Microsoft

PRODUIT OFFICIEL DE FORMATION MICROSOFT

22413B

Conception et implémentation d'une infrastructure Server

Contenu d'accompagnement

Numéro de produit : 22413B

Numéro de référence : X18-86872

Date de publication : 3/2013

TERMES DU CONTRAT DE LICENCE MICROSOFT
COURS MICROSOFT AVEC FORMATEUR

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

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

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

1. DÉFINITIONS.

a. « Centre de Formation Agréé » désigne un Membre du Programme Microsoft IT Academy ou un Membre Microsoft Learning Competency, ou toute autre entité que Microsoft peut occasionnellement désigner.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

i. Chaque licence achetée en votre nom ne peut être utilisée que pour consulter une (1) copie du cours Microsoft avec Formateur sous la forme sous laquelle il vous a été fourni. Si le Cours Microsoft avec Formateur est en format numérique, vous êtes autorisé à installer une (1) copie sur un maximum de trois (3) Dispositifs Personnels. Vous n'êtes pas autorisé à installer le Cours Microsoft avec Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas.

ii. Pour chaque licence que vous achetez au nom d'un Utilisateur Final ou Formateur, vous êtes autorisé à :

1. distribuer une (1) version papier du Cours Microsoft avec Formateur à un (1) Utilisateur Final qui est inscrit à la Session de Formation Agréée et uniquement immédiatement avant le début de la Session de Formation Agréée qui est l'objet du Cours Microsoft avec Formateur fourni, **ou**
2. fournir à un (1) Utilisateur Final le code d'accès unique et les instructions permettant d'accéder à une (1) version numérique du Cours Microsoft avec Formateur, **ou**
3. fournir à un (1) Formateur le code d'accès unique et les instructions permettant d'accéder à un (1) Contenu Formateur,

pour autant que vous vous conformiez à ce qui suit :

iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,

iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,

v. vous veillerez à ce que chaque Utilisateur Final ayant reçu la version papier du Cours Microsoft avec Formateur reçoive une copie du présent contrat et reconnaisse que son utilisation du Cours Microsoft avec Formateur sera soumises aux termes du présent accord, et ce avant de lui fournir ledit Cours Microsoft avec Formateur. Chacun devra confirmer son acceptation du présent contrat d'une manière opposable aux termes de la réglementation locale avant d'accéder au Cours Microsoft avec Formateur,

vi. vous veillerez à ce que chaque Formateur donnant une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,

vii. vous n'utiliserez que des Formateurs qualifiés qui ont une connaissance et une expérience approfondies de la technologie Microsoft qui est l'objet du Cours Microsoft avec Formateur donné pour toutes vos Sessions de Formation Agréées.

viii. vous ne donnerez qu'un maximum de 15 heures de formation par semaine pour chaque Session de Formation Agréée qui utilise un cours MOC, et

ix. vous reconnaissez que les Formateurs qui ne sont pas MCT n'auront pas accès à l'ensemble des ressources destinées au formateur du Cours Microsoft avec Formateur.

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

i. Chaque licence achetée en votre nom ne peut être utilisée que pour consulter une (1) copie du cours Microsoft avec Formateur sous la forme sous laquelle il vous a été fourni. Si le Cours Microsoft avec Formateur est en format numérique, vous êtes autorisé à installer une (1) copie sur un maximum de trois (3) Dispositifs Personnels. Vous n'êtes pas autorisé à installer le Cours Microsoft avec Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas.

ii. Pour chaque licence que vous achetez au nom d'un Utilisateur Final ou Formateur, vous êtes autorisé à :

1. distribuer une (1) version papier du Cours Microsoft avec Formateur à un (1) Utilisateur Final participant à la Session de Formation Agréée et uniquement immédiatement avant le début de la Session de Formation Agréée qui est l'objet du Cours Microsoft avec Formateur fourni, **ou**
2. fournir à un (1) Utilisateur Final participant à la Session de Formation Agréée le code d'accès unique et les instructions permettant d'accéder à une (1) version numérique du Cours Microsoft avec Formateur, **ou**
3. fournir à un (1) Formateur le code d'accès unique et les instructions permettant d'accéder à un (1) Contenu Formateur,

pour autant que vous vous conformiez à ce qui suit :

iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,

iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Agréée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Agréée,

