Activé**.
5. Dans la zone **Options**, sous **Actions de la publication de hachages**, sélectionnez **Autoriser la publication de hachages uniquement pour les dossiers partagés dans lesquels BranchCache est activé**, puis cliquez sur **OK**.
6. Fermez l'Éditeur de stratégie de groupe locale

#### Activer BranchCache pour un partage de fichiers

1. Dans la barre des tâches, cliquez sur l'icône de l'Explorateur de fichiers.
2. Dans l'Explorateur de fichiers, cliquez sur **Disque local (C:)**.
3. Dans la barre d'accès rapide située du côté supérieur gauche de la fenêtre, cliquez sur **Nouveau dossier**, saisissez **Partage**, puis appuyez sur Entrée.
4. Cliquez avec le bouton droit sur **Partage**, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de : Partage**, cliquez sur l'onglet **Partage**, puis cliquez sur **Partage avancé**.

6. Dans la boîte de dialogue **Partage avancé**, cliquez sur **Partager ce dossier**, puis sur **Mise en cache**.
7. Dans la boîte de dialogue **Paramètres hors connexion**, activez la case à cocher **Activer BranchCache**, puis cliquez sur **OK**.
8. Dans la boîte de dialogue **Partage avancé**, cliquez sur **OK**, puis sur **Fermer**.
9. Fermez toutes les fenêtres.

## Leçon 3

# Optimisation de l'utilisation du stockage

### Table des matières :

Questions et réponses	32
Documentation supplémentaire	32
Démonstration	32

## Questions et réponses

### Qu'est-ce que le Gestionnaire de ressources du serveur de fichiers ?

**Question :** Utilisez-vous actuellement le Gestionnaire de ressources du serveur de fichiers dans Windows Server 2008 R2 ? Si oui, pour quels domaines l'utilisez-vous ?

**Réponse :** Les réponses varieront selon l'expérience des stagiaires avec le Gestionnaire de ressources du serveur de fichiers dans Windows Server 2008 R2. Le Gestionnaire de ressources du serveur de fichiers est utilisé dans les domaines suivants :

- Infrastructure de classification des fichiers
- Tâches de gestion de fichiers
- Gestion des quotas
- Gestion du filtrage des fichiers

## Documentation supplémentaire

### Qu'est-ce que le Gestionnaire de ressources du serveur de fichiers ?



**Documentation supplémentaire :** Pour plus d'informations sur FSRM, consultez la page Nouveautés du Gestionnaire de ressources du serveur de fichiers à l'adresse <http://go.microsoft.com/fwlink/?LinkId=270039>.

## Démonstration

### Démonstration : Configuration de la classification des fichiers

#### Procédure de démonstration

1. Sur LON-SVR1, la console Gestionnaire de serveur doit s'ouvrir automatiquement. Dans le coin supérieur droit de la console Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire de ressources du serveur de fichiers**.
2. Dans le Gestionnaire de ressources du serveur de fichiers, développez **Gestion de la classification**, cliquez puis cliquez avec le bouton droit sur **Propriétés de classification**, puis cliquez sur **Créer une propriété locale**.
3. Dans la fenêtre Créer la propriété de classification locale, dans le champ **Nom**, saisissez **Corporate Documentation** puis, dans la zone de liste déroulante **Type de propriété**, vérifiez que **Oui/Non** est sélectionné, et cliquez sur **OK**.
4. Dans le Gestionnaire de ressources du serveur de fichiers, développez **Gestion de la classification**, cliquez sur **Règles de classification** puis, dans le volet Action, cliquez sur **Créer une règle de classification**.
5. Dans la fenêtre Créer une règle de classification, sur l'onglet **Général**, dans le champ **Nom de la règle**, saisissez **Corporate Documents Rule** et vérifiez que la case à cocher **Activer** est sélectionnée.

6. Dans la fenêtre Créer une règle de classification fenêtre, dans l'onglet **Portée**, cliquez sur **Ajouter**.
7. Dans la fenêtre Rechercher un dossier, développez **Allfiles (E:)**, développez **Labfiles**, cliquez sur le dossier **Corporate Documentation**, puis sur **OK**.
8. Dans la fenêtre Créer une règle de classification, sur l'onglet **Classification**, dans la zone de liste déroulante **Méthode de classification**, cliquez sur **Classificateur de dossiers**. Dans la zone de liste déroulante **Propriété-Choisissez une propriété à attribuer aux fichiers**, cliquez sur **Corporate Documentation** puis, dans la zone de liste déroulante **Propriété-Spécifier une valeur**, cliquez sur **Oui**.
9. Dans la fenêtre Créer une règle de classification, sur l'onglet **Type d'évaluation**, cliquez sur **Réévaluer les valeurs de propriété existantes**, vérifiez que la case d'option **Agréger les valeurs** est sélectionnée, puis cliquez sur **OK**.
10. Dans le Gestionnaire de ressources du serveur de fichiers, dans le volet Action, cliquez sur **Exécuter la classification avec toutes les règles maintenant**.
11. Dans la fenêtre Exécuter la classification, sélectionnez la case d'option **Attendre la fin de la classification**, puis cliquez sur **OK**.
12. Examinez le **Rapport de classification automatique** qui s'affiche dans Windows Internet Explorer® et vérifiez que le rapport affiche le même nombre de fichiers classés que dans le dossier **Documentation d'entreprise**.
13. Fermez Internet Explorer.

## Démonstration : Configuration de la déduplication des données

### Procédure de démonstration

#### Ajouter le service de rôle de déduplication des données

1. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur le menu **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, développez **Service de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, activez la case à cocher **Déduplication des données**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
8. Une fois l'installation terminée, cliquez sur **Fermer**.

### Activer la déduplication des données

1. Dans Gestionnaire de serveur, cliquez dans le volet de navigation sur **Services de fichiers et de stockage**.
2. Dans le volet Services de fichiers et de stockage, cliquez sur **Volumes**.
3. Dans le volet Volumes, cliquez avec le bouton droit sur le lecteur **E:** puis, dans la zone de liste déroulante, cliquez sur **Configurer la déduplication des données**.
4. Dans la boîte de dialogue **Paramètres de déduplication Allfiles (E:\)**, activez la case à cocher **Activer la déduplication des données** et, dans la zone **Dédupliquer les fichiers de plus de (en jours)**, saisissez **3**, puis cliquez sur **Définir la planification de la déduplication**.
5. Dans la boîte de dialogue **LON-SVR1 Planification de la déduplication**, cliquez sur **Activer l'optimisation du débit**, dans la zone de liste déroulante **Heure de début**, cliquez sur l'heure actuelle, puis cliquez sur **OK**.
6. Dans la boîte de dialogue **Paramètres de déduplication Allfiles (E:\)**, cliquez sur **OK**.

### Tester la déduplication des données

1. Sur LON-SVR1, ouvrez une fenêtre de l'explorateur de fichiers, naviguez jusqu'au lecteur E:, cliquez avec le bouton droit sur le fichier **OBSInstaller.exe**, puis cliquez sur **Copier**.
2. Collez le fichier **OBSInstaller.exe** dans les dossiers **Labfiles**.
3. Sur LON-SVR1, ouvrez le dossier E:\LabFiles, cliquez avec le bouton droit sur **OBSInstaller.exe**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés**, notez les valeurs pour **Taille** et **Taille sur le disque**.
5. Répétez les étapes 5 à 7 pour **OBSInstaller.exe** dans le dossier racine du lecteur **E:**.
6. Sur LON-SVR1, ouvrez la fenêtre de Windows PowerShell.
7. À l'invite Windows PowerShell, saisissez l'applet de commande suivante, puis appuyez sur Entrée :

```
Start-DedupJob -Type Optimization -Volume E:
```

8. Saisissez **Get-DedupJob**, puis appuyez sur Entrée. Vérifiez que le processus s'exécute.
9. Attendez une minute ou deux, puis répétez la commande **Get-Dedupjob**.
10. Si vous n'obtenez aucun résultat, cela signifie que la tâche de déduplication est terminée.
11. Dans le dossier racine du lecteur **E:**, cliquez avec le bouton droit sur **OBSInstaller.exe**, puis cliquez sur **Propriétés**.
12. Dans la boîte de dialogue **Propriétés**, notez les valeurs pour **Taille** et **Taille sur le disque**. La taille sur le disque devrait être beaucoup plus petite qu'elle l'était précédemment.

# Contrôle des acquis et éléments à retenir

## Méthode conseillée

- Lorsque vous envisagez une solution de stockage iSCSI pour votre organisation, consacrez la plus grande partie de votre temps au processus de conception. Le processus de conception est essentiel parce qu'il vous permet d'optimiser la solution pour toutes les technologies qui utiliseront le stockage iSCSI, comme les services de fichier, Exchange Server ou SQL Server. La conception doit également s'adapter à la croissance future des données d'entreprise de votre organisation. Les processus de conception réussis garantissent un déploiement réussi de la solution, qui répondra aux exigences stratégiques de votre organisation.
- Lorsque vous planifiez un déploiement de BranchCache, assurez-vous de travailler en étroite collaboration avec vos administrateurs réseau, afin de pouvoir optimiser le trafic sur le réseau WAN.
- En planifiant la classification des fichiers, veillez à commencer par les exigences stratégiques de votre organisation. Identifiez les classifications que vous appliquerez aux documents, puis définissez une méthode que vous utiliserez pour identifier des documents pour la classification. Avant de déployer l'infrastructure de classification des fichiers, créez un environnement de test et testez les scénarios pour vous assurer que la solution se traduira par un déploiement réussi, et que les exigences stratégiques de votre organisation seront satisfaites.

## Questions de contrôle des acquis

**Question :** En quoi la fonctionnalité BranchCache diffère-t-elle du système de fichiers distribués (DFS) ?

**Réponse :** BranchCache ne met en cache que les fichiers que des utilisateurs distants ont consultés. La technologie DFS réplique les fichiers entre le siège social et un emplacement distant pour que tous les fichiers existent dans les deux emplacements.

**Question :** Pourquoi préféreriez-vous implémenter BranchCache en mode de cache hébergé plutôt qu'en mode de cache distribué ?

**Réponse :** Lorsque vous utilisez le mode de cache distribué, le cache est distribué à tous les ordinateurs exécutant Windows 8. Cependant, il peut arriver que des ordinateurs de bureau ou portables qui exécutent Windows 8 soient éteints ou retirés du bureau. Cela signifie qu'un fichier mis en cache peut ne pas être disponible, ce qui forcera le fichier à être à nouveau téléchargé via la liaison WAN. Il est toutefois probable que le mode de cache hébergé soit utilisé lorsqu'un ordinateur qui exécute le système d'exploitation Windows Server 2012 est disponible dans la succursale.

**Question :** Pouvez-vous configurer la déduplication des données sur un volume de démarrage ?

**Réponse :** Non. Il n'est pas possible de configurer la déduplication des données sur un volume de démarrage. Il n'est possible de configurer la déduplication des données que sur les volumes qui ne sont ni des volumes système, ni des volumes de démarrage. La déduplication des données n'est pas non plus prise en charge par le système ReFS (Resilient File System).

**Question :** Pourquoi implémenteriez-vous une infrastructure de classification des fichiers ?

**Réponse :** L'infrastructure de classification des fichiers vous permet de gérer des groupes de fichiers selon divers attributs de fichier et dossier. Avec la technologie de classification des fichiers, vous pouvez automatiser les tâches de maintenance des fichiers et des dossiers (par ex. : le nettoyage des données périmées ou la protection des informations confidentielles).

## Problèmes réels et scénarios

Votre organisation envisage de déployer une solution iSCSI. Vous êtes l'administrateur Windows Server 2012 responsable de la conception et du déploiement de la nouvelle solution. Cette nouvelle solution sera utilisée par différents types de technologies, dont le serveur de fichiers Windows Server 2012, Exchange Server et SQL Server. Vous devez relever le défi de concevoir une solution iSCSI optimale, mais en même temps vous n'êtes pas sûr si la solution que vous allez proposer à votre organisation répondra aux exigences de toutes les technologies qui accéderont au stockage iSCSI. Que devez-vous faire ?

**Réponse :** vous devriez inclure dans l'équipe qui concevra et déploiera la solution iSCSI des experts issus de différents domaines de spécialisation. Les membres de l'équipe impliqués dans le projet devraient inclure des administrateurs Windows Server 2012, des administrateurs réseau, des administrateurs de stockage et des administrateurs de sécurité. C'est en effet nécessaire pour que la solution de stockage iSCSI bénéficie de performances et d'une sécurité optimales et pour que les procédures de gestion et d'exécution soient homogènes.

Votre organisation envisage de déployer une solution BranchCache. Vous êtes l'administrateur Windows Server 2012 responsable de la conception et du déploiement de la nouvelle solution dans votre organisation. Les directeurs commerciaux de l'organisation sont préoccupés par la sécurité des données qui seront stockées dans les succursales. Ils s'inquiètent également de la façon dont l'organisation gèrera les risques de sécurité tels que l'altération des données, la divulgation d'informations et les attaques par déni de service. Que devez-vous faire ?

**Réponse :** vous devriez inclure un expert de la sécurité dans votre équipe de conception. Vous devriez également songer au modèle de défense en profondeur pour l'analyse des risques de sécurité. BranchCache aborde les risques de sécurité comme suit :

- Falsification des données. La technologie de BranchCache utilise des hachages pour confirmer que, pendant la communication, l'ordinateur client et le serveur n'ont pas modifié les données.
- Divulgation d'informations. BranchCache envoie un contenu chiffré aux clients, qui doivent avoir la clé de chiffrement pour le déchiffrer. Comme les utilisateurs malveillants n'ont pas la clé de chiffrement, toute tentative de surveiller le trafic réseau pour accéder aux données durant leur transit entre clients est vouée à l'échec.
- Déni de service. Si une personne malveillante tente de surcharger le client avec des demandes de données, la technologie de BranchCache inclut des compteurs et des minuteurs de gestion de file d'attente pour empêcher les clients d'être surchargés.

Votre organisation utilise de grandes quantités d'espace disque pour le stockage des données et rencontre des difficultés pour organiser et gérer ces données. Votre organisation doit par ailleurs répondre à certaines exigences en matière de sécurité, de conformité et de prévention des vols de données pour les informations confidentielles. Que devez-vous faire ?

**Réponse :** vous devriez déployer une infrastructure de classification des fichiers. Selon la classification des fichiers, vous pouvez configurer des tâches de gestion qui vous permettront de gérer des groupes de fichiers en fonction des attributs des fichiers et des dossiers. Vous pouvez également automatiser les tâches de maintenance des fichiers et des dossiers, comme de nettoyer les données périmées ou protéger les informations confidentielles.

## Outils

Outil	Utilisation	Emplacement
Serveur cible iSCSI	Configurer des cibles iSCSI	Dans le Gestionnaire de serveur, sous Serveurs de fichiers et de stockage
Initiateur iSCSI	Configurer un client pour se connecter à un disque virtuel de cible iSCSI	Dans le Gestionnaire de serveur, dans la zone de liste déroulante Outils
Outil d'évaluation de la déduplication (DDPEval.exe)	Analyser un volume pour découvrir les gains potentiels de la déduplication des données	C:\windows\system32
Gestionnaire de ressources du serveur de fichiers	Ensemble de fonctionnalités qui vous permettent de gérer et classer les données stockées sur des serveurs de fichiers	Gestionnaire de serveur

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique : Implémentation de la fonctionnalité BranchCache

**Question :** Dans cet atelier pratique, vous avez déplacé LON-SVR1 dans sa propre unité d'organisation (OU). Pourquoi ?

**Réponse :** Les paramètres de configuration client ont été configurés dans la Stratégie de domaine par défaut, qui est liée à la racine du domaine. Ces paramètres de Stratégie de groupe empêchent le mode de cache hébergé d'être configuré sur LON-SVR1. En déplaçant LON-SVR1 dans sa propre unité d'organisation, vous pourriez bloquer l'héritage de la Stratégie de groupe vers cette unité d'organisation et empêcher ces paramètres de s'appliquer à LON-SVR1.

**Question :** Quand envisageriez-vous d'implémenter BranchCache dans votre propre organisation ?

**Réponse :** Les réponses varieront, mais BranchCache n'est important que si vous avez une succursale ou un site connecté au siège de votre organisation avec une liaison de bande passante à faible débit.

# Module 3

## Implémentation du contrôle d'accès dynamique

### Table des matières :

Contrôle des acquis et éléments à retenir	40
Questions et réponses de contrôle des acquis de l'atelier pratique	42

## Contrôle des acquis et éléments à retenir

### Méthode conseillée

- Utilisez des stratégies d'accès centralisé au lieu de configurer des expressions conditionnelles sur les ressources.
- Activez les paramètres d'assistance en cas d'accès refusé.
- Testez toujours les modifications que vous avez apportées aux règles d'accès centralisées et aux stratégies d'accès centralisé avant de les implémenter.
- Utilisez les classifications de fichiers pour attribuer des propriétés aux fichiers.

### Questions de contrôle des acquis

**Question :** Qu'est-ce qu'une revendication ?

**Réponse :** Une revendication désigne les informations qu'AD DS énonce au sujet d'un objet, généralement un utilisateur ou un ordinateur.

**Question :** Quel est le rôle des stratégies d'accès centralisé ?

**Réponse :** Les stratégies d'accès centralisé permettent aux administrateurs de créer des stratégies qui sont appliquées à un ou plusieurs serveurs de fichiers d'une entreprise. Les stratégies d'accès centralisé contiennent une ou plusieurs règles de stratégie d'accès centralisée. Chaque règle contient les paramètres qui déterminent l'applicabilité et les autorisations.