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

c. **Si vous êtes un Membre MPN :**

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

    pour autant que vous vous conformiez à ce qui suit :
iii. vous ne donnerez accès au Contenu Concédé sous Licence qu'aux personnes qui ont acheté une licence valide du Contenu Concédé sous Licence,
iv. vous veillerez à ce que chaque Utilisateur Final participant à une Session de Formation Privée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Privée,
v. vous veillerez à ce que chaque Utilisateur Final ayant reçu une version papier du Cours Microsoft avec Formateur reçoive une copie du présent contrat et reconnaisse que son utilisation du Cours Microsoft avec Formateur sera soumise aux termes du présent accord, et ce avant de lui fournir ledit Cours Microsoft avec Formateur. Chacun devra confirmer son acceptation du présent contrat d'une manière opposable aux termes de la réglementation locale avant d'accéder au Cours Microsoft avec Formateur,

vi. vous veillerez à ce que chaque Formateur donnant une Session de Formation Privée dispose de sa propre copie concédée sous licence valide du Cours Microsoft avec Formateur qui est l'objet de la Session de Formation Privée,
vii. vous n'utiliserez que des Formateurs qualifiés qui possèdent la Certification Microsoft applicable qui est l'objet du Cours Microsoft avec Formateur donné pour toutes vos Sessions de Formation Privées,
viii. vous n'utiliserez que des MCT qualifiés qui possèdent la Certification Microsoft applicable qui est l'objet du cours MOC donné pour toutes vos Sessions de Formation Privées utilisant MOC,
ix. vous ne donnerez accès au Cours Microsoft avec Formateur qu'aux Utilisateurs Finaux, et
x. vous ne donnerez accès au Contenu du Formateur qu'aux Formateurs.

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

e. **Si vous êtes un Formateur :**
i. Pour chaque licence que vous achetez, vous êtes autorisé à installer et utiliser une (1) copie du Contenu du Formateur sous la forme dans laquelle il vous a été fourni sur un (1) Dispositif Personnel exclusivement pour préparer et donner une Session de Formation Agréée ou une Session de Formation Privée, et à installer une (1) copie supplémentaire sur un autre Dispositif Personnel comme copie de sauvegarde, utilisable uniquement pour réinstaller le Contenu du Formateur. Vous n'êtes pas autorisé à installer ou utiliser une copie du Contenu du Formateur sur un dispositif qui ne vous appartient pas ou que vous ne contrôlez pas. Vous êtes également autorisé à imprimer une (1) copie du Contenu du Formateur uniquement pour préparer et assurer une Session de Formation Agréée ou une Session de Formation Privée.
ii. Vous pouvez personnaliser les parties écrites du Contenu du Formateur qui sont logiquement associées à la présentation d'une session de formation conformément à la version la plus récente du contrat MCT. Si vous choisissez d'exercer les droits qui précèdent, vous acceptez de vous conformer à ce qui suit : (i) les personnalisations ne peuvent être utilisées que pour donner des Sessions de Formation Agréées et des Sessions de Formation Privées, et (ii) toutes les personnalisations seront conformes au présent contrat. À des fins de clarté, toute utilisation de « *personnaliser* » ne fait référence qu'à la modification de l'ordre des diapositives et du contenu, et/ou à la non-utilisation de l'ensemble du contenu ou des diapositives, et ne signifie pas le changement ou la modification d'aucune diapositive ni d'aucun contenu.

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

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

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

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

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

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

b. **Commentaires**. Si vous acceptez de faire part à Microsoft de vos commentaires concernant le Contenu Concédé sous Licence, directement ou par l'intermédiaire de son représentant tiers, vous concédez à Microsoft, gratuitement, le droit d'utiliser, de partager et de commercialiser vos commentaires de quelque manière et à quelque fin que ce soit. Vous concédez également à des tiers, à titre gratuit, tout droit de propriété sur leurs produits, technologies et services, nécessaires pour utiliser ou interfacer des parties spécifiques d'un logiciel, produit ou service Microsoft qui inclut les commentaires. Vous ne donnerez pas d'informations faisant l'objet d'une licence qui impose à Microsoft de concéder sous licence son logiciel, ses technologies ou produits à des tiers parce que nous y incluons vos commentaires. Ces droits survivent au présent contrat.

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

4. **CHAMP D'APPLICATION DE LA LICENCE.** Le Contenu Concédé sous Licence n'est pas vendu. Le présent contrat ne fait que vous conférer certains droits d'utilisation du Contenu Concédé sous Licence. Microsoft se réserve tous les autres droits. Sauf si la réglementation applicable vous confère d'autres droits, nonobstant la présente limitation, vous n'êtes autorisé à utiliser le Contenu Concédé sous Licence qu'en conformité avec les termes du présent contrat. Ce faisant, vous devez vous conformer aux restrictions techniques contenues dans le Contenu Concédé sous Licence qui ne vous permettent de l'utiliser que d'une certaine façon. Sauf stipulation expresse dans le présent contrat, vous n'êtes pas autorisé à :
   - accéder au Contenu Concédé sous Licence ou à y autoriser l'accès à quiconque qui n'a pas acheté une licence valide du Contenu Concédé sous Licence,
   - modifier, supprimer ou masquer les mentions de droits d'auteur ou autres notifications de protection (y compris les filigranes), marques ou identifications contenue dans le Contenu Concédé sous Licence,
   - modifier ou créer une œuvre dérivée d'un Contenu Concédé sous Licence,
   - présenter en public ou mettre à disposition de tiers le Contenu Concédé sous Licence à des fins d'accès ou d'utilisation,
   - copier, imprimer, installer, vendre, publier, transmettre, prêter, adapter, réutiliser, lier ou publier, mettre à disposition ou distribuer le Contenu Concédé sous Licence à un tiers,
   - contourner les restrictions techniques contenues dans Contenu Concédé sous Licence, ou
   - reconstituer la logique, décompiler, supprimer ou contrecarrer des protections, ou désassembler le Contenu Concédé sous Licence, sauf dans la mesure où ces opérations seraient expressément permises par les termes du contrat de licence ou la réglementation applicable nonobstant la présente limitation.

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

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

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

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

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

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

11. **RÉGLEMENTATION APPLICABLE.**

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

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

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

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

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

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

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

Dernière mise à jour : septembre 2012.

Module 1

Planification de la mise à niveau et de la migration d'un serveur

Table des matières :

Leçon 1

Éléments à prendre en compte pour la mise à niveau et la migration

Table des matières :

Documentation supplémentaire

Configuration requise pour la préinstallation

Documentation supplémentaire: Pour plus d'informations sur le programme Windows Server Virtualization Validation Program, consultez l'article Welcome to the Windows Server Virtualization Validation Program à l'adresse http://go.microsoft.com/fwlink/?linkid=279917 (*Certains de ces sites adressées dans ce cours sont en anglais.*).

Mise à niveau sur place et migration de serveur

Documentation supplémentaire: Pour plus d'informations sur la migration, consultez l'article Install, Use, and Remove Windows Server Migration Tools à l'adresse http://go.microsoft.com/fwlink/?linkid=280376.

Outils disponibles pour aider à planifier la mise à niveau et la migration

Liens de référence : Pour plus d'informations sur la boîte à outils Microsoft Assessment and Planning (MAP) pour Windows Server 2012, consultez http://go.microsoft.com/fwlink/?linkid=279918.

Leçon 2

Création d'un plan de mise à niveau et de migration d'un serveur

Table des matières :

Questions et réponses

Discussion : Planification de l'activation en volume

Question : L'infrastructure informatique de votre organisation se compose d'ordinateurs personnels et de serveurs exécutant différentes éditions des systèmes d'exploitation clients Windows et des systèmes d'exploitation Windows Server. Le mois prochain, votre organisation envisage de déployer 500 ordinateurs clients Windows 8, et 20 serveurs Windows Server 2012. Le département finance dispose d'une application héritée, vous devez donc déployer 10 ordinateurs clients exécutant Windows 7 et deux serveurs exécutant Windows Server 2008 R2. Quel type d'activation en volume devez-vous implémenter ?