**Question :** Qu'est-ce que l'assistance en cas d'accès refusé ?

**Réponse :** L'assistance en cas d'accès refusé est une nouvelle fonctionnalité de Windows Server 2012 qui aide les utilisateurs à résoudre les problèmes d'accès refusé avant d'appeler l'assistance technique. L'assistance en cas d'accès refusé fournit des informations au sujet du problème et dirige les utilisateurs vers l'adresse appropriée pour obtenir de l'aide.

### Outils

Outil	Utilisation	Emplacement
Centre d'administration Active Directory	Administrer et créer des revendications, des propriétés de ressource, des règles et des stratégies	Outils d'administration
Console de gestion des stratégies de groupe (GPMC, Group Policy Management Console)	Gérer une stratégie de groupe	Outils d'administration
Éditeur de gestion des stratégies de groupe	Modifier des objets de stratégie de groupe (GPO)	GPMC

## Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Les revendications ne sont pas remplies avec les valeurs appropriées.	Vérifiez que l'attribut approprié est sélectionné pour la revendication. En outre, vérifiez que la valeur d'attribut est remplie pour un objet spécifique.
Une expression conditionnelle bloque l'accès.	Vérifiez que l'expression est définie correctement. En outre, essayez d'utiliser l'onglet <b>Accès effectif</b> pour résoudre le problème.

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique : Implémentation du contrôle d'accès dynamique

**Question :** Y a-t-il des revendications par défaut qui sont définies pour des utilisateurs ?

**Réponse :** Non, vous devez définir des revendications pour les utilisateurs.

**Question :** Comment les classifications des fichiers améliorent-elles le contrôle d'accès dynamique ?

**Réponse :** À l'aide des classifications de fichiers, vous pouvez définir des attributs sur des fichiers automatiquement, puis utiliser ces attributs dans des expressions conditionnelles en implémentant le contrôle d'accès dynamique.

**Question :** Pouvez-vous implémenter le contrôle d'accès dynamique sans utiliser une stratégie d'accès centralisé ?

**Réponse :** Oui, vous pouvez définir des expressions conditionnelles directement sur les ressources.

# Module 4

## Implémentation des déploiements de services de domaine Active Directory distribués

### Table des matières :

Leçon 1: Vue d'ensemble des déploiements AD DS distribués	44
Leçon 2: Déploiement d'un environnement AD DS distribué	46
Leçon 3: Configuration d'approbations AD DS	49
Contrôle des acquis et éléments à retenir	52
Questions et réponses de contrôle des acquis de l'atelier pratique	53

## Leçon 1

# Vue d'ensemble des déploiements AD DS distribués

### Table des matières :

Questions et réponses

45

## Questions et réponses

### Discussion : Vue d'ensemble des composants AD DS

**Question :** Qu'est-ce qu'un domaine AD DS ?

**Réponse :** Un domaine AD DS est un regroupement logique d'utilisateurs, ordinateurs et objets collectifs dans un but de gestion et de sécurité. Tous ces objets sont enregistrés dans la base de données AD DS, et une copie de ces données est enregistrée sur chaque contrôleur de domaine dans le domaine AD DS. C'est pour cela que la base de données AD DS est à tolérance de panne, et les clients peuvent accéder aux informations de domaine AD DS à partir de n'importe quel contrôleur de domaine AD DS du domaine AD DS. AD DS fournit un répertoire hiérarchisé interrogeable et une infrastructure pour l'application de la configuration et des paramètres de sécurité aux objets de l'entreprise. Vous pouvez utiliser AD DS et les objets de stratégie de groupe (GPO) pour appliquer la configuration et les paramètres de sécurité aux comptes d'utilisateur et d'ordinateur.

**Question :** Qu'est-ce qu'une arborescence de domaine AD DS ?

**Réponse :** Une arborescence de domaine AD DS est un ensemble d'un ou plusieurs domaines AD DS qui forment un espace de noms contigus. Par exemple, si le premier domaine de la forêt est adatum.com, vous pouvez créer un domaine supplémentaire en tant que domaine enfant dans cet espace de noms. Exemple : atl.adatum.com.

Parfois il est bon d'avoir plus d'un domaine dans la forêt. Quand vous ajoutez un domaine à une forêt existante, vous pouvez l'ajouter en tant que domaine enfant à un domaine existant. Ainsi, vous ajoutez le domaine à l'arborescence de domaine. Vous pouvez également créer le domaine en tant que nouvelle arborescence de domaine dans la forêt. Exemple : A. Datum Corporation est une société établie avec une forêt AD DS appelée adatum.com. Cette société acquiert une société du nom de Fabrikam, Inc. Une arborescence supplémentaire appelée fabrikam.com pourrait être créée dans la forêt d'adatum.com. Bien que le nouveau domaine soit une nouvelle arborescence de domaine, il est tout de même intégré à la forêt existante.

**Question :** Qu'est-ce qu'une forêt AD DS ?

**Réponse :** Une forêt AD DS est une collection d'une ou de plusieurs arborescences AD DS. Chaque arborescence AD DS contient un ou plusieurs domaines AD DS. La forêt AD DS est la toute dernière limite pour la sécurité et l'administration AD DS.

**Question :** Que sont les relations d'approbation ?

**Réponse :** Les relations d'approbation (approbations) sont des pipelines d'authentification entre différents domaines. Certaines approbations sont générées automatiquement dans le cadre de la procédure d'installation de domaine ; d'autres peuvent être créées manuellement. Les relations d'approbation forment l'infrastructure qui permet le partage de ressources entre les domaines. Elles fournissent également la structure qui prend en charge l'authentification entre les domaines.

**Question :** Qu'est-ce que le catalogue global ?

**Réponse :** Le catalogue global fournit un répertoire central de chaque objet dans la forêt. Il est unique dans chaque forêt AD DS. À la différence des partitions individuelles de domaine qui stockent un jeu d'attributs accessibles en écriture pour tous les objets du domaine, le catalogue global est une liste en lecture seule de certains attributs pour chaque objet de la forêt. Le catalogue global facilite la localisation des objets de différents domaines dans une forêt multi domaine. Par exemple, Microsoft® Exchange Server 2000 et les versions plus récentes utilisent le catalogue global pour localiser tous les destinataires de courrier électronique dans une forêt.

## Leçon 2

# Déploiement d'un environnement AD DS distribué

### Table des matières :

Documentation supplémentaire	47
Démonstration	47

## Documentation supplémentaire

### Niveaux fonctionnels de domaine AD DS

 **Documentation supplémentaire** : Pour en savoir plus au sujet des niveaux fonctionnels de domaine AD DS, référez-vous à Comprendre les niveaux fonctionnels des services de domaine Active Directory à l'adresse suivante : <http://go.microsoft.com/fwlink/?LinkId=270028>.

### Faire la migration vers Windows Server 2012 AD DS à partir d'une version antérieure

 **Documentation supplémentaire** :

- Vous pouvez télécharger la version 3.2 de l'outil de migration Active Directory sur <http://go.microsoft.com/fwlink/?LinkId=270029>.
- Vous pouvez télécharger le manuel de l'outil de migration Active Directory sur <http://go.microsoft.com/fwlink/?LinkId=270045>.

## Démonstration

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

#### Procédure de démonstration

#### Configurez LON-SVR1 en tant que contrôleur de domaine AD DS dans atl.adatum.com

1. Ouvrez une session sur **LON-DC1** en tant qu' **ADATUM\Administrateur** avec le mot de passe **Pa\$w0rd**.
2. Dans le Gestionnaire de serveurs, dans la colonne de gauche, cliquez sur **Tous les serveurs**.
3. Cliquez avec le bouton droit sur **Tous les serveurs**, puis cliquez sur **Ajouter des serveurs**.
4. Dans la fenêtre du nom (CN) :, saisissez **LON-SVR1**, puis cliquez sur **Rechercher maintenant**.
5. Sélectionnez **LON-SVR1**, cliquez sur la flèche d'ajout, puis cliquez sur **OK**.
6. Dans le Gestionnaire de serveurs, dans la fenêtre Serveurs, cliquez avec le bouton droit sur **LON-SVR1**, puis cliquez sur **Ajouter des rôles et fonctionnalités**.
7. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
8. Dans la page **Sélectionner le type d'installation**, assurez-vous que l'option **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.
9. Sur la page **Sélectionner le serveur de destination**, confirmez que l'option **Sélectionner un serveur du pool de serveurs** est sélectionnée. Dans la page **Pool de serveurs**, vérifiez que **LON-SVR1.Adatum.com** est mis en surbrillance puis cliquez sur **Suivant**.
10. Dans la page **Sélectionner des rôles de serveurs** activez la case à cocher **Services AD DS**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.

11. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
12. Sur la page **Services de domaine Active Directory**, examinez le message, puis cliquez sur **Suivant**.
13. Sur la page **Confirmer les sélections d'installation**, examinez le message, puis cliquez sur **Installer**.  
L'installation dure quelques minutes.
14. Sur la page **Résultats**, cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.  
L'assistant continue.

### **Accédez à LON-SVR1 en tant qu'Adatum\Administrateur**

1. Sur la page **Configuration de déploiement**, sélectionnez l'option **Ajouter un nouveau domaine à une forêt existante**, puis, à côté de **Sélectionnez le type de domaine**, vérifiez que l'option **Domaine enfant** est sélectionnée.
2. Dans le champ **Nom du domaine parent**, vérifiez que **Adatum.com** est listé.
3. Dans la zone **Nouveau nom de domaine**, saisissez **atl**, puis cliquez sur **Modifier**.
4. Lorsque vous êtes invité à donner les informations d'identification pour exécuter cette opération, utilisez le nom d'utilisateur **Adatum\Administrateur** et le mot de passe **Pa\$\$w0rd**, puis cliquez sur **OK**.
5. Dans la fenêtre Configuration de déploiement, cliquez sur **Suivant**.
6. Sur la page **Options du contrôleur de domaine**, vérifiez que **Windows Server 2012** est sélectionné en tant que **Niveau fonctionnel du domaine**, que **Serveur DNS (Domain Name System)** est sélectionné, et que **Catalogue global (GC)** est sélectionné.
7. Dans les zones de texte **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)** saisissez **Pa\$\$w0rd** dans les deux zones, puis cliquez sur **Suivant**.
8. Sur la page **Options DNS**, cliquez sur **Suivant**.
9. Dans les trois fenêtres suivantes (Options supplémentaires, chemins d'accès, et Options d'examen), cliquez sur **Suivant**. Dans la fenêtre Vérification de la configuration requise, cliquez sur **Installer**.
10. Vérifiez les informations, et laissez LON-SVR1 redémarrer en tant que contrôleur de domaine AD DS dans le nouveau domaine AD DS que vous avez créé dans la forêt AD DS.
11. Dans l'Assistant de configuration des services de domaine Active Directory, cliquez sur **Fermer**.
12. Dans l'Assistant d'ajout de rôles et de fonctionnalités, cliquez sur **Fermer**.
13. Connectez-vous à LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa\$\$w0rd**, et vérifiez quelques outils AD DS avant de confirmer l'installation du nouveau domaine.

## Leçon 3

# Configuration d'approbations AD DS

### Table des matières :

Documentation supplémentaire	50
Démonstration	50

# Documentation supplémentaire

## Configuration des paramètres avancés d'approbation AD DS



### Documentation supplémentaire :

- Pour plus d'informations sur la configuration du filtre SID mettant en quarantaine les approbations externes, voir <http://go.microsoft.com/fwlink/?LinkId=270030>.
- Pour plus d'informations sur l'activation de l'authentification sélective d'une approbation de forêt, voir <http://go.microsoft.com/fwlink/?LinkId=270046>.
- Pour plus d'informations sur le routage de suffixe de nom, voir <http://go.microsoft.com/fwlink/?LinkId=270047>.

## Démonstration

### Démonstration : Configurer une approbation de forêt

#### Procédure de démonstration

#### Configurez la résolution de nom DNS à l'aide d'un redirecteur conditionnel.

1. Sur LON-DC1, dans le Gestionnaire de Serveurs, cliquez sur le menu **Outils** et dans la liste déroulante, cliquez sur **DNS**. Le Gestionnaire DNS s'ouvre.
2. Dans le Gestionnaire DNS, développez **LON-DC1**, cliquez et cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez sur **Nouveau redirecteur conditionnel**.
3. Dans la nouvelle fenêtre de redirecteur conditionnel, dans le champ **Domaine DNS** : saisissez **treyresearch.net**.
4. Dans la zone de texte **Adresses IP des serveurs maîtres** : saisissez **172.16.10.10**. Cliquez dans l'espace ouvert, puis cliquez sur **OK**. (Si un message d'erreur s'affiche, n'en tenez pas compte).
5. Fermez le **Gestionnaire DNS**.
6. Basculez vers **MUN-DC1**, et répétez les étapes 1 à 5. Utilisez le nom de domaine d'**Adatum.com** avec l'adresse IP **172.16.0.10**.

#### Configurez une approbation de forêt sélective bidirectionnelle.

1. Dans **LON-DC1**, dans le menu **Outils** cliquez sur **Domaines et approbations Active Directory**.
2. Quand 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**, sous l'onglet **Approbations**, cliquez sur **Nouvelle approbation**.
4. Dans l'assistant de nouvelle approbation, cliquez sur **Suivant**.
5. Sur la page **Nom d'approbation**, dans le champ **Nom** , saisissez **treyresearch.net**, puis cliquez sur **Suivant**.

6. Dans l'Assistant de nouvelle approbation, cliquez sur **Approbation de forêt**, puis cliquez sur **Suivant**.
7. Sur la page **Direction de l'approbation** cliquez sur **Bidirectionnel**, puis cliquez sur **Suivant**.
8. Sur la page **Sens de l'approbation** cliquez sur **Ce domaine et le domaine spécifié**, puis cliquez sur **Suivant**.
9. Dans la zone de texte **Nom d'utilisateur** : saisissez **Administrateur**. Dans la zone de texte **Mot de passe** saisissez **Pa\$\$w0rd**, puis cliquez sur **Suivant**.
10. Sur la page **Niveau d'authentification d'approbations sortantes - Forêt locale** cliquez sur **Authentification sélective**, puis cliquez sur **Suivant**,
11. Sur la page **Niveau d'authentification d'approbations sortantes - Forêt spécifiée** cliquez sur **Authentification sélective**, puis cliquez sur **Suivant**,
12. Sur la page **Fin de la sélection des approbations** cliquez sur **Suivant**.
13. Sur la page **Fin de la création de l'approbation** cliquez sur **Suivant**.
14. Sur la page **Confirmer l'approbation sortante** cliquez sur **Oui, confirmer l'approbation sortante**, puis sur **Suivant**.
15. Sur la page **Confirmer l'approbation entrante** cliquez sur **Oui, confirmer l'approbation entrante**, puis sur **Suivant**.
16. Sur la page **Fin de l'assistant de nouvelle approbation** cliquez sur **Terminer**.
17. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur **OK**.

## Contrôle des acquis et éléments à retenir

### Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Vous recevez des messages d'erreur comme : Échec de recherche DNS, serveur RPC non disponible, le domaine n'existe pas, le contrôleur de domaine n'a pas été trouvé.	Habituellement ces erreurs sont provoquées par un échec de recherche d'enregistrement DNS. Assurez-vous qu'il y a au moins deux serveurs DNS fonctionnels disponibles sur le réseau. Assurez-vous que chaque ordinateur a au moins deux serveurs DNS qui sont configurés en configuration réseau. Vérifiez que les serveurs DNS peuvent résoudre avec succès des requêtes pour des enregistrements DNS en dehors de leur domaine DNS (par exemple adresses Internet). Utilisez différents outils de dépannage tels que nslookup, dnslint, DCdiag, netdiag, repadmin, replmon, et Observateur d'événements.
L'utilisateur ne peut pas être authentifié pour accéder à des ressources sur un autre domaine AD DS ou Kerberos.	Utilisez la console de domaines et d'approbations Active Directory (Domain.msc), ou netdom pour valider les relations d'approbation. S'il y a lieu, réinitialisez le mot de passe d'approbation. Vérifiez que les relations d'approbation sont configurées dans la bonne direction. Vérifiez que tous les contrôleurs de domaine AD DS ont inscrit tous les enregistrements SRV corrects dans la base de données DNS. (Vous pouvez redémarrer le service de netlogon sur un contrôleur de domaine AD DS pour le forcer à enregistrer de nouveau les enregistrements SRV dans la base de données DNS).

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique: Implémentation de déploiements AD DS distribués

**Question :** Pourquoi avez-vous configuré un enregistrement délégué de sous-domaine dans le DNS sur LON-DC1 avant d'ajouter le domaine enfant na.adatum.com ?

**Réponse :** Pour que le DNS s'exécutant sur LON-DC1 puisse localiser un serveur DNS pour le domaine DNS de na.adatum.com.

**Question :** Quelles sont les solutions alternatives pour créer un enregistrement délégué de sous-domaine dans la question précédente ?

**Réponse :** Sur LON-DC1, il est possible de créer une zone de stub pour que na.adatum.com fournisse une liste à jour des serveurs DNS pour le domaine DNS de na.adatum.com. Il est également possible de configurer sur LON-DC1 un fichier de zone DNS secondaire pour na.adatum.com, mais cela entraînerait plus de trafic de réplication DNS.

**Question :** Lors de la création d'une approbation de forêt, pourquoi créeriez-vous une approbation sélective au lieu d'une approbation totale ?

**Réponse :** Si vous n'aviez pas besoin d'un lien complet entre deux forêts, mais souhaitez une quantité strictement contrôlée d'interactivité.

# Module 5

## **Implémentation des sites et de la réplication Active Directory Domain Services (AD DS)**

### **Table des matières :**

<b>Leçon 2:</b> Configuration des sites AD DS	55
<b>Leçon 3:</b> Configuration et contrôle de la réplication AD DS	57
Contrôle des acquis et éléments à retenir	60
Questions et réponses de contrôle des acquis de l'atelier pratique	62

## Leçon 2

# Configuration des sites AD DS

### Table des matières :

Documentation supplémentaire	56
Démonstration	56

## Documentation supplémentaire

### Comment les ordinateurs client localisent des contrôleurs de domaine dans les sites



**Documentation supplémentaire** : Pour plus d'informations sur la façon dont la couverture de site est évaluée, consultez <http://go.microsoft.com/fwlink/?LinkId=168550>.

## Démonstration

### Démonstration : Configuration des sites AD DS

#### Procédure de démonstration

1. Dans LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
2. Dans sites et services Active Directory, développez **Sites** puis cliquez sur **Default-First-Site-Name**.
3. Cliquez avec le bouton droit sur **Default-First-Site-Name**, puis cliquez sur **Renommer**.
4. Tapez **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 **OK**.
8. Dans la boîte de dialogue **Services de domaine Active Directory** cliquez sur **OK**.
9. Dans le volet de navigation, cliquez avec le bouton droit de **Subnets**, 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. Dans la catégorie **Sélectionnez un objet du site pour ce préfixe**, cliquez sur **LondonHQ**, puis cliquez sur **OK**.
12. Dans le volet de navigation, cliquez avec le bouton droit de **Subnets**, 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. Dans la catégorie **Sélectionnez un objet du site pour ce préfixe**, cliquez sur **Toronto**, puis cliquez sur **OK**.
15. Dans le volet de navigation, développez **LondonHQ**, puis développez **Servers**.
16. Cliquez avec le bouton droit sur **TOR-DC1**, puis cliquez 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 développez **Servers**.
19. Vérifiez que TOR-DC1 est maintenant situé dans le site de Toronto.

## Leçon 3

# Configuration et contrôle de la réplication AD DS

### Table des matières :

Démonstration

58

## Démonstration

### Démonstration : Configurer la réplication Active Directory DS intersite

#### Procédure de démonstration

1. Sur TOR-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
2. Dans Sites et services Active Directory, développez **Sites**, puis développez **Inter-Site Transports**.
3. Cliquez sur **IP**, cliquez avec le bouton droit sur **DEFAULTIPSITELINK**, puis cliquez sur **Renommer**.
4. Tapez **LON-TOR** puis appuyez sur Entrée.
5. Cliquez avec le bouton droit sur **LON-TOR**, puis cliquez sur **Propriétés**. Décrivez le **Coût**, **Réplication toutes les** et les options **Modifier la planification**.
6. Dans la boîte de dialogue **Propriétés de : LON-TOR**, à côté de **Réplication toutes les**, configurez la valeur à **60 minutes**.
7. Cliquez sur **Modifier la planification**.
8. Mettez la plage en surbrillance depuis **Lundi 12h à Vendredi 16h**, cliquez sur **Réplication non disponible**, puis sur **OK**.
9. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de LON-TOR**.
10. Dans le volet de navigation, cliquez avec le bouton droit sur **IP**, puis cliquez sur **Propriétés**.
11. Dans la boîte de dialogue **Propriétés de : IP**, indiquez et expliquez l'option **Relier tous les liens de sites**.
12. Cliquez sur **OK** pour que la boîte de dialogue **Propriétés de : IP** se ferme.

### Démonstration : Configurer les stratégies de réplication du mot de passe

#### Procédure de démonstration

1. Sur LON-DC1, depuis le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console, développez le domaine **Adatum.com**, puis cliquez sur l'unité d'organisation de **Domain Controllers**.
3. Cliquez avec le bouton droit sur **Domain Controllers**, puis cliquez sur **Créer au préalable un compte de contrôleur de domaine en lecture seule**.
4. Dans l'Assistant Installation des services de domaine Active Directory, sur la page **Assistant Installation des services de domaine Active Directory** cliquez sur **Suivant**.
5. Dans la page **Informations d'identification réseau**, cliquez sur **Suivant**.

6. Dans la page **Spécifiez le nom de l'ordinateur**, tapez **LON-RODC1**, puis cliquez sur **Suivant**.
7. Dans la page **Sélectionnez un site**, cliquez sur **Toronto**, puis cliquez sur **Suivant**.
8. Sur la page **Options supplémentaires pour le contrôleur de domaine**, cliquez sur **Suivant**.



**Remarque :** Notez que l'option **Contrôleur de domaine en lecture seule** est sélectionnée et ne peut pas être désactivée. La raison est que vous avez lancé l'Assistant en choisissant de précréer un compte de contrôleur de domaine en lecture seule.

9. Sur la page **Délégation de l'installation et de l'administration du RODC**, cliquez sur **Suivant**.
10. Vérifiez vos sélections sur la page **Résumé**, puis cliquez sur **Suivant**.
11. Sur la page **Fin de l'Assistant Installation des services de domaine Active Directory**, puis cliquez sur **Terminer**.
12. Dans la console, cliquez sur l'unité d'organisation **Domain Controllers**.
13. Cliquez avec le bouton droit sur **LON-RODC1**, puis cliquez sur **Propriétés**.
14. Cliquez sur l'onglet **Stratégie de répllication de mot de passe**, puis affichez la stratégie par défaut.
15. Cliquez sur **Annuler** pour fermer la section **LON-RODC1** concernant les **Propriétés**.
16. Dans la console **Utilisateurs et ordinateurs Active Directory** cliquez sur le conteneur **Users**.
17. Double-cliquez sur **Groupe de répllication dont le mot de passe RODC est autorisé**, puis cliquez sur l'onglet **Membres**.
18. Examinez les membres par défaut du groupe autorisé de répllication de mot de passe de contrôleur de domaine en lecture seule, puis cliquez sur **OK**. Il ne devrait y avoir aucun membre par défaut.
19. Double-cliquez sur **Groupe de répllication dont le mot de passe RODC est refusé**.
20. Sélectionnez l'onglet **Membres**.
21. Cliquez sur **Annuler** pour fermer Propriétés de : **Groupe de répllication dont le mot de passe...**

# Contrôle des acquis et éléments à retenir

## Méthode conseillée

Mettez en œuvre les recommandations suivantes quand vous gérez les sites et la répllication Active Directory dans votre environnement :

- Fournissez toujours au moins un ou plusieurs serveurs de catalogue global par site.
- Assurez-vous que tous les sites ont des sous-réseaux associés appropriés.
- Ne paramétrez pas de longs intervalles sans répllication quand vous configurez des planifications de répllication pour la répllication intersite.
- Évitez d'utiliser SMTP comme protocole pour la répllication.

## Questions de contrôle des acquis

**Question :** Pourquoi est-il important que tous les sous-réseaux soient identifiés et associés à un site dans une entreprise multi sites ?

**Réponse :** Il est possible de rendre le processus de localisation des contrôleurs de domaine et d'autres services plus efficaces en référant les clients au site correct en fonction de leur adresse IP et en fonction de la définition des sous-réseaux. Si un client a une adresse IP qui n'appartient pas à un site, le client lancera une requête pour tous les contrôleurs de domaine dans le domaine. Ce n'est pas une stratégie efficace. En fait, un client unique peut effectuer des actions sur des contrôleurs de domaine de différents sites, ce qui peut mener à des résultats étranges si ces modifications n'ont pas encore été répliquées. Par conséquent, il est crucial que chaque client sache dans quel site il se trouve, et pour cela il vous faut vous assurer que les contrôleurs de domaine sont capables d'identifier quel est l'emplacement d'un client.

**Question :** Quels sont les avantages et les inconvénients de réduire l'intervalle de répllication intersite?

**Réponse :** Réduire l'intervalle de répllication intersite améliore la convergence. Les modifications effectuées dans un site sont répliquées plus rapidement à d'autres sites. Il y a peu, voire aucun inconvénient. Si vous considérez que ces modifications doivent être répliquées, qu'elles attendent 15 minutes ou trois heures, il s'agit là d'une question de temps de répllication plutôt qu'une question de quantité de répllication. Cependant, dans quelques situations extrêmes, il est possible que permettre à un plus petit nombre de modifications de se produire plus fréquemment pourrait être moins préférable que de permettre à un grand nombre de modifications de se répliquer moins fréquemment.

**Question :** Quelle est la fonction d'un serveur tête de pont ?

**Réponse :** Le serveur tête de pont est responsable de toute la répllication dans le site et en dehors. 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 des serveurs tête de pont pour gérer la répllication intersite.

## Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Le client ne peut pas localiser le contrôleur de domaine dans son site.	Vérifiez que tous les enregistrements de ressource de service (SRV) pour le contrôleur de domaine sont présents dans le DNS. Vérifiez que le contrôleur de domaine a une adresse IP du sous-réseau qui est associé avec ce site. Vérifiez que le client est un membre du domaine et a l'horaire correct.
La réplication entre les sites ne fonctionne pas.	Vérifiez que les liens de sites sont correctement configurés. Vérifiez la planification de réplication. Vérifiez que le pare-feu entre les sites permet le trafic pour la réplication Active Directory.
La réplication entre deux contrôleurs de domaine dans le même site ne fonctionne pas.	Vérifiez que les deux contrôleurs de domaine apparaissent dans le même site. Vérifiez que AD DS fonctionne correctement sur les contrôleurs de domaine. Vérifiez la communication réseau, et vérifiez que l'heure sur chaque serveur est correct.

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Questions de contrôle des acquis : Implémentation des sites et de la réplication AD DS

**Question :** Vous décidez d'ajouter un nouveau contrôleur de domaine au site de LondonHQ nommé LON-DC2. Comment pouvez-vous vérifier que LON-DC2 est utilisé pour passer tout le trafic de réplication au site de Toronto ?

**Réponse :** Il vous faudrait configurer ce nouveau contrôleur de domaine en tant que serveur tête de pont par défaut pour le site de LondonHQ.

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

**Réponse :** Il est probable que toutes les partitions excepté la partition de schéma soient modifiées. Vous ajoutez le nouveau contrôleur de domaine à la partition de domaine et à la partition de configuration pour vérifier que la réplication AD DS est configuré correctement. Si vous utilisez le DNS avec AD DS intégré, alors les enregistrements de contrôleur de domaine se mettront également à jour dans les partitions d'application DNS.

**Question :** Dans l'atelier pratique, vous avez créé un lien de sites distinct pour les sites Toronto et TestSite. Que pourriez-vous également devoir faire pour vérifier que LondonHQ ne crée pas automatiquement un objet de connexion directement avec le site TestSite ?

**Réponse :** Vous pourriez également devoir arrêter la liaison automatique de sites afin de désactiver la transitivité de site entre LondonHQ, Toronto, et TestSite.

# Module 6

## Implémentation des services de certificats Active Directory

### Table des matières :

Leçon 1: Présentation de l'infrastructure à clé publique (PKI)	64
Leçon 2: Déploiement d'autorités de certification	66
Leçon 3: Déploiement et gestion des modèles de certificats	69
Leçon 4: Implémentation de la distribution et de la révocation de certificats	71
Leçon 5: Gestion de la récupération de certificats	75
Contrôle des acquis et éléments à retenir	79
Questions et réponses de contrôle des acquis de l'atelier pratique	82

## Leçon 1

# Présentation de l'infrastructure à clé publique (PKI)

### Table des matières :

Questions et réponses

65

## Questions et réponses

### Qu'est-ce qu'une hiérarchie de certification croisée ?

**Question :** Votre société acquiert une autre société. Les deux sociétés exécutent leur propre PKI. Que pourriez-vous faire pour réduire le temps d'arrêt et continuer à fournir des services de PKI de manière transparente ?

**Réponse :** Vous pourriez implémenter une hiérarchie de certification croisée.

## Leçon 2

# Déploiement d'autorités de certification

### Table des matières :

Démonstration

67

# Démonstration

## Démonstration : Déploiement d'une AC racine

### Procédure de démonstration

#### Déploiement d'une AC racine

1. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, sélectionnez **Services de certificats Active Directory**. Dans l'Assistant Ajouter des rôles et des fonctionnalités, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Sur la page **Services de certificats Active Directory**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner des services de rôle**, vérifiez que l'option **Autorité de certification** est sélectionnée, puis cliquez sur **Suivant**.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Sur la page **Progression de l'installation**, après l'installation, cliquez sur le texte **Configurer les services de certificats Active Directory sur le serveur de destination**.
11. Dans l'Assistant de configuration AD CS, sur la page **Informations d'identification**, cliquez sur **Suivant**.
12. Sur la page **Services de rôle**, sélectionnez **Autorité de certification**, puis cliquez sur **Suivant**.
13. Sur la page **Type d'installation**, sélectionnez **Autorité de certification d'entreprise**, puis cliquez sur **Suivant**.
14. Sur la page **Type d'autorité de certification**, cliquez sur l'option **Autorité de certification racine**, puis sur **Suivant**.
15. Sur la page **Clé privée**, vérifiez que l'option **Créer une clé privée** est sélectionnée, puis cliquez sur **Suivant**.
16. Sur la page **Chiffrement pour l'autorité de certification**, conservez les sélections par défaut pour CSP et l'algorithme de hachage, mais définissez la **Longueur de la clé** sur **4 096**, puis cliquez sur **Suivant**.
17. Sur la page **Nom de l'autorité de certification**, dans la zone **Nom commun de cette AC**, tapez **AdatumRootCA**, puis cliquez sur **Suivant**.
18. Sur la page **Période de validité**, cliquez sur **Suivant**.

19. Sur la page **Base de données de l'autorité de certification**, cliquez sur **Suivant**.
20. Sur la page **Confirmation**, cliquez sur **Configurer**.
21. Sur la page **Résultats**, cliquez sur **Fermer**.
22. Sur la page **Progression de l'installation**, cliquez sur **Fermer**.

## Leçon 3

# Déploiement et gestion des modèles de certificats

### Table des matières :

Démonstration

70

# Démonstration

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

### Procédure de démonstration

#### Modifier et activer un modèle de certificat

1. Sur LON-SVR1, cliquez sur l'icône du Gestionnaire de serveur dans la barre des tâches.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Autorité de certification**.
3. Dans la console **Autorité de certification (Local)**, développez **AdatumRootCA**, cliquez avec le bouton droit sur **Modèles de certificats**, puis cliquez sur **Gérer**.
4. Passez en revue la liste des modèles par défaut. Examinez les modèles et leurs propriétés.
5. Dans le volet **Détails**, double-cliquez sur **IPSec**.
6. Dans la boîte de dialogue **Propriétés de : IPSec**, passez sur les onglets et notez ce que vous pouvez modifier sous chaque onglet. Notez que sous l'onglet **Sécurité**, vous pouvez définir des autorisations pour l'inscription. Cliquez sur **Annuler** pour fermer le modèle.
7. Dans la **Console des modèles de certificat**, dans le volet **Détails**, cliquez avec le bouton droit sur le modèle de certificat **Utilisateur Exchange**, puis cliquez sur **Dupliquer le modèle**.
8. Dans la boîte de dialogue **Propriétés du nouveau modèle**, passez en revue les options sous l'onglet **Compatibilité**.
9. Cliquez sur l'onglet **Général**, puis dans la zone de texte **Nom complet du modèle**, tapez **Exchange User Test1**.
10. Cliquez sur l'onglet **Modèles obsolètes**, puis sur **Ajouter**.
11. Cliquez sur le modèle **Utilisateur Exchange**, puis sur **OK**.
12. Cliquez sur l'onglet **Sécurité**, puis sur **Utilisateurs authentifiés**.
13. Dans le nœud **Autorisations pour Utilisateurs authentifiés**, activez les cases à cocher **Autoriser** pour les options **Lecture**, **Inscrire** et **Inscription automatique**, puis cliquez sur **OK**.
14. Fermez la **Console des modèles de certificat**.
15. Dans la console **Autorité de certification (Local)**, cliquez avec le bouton droit sur **Modèles de certificats**, pointez sur **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
16. Dans la boîte de dialogue **Activer les modèles de certificat**, sélectionnez le certificat **Exchange User Test1** et cliquez sur **OK**.