Réponse : Vous devez implémenter le programme de licence en volume basé sur le service Gestionnaire de clés (KMS). En effet, votre organisation déploie différentes éditions des systèmes d'exploitation clients Windows® et des systèmes d'exploitation Windows Server.

Question : L'infrastructure informatique de votre organisation a été mise à niveau à partir de différentes éditions des systèmes d'exploitation clients Windows et des systèmes d'exploitation Windows Server vers Windows 8 et Windows Server 2012. Quel type d'activation en volume devez-vous implémenter ?

Réponse : Vous devez implémenter le programme de licence en volume basé sur l'activation Active Directory®. En effet, votre organisation déploie des systèmes d'exploitation Windows 8 et Windows Server 2012, et l'activation basée sur Active Directory est prise en charge seulement sur des ordinateurs exécutant Windows Server 2012 et Windows 8.

Documentation supplémentaire

Détermination des rôles pouvant être migrés

Liens de référence : Pour plus d'informations sur la détermination des rôles et des fonctionnalités à migrer, consultez l'article Migrate Roles and Features to Windows Server 2012 à l'adresse http://go.microsoft.com/fwlink/?linkid=280377.

Leçon 3

Planification de la virtualisation

Table des matières :

Questions et réponses

Discussion : Choix entre les déploiements physiques et virtuels

Question : Dans quelle situation allez-vous choisir de déployer vos applications métier ou vos services d'infrastructure dans un environnement virtuel ?

Réponse : Les réponses varient.

Question : Quels rôles serveur, fonctionnalités ou services d'application avez-vous déployés dans votre environnement physique ?

Réponse : Les réponses varient.

Question : Si vous avez un environnement virtuel pour votre organisation, qu'avez-vous actuellement déployé dans votre environnement virtuel, et pourquoi ?

Réponse : Les réponses varient.

Contrôle des acquis et éléments à retenir

Méthode conseillée

Lorsque vous planifiez le déploiement de Windows Server 2012 dans un environnement physique ou virtuel, prenez toujours en compte la stratégie de haute disponibilité et de sauvegarde/restauration pour les services ou les applications qui s'exécutent sur ce système d'exploitation. Si vous exécutez des solutions dans le cloud privé, veillez toujours à utiliser des outils de gestion et d'analyse (tels que System Center 2012), pour permettre à l'environnement informatique de s'exécuter efficacement. Assurez-vous en outre d'avoir une solution de stockage correctement conçue avec une taille et des performances appropriées pour les ordinateurs virtuels.

Question(s) de contrôle des acquis

Question : Quels sont les principaux éléments à prendre en compte pour guider la stratégie de votre organisation à propos des divers scénarios pour le déploiement du système d'exploitation Windows Server 2012 ?

Réponse : Plusieurs éléments affectent la stratégie d'une organisation, tels que les exigences stratégiques, le cloud computing, la consolidation de l'infrastructure actuelle de serveur, et la capacité des solutions actuelles d'application et d'infrastructure à être mises à jour ou migrées vers Windows Server 2012.

Problèmes réels et scénarios

Votre organisation utilise peu les technologies de virtualisation. Vous avez déployé le système d'exploitation de l'édition Standard de Windows Server 2012 prenant en charge deux instances d'un ordinateur virtuel. La direction est préoccupée par de futurs projets qui impliquent de déployer de nouveaux produits dans un environnement virtuel. Elle souhaiterait avoir une solution évolutive et extensible sans avoir à acheter de licences supplémentaires lorsqu'elle déploie de nouveaux produits.

Elle a par conséquent demandé au service informatique de créer une stratégie de déploiement de serveur qui comprend l'exécution d'une solution matérielle sur l'édition Datacenter de Windows Server 2012. Cela permettra à l'organisation de déployer des applications dans un environnement virtuel et d'avoir de la flexibilité sans avoir besoin de licences supplémentaires.