## Leçon 4

# Implémentation de la distribution et de la révocation de certificats

### Table des matières :

Démonstration

72

# Démonstration

## Démonstration : Configuration de l'agent d'inscription restreint

### Procédure de démonstration

#### Configurer l'agent d'inscription restreint

1. Sur LON-SVR1, cliquez sur l'icône du Gestionnaire de serveur dans la barre des tâches.
2. Dans la console Gestionnaire de serveur, cliquez sur **Outils**, puis ouvrez l'**Autorité de certification**.
3. Dans la console certsrv, développez **AdatumRootCA**, cliquez avec le bouton droit sur **Modèles de certificats**, puis cliquez sur **Gérer**.
4. Dans la console Modèles de certificats, double-cliquez sur **Agent d'inscription**, cliquez sur l'onglet **Sécurité**, puis cliquez sur **Ajouter**.
5. Dans la fenêtre Sélectionner les utilisateurs, ordinateurs, comptes de service ou groupes, tapez **Allie**, cliquez sur **Vérifier les noms**, puis sur **OK**.
6. Sous l'onglet **Sécurité**, cliquez sur **Allie Bellew (Allie@adatum.com)**, sélectionnez **Autoriser** pour les autorisations **Lecture** et **Inscrire**, puis cliquez sur **OK**.
7. Fermez la console Modèles de certificats.
8. Dans la console certsrv, cliquez avec le bouton droit sur **Modèles de certificats**, pointez sur **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
9. Dans la liste de modèles, cliquez sur **Agent d'inscription**, puis sur **OK**.
10. Basculez vers LON-CL1, puis ouvrez une session avec le nom d'utilisateur **Adatum\Allie** et le mot de passe **Pa\$\$w0rd**.
11. Dans l'écran Accueil, tapez **mmc.exe** et appuyez sur Entrée.
12. Dans **Console1**, ouvrez le menu **Fichier**, puis cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
13. Cliquez sur **Certificats**, sur **Ajouter**, puis sur **OK**.
14. Développez **Certificats - Utilisateur actuel**, puis cliquez sur **Personnel**.
15. Cliquez avec le bouton droit sur **Personnel**, pointez sur **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.
16. Dans l'Assistant Inscription de certificat, sur la page **Avant de commencer**, cliquez sur **Suivant**.
17. Sur la page **Sélectionner la stratégie d'inscription de certificat**, cliquez sur **Suivant**.
18. Sur la page **Demander des certificats**, sélectionnez **Agent d'inscription**, cliquez sur **Inscription**, puis sur **Terminer**.
19. Basculez vers **LON-SVR1**.
20. Dans la console Autorité de certification, cliquez avec le bouton droit **AdatumRootCA**, puis cliquez sur **Propriétés**.

21. Dans la boîte de dialogue **Propriétés de : AdatumRootCA**, cliquez sur l'onglet **Agents d'inscription**.
22. Sous l'onglet **Agents d'inscription**, cliquez sur **Restreindre les agents d'inscription**.
23. Dans la fenêtre contextuelle, cliquez sur **OK**.
24. Sous l'onglet **Agents d'inscription**, sous **Agents d'inscription**, cliquez sur **Ajouter**.
25. Dans la fenêtre Sélectionner les utilisateurs, les ordinateurs ou les groupes, tapez **Allie**, cliquez sur **Vérifier les noms**, puis sur **OK**.
26. Cliquez sur **Tout le monde**, puis sur **Supprimer**.
27. Dans la section **Modèles de certificats**, cliquez sur **Ajouter**.
28. Dans la liste de modèles, sélectionnez **Utilisateur**, puis cliquez sur **OK**.
29. Dans la section **Modèles de certificats**, cliquez sur **<Tous>**, puis cliquez sur **Supprimer**.
30. Dans la section Autorisation, cliquez sur **Ajouter**.
31. Dans la fenêtre Sélectionner les utilisateurs, les ordinateurs ou les groupes, tapez **Marketing**, cliquez sur **Vérifier les noms**, puis sur **OK**.
32. Dans la section Autorisation, cliquez sur **Tout le monde**, sur **Supprimer**, puis sur **OK**.

## Démonstration : Configuration d'un répondeur en ligne

### Procédure de démonstration

#### Configurer un répondeur en ligne

1. Sur LON-SVR1, cliquez sur l'icône du Gestionnaire de serveur dans la barre des tâches.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Cliquez sur **Suivant** à trois reprises.
4. Sur la page **Sélectionner des rôles serveur**, développez **Services de certificats Active Directory (Installé)**, puis sélectionnez **Répondeur en ligne**.
5. Cliquez sur **Ajouter des fonctionnalités**.
6. Cliquez sur **Suivant** à deux reprises, puis cliquez sur **Installer**.
7. Lorsque le message affiche que l'installation a réussi, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.
8. Dans l'Assistant Configuration AD CS, cliquez sur **Suivant**.
9. Sélectionnez **Répondeur en ligne**, puis cliquez sur **Suivant**.
10. Cliquez sur **Configurer**, puis cliquez à deux reprises sur **Fermer**.
11. Dans la console **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur la console Autorité de certification dans **LON-SVR1**.
12. Dans la console Autorité de certification, cliquez avec le bouton droit **AdatumRootCA**, puis cliquez sur **Propriétés**.

13. Dans la boîte de dialogue **Propriétés de : AdatumRootCA**, sous l'onglet **Extensions**, dans la liste **Sélectionner l'extension**, cliquez sur **Accès aux informations de l'Autorité (AIA)**, puis sur **Ajouter**.
14. Dans la boîte de dialogue **Ajouter un emplacement**, tapez **http://LON-SVR1/ocsp**, puis cliquez sur **OK**.
15. Activez la case à cocher **Inclure dans l'extension AIA des certificats émis**.
16. Activez la case à cocher **Inclure dans l'extension OCSP (Online Certificate Status Protocol)**, puis cliquez sur **OK**.
17. Dans la zone **Autorité de certification**, redémarrez Active Directory Certificate Services en cliquant sur **Oui**.
18. Dans la console certsrv, développez **AdatumRootCA**, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
19. Dans la console Modèles de certificats, double-cliquez sur le modèle **Signature de réponse OCSP**.
20. Dans la boîte de dialogue **Propriétés de : Signature de réponse OCSP**, cliquez sur l'onglet **Sécurité**. Sous **Autorisations pour Utilisateurs authentifiés**, activez la case à cocher **Autoriser** pour **Inscrire**, puis cliquez sur **OK**.
21. Fermez la console Modèles de certificats.
22. Dans la console Autorité de certification, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, pointez sur **Nouveau**, puis cliquez sur **Modèle de certificat à délivrer**.
23. Dans la boîte de dialogue **Activer les modèles de certificat**, sélectionnez le modèle **Signature de réponse OCSP**, puis cliquez sur **OK**.
24. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des répondeurs en ligne**.
25. Dans la console Gestion des répondeurs en ligne, cliquez avec le bouton droit sur **Configuration de révocation**, puis cliquez sur **Ajouter une configuration de révocation**.
26. Dans l'Assistant Ajouter une configuration de révocation, cliquez sur **Suivant**.
27. Sur la page **Nom de la configuration de révocation**, dans la zone de texte **Nom**, tapez **Répondeur en ligne AdatumCA**, puis cliquez sur **Suivant**.
28. Sur la page **Sélectionner un emplacement de certificat d'autorité de certification**, cliquez sur **Suivant**.
29. Sur la page **Choisir un certificat d'autorité de certification**, cliquez sur **Parcourir**, sur le certificat **AdatumRootCA**, sur **OK**, et sur **Suivant**.
30. Sur la page **Sélectionner le certificat utilisé pour la signature**, vérifiez que les options **Sélectionner automatiquement un certificat de signature** et **Inscription automatique pour un certificat de signature OCSP** sont sélectionnées, puis cliquez sur **Suivant**.
31. Sur la page **Fournisseur de révocation**, cliquez sur **Terminer**. L'état de la configuration de révocation est **En cours de calcul**.
32. Fermez la console Répondeur en ligne.

## Leçon 5

# Gestion de la récupération de certificats

### Table des matières :

Démonstration

76

# Démonstration

## Démonstration : Configuration d'une autorité de certification pour l'archivage de clé

### Procédure de démonstration

#### Configurer l'archivage de clé automatique

1. Sur LON-SVR1, ouvrez la console Autorité de certification.
2. Dans la console Autorité de certificat, développez le nœud **AdatumRootCA**, cliquez avec le bouton droit sur le dossier **Modèles de certificats**, puis cliquez sur **Gérer**.
3. Dans le volet Détails, cliquez avec le bouton droit sur le certificat **Agent de récupération de clé**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de : Agent de récupération de clé**, sous l'onglet **Conditions d'émission**, désactivez la case à cocher **Approbation du gestionnaire de certificat de l'Autorité de certification**.



**Remarque :** Cet onglet est proposé à titre de test uniquement. Dans un environnement de production, vous ne devez pas modifier cette valeur.

5. Sous l'onglet **Sécurité**, notez que les Admins du domaine et les administrateurs de l'entreprise sont les seuls groupes qui ont l'autorisation **Inscrire**, puis cliquez sur **OK**. N'apportez aucune modification.
6. Fermez la console Modèles de certificats.
7. Dans la console Autorité de certificat, cliquez avec le bouton droit sur **Modèles de certificats**, cliquez sur **Nouveau**, sur **Modèle de certificat à délivrer**, sur **Agent de récupération de clé** et sur **OK**. Ce processus configure une autorité de certification pour qu'elle délivre des certificats selon le modèle d'agent de récupération de clé.
8. Cliquez sur l'écran Accueil, tapez **mmc.exe**, puis appuyez sur Entrée.
9. Dans la fenêtre Console 1, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
10. Sur la page **Ajouter ou supprimer des composants logiciels enfichables**, sélectionnez **Certificats**, puis cliquez sur **Ajouter**.
11. Sélectionnez **Mon compte d'utilisateur**, cliquez sur **Terminer**, puis sur **OK**.
12. Développez **Certificats - Utilisateur actuel**, puis cliquez sur **Personnel**. Cliquez avec le bouton droit sur **Personnel**, sélectionnez **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.
13. Dans l'Assistant Inscription de certificat, cliquez sur **Suivant** à deux reprises.
14. Sur la page **Demander des certificats**, sélectionnez **Agent de récupération de clé** et cliquez sur **Inscription**.
15. Cliquez sur **Terminer**.

16. Confirmez que le nouveau certificat s'affiche dans la banque de certificats. S'il s'affiche, vous avez inscrit l'administrateur comme KRA. Réduisez la console Certificats.
17. Ouvrez les propriétés d'AdatumRootCA.
18. Sous l'onglet **Agents de récupération**, cliquez sur **Archiver la clé**, puis sur **Ajouter**, puis choisissez le certificat d'administrateur. Cliquez sur **OK**.
19. Cliquez sur **OK** et sur Oui pour redémarrer AD CS.
20. Cliquez avec le bouton droit sur **Modèles de certificats**, puis cliquez sur **Gérer**.
21. Double-cliquez sur le certificat **Exchange User Test1** pour ouvrir la boîte de dialogue **Propriétés de : Exchange User Test1**. Sous l'onglet **Traitement de la demande**, cliquez sur **Archiver la clé privée de chiffrement du sujet** et sur **Inclure des algorithmes symétriques autorisés par le sujet**. Si la fenêtre contextuelle s'affiche, cliquez sur **OK**.
22. Cliquez sur **OK** pour fermer le modèle.

## Démonstration : Récupération d'une clé privée perdue (en option)

### Procédure de démonstration

#### Récupérer une clé privée perdue

1. Sur LON-SVR1, cliquez sur l'écran Accueil, tapez **mmc.exe**, puis appuyez sur Entrée.
2. Cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
3. Sélectionnez **Certificats**, puis cliquez sur **Ajouter**.
4. Cliquez sur **Mon compte d'utilisateur**, puis sur **Terminer** et sur **OK**.
5. Développez **Certificats - Utilisateur actuel et Personnel**, puis cliquez avec le bouton droit sur **Certificats**, sélectionnez **Toutes les tâches** et cliquez sur **Demander un nouveau certificat**.
6. Inscrivez-vous pour le certificat Exchange User Test1 à l'aide de l'Assistant. Quand vous sélectionnez le modèle **Exchange User Test1** dans l'Assistant, cliquez pour ouvrir les paramètres dans une note pour entrer le nom du sujet. Dans la liste **Type**, cliquez sur **Adresse de messagerie**, dans le champ de valeur, tapez **administrateur@adatum.com**, cliquez sur **Ajouter**, sur **OK** et sur **Inscription**.
7. Vérifiez que le certificat s'affiche dans le magasin de certificats personnels.
8. Simulez une clé privée perdue en supprimant le certificat **administrateur@adatum.com** du magasin de certificats personnels. Pour ce faire, cliquez avec le bouton droit sur **administrateur@adatum.com**, cliquez sur **Supprimer**, puis sur **Oui**. Réduisez la console Certificats (Console1).
9. Dans la console Autorité de certification, dans le dossier Certificats délivrés, double-cliquez sur le certificat avec le nom de modèle **Exchange User Test1**. C'est le certificat que vous avez publié lors d'une étape précédente. Depuis l'onglet **Détails**, enregistrez le numéro de série. (Vous pouvez le copier et le coller dans le Bloc-notes, puis supprimer les espaces entre les numéros.)
10. Ouvrez une fenêtre d'invite de commandes avec des privilèges élevés. (Dans le menu **Accueil**, tapez **cmd**, cliquez avec le bouton droit sur **Invite de commandes**, puis cliquez sur **Exécuter en tant qu'administrateur**.)

11. Dans la fenêtre d'invite de commandes, basculez vers la racine du lecteur C en tapant **cd.**, puis appuyez sur Entrée. (Vous pourriez devoir le faire deux fois.)
12. Sélectionnez le numéro de série de certificat dans le Bloc-notes, cliquez avec le bouton droit sur le numéro, puis choisissez **Copier**.
13. Repassez à la fenêtre d'invite de commandes et tapez la commande suivante :

```
Certutil -getkey <numéro de série> outputblob
```

**où <numéro de série> est un numéro que vous collez depuis le Bloc-notes. Appuyez sur Entrée.**



**Remarque :** Si un point d'interrogation s'affiche au début du numéro après son collage, supprimez-le. Veillez également à supprimer tous les espaces du numéro de série, ou à entourer le numéro de série de guillemets.

14. Lorsque la commande a réussi, ouvrez le lecteur C et vérifiez que le fichier **Outputblob** s'affiche.
15. Repassez à la fenêtre d'invite de commandes. À l'invite de commandes, tapez ce qui suit et appuyez sur Entrée :

```
Certutil -recoverkey outputblob recover.pfx
```

16. À l'invite, tapez **Pa\$\$w0rd** comme nouveau mot de passe, puis confirmez le mot de passe.
17. Accédez au lecteur C, puis vérifiez que le fichier Recover.pfx, la clé récupérée, est créé.
18. Double-cliquez sur **recover.pfx**.
19. Cliquez deux fois sur **Suivant**.
20. Entrez le mot de passe **Pa\$\$w0rd**, cliquez sur **Suivant** à deux reprises, cliquez sur **Terminer**, puis sur **OK**.
21. Restaurez la console Certificats (Console 1). Actualisez le magasin de certificats.
22. Vérifiez que le certificat administrateur@adatum.com s'affiche maintenant.

# Contrôle des acquis et éléments à retenir

## Méthode conseillée

- En déployant l'infrastructure d'autorité de certification, déployez une autorité de certification racine autonome (non joint au domaine) et une autorité de certification d'entreprise secondaire (autorité de certification de publication). Après que l'autorité de certification secondaire d'entreprise reçoit un certificat d'autorité de certification racine, mettez l'autorité de certification racine hors connexion.
- Délivrez un certificat pour l'autorité de certification racine pendant une longue période, comme 15 ou 20 ans.
- Utilisez l'inscription automatique pour les certificats qui sont très utilisés.
- Utilisez un agent d'inscription restreint dès que possible.
- Utilisez les cartes à puce virtuelles pour améliorer la sécurité de l'ouverture de session.

## Questions de contrôle des acquis

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

**Réponse :** Amélioration de la sécurité, contrôle d'identité et signature numérique de code.

**Question :** Quelles sont certaines raisons pour lesquelles une organisation utiliserait une autorité de certification racine d'entreprise ?

**Réponse :** Si une organisation souhaite utiliser une seule autorité de certification et des modèles de certificats et l'inscription automatique, alors une autorité de certification racine d'entreprise est le seul choix possible.

**Question :** Citez les conditions pour utiliser l'inscription automatique pour des certificats.

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

**Question :** Quelles sont les étapes pour configurer un répondeur en ligne ?

**Réponse :** Pour configurer un répondeur en ligne, vous devez créer la configuration de répondeur et vous devez vous inscrire pour un certificat de signature OCSP. Vous devez également ajouter une URL de répondeur à AIA.

## Problèmes réels et scénarios

Contoso, Ltd souhaite déployer la PKI pour prendre en charge et sécuriser plusieurs services. Elle a décidé d'utiliser des services de certificats Windows Server 2012 comme plateforme pour la PKI. Les certificats seront principalement utilisés pour EFS, la signature numérique et des serveurs Web. Puisque les documents qui seront chiffrés sont importants, il est crucial d'avoir une stratégie de récupération après sinistre en cas de perte de clé. En outre, les clients qui auront accès aux parties sécurisées du site Web de la société ne doivent recevoir aucun avertissement sur leurs navigateurs.

1. Quel type de déploiement Contoso devrait-elle choisir ?
2. Quel type de certificats Contoso devrait-elle utiliser pour EFS et la signature numérique ?
3. Quel type de certificats Contoso devrait-elle utiliser pour un site Web ?
4. Comment Contoso vérifiera-t-elle que les données chiffrées par EFS ne sont pas perdues si un utilisateur perd un certificat ?

## Outils

- Console Autorité de certification
- Console Modèles de certificats
- Console Certificats
- Certutil.exe

## Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
L'emplacement du certificat d'Autorité de certification qui est spécifié dans l'extension d'accès à l'information d'autorité n'est pas configuré pour inclure le suffixe de nom de certificat. Les clients peuvent ne pas pouvoir localiser la version correcte du certificat d'autorité de certification de publication pour générer une chaîne de certificats, et la validation de certificat peut échouer.	Le composant logiciel enfichable de l'autorité de certification permet de configurer l'extension d'accès à l'information d'autorité pour inclure le suffixe de nom de certificat dans chaque emplacement.

*(suite)*

Problème courant	Conseil relatif à la résolution des problèmes
<p>L'autorité de certification n'est pas configurée pour inclure des emplacements de point de distribution de liste de révocation de certificats dans les extensions des certificats émis. Les clients peuvent ne pas pouvoir localiser une liste de révocation de certificats pour contrôler l'état de révocation d'un certificat, et la validation de certificat peut échouer.</p>	<p>Utilisez le composant logiciel enfichable d'autorité de certification pour configurer l'extension de point de distribution de liste de révocation de certificats et pour spécifier l'emplacement réseau de la liste de révocation de certificats.</p> <p>Les emplacements par défaut de la liste de révocation de certificats sont ajoutés aux paramètres d'extension de point de distribution de liste de révocation de certificats pendant l'installation de l'autorité de certification, et l'autorité de certification est configurée pour inclure les emplacements par défaut dans les extensions de tous les certificats émis.</p>
<p>L'autorité de certification a été installée comme AC d'entreprise, mais des paramètres de stratégie de groupe pour l'inscription automatique d'utilisateur n'ont pas été activés. Une AC d'entreprise peut utiliser l'inscription automatique pour simplifier l'émission et le renouvellement de certificats. Si l'inscription automatique n'est pas activée, l'émission et le renouvellement de certificats peuvent ne pas se produire comme prévu.</p>	<p>Utilisez la console GPMC pour configurer des paramètres de stratégie d'inscription automatique d'utilisateur et utilisez le composant logiciel enfichable de modèles de certificats pour configurer des paramètres d'inscription automatique sur le modèle de certificat.</p>

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique A : Déploiement et configuration de la hiérarchie d'autorités de certification

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

**Réponse :** Pour des raisons de sécurité, les AC racine doivent être hors connexion, sans accès au réseau. Les AC racines d'entreprise ne peuvent pas être mises hors connexion. Par conséquent, il n'existe pas de protection maximale pour cette clé.

### Atelier pratique B : Déploiement et gestion de certificats

**Question :** Quel est le principal avantage d'OCSP par rapport à la liste de révocation de certificats ?

**Réponse :** OCSP fournit l'état d'un seul certificat que les clients demandent, au lieu de télécharger l'ensemble de la liste de révocation de certificats et des listes CRL delta. En outre, les réponses sont beaucoup plus rapides et plus fiables, parce que les clients ne les mettent pas en cache.

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

**Réponse :** Pour récupérer des clés privées, vous devez configurer l'autorité de certification pour qu'elle archive des clés privées pour des modèles spécifiques, et vous devez délivrer un certificat d'agent de récupération de clé.

# Module 7

## **Implémentation des services AD RMS (Active Directory Rights Management Services)**

### **Table des matières :**

Leçon 2: Déploiement et gestion d'une infrastructure d'AD RMS	84
Leçon 3: Configuration de la protection du contenu AD RMS	87
Leçon 4: Configuration d'un accès externe à AD RMS	90
Contrôle des acquis et éléments à retenir	92
Questions et réponses de contrôle des acquis de l'atelier pratique	93

## Leçon 2

# Déploiement et gestion d'une infrastructure d'AD RMS

### Table des matières :

Démonstration

85

# Démonstration

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

### Procédure de démonstration

#### Configurer un compte de service

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
2. Sélectionnez puis 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 le champ **Nom**, saisissez **Comptes de service**, puis cliquez sur **OK**.
4. Cliquez avec le bouton droit sur l'unité d'organisation (OU) **Comptes de service**, cliquez sur **Nouveau**, puis sur **Utilisateur**.
5. Dans la boîte de dialogue **Créer un utilisateur**, entrez les détails suivants, puis cliquez sur **OK** :
  - Prénom : **ADMSSVC**
  - Nom d'ouverture de session de l'utilisateur principal : **ADMSSVC**
  - Mot de passe : **Pa\$\$w0rd**
  - Confirmer le mot de passe : **Pa\$\$w0rd**
  - Le mot de passe n'expire jamais : **Activé**
  - L'utilisateur ne peut pas changer de mot de passe : **Activé**

#### Préparer un DNS

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

#### Installer le rôle AD RMS

1. Connectez-vous à LON-SVR1 à l'aide du compte **ADATUM\Administrateur** et du mot de passe **Pa\$\$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez trois fois sur **Suivant**.
4. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Services AD RMS (Active Directory Rights Management Services)**.

5. Dans la boîte de dialogue **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez quatre fois sur **Suivant**.
6. Cliquez sur **Installer**, puis cliquez sur **Fermer**.

### Configurer AD RMS

1. Dans le Gestionnaire de serveur, cliquez sur le nœud **AD RMS**.
2. À côté de Configuration requise pour Active Directory Rights Management Services au niveau de LON-SVR1, cliquez sur **Autres...**
3. Sur la page **Détails de la tâche Tous les serveurs**, cliquez sur **Effectuer une configuration supplémentaire**.
4. 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 nouveau cluster racine AD RMS**, puis cliquez sur **Suivant**.
6. Sur la page **Base de données de configuration**, cliquez sur **Utiliser la base de données interne de Windows sur ce serveur**, puis cliquez sur **Suivant**.
7. Dans la page **Compte de service**, cliquez sur **Spécifier**.
8. Dans la boîte de dialogue **Sécurité de Windows**, entrez les détails suivants, cliquez sur **OK** puis sur **Suivant** :
  - o Nom d'utilisateur : **ADRMSSVC**
  - o Mot de passe : **Pa\$\$w0rd**
9. Sur la page **Mode de chiffrement**, cliquez sur **Mode de chiffrement 2**, puis cliquez sur **Suivant**.
10. Sur la page **Stockage de clé de cluster**, cliquez sur **Utiliser le stockage de clé AD RMS géré de manière centralisée**, puis cliquez sur **Suivant**.
11. Sur la page **Mot de passe de clé de cluster**, entrez le mot de passe **Pa\$\$w0rd** deux fois, puis cliquez sur **Suivant**.
12. Dans la page **Default Web Site**, vérifiez que **Site Web par défaut** est sélectionné, puis cliquez sur **Suivant**.
13. Sur la page **Adresse du cluster**, fournissez les informations suivantes, puis cliquez sur **Suivant**:
  - o Type de connexion : **Utiliser une connexion non chiffrée (http://)**
  - o Nom de domaine complet : **adrms.adatum.com**
  - o Port : **80**
14. Sur la page **Certificat de licence**, saisissez **Adatum AD RMS**, puis cliquez sur **Suivant**.
15. Dans la page **Inscription du SCP**, cliquez sur **Enregistrer le point de connexion de service maintenant**, puis cliquez sur **Suivant**.
16. Cliquez sur **Installer**, puis cliquez sur **Fermer**.
17. Dans l'écran Accueil, cliquez sur **Administrateur**, puis cliquez sur **Se déconnecter**.



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

## Leçon 3

# Configuration de la protection du contenu AD RMS

### Table des matières :

Documentation supplémentaire	88
Démonstration	88

# Documentation supplémentaire

## Que sont les stratégies d'exclusion ?



**Documentation supplémentaire** : Pour en savoir plus au sujet de l'activation des stratégies d'exclusion, consultez la rubrique Activation des stratégies d'exclusion à l'adresse <http://go.microsoft.com/fwlink/?LinkId=270031>.

## Démonstration

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

#### Procédure de démonstration

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Services AD RMS**.
2. Dans la console Active Directory Rights Management Services, 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 des informations d'identification du modèle**, entrez les informations suivantes, puis cliquez sur **Ajouter**, puis cliquez sur **Suivant** :
  - o Langue : **français (France)**
  - o Nom : **ReadOnly**
  - o Description : **Accès en lecture seule. Aucune copie ou impression.**
6. Dans la page **Ajouter des droits d'utilisateur**, cliquez sur **Ajouter**.
7. Sur la page **Ajouter un utilisateur ou un groupe**, saisissez **executives@adatum.com**, puis cliquez sur **OK**.
8. Quand **executives@adatum.com** est sélectionné, sous Droits, cliquez sur **Afficher**. Vérifiez que l'option **Octroyer le contrôle total au propriétaire (auteur) sans date d'expiration** est sélectionnée, puis cliquez sur **Suivant**.
9. Dans la page **Spécifier la stratégie d'expiration**, choisissez les paramètres suivants, puis cliquez sur **Suivant** :
  - o Expiration du contenu : Expire après (jours) : **7**
  - o Expiration de la licence d'utilisation : Expire après (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)**, cliquez sur **Suivant**, puis cliquez sur **Terminer**.

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

### Procédure de démonstration

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

## Leçon 4

# Configuration d'un accès externe à AD RMS

### Table des matières :

Documentation supplémentaire

91

## Documentation supplémentaire

### Options d'activation des utilisateurs externes ayant accès à AD RMS

 **Documentation supplémentaire** : Pour en savoir plus au sujet des stratégies d'approbation AD RMS, consultez la page <http://go.microsoft.com/fwlink/?LinkId=270032>.

### Implémentation de la réplication TPD

 **Documentation supplémentaire** : Pour en savoir plus au sujet de l'importation des TPD, consultez la rubrique Ajouter un domaine de publication approuvé à l'adresse <http://go.microsoft.com/fwlink/?LinkId=270033>.

### Partage de documents protégés par AD RMS à l'aide de Windows Live ID

 **Documentation supplémentaire** : Pour en savoir plus au sujet de l'utilisation de Windows Live ID établir des certificats de compte des droits pour les utilisateurs, consultez la page <http://go.microsoft.com/fwlink/?LinkId=270034>.

## Contrôle des acquis et éléments à retenir

### Méthode conseillée

- Avant de déployer AD RMS, vous devez analyser les exigences stratégiques de votre organisation et créer les modèles nécessaires. Vous devez rencontrer les utilisateurs pour les informer de la fonctionnalité AD RMS et pour demander également des commentaires sur les types de modèles dont ils aimeraient disposer.
- Contrôlez strictement l'appartenance au groupe de super utilisateurs. Les utilisateurs présents dans ce groupe peuvent accéder à tout le contenu protégé. Accorder l'appartenance à ce groupe à un utilisateur lui donne un accès complet à tout le contenu protégé par AD RMS.

### Questions de contrôle des acquis

**Question :** Quels sont les avantages d'avoir un certificat SSL installé sur le serveur AD RMS quand vous effectuez la configuration AD RMS ?

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

**Question :** Vous devez permettre d'accéder au contenu protégé par les services AD RMS à cinq utilisateurs qui sont des entrepreneurs indépendants et qui ne sont pas des membres de votre organisation. Quelle méthode devez-vous utiliser pour fournir cet accès ?

**Réponse :** Utilisez Windows Live ID pour fournir un certificat de compte de droits aux entrepreneurs indépendants.

**Question :** Vous souhaitez empêcher des utilisateurs de protéger le contenu Office PowerPoint en utilisant des modèles AD RMS. Quelles mesures devez-vous prendre pour accomplir cet objectif ?

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

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique : Implémentation AD RMS

**Question :** Quelles mesures pouvez-vous prendre pour vérifier que vous pouvez utiliser la Gestion des droits relatifs à l'information avec le rôle AD RMS ?

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

# Module 8

## **Implémentation des services AD FS (Active Directory Federation Services)**

### **Table des matières :**

<b>Leçon 1:</b> Vue d'ensemble d'AD FS	95
<b>Leçon 2:</b> Déploiement d'AD FS	97
<b>Leçon 3:</b> Implémentation d'AD FS pour une seule organisation	100
<b>Leçon 4:</b> Déploiement d'AD FS dans un scénario de fédération B2B	103
Contrôle des acquis et éléments à retenir	106
Questions et réponses de contrôle des acquis de l'atelier pratique	108

## Leçon 1

# Vue d'ensemble d'AD FS

### Table des matières :

Documentation supplémentaire

95

## Documentation supplémentaire

### Qu'est-ce qu'AD FS ?



**Documentation supplémentaire** : Pour obtenir des informations sur les différents produits de fédération d'identité qui peuvent interagir avec AD FS et des guides étape par étape sur la façon de configurer les produits, consultez le guide étape par étape et le guide pratique AD FS 2.0 à l'adresse <http://go.microsoft.com/fwlink/?LinkId=270035>.

## Leçon 2

# Déploiement d'AD FS

### Table des matières :

Démonstration	97
---------------	----

# Démonstration

## Démonstration : Installation du rôle serveur AD FS

### Procédure de démonstration

#### Installer le rôle serveur AD FS

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
2. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services AD FS (Active Directory Federation 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 AD FS (Active Directory Federation Services)**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner les services de rôle**, cliquez sur **Suivant**.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer** et patientez jusqu'à la fin de l'installation. Ne fermez pas la fenêtre.

#### Configurer le rôle serveur AD FS

1. Sur la page **Progression de l'installation**, cliquez sur **Exécuter le composant logiciel enfichable Gestion AD FS**.
2. Dans le volet Vue d'ensemble, cliquez sur le lien **Assistant Configuration du serveur de fédération AD FS**.
3. Sur la page **Bienvenue**, vérifiez que l'option **Créer un service de fédération** est sélectionnée, puis cliquez sur **Suivant**.
4. Sur la page **Sélectionner un déploiement autonome ou de batterie**, cliquez sur **Serveur de fédération autonome**, puis cliquez sur **Suivant**.
5. Sur la page **Spécifier le nom du service de fédération**, vérifiez les paramètres suivants, puis cliquez sur **Suivant** :
  - Certificat SSL : **LON-DC1.Adatum.com** ;
  - port : **443**
  - nom du service de fédération : **LON-DC1.Adatum.com**.

6. Sur la page **Prêt à appliquer les paramètres**, vérifiez que les paramètres de configuration corrects sont répertoriés, puis cliquez sur **Suivant**.
7. Patientez jusqu'à la fin de la configuration, puis cliquez sur **Fermer**.
8. Ouvrez Windows® Internet Explorer®, puis connectez-vous à l'adresse **<https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml>**.
9. Décrivez les informations de métadonnées aux stagiaires.
10. Fermez Internet Explorer.

## Leçon 3

# Implémentation d'AD FS pour une seule organisation

### Table des matières :

Démonstration

101

## Démonstration

### Démonstration : Configuration des approbations de fournisseur de revendications et de partie de confiance

#### Procédure de démonstration

##### Configurer une approbation de fournisseur de revendications

1. Sur LON-DC1, dans la console AD FS, développez **Relations d'approbation**, puis cliquez sur **Approbations de fournisseur de revendications**.
2. Dans le volet central, cliquez avec le bouton droit sur **Active Directory**, puis cliquez sur **Modifier les règles de revendication**.
3. Dans la boîte de dialogue Modifier les règles de revendication pour Active Directory, sur l'onglet **Règles de transformation d'approbation**, cliquez sur **Ajouter une règle**. L'Assistant Ajouter une règle de revendication de transformation s'ouvre.
4. Sur la page Sélectionner un modèle de règle, sous **Modèle de règle de revendication**, cliquez sur **Envoyer les attributs LDAP en tant que revendications**, puis sur **Suivant**.
5. Sur la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, saisissez **Règle d'attributs LDAP sortants**.
6. Dans la liste déroulante **Magasin d'attributs**, cliquez sur **Active Directory**.
7. Dans la section **Mappage des attributs LDAP aux types de revendications sortantes**, sélectionnez les valeurs suivantes pour l'attribut LDAP et le type de revendication sortante :
  - Adresses de messagerie = **Adresse de messagerie**
  - Nom d'utilisateur principal = **UPN**
8. Cliquez sur **Terminer**, puis sur **OK**.

##### Configurer une application Windows Identity Foundation pour AD FS

1. Sur LON-SVR1, basculez vers l'écran d'accueil, puis cliquez sur l'**Utilitaire de fédération Windows Identity Foundation**.
2. Sur la page **Bienvenue dans l'Assistant Utilitaire de fédération**, dans **Emplacement de configuration de l'application**, saisissez **C:\inetpub\wwwroot\AdatumTestApp\web.config** pour l'emplacement du fichier d'exemple web.config.
3. Dans **URI d'application**, pour indiquer le chemin d'accès à l'exemple d'application qui approuvera les revendications entrantes du serveur de fédération, saisissez **https://lon-svr1.adatum.com/AdatumTestApp/**, puis cliquez sur **Suivant**.
4. Sur la page **Service d'émission de jeton de sécurité**, sélectionnez l'option **Utiliser un STS existant**, pour l'emplacement du document de métadonnées WS-Federation du STS, saisissez **https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml**, puis cliquez sur **Suivant**.
5. Sur la page **Erreur de validation de la chaîne de certificat de signature du STS**, sélectionnez l'option **Désactiver la validation de la chaîne de certificat**, puis cliquez sur **Suivant**.

6. Sur la page **Chiffrement de jeton de sécurité**, sélectionnez l'option **Aucun chiffrement**, puis cliquez sur **Suivant**.
7. Sur la page **Revendications offertes**, vérifiez les revendications qui seront offertes par le serveur de fédération, puis cliquez sur **Suivant**.
8. Sur la page **Résumé**, vérifiez les modifications qui seront apportées à l'exemple d'application par l'Assistant Utilitaire de fédération, faites défiler les éléments pour comprendre ce que fait chaque élément, cliquez sur **Terminer**, et sur **OK**.