Outils

Outil	Utilisé pour	Emplacement
Microsoft Assessment and Planning Toolkit (MAP)	Analyser l'inventaire de l'infrastructure du serveur d'une organisation, exécuter une évaluation, puis créer des rapports que vous pouvez utiliser pour des plans de mise à niveau et de migration.	Site Web de Microsoft http://go.microsoft.com/fwlink/?linkid=279918

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

Atelier pratique A : Planification de la mise à niveau et de la migration d'un serveur

Questions et réponses

Question : Pourquoi choisir d'utiliser l'outil MAP lorsque vous planifiez la mise à niveau et la stratégie de migration ?

Réponse : L'outil MAP analyse l'inventaire de l'infrastructure du serveur d'une organisation, exécute une évaluation, puis crée des rapports que vous pouvez utiliser pour des plans de mise à niveau et de migration. L'analyse détaillée effectuée par cet outil vous aide dans vos décisions concernant les stratégies de mise à niveau et de migration.

Question : Pourquoi choisir l'édition Datacenter de Windows Server 2012 pour la virtualisation et la consolidation des réseaux internes et de périmètre d'A. Datum ?

Réponse : L'édition Datacenter de Windows Server 2012 prend en charge un nombre d'instances illimité d'ordinateurs virtuels. Même si le nombre d'ordinateurs virtuels par serveur physique est passé à quatre, A. Datum ne va pas exiger plus de licences pour un développement futur, alors que ça serait le cas s'il utilisait l'édition Standard de Windows Server 2012.

Module 2

Planification et implémentation d'une infrastructure de déploiement de serveur

Table des matières :

Leçon 1

Sélection d'une stratégie de création d'images serveur appropriée

Table des matières :

Questions et réponses

Exécution de déploiements avec un degré important d'intervention (High-touch) à l'aide de supports commercialisés

Question : Quelles sont les limites de la méthode de déploiement avec un degré important d'intervention (High-touch) à l'aide de supports commercialisés ?

Réponse : Les réponses varient, mais peuvent inclure les suivantes :

- Il est nécessaire de faire appel à des professionnels de l'informatique pour initialiser les installations interactives.
- L'utilisation d'un périphérique USB à mémoire flash n'est pas efficace pour les fichiers de réponses individuels.
- Plusieurs copies du support commercialisé sont requises.
- La méthode manque de souplesse et convient aux petits déploiements uniques.

Documentation supplémentaire

Exécution de déploiements à volume élevé de type Lite-touch

 **Documentation supplémentaire:** Pour plus d'informations sur le scénario d'utilisation de déploiement avancé à l'aide de la mise à jour 1 de MDT 2012, consultez la page : http://go.microsoft.com/fwlink/?LinkID=277143.

Leçon 2

Sélection d'une stratégie d'automatisation du déploiement

Table des matières :

Questions et réponses

Discussion : Quelle est votre stratégie de déploiement actuelle ?

Question : Actuellement, de quelle manière effectuez-vous le déploiement des systèmes d'exploitation dans votre organisation ?

Réponse : Les réponses sont variables, mais la plupart des organisations implémentent plusieurs types de stratégies de création d'images et beaucoup utilisent des services d'infrastructure pour distribuer des images.

Question : Quels sont les avantages et les inconvénients de la stratégie de déploiement que vous avez choisie ?

Réponse : Les réponses peuvent varier, mais peuvent inclure les éléments suivants :

- des filiales sans personnel informatique sur site ;
- plusieurs serveurs à déployer dans l'ensemble de l'organisation ;
- des configurations similaires de serveurs dans l'ensemble de l'organisation.

Question : Votre stratégie de déploiement est-elle basée sur des fichiers ou des images binaires ?

Réponse : Il est possible que certains participants utilisent encore des images binaires. Vous devez donc présenter et comparer les avantages des images basées sur des fichiers en termes de flexibilité et de maintenance hors ligne.

Leçon 3

Implémentation d'une stratégie de déploiement automatisé

Table des matières :

Questions et réponses

Sélection d'un scénario de déploiement

Question : En général, quand exécutez-vous une nouvelle installation de Windows Server 2012 ?

Réponse : Dans certaines circonstances, une nouvelle installation est la seule solution. Ces types sont les suivants :

- Aucun système d'exploitation n'est installé sur l'ordinateur.
- Le système d'exploitation installé ne prend pas en charge la mise à niveau vers Windows Server