### **Configurer une approbation de partie de confiance**

1. Sur LON-DC1, dans la console AD FS, cliquez sur **AD FS**.
2. Dans le volet central, cliquez sur **Requis : Ajouter une approbation de partie de confiance**.
3. Dans l'Assistant Ajouter une approbation de partie de confiance, sur la page **Bienvenue**, cliquez sur **Démarrer**.
4. Sur la page **Sélectionner les sources de données**, sélectionnez l'option **Importer les données relatives à la partie de confiance publiées en ligne ou sur un réseau local**, puis saisissez **https://lon-svr1.adatum.com/adatumtestapp**.
5. Pour continuer, cliquez sur **Suivant**. Cette action invite l'Assistant à vérifier les métadonnées de l'application que le rôle serveur Web héberge.
6. Sur la page **Indiquer le nom complet**, dans la zone **Nom complet**, saisissez **ADatum Test App**, puis cliquez sur **Suivant**.
7. Sur la page **Choisir les règles d'autorisation d'émission**, vérifiez que l'option **Autoriser tous les utilisateurs à accéder à cette partie de confiance** est sélectionnée, puis cliquez sur **Suivant**.
8. Sur la page **Prêt à ajouter l'approbation**, vérifiez les paramètres d'approbation de partie de confiance, puis cliquez sur **Suivant**.
9. Sur la page **Terminer**, cliquez sur **Fermer**. La boîte de dialogue **Modifier les règles de revendication pour Adatum Test App** s'ouvre.

## Leçon 4

# Déploiement d'AD FS dans un scénario de fédération B2B

### Table des matières :

Documentation supplémentaire	104
Démonstration	104

# Documentation supplémentaire

## Fonctionnement de la découverte du domaine d'accueil



**Documentation supplémentaire** : Pour en savoir plus sur RelayState, reportez-vous au site Web Supporting Identity Provider Initiated RelayState (en anglais) à l'adresse suivante : <http://go.microsoft.com/fwlink/?LinkId=270036>.

## Démonstration

### Démonstration : Configuration des règles de revendication

#### Procédure de démonstration

#### Configurer les règles de revendication

1. Sur LON-DC1, si nécessaire, ouvrez la console AD FS.
2. Sous **Relations d'approbation**, cliquez sur **Approbatons de partie de confiance**.
3. Sélectionnez **ADatum Test App** et dans le volet Actions, cliquez sur **Modifier les règles de revendication**.
4. Sur l'onglet **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.
5. Sous **Modèle de règle de revendication**, cliquez sur **Passer ou filtrer une revendication entrante**, puis cliquez sur **Suivant**.
6. Sous le nom de la **Règle de revendication**, saisissez **Envoyer la règle du nom de groupe**.
7. Dans la liste déroulante **Type de revendication entrante**, cliquez sur **Groupe**, puis sur **Terminer**.
8. Dans la boîte de dialogue **Modifier les règles de revendication pour ADatum Test App**, sur l'onglet **Règles d'autorisation d'émission**, sélectionnez la règle nommée **Autoriser l'accès à tous les utilisateurs**, puis cliquez sur **Supprimer une règle**. Cliquez sur **Oui** pour confirmer. Sans règle, l'accès est refusé aux utilisateurs.
9. Sur l'onglet **Règles d'autorisation d'émission**, cliquez sur **Ajouter une règle**.
10. Sur la page Sélectionner un modèle de règle, sous **Modèle de règle de revendication**, sélectionnez **Autoriser ou refuser l'accès des utilisateurs en fonction d'une revendication entrante**, puis cliquez sur **Suivant**.
11. Sur la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, saisissez **Autoriser la règle du groupe Production** et dans la liste déroulante **Type de revendication entrante**, sélectionnez **Groupe**. Dans le champ **Valeur de revendication entrante**, saisissez **Production**, sélectionnez l'option **Autoriser l'accès aux utilisateurs avec cette revendication entrante**, puis cliquez sur **Terminer**.
12. Sur l'onglet **Règles d'autorisation d'émission**, cliquez sur **Ajouter une règle**.

13. Sur la page **Sélectionner le modèle de règle**, sous **Modèle de règle de revendication**, sélectionnez **Autoriser ou refuser l'accès des utilisateurs en fonction d'une revendication entrante**, puis cliquez sur **Suivant**.
14. Sur la page **Configurer la règle**, dans la zone **Nom de la règle de revendication**, saisissez **Autoriser les utilisateurs A. Datum** et dans la liste déroulante **Type de revendication entrante**, sélectionnez **UPN**. Dans le champ **Valeur de revendication entrante**, saisissez **@adatum.com**, sélectionnez l'option **Autoriser l'accès aux utilisateurs avec cette revendication entrante**, puis cliquez sur **Terminer**.
15. Cliquez sur la règle **Autoriser les utilisateurs A. Datum**, puis cliquez sur **Modifier une règle**.
16. Dans la boîte de dialogue **Modifier la règle – Autoriser les utilisateurs A. Datum**, cliquez sur **Afficher le langage de règles**. Notez que les stagiaires modifieront le langage des règles au cours de l'atelier pratique.
17. Cliquez sur **OK**, puis sur **Annuler**.

## Contrôle des acquis et éléments à retenir

### Méthode conseillée

**Question :** Quels sont les avantages du déploiement d'AD FS avec une application ou un service de basés sur le cloud ?

**Réponse :** Les principaux avantages résident dans le fait que les organisations doivent uniquement gérer les comptes d'utilisateurs dans le domaine AD DS local et les utilisateurs doivent mémoriser un seul jeu d'informations d'identification. En outre, seule l'organisation sur site doit gérer les comptes d'utilisateurs, pendant que seule société d'hébergement de l'application du cloud doit gérer ses applications.

**Question :** Dans quelles circonstances choisiriez-vous de déployer un serveur proxy de fédération ? Dans quelles circonstances n'avez-vous pas besoin de déployer un serveur proxy de fédération ?

**Réponse :** Vous devez déployer un serveur proxy de fédération lorsque les utilisateurs qui sont en dehors du réseau ont besoin d'accéder au déploiement d'AD FS. Si les seuls utilisateurs qui ont accès au déploiement d'AD FS sont internes au réseau, vous n'avez donc pas besoin d'un serveur de proxy de fédération.

### Problèmes réels et scénarios

**Question :** Tailspin Toys déploie une nouvelle application Web prenant en charge les revendications, qui doit être accessible à la fois aux utilisateurs de Tailspin Toys et aux utilisateurs de Trey Research. Quels composants AD FS devez-vous déployer au sein de Tailspin Toys pour permettre ce niveau d'accès ?

**Réponse :** Vous devez déployer un serveur proxy de fédération. En outre, sur le serveur de fédération de Tailspin Toys, vous devez configurer l'approbation de fournisseur de revendications Active Directory et créer une approbation de fournisseur de revendications pour Trey Research. Vous devez également configurer une approbation de partie de confiance sur le serveur de fédération de Tailspin Toys pour l'application Web.

**Question :** Fabrikam, Inc. examine les configurations requises pour AD FS. La société souhaite utiliser un serveur proxy de fédération pour garantir une sécurité maximale. Fabrikam bénéficie actuellement d'un réseau interne avec des serveurs DNS internes et son DNS Internet est hébergé par une société d'hébergement. Le réseau de périmètre utilise les serveurs DNS de la société d'hébergement pour la résolution DNS. Que doit faire la société pour préparer le déploiement ?

**Réponse :** Le serveur proxy de fédération doit pouvoir résoudre les adresses IP pour le serveur AD FS interne. Par conséquent, vous devez ajouter les serveurs AD FS internes à un fichier Hôtes sur le serveur proxy de fédération ou modifier la façon dont les serveurs du réseau de périmètre résolvent les noms.

## Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Erreurs de certificat sur le serveur de fédération	<ul style="list-style-type: none"> <li>• Vérifiez si le certificat se trouve dans le magasin de certificats.</li> <li>• Vérifiez si le certificat a expiré ou est révoqué.</li> <li>• Vérifiez si le certificat a une clé privée associée.</li> <li>• Vérifiez pour garantir la validité des autorisations figurant sur le certificat.</li> <li>• Vérifiez que le certificat est approuvé.</li> </ul>
Erreurs de certificat sur le client	Vérifiez que tous les certificats nécessaires à l'interaction des clients sont approuvés.
Échec de l'authentification avec AD FS de l'application cliente	<ul style="list-style-type: none"> <li>• Validez la configuration des règles de revendication et des revendications.</li> <li>• Demandez à l'utilisateur de tenter de se connecter à d'autres applications.</li> <li>• Vérifiez que le compte n'a pas expiré ou n'est pas verrouillé.</li> </ul>

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique : Implémentation des services AD FS (Active Directory Federation Services)

**Question :** Dans cet atelier pratique, vous avez implémenté l'accès à un application prenant en charge les revendications à la fois pour les utilisateurs internes et externes. Quelles mesures supplémentaires devez-vous prendre dans la partie de confiance pour autoriser l'accès aux utilisateurs externes ?

**Réponse :** Vous devez configurer une approbation de fournisseur de revendications dans la partie de confiance. Les utilisateurs ont eu accès à l'application dès que le serveur de fédération de la partie de confiance a approuvé les informations d'identification à partir du fournisseur de revendications. Vous remarquerez que vous devez également configurer une approbation de partie de confiance sur le fournisseur de revendications. En pratique, vous configurerez probablement des règles d'approbation supplémentaires pour limiter les utilisateurs qui peuvent accéder à l'application.

**Question :** Comment pouvez-vous identifier les revendications qui sont utilisées pour autoriser l'utilisateur à accéder à l'exemple d'application Windows Identity Foundation que vous avez utilisé dans l'atelier pratique?

**Réponse :** Le site Web qui s'affiche lorsque l'utilisateur accède au site affiche les informations sur les revendications présentées par l'utilisateur pour accéder au site.

# Module 9

## Implémentation de l'équilibrage de la charge réseau

### Table des matières :

Leçon 2: Configuration d'un cluster NLB	110
Leçon 3: Planification d'une implémentation NLB	114
Contrôle des acquis et éléments à retenir	116
Questions et réponses de contrôle des acquis de l'atelier pratique	117

## Leçon 2

# Configuration d'un cluster NLB

### Table des matières :

Démonstration

111

# Démonstration

## Démonstration : Déploiement NLB

### Procédure de démonstration

#### Créer un cluster NLB dans Windows Server 2012

1. Sur LON-SVR1, cliquez sur l'icône du Gestionnaire de serveur dans la barre des tâches.
2. Dans la console Gestionnaire de serveur, cliquez sur le menu **Outils**, puis sur **Windows PowerShell ISE**.
3. Dans la fenêtre Windows PowerShell ISE, entrez la commande suivante et appuyez sur Entrée :

```
Invoke-Command -ComputersName LON-SVR1,LON-SVR2 -command {Install-
WindowsFeature NLB,RSAT-NLB}
```

4. Saisissez la commande suivante puis appuyez sur Entrée :

```
New-NlbCluster -InterfaceName "Connexion au réseau local" -OperationMode Multicast -
ClusterPrimaryIP 172.16.0.42 -ClusterName LON-NLB
```

5. Saisissez la commande suivante puis appuyez sur Entrée :

```
Add-NlbClusterNode -InterfaceName "Connexion au réseau local" -NewNodeName "LON-SVR2"
-NewNodeInterface "Connexion au réseau local"
```

6. Dans la console Gestionnaire de serveur, cliquez sur le menu **Outils**, puis cliquez sur **Gestionnaire d'équilibrage de la charge réseau**.
7. Vérifiez que les nœuds LON-SVR1 et LON-SVR2 s'affichent avec l'état **Convergé** pour le cluster LON-NLB.
8. Cliquez avec le bouton droit sur le cluster **LON-NLB**, puis cliquez sur **Propriétés du cluster**.
9. Dans la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.42)**, sous l'onglet **Paramètres de cluster**, vérifiez que le cluster est défini pour utiliser le mode d'opérations de multidiffusion.
10. Sous l'onglet **Règles de port**, vérifiez qu'il n'y a qu'une seule règle de port nommée **Tous** qui commence au port **0** et se termine au port **65535** pour le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol), et utilise l'affinité unique.
11. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.42)**.

## Démonstration : Configuration de l'affinité et des règles de port NLB

### Procédure de démonstration

#### Configurer l'affinité pour des nœuds de cluster NLB

1. Sur LON-SVR2, dans la barre des tâches, cliquez sur l'icône Windows PowerShell.
2. Dans l'invite Windows PowerShell, tapez les commandes suivantes, en appuyant sur Entrée après chaque commande :

```
Cmd.exe
Mkdir c:\porttest
Xcopy /s c:\inetpub\wwwroot c:\porttest
Exit
New-Website -Name PortTest -PhysicalPath "C:\porttest" -Port 5678
New-NetFirewallRule -DisplayName PortTest -Protocol TCP -LocalPort 5678
```

#### Configurer des règles de port NLB

1. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire d'équilibrage de la charge réseau**.
2. Dans le Gestionnaire d'équilibrage de la charge réseau, cliquez avec le bouton droit sur **LON-NLB**, puis cliquez sur **Propriétés du cluster**.
3. Dans la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.42)**, sous l'onglet **Règles de port**, sélectionnez la règle **Tous les ports**, puis cliquez sur **Supprimer**.
4. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés du cluster**.
5. Dans le Gestionnaire d'équilibrage de la charge réseau, cliquez avec le bouton droit sur **LON-NLB**, puis cliquez sur **Propriétés du cluster**.
6. Dans la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.42)**, sous l'onglet **Règles de port**, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Ajouter/Modifier une règle de port**, entrez les informations suivantes, puis cliquez sur **OK** :
  - o Étendue du port : **80 à 80**
  - o Protocoles : **Les deux**
  - o Mode de filtrage : **Hôte multiple**
  - o Affinité : **Aucune**
8. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : LON-NLB(172.16.0.42)**.
9. Dans le Gestionnaire d'équilibrage de la charge réseau, cliquez avec le bouton droit sur **LON-NLB**, puis cliquez sur **Propriétés du cluster**.
10. Sous l'onglet **Règles de port**, cliquez sur **Ajouter**.

11. Dans la boîte de dialogue **Ajouter/Modifier une règle de port**, entrez les informations suivantes, puis cliquez sur **OK** :
  - Étendue du port : **5678 à 5678**
  - Protocoles : **Les deux**
  - Mode de filtrage : **Hôte unique**
12. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés du cluster**.
13. Dans le Gestionnaire d'équilibrage de la charge réseau, cliquez avec le bouton droit sur **LON-SVR1**, puis cliquez sur **Propriétés de l'hôte**.
14. Sur l'onglet **Règles de port**, cliquez sur la règle de port qui a **5678** comme valeur de début et de fin, puis cliquez sur **Modifier**.
15. Cliquez sur la valeur **Priorité de traitement** et modifiez-la avec la valeur **10**.
16. Cliquez sur **OK** deux fois pour fermer la boîte de dialogue **Ajouter/Modifier une règle de port** et la boîte de dialogue **Propriétés de l'hôte**.

## Leçon 3

# Planification d'une implémentation NLB

### Table des matières :

Documentation supplémentaire

115

## Documentation supplémentaire

### Remarques relatives à la mise à niveau des clusters NLB



**Référence liens** : Pour plus d'informations sur la mise à niveau des clusters NLB, consultez <http://go.microsoft.com/fwlink/?LinkId=270037>.

## Contrôle des acquis et éléments à retenir

### Questions de contrôle des acquis

**Question :** Vous avez créé un cluster NLB de Windows Server 2012 comportant quatre nœuds. Le cluster héberge un site Web qui est hébergé sur IIS. Quels sont les conséquences sur le cluster si vous arrêtez le service de publication World Wide Web sur l'un des nœuds ?

**Réponse :** Rien ne se produira, car NLB détecte uniquement la défaillance de serveur et non la défaillance d'une application particulière.

**Question :** Vous souhaitez héberger les sites Web `www.contoso.com`, `www.adatum.com` et `www.fabrikam.com` sur un cluster NLB de quatre nœuds. L'adresse IP du cluster sera une adresse IP publique et chaque nom de domaine complet est mappé dans le DNS à l'adresse IP publique du cluster. Quelles mesures devez-vous appliquer à chaque nœud pour vérifier que le trafic est dirigé vers le site approprié ?

**Réponse :** Vous devrez configurer des en-têtes d'hôte pour chaque site sur chaque nœud. En outre, vous devez vérifier que la configuration d'en-tête d'hôte est identique.

**Question :** Vous avez un cluster NLB de Windows de huit nœuds qui héberge une application Web. Vous souhaitez vous assurer que le trafic d'un client qui utilise le cluster demeure dans le même nœud au cours de la session, mais que le trafic des clients distincts est distribué équitablement entre tous les nœuds. Quelle option configurez-vous pour atteindre cet objectif ?

**Réponse :** Pour cela, vous devez configurer les paramètres d'affinité.

### Problèmes réels et scénarios

Pour obtenir une véritable solution de haute disponibilité, utilisez une solution de surveillance avec NLB qui détectera la défaillance d'application. Cela est lié au fait que les clusters NLB continueront à diriger le trafic direct vers les nœuds avec des applications défaillantes si NLB, qui est indépendant de l'application, continue à envoyer le trafic de pulsation.

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique : Implémentation de l'équilibrage de la charge réseau

**Question :** Combien de nœuds supplémentaires pouvez-vous ajouter au cluster LON-NLB ?

**Réponse :** Le cluster LON-NLB peut accueillir jusqu'à 32 nœuds.

**Question :** Quelles étapes effectueriez-vous pour vérifier que LON-SVR1 gère toujours les demandes du trafic web sur le port 5678, en tenant compte des règles de port fournies à la fin de cet exercice ?

**Réponse :** Vous configurez la priorité d'hôte. Vous définissez également la règle permettant d'utiliser le mode de filtrage hôte unique.

**Question :** Quelle est la différence entre une action Arrêter et Drainer et arrêter ?

**Réponse :** L'action Arrêter termine toutes les connexions actives immédiatement. L'action Drainer et arrêter bloque les nouvelles connexions, mais permet aux connexions existantes de se terminer normalement.

# Module 10

## Implémentation du clustering avec basculement

### Table des matières :

<b>Leçon 2:</b> Implémentation d'un cluster de basculement	119
<b>Leçon 3:</b> Configuration d'applications et de services hautement disponibles sur un cluster de basculement	121
<b>Leçon 4:</b> Maintenance d'un cluster de basculement	123
Contrôle des acquis et éléments à retenir	126
Questions et réponses de contrôle des acquis de l'atelier pratique	128

## Leçon 2

# Implémentation d'un cluster de basculement

### Table des matières :

Démonstration	120
---------------	-----

# Démonstration

## Démonstration : Validation et configuration d'un cluster de basculement

### Procédure de démonstration

#### Valider et configurer un cluster

1. Sur LON-SVR3, cliquez sur l'icône du Gestionnaire de serveur dans la barre des tâches.
2. Dans Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire du cluster de basculement**.
3. Dans le composant logiciel enfichable Gestionnaire du cluster de basculement, dans l'arborescence de la console, vérifiez que **Gestionnaire du cluster de basculement** est sélectionné, puis sous **Administration**, cliquez sur **Validez la configuration**, puis cliquez sur **Suivant**.
4. Dans le champ **Entrez un nom**, tapez **LON-SVR3**, puis cliquez sur **Ajouter**.
5. Dans le champ **Entrez un nom**, tapez **LON-SVR4**.
6. Cliquez sur **Ajouter**, puis sur **Suivant**.
7. Vérifiez que l'option **Exécuter tous les tests (recommandé)** est sélectionnée, puis cliquez sur **Suivant**.
8. Dans la fenêtre Confirmation, cliquez sur **Suivant**.
9. Attendez que les tests de validation se terminent, puis dans la fenêtre Résumé, cliquez sur **Rapport**.
10. Consultez les informations, puis fermez le rapport.
11. Dans l'Assistant Validation d'une configuration, désactivez la case à cocher en regard de **Créer le cluster maintenant en utilisant les nœuds validés**, puis cliquez sur **Terminer**.
12. Sur LON-SVR3, dans Gestionnaire du cluster de basculement, sous la section **Administration** du volet central, cliquez sur **Créer le cluster**.
13. Consultez la page **Avant de commencer**.
14. Cliquez sur **Suivant**, tapez **LON-SVR3**, puis cliquez sur **Ajouter**. Tapez **LON-SVR4**, puis cliquez sur **Ajouter**.
15. Vérifiez les entrées, puis cliquez sur **Suivant**.
16. Sur la page **Point d'accès pour l'administration du cluster**, entrez **Cluster1** comme Nom du cluster. Sous **Adresse**, dans le champ **Adresse IP**, tapez **172.16.0.125**, puis cliquez sur **Suivant**.
17. Dans la boîte de dialogue **Confirmation**, vérifiez les informations, désactivez la case à cocher en regard de **Ajouter la totalité du stockage disponible au cluster**, puis cliquez sur **Suivant**.
18. Sur la page **Résumé**, cliquez sur **Terminer** pour revenir au Gestionnaire du cluster de basculement.

## Leçon 3

# Configuration d'applications et de services hautement disponibles sur un cluster de basculement

### Table des matières :

Démonstration

122

# Démonstration

## Démonstration : Clustering d'un rôle de serveur de fichiers

### Procédure de démonstration

#### Mettre en cluster un rôle de serveur de fichiers

1. Sur LON-SVR3, ouvrez le **Gestionnaire du cluster de basculement**.
2. Développez **Cluster1.Adatum.com**, puis développez **Stockage** et cliquez sur **Disques**.
3. Dans le volet Actions, cliquez sur **Ajouter un disque**.
4. Désactivez les trois cases à cocher.
5. Activez la case à cocher en regard de **Disque du cluster 2**, puis cliquez sur **OK**.
6. Cliquez avec le bouton droit sur **Rôles**, puis cliquez sur **Configurer un rôle**.
7. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner un rôle**, cliquez sur **Serveur de fichiers**, puis sur **Suivant**.
9. Sur la page **Type de serveur de fichiers**, cliquez sur **Serveur de fichiers pour une utilisation générale**, puis sur **Suivant**.
10. Sur la page **Point d'accès client**, dans la zone **Nom**, saisissez **Adatum-FS**. Dans la zone **Adresse**, tapez **172.16.0.55** et cliquez sur **Suivant**.
11. Sur la page **Sélectionner le stockage**, cliquez sur la case à cocher précédant **Disque de cluster 2**, puis cliquez sur **Suivant**.
12. Sur la page **Confirmation**, cliquez sur **Suivant**.
13. Sur la page **Résumé**, cliquez sur **Terminer**.

## Leçon 4

# Maintenance d'un cluster de basculement

### Table des matières :

Démonstration	124
---------------	-----

# Démonstration

## Démonstration : Configuration de CAU

### Procédure de démonstration

#### Configurer les services CAU

1. Ouvrez une session sur LON-DC1 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa\$\$w0rd**.
2. Dans Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'Assistant Ajout de rôles et de fonctionnalités, sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, dans la liste de fonctionnalités, cliquez sur **Clustering avec basculement**.
8. Dans la boîte de dialogue **Ajouter les fonctionnalités requises pour Clustering avec basculement?** cliquez sur **Ajouter des fonctionnalités**, 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. Sur LON-DC1, dans Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Mise à jour adaptée aux clusters**.
12. Dans la fenêtre Mise à jour adaptée aux clusters, dans la liste déroulante **Se connecter à un cluster de basculement**, cliquez sur **Cluster1**, puis sur **Connecter**.
13. Dans le volet Actions de cluster, cliquez sur **Afficher un aperçu des mises à jour pour ce cluster**.
14. Dans la fenêtre Afficher un aperçu des mises à jour-Cluster1, cliquez sur **Générer la liste des aperçus de mises à jour**.



**Remarque :** Vous devez disposer d'une connexion Internet pour réaliser cette étape.

15. Après quelques minutes, des mises à jour apparaissent dans la liste. Examinez les mises à jour, puis cliquez sur **Fermer**.
16. Dans le volet Actions de cluster, cliquez sur **Créer ou modifier un profil d'Exécution de mise à jour**.
17. Examinez et expliquez les options disponibles. N'effectuez aucune modification, puis lorsque vous avez terminé, cliquez sur **Fermer**.

18. Cliquez sur **Appliquer les mises à jour à ce cluster**.
19. Sur la page **Mise en route**, cliquez sur **Suivant**.
20. Sur la page **Options de mise à jour supplémentaires**, examinez les options de mise à jour, puis cliquez sur **Suivant**.
21. Sur la page **Options de mise à jour supplémentaires**, cliquez sur **Suivant**.
22. Sur la page **Confirmation**, cliquez sur **Mettre à jour**, puis sur **Fermer**.
23. Dans le volet Nœuds de cluster, vous pouvez examiner la progression de la mise à jour.



**Remarque** : Soulignez qu'un nœud du cluster est En attente, tandis que l'autre nœud redémarre une fois qu'il a été mis à jour).

24. Patientez jusqu'à la fin du processus. (Remarque : le redémarrage des deux nœuds peut être requis.)
25. Ouvrez une session sur LON-SVR3 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa\$\$w0rd**.
26. Sur LON-SVR3, dans Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Mise à jour adaptée aux clusters**.
27. Dans la fenêtre Mise à jour adaptée aux clusters, dans la liste déroulante **Se connecter à un cluster de basculement**, sélectionnez **Cluster1**, puis cliquez sur **Connexion**.
28. Cliquez sur **Configurer les options de mise à jour automatique du cluster**.
29. Sur la page **Mise en route**, cliquez sur **Suivant**.
30. Sur la page **Ajouter le rôle en cluster de la mise à jour adaptée aux clusters avec la mise à jour automatique activée**, cliquez sur **Ajouter le rôle en cluster de la mise à jour adaptée aux clusters, avec le mode de mise à jour automatique activé, à ce cluster**, puis sur **Suivant**.
31. Dans la zone **Spécifier la planification de la mise à jour automatique**, cliquez sur **Chaque semaine**, sélectionnez **04:00** pour Heure du jour, puis sélectionnez **Dimanche** pour Jour de la semaine, puis cliquez sur **Suivant**.
32. Sur la page **Options de mise à jour supplémentaires**, cliquez sur **Suivant**.
33. Sur la page **Options de mise à jour supplémentaires**, cliquez sur **Suivant**.
34. Sur la page **Confirmation**, cliquez sur **Appliquer**.
35. Sur la page Achèvement, cliquez sur **Terminer**.

## Contrôle des acquis et éléments à retenir

### Questions de contrôle des acquis

**Question :** Pourquoi l'utilisation d'une configuration de quorum Pas de majorité : Disque uniquement est-elle généralement déconseillée ?

**Réponse :** Lorsque vous utilisez une configuration de quorum Pas de majorité : Disque uniquement, le cluster de basculement cesse de fonctionner si le numéro d'unité logique qui est utilisé en tant que disque quorum échoue. Même si toutes les autres ressources (notamment les disques pour les applications) sont disponibles, aucun des nœuds ne fournit de service lorsque le disque quorum n'est pas disponible.

**Question :** Quel est l'objectif de la mise à jour adaptée aux clusters ?

**Réponse :** La mise à jour adaptée aux clusters est une fonctionnalité qui permet aux administrateurs de mettre à jour automatiquement des nœuds de cluster, en entraînant peu ou pas de perte de disponibilité pendant le processus de mise à jour, ce qui garantit la mise à jour de chaque nœud du cluster.

**Question :** Quelle est la principale différence entre la réplication synchrone et asynchrone dans un scénario de cluster multisite ?

**Réponse :** Lorsque vous utilisez la réplication synchrone, l'hôte reçoit une réponse « Écriture terminée » en provenance du système de stockage principal, une fois que les données ont été correctement écrites sur les deux systèmes de stockage. En cas d'échec de l'écriture des données sur les deux systèmes de stockage, l'application doit tenter d'écrire sur le disque une nouvelle fois. Avec la réplication synchrone, les deux systèmes de stockage sont identiques.

Lorsque vous utilisez la réplication asynchrone, le nœud reçoit une réponse « Écriture terminée » en provenance du système de stockage principal, une fois que les données ont été correctement écrites sur le système de stockage principal. Les données sont écrites dans le système de stockage secondaire à un autre moment, en fonction de l'implémentation du fournisseur de matériel ou de logiciels.

**Question :** Qu'est-ce qu'une fonctionnalité améliorée dans les clusters multisites Windows Server 2012 ?

**Réponse :** Dans Windows Server 2012, vous pouvez régler les paramètres de quorum du cluster de sorte que lorsque le cluster détermine s'il a le quorum, certains nœuds ont un vote et d'autres non.

### Problèmes réels et scénarios

**Question :** Votre entreprise envisage d'utiliser un cluster géographiquement dispersé qui inclut un centre de données alternatif. Votre entreprise possède un seul site physique, ainsi qu'un centre de données alternatif. Cette configuration vous permet-elle de fournir un basculement automatique ?

**Réponse :** Non, cette configuration ne vous permet pas de fournir un basculement automatique. Pour fournir un basculement automatique, vous devez posséder au moins trois sites.

## Outils

Les outils d'implémentation du clustering avec basculement comprennent :

- la console Gestionnaire du cluster de basculement ;
- la console Mise à jour adaptée aux clusters ;
- Windows PowerShell
- Gestionnaire de serveur
- Initiateur iSCSI
- Gestion des disques

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique : Implémentation du clustering avec basculement

**Question :** Quelles informations devez-vous collecter lors de la planification d'une implémentation de cluster de basculement et la sélection d'un mode de quorum ?

**Réponse :** Vous devez collecter les informations suivantes :

- le nombre d'applications ou de services que vous déploierez sur le cluster ;
- les exigences en matière de performances et les caractéristiques pour chaque application ou service ;
- le nombre de serveurs qui doivent être disponibles pour répondre aux exigences en matière de performances ;
- l'emplacement des utilisateurs qui utilisent le cluster de basculement ;
- le type de stockage utilisé pour l'espace de stockage en cluster partagé.

**Question :** Une fois l'Assistant Validation d'une configuration exécuté, comment pouvez-vous résoudre le point de défaillance unique sur la communication réseau ?

**Réponse :** Vous pouvez résoudre le point de défaillance unique sur la communication réseau en ajoutant des cartes réseau sur un réseau distinct. Cela garantira la redondance de la communication entre les nœuds du cluster.

**Question :** Dans quelles situations peut-il être important d'activer la restauration automatique d'une application en cluster pendant des périodes spécifiques uniquement ?

**Réponse :** Si vous devez garantir que la restauration automatique n'interfère pas avec des connexions clientes, des fenêtres de sauvegarde ou toute autre opération de maintenance qu'une restauration automatique interromprait, il est important de configurer la restauration automatique sur un nœud favori à une heure spécifique.

# Module 11

## **Implémentation du clustering avec basculement à l'aide d'Hyper-V**

### **Table des matières :**

<b>Leçon 2:</b> Implémentation des ordinateurs virtuels d'Hyper-V sur des clusters de basculement	130
<b>Leçon 3:</b> Implémentation des déplacements d'ordinateurs virtuels Hyper-V	132
Contrôle des acquis et éléments à retenir	135
Questions et réponses de contrôle des acquis de l'atelier pratique	136

## Leçon 2

# Implémentation des ordinateurs virtuels d'Hyper-V sur des clusters de basculement

### Table des matières :

Démonstration

131

# Démonstration

## Démonstration : Implémentation des ordinateurs virtuels sur des groupes (facultatif)

### Procédure de démonstration

#### Déplacer le stockage de l'ordinateur virtuel vers la cible iSCSI

1. Sur LON-HOST1, ouvrez une fenêtre® Explorateur de fichiers. Dans l'Explorateur de fichiers, développez le lecteur **E**, développez **Programmes**, développez **Microsoft Learning**, développez **22412**, développez **22412B-LON-CORE**, puis **Virtual Hard Disks**.
2. Dans le dossier Virtual Hard Disks, déplacez le fichier de disque dur virtuel **22412B-LON-CORE.vhd** à l'emplacement **C:\ClusterStorage\Volume1**.

#### Configurer l'ordinateur en tant qu'ordinateur à haut niveau de disponibilité

1. Dans la console Gestionnaire du cluster de basculement, cliquez sur **Rôles**, et dans le volet Actions, cliquez sur **Ordinateurs virtuels**.
2. Cliquez sur **Nouvel ordinateur virtuel**.
3. Cliquez sur **LON-HOST2**, puis sur **OK**.
4. Dans l'Assistant Nouvel ordinateur virtuel, cliquez sur **Suivant**.
5. Sur la page **Spécifier le nom et l'emplacement**, dans la zone de texte **Nom**, tapez **TestClusterVM**, cliquez sur **Stocker l'ordinateur virtuel à un autre emplacement**, puis sur **Parcourir**.
6. Accédez à et sélectionnez **C:\ClusterStorage\Volume1**, cliquez sur **Sélectionner un dossier**, puis sur **Suivant**.
7. Sur la page **Affecter la mémoire**, tapez **1536**, puis cliquez sur **Suivant**.
8. Sur la page **Configurer la mise en réseau**, cliquez sur **Réseau externe**, puis sur **Suivant**.
9. Sur la page **Connecter un disque dur virtuel**, cliquez sur **Utiliser un disque dur virtuel existant**, puis sur **Parcourir**.
10. Accédez à **C:\ClusterStorage\Volume1**, sélectionnez **22412B-LON-CORE.vhd**, puis cliquez sur **Ouvrir**.
11. Cliquez sur **Suivant**, puis sur **Terminer**.
12. Dans l'Assistant Haute disponibilité, sur la page **Résumé**, cliquez sur **Terminer**.
13. Cliquez avec le bouton droit sur **TestClusterVM**, puis sur **Démarrer**.
14. Assurez-vous que l'ordinateur démarre correctement.

## Leçon 3

# Implémentation des déplacements d'ordinateurs virtuels Hyper-V

### Table des matières :

Démonstration

133

# Démonstration

## Démonstration : Implémentation de la fonction Réplica Hyper-V (facultatif)

### Procédure de démonstration

#### Configurer un réplica

1. Sur LON-HOST2, ouvrez le Gestionnaire Hyper-V.
2. Dans le Gestionnaire Hyper-V, cliquez avec le bouton droit sur **LON-HOST2**, puis cliquez sur **Paramètres Hyper-V**.
3. Dans **Paramètres Hyper-V pour LON-HOST2**, cliquez sur **Configuration de la réplication**.
4. Dans le volet Configuration de la réplication, cliquez sur **Activer cet ordinateur en tant que serveur de réplication**.
5. Dans la section Authentification et ports, cliquez sur **Utiliser Kerberos (HTTP)**.
6. Dans la section Autorisation et stockage, cliquez sur **Autoriser la réplication à partir de tout serveur authentifié**, puis cliquez sur **Parcourir**.
7. Cliquez sur **Ordinateur**, double-cliquez sur **Disque local (E)**, cliquez sur **Nouveau dossier**, dans la zone de texte **Nom**, entrez **VMReplica**, puis appuyez sur Entrée.
8. Cliquez sur le dossier **E:\VMReplica\**, puis cliquez sur **Sélectionner un dossier**.
9. Dans **Paramètres Hyper-V pour LON-HOST2**, cliquez sur **OK**.
10. Dans la fenêtre Paramètres, lisez la notification et cliquez sur **OK**.
11. Cliquez sur **Démarrer**, sur **Panneau de configuration**, sur **Système et Sécurité**, puis sur **Pare-feu Windows**.
12. Cliquez sur **Paramètres avancés**, puis cliquez sur **Règles de trafic entrant**.
13. Dans le volet droit, dans la liste de règles, recherchez la règle **Port d'écoute HTTP de réplica Hyper-V (TCP/IN)**. Cliquez avec le bouton droit sur la règle et cliquez sur **Activer la règle**.
14. Fermez la console Pare-feu Windows Firewall avec fonctions avancées de sécurité, puis fermez le Pare-feu Windows.
15. Répétez les étapes 1 à 14 sur LON-HOST1.

#### Configurer la réplication

1. Sur LON-HOST1, ouvrez le Gestionnaire Hyper-V, cliquez sur **LON-HOST1**, cliquez avec le bouton droit sur **22412B-LON-CORE**, puis cliquez sur **Activer la réplication**.
2. Dans la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Spécifier le serveur de réplication**, cliquez sur **Parcourir**.
4. Dans la fenêtre Sélectionner l'ordinateur, saisissez **LON-HOST2**, cliquez sur **Vérifier les noms**, cliquez sur **OK**, puis sur **Suivant**.
5. Sur la page **Spécifier les paramètres de connexion**, examinez les paramètres et assurez-vous que l'option **Utiliser l'authentification Kerberos (HTTP)** est sélectionnée, puis cliquez sur **Suivant**.

6. Sur la page **Choisir les disques durs virtuels de réplication**, assurez-vous que le fichier **22412B-LON-CORE.vhd** est sélectionné, puis cliquez sur **Suivant**.
7. Sur la page **Configurer l'historique de récupération**, cliquez sur **Uniquement le dernier point de récupération**, puis cliquez sur **Suivant**.
8. Sur la page **Choisir la méthode de réplication initiale**, cliquez sur **Envoyer la copie initiale sur le réseau**, cliquez sur **Démarrer la réplication immédiatement**, puis sur **Suivant**.
9. Sur la page **Fin de l'Assistant Activation de la réplication**, cliquez sur **Terminer**.
10. Patientez 10 à 15 minutes. Dans le Gestionnaire Hyper-V, dans la colonne **État**, vous pouvez suivre la progression de la réplication initiale. Quand la réplication est terminée, assurez-vous que 22412B-LON-CORE s'affiche sur LON-HOST2 dans le Gestionnaire Hyper-V.

# Contrôle des acquis et éléments à retenir

## Méthode conseillée

- Développez les configurations standard avant d'implémenter les ordinateurs virtuels à haut niveau de disponibilité. Les ordinateurs hôtes doivent être configurés de la façon la plus proche possible. Afin de vous assurer que vous avez une plateforme Hyper-V cohérente, configurez des noms réseau standard et utilisez des normes d'affectation de noms cohérentes pour les volumes CSV.
- Implémentez la protection VMM. VMM fournit une couche de gestion sur Hyper-V et le Gestionnaire du cluster de basculement pouvant vous empêcher de réaliser des erreurs de gestion des ordinateurs virtuels hautement disponible. Par exemple, cela vous empêche de créer des ordinateurs virtuels sur un stockage qui n'est pas accessible à partir de tous les nœuds du cluster.

## Questions de contrôle des acquis

**Question :** Dans Windows Server 2008 R2, devez-vous implémenter CSV afin de fournir une haute disponibilité aux ordinateurs virtuels dans VMM ?

**Réponse :** Non vous ne devez pas implémenter CSV pour fournir la haute disponibilité. Toutefois, CSV facilite beaucoup l'implémentation et la gestion d'un environnement où plusieurs hôtes Hyper-V accèdent à plusieurs numéros d'unité logique sur un stockage partagé.

## Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Le basculement d'ordinateur virtuel échoue après l'implémentation de CSV et la migration du stockage partagé sur CSV	Le dossier de base de CSV se trouve sur le lecteur système du serveur hôte. Vous ne pouvez pas le déplacer. Si les ordinateurs hôtes utilisent des lecteurs système différents, les basculements échoueront car les hôtes ne peuvent pas accéder au même emplacement de stockage. Tous les nœuds de cluster de basculement doivent utiliser la même configuration du disque dur.
Un ordinateur virtuel bascule vers un autre nœud du cluster hôte, mais perd toute la connectivité réseau	Tous les nœuds dans un cluster hôte doivent avoir les mêmes réseaux configurés. Si ce n'est pas le cas, les ordinateurs virtuels ne pourront pas ensuite se connecter à un réseau au moment du basculement vers un autre nœud.
Quatre heures après le redémarrage d'un hôte Hyper-V membre d'un cluster hôte, aucun ordinateur virtuel ne s'exécute encore sur l'hôte.	Par défaut, les ordinateurs virtuels ne sont pas restaurés automatiquement sur un ordinateur hôte à l'issue de leur migration vers un autre hôte. Vous pouvez activer la récupération automatique dans les propriétés de l'ordinateur virtuel dans le Gestionnaire du cluster de basculement ou implémenter PRO dans VMM.

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique : Implémentation du clustering avec basculement à l'aide d'Hyper-V

**Question :** Quel est le but principal de la technologie Réplica Hyper-V ?

**Réponse :** La technologie Réplica Hyper-V fournit principalement une copie de réserve d'un ordinateur virtuel en cours d'exécution sur un autre hôte que vous pouvez activer à la demande. Vous pouvez utiliser cet ordinateur virtuel dans des scénarios de récupération d'urgence.

**Question :** Quelle est la différence principale entre la migration dynamique et la migration de stockage ?

**Réponse :** Avec la migration dynamique, vous devez implémenter le clustering avec basculement avec Hyper-V. Avec la migration dynamique, les nœuds de cluster doivent posséder un stockage partagé sur lequel sont enregistrés les fichiers de l'ordinateur virtuel. La migration de stockage peut migrer des fichiers d'ordinateur virtuel sur un seul serveur, ou entre deux serveurs, sans stockage partagé, ni clustering.

# Module 12

## Implémentation de la récupération d'urgence

### Table des matières :

Leçon 2: Implémentation de la Sauvegarde Windows Server	138
Leçon 3: Implémentation de la récupération de données et de serveurs	141
Contrôle des acquis et éléments à retenir	143
Questions et réponses de contrôle des acquis de l'atelier pratique	145

## Leçon 2

# Implémentation de la Sauvegarde Windows Server

### Table des matières :

Documentation supplémentaire	139
Démonstration	139

# Documentation supplémentaire

## Qu'est-ce que Windows Azure Online Backup ?

 **Référence liens** : Pour plus d'informations sur Windows Azure, consultez la page <http://go.microsoft.com/fwlink/?LinkId=270041>.

 **Remarque** : Pour l'instant, Windows Azure Online Backup n'est pas disponible dans tous les pays. Pour obtenir des informations mises à jour, consultez la page <http://go.microsoft.com/fwlink/?LinkId=270042>.

## Démonstration

### Démonstration : Configuration d'une sauvegarde planifiée

#### Procédure de démonstration

1. Basculez vers LON-SVR1.
2. Sur LON-SVR1, dans le Gestionnaire de serveurs, cliquez sur **Outils**, puis sur **Sauvegarde de Windows Server**.
3. Cliquez sur **Sauvegarde locale**, puis dans le volet Actions, cliquez sur **Planification de sauvegarde**.
4. Dans l'Assistant Planification de sauvegarde, sur la page **Modifier les paramètres de la sauvegarde planifiée**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner la configuration de la sauvegarde**, cliquez sur **Personnalisé**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner les éléments à sauvegarder**, cliquez sur **Ajouter des éléments**.
7. Développez **Disque local (C:)**, sélectionnez la case à cocher **HR Data**, puis cliquez sur **OK**.
8. Cliquez sur **Paramètres avancés**.
9. Cliquez sur **Ajouter une exclusion**, cliquez sur **C:\HR Data\Old HR file.txt**, puis cliquez sur **OK**.
10. Cliquez sur **OK** pour fermer la boîte de dialogue **Paramètres avancés**.
11. Cliquez sur **Suivant**.
12. Sur la page **Spécifier l'heure de sauvegarde**, à côté de **Sélectionner l'heure**, sélectionnez **01:00**, puis cliquez sur **Suivant**.
13. Sur la page **Spécifier le type de destination**, cliquez sur **Sauvegarder sur un dossier réseau partagé**, puis cliquez sur **Suivant**. Consultez l'avertissement, puis cliquez sur **OK**.
14. Sur la page **Spécifier le dossier partagé distant**, dans la zone de texte **Chemin**, tapez **\\LON-DC1\Sauvegarde**, puis cliquez sur **Suivant**.
15. Dans la boîte de dialogue **Enregistrer la planification de sauvegarde**, dans la zone de texte **Nom d'utilisateur**, tapez **Administrateur**, dans la zone de texte **Mot de passe**, tapez **Pa\$\$w0rd**, puis cliquez sur **OK**.

16. Cliquez sur **Terminer**, puis sur **Fermer**.
17. Dans le volet Actions, cliquez sur **Sauvegarde unique**.
18. Dans l'Assistant Sauvegarde unique, sur la page **Options de sauvegarde planifiée**, puis cliquez sur **Suivant**.
19. Sur la page **Confirmation**, cliquez sur **Sauvegarde**.
20. Sur la page **Progression de la sauvegarde**, cliquez sur **Fermer**.
21. Fermez Sauvegarde Windows Server.

## Leçon 3

# Implémentation de la récupération de données et de serveurs

### Table des matières :

Démonstration

142

## Démonstration

### Démonstration : Utilisation de l'utilitaire Sauvegarde Windows Server pour restaurer un dossier

#### Procédure de démonstration

1. Sur LON-SVR1, ouvrez l'Explorateur de fichiers, accédez au lecteur C, puis supprimez le dossier **HR Data**.
2. Dans le Gestionnaire de serveur, démarrez **Sauvegarde Windows Server**, puis cliquez sur **Récupérer**.
3. Dans l'Assistant Récupération, sur la page **Mise en route**, sélectionnez **Un autre emplacement**, puis cliquez sur **Suivant**.
4. Sur la page **Spécifier un type d'emplacement**, cliquez sur **Dossier partagé distant**, puis sur **Suivant**.
5. Sur la page **Spécifier un dossier distant**, saisissez `\\LON-DC1\Sauvegarde`, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner une date de sauvegarde**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner le type de récupération**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner les éléments à récupérer**, développez **LON-SVR1**, cliquez sur **Disque local (C:)** et cliquez sur **HR Data**, dans le volet droit, puis cliquez sur **Suivant**.
9. Sur la page **Spécifier les options de récupération**, sous **Autre emplacement**, saisissez `C:\`, puis cliquez sur **Suivant**.
10. Sur la page **Confirmation**, cliquez sur **Récupérer**.
11. Sur la page **Statut de la récupération**, cliquez sur **Fermer**.
12. Dans l'Explorateur de fichiers, accédez au lecteur C et vérifiez que le dossier **HR Data** est restauré.

# Contrôle des acquis et éléments à retenir

## Méthode conseillée

- Analysez vos ressources en infrastructure importantes et vos données essentielles à l'accomplissement de votre mission et à votre entreprise. En fonction de cette analyse, créez une stratégie de sauvegarde qui protégera les ressources en infrastructure et les données commerciales essentielles de l'entreprise.
- Avec l'aide des directeurs commerciaux de l'organisation, identifiez le temps de récupération minimum pour les données essentielles de l'entreprise. En fonction de ces informations, créez une stratégie de restauration optimale.
- Testez régulièrement les procédures de sauvegarde et de restauration. Réalisez l'essai dans un environnement isolé et non en cours de production.

## Questions de contrôle des acquis

**Question :** Vous souhaitez créer une stratégie pour sauvegarder différentes technologies qui sont utilisées dans votre organisation, telles que DHCP, DNS, AD DS et SQL Server. Que devez-vous faire ?

**Réponse :** Chaque technologie présentant des recommandations spécifiques au niveau de la sauvegarde et de la restauration, lisez la documentation sur la stratégie de sauvegarde optimale pour chaque technologie spécifique. Puis, selon ces informations, créez la documentation et une liste de contrôle pour les procédures de sauvegarde et de restauration.

**Question :** À quelle fréquence devez-vous effectuer les sauvegardes des données essentielles ?

**Réponse :** La fréquence à laquelle vous effectuez une sauvegarde des données essentielles dépend des exigences de votre organisation et de la cadence de modification des données. Vous devriez toujours prévoir des stratégies de sauvegarde en fonction des évaluations des risques. Si vos données essentielles changent sensiblement au cours de la journée, alors vous devriez effectuer la sauvegarde au moins une fois par jour, et envisager d'effectuer plusieurs captures instantanées VSS au cours de la journée.

## Problèmes réels et scénarios

Votre organisation a besoin d'informations sur les données à sauvegarder, sur la fréquence des sauvegardes des différents types de données et technologies, sur le lieu de stockage des données sauvegardées (sur site ou sur le cloud), et sur la vitesse à laquelle elle peut restaurer les données sauvegardées. Comment amélioreriez-vous la capacité de votre organisation à restaurer efficacement des données lorsque cela s'avère nécessaire ?

**Réponse :** Votre société devrait développer des stratégies de sauvegarde et de restauration selon plusieurs paramètres, tels que les besoins de l'entreprise en matière de continuité, les procédures d'évaluation du risque, et l'identification des ressources et des données essentielles. Vous devez développer des stratégies qui devraient ensuite être évaluées et testées. Ces stratégies devraient prendre en considération les modifications dynamiques consécutives à l'adoption de nouvelles technologies et aux modifications résultant de la croissance de l'organisation.

## Outils

Outil	Utilisez	Emplacement
Sauvegarde Windows Server	Exécution de sauvegardes à la demande ou planifiées, et restauration des données et des serveurs	Gestionnaire de serveur - Outils
Windows Azure Online Backup	Exécution de sauvegardes à la demande ou planifiées vers le cloud, et restauration de données à partir de la sauvegarde située dans le cloud.	Gestionnaire de serveur - Outils

## Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Des composants du serveur ont rencontré une défaillance importante.	Effectuez une restauration complète sur un nouveau système à l'aide du jeu de sauvegarde que vous avez créé. Utilisez la documentation et la liste de contrôle que vous avez créées dans le cadre de la stratégie et des procédures de sauvegarde et de restauration de votre société.

## Questions et réponses de contrôle des acquis de l'atelier pratique

### Atelier pratique : Implémentation des fonctionnalités de sauvegarde et de restauration de Windows Server

**Question :** Vous vous préoccupez des données essentielles qui se trouvent sur les serveurs de votre entreprise. Vous souhaitez effectuer des sauvegardes quotidiennement, mais pas pendant les heures de bureau. Que devez-vous faire ?

**Réponse :** Vous devriez effectuer une sauvegarde planifiée qui s'exécute chaque jour après les heures de bureau, par exemple à 1 h 00 du matin.

**Question :** Les utilisateurs signalent qu'ils ne peuvent plus accéder aux données qui se trouvent sur le serveur. Vous vous connectez au serveur, et vous vous rendez compte que le dossier partagé dans lequel les utilisateurs accédaient aux données est manquant. Que devez-vous faire ?

**Réponse :** Vous devriez restaurer le dossier à l'aide de l'utilitaire Sauvegarde de Windows Server.

**Question :** Les serveurs stockant les données financières de l'organisation sont sauvegardés à l'aide de Windows Azure Online Backup. Un des serveurs rencontre une défaillance et doit être remplacé, ce qui pourrait prendre une journée de travail. Les utilisateurs doivent accéder aux données financières dès que possible. Que devez-vous faire ?

**Réponse :** Vous devriez utiliser Windows Azure Online Backup pour restaurer les données financières sur un autre serveur exécutant le système d'exploitation Windows Server 2012.

## Envoyez-nous vos commentaires

Vous pouvez rechercher les problèmes connus dans la Base de connaissances Microsoft sur le site [Aide et support Microsoft](#) avant d'envoyer vos commentaires. Pour ce faire, utilisez soit le numéro et la version du cours, soit le titre du cours.

**Remarque** Tous les produits de formation n'ont pas forcément un article qui leur correspond dans la Base de connaissances. Si tel est le cas, demandez à votre instructeur s'il existe un journal des erreurs.

### Commentaires sur le cours

Envoyez tous vos commentaires sur le cours à [support@mscourseware.com](mailto:support@mscourseware.com). Nous vous sommes reconnaissants du temps que vous y aurez consacré et de la peine que vous vous serez donnée. Nous étudions tous les courriers électroniques reçus et transmettons leur contenu à l'équipe concernée. Malheureusement, compte tenu du nombre important de courriers traités, nous ne sommes pas en mesure de répondre à chaque courrier reçu, mais soyez assuré que nous utilisons vos commentaires pour améliorer l'expérience que vous vivrez avec les prochains produits de formation Microsoft.

### Création de rapports d'erreurs

En envoyant vos commentaires, indiquez le nom et le numéro du produit de formation dans l'objet de votre message électronique. Lorsque vous envoyez des commentaires ou signalez des bogues, indiquez les éléments suivants :

1. Numéro de référence du document ou du CD-ROM
2. Numéro de page ou emplacement
3. Description complète de l'erreur ou de la modification suggérée

Veillez fournir tous les détails qui nous permettent de vérifier le problème.

**Important** Toutes les erreurs et suggestions sont évaluées, mais seules celles validées sont ajoutées à l'article de la Base de connaissances du produit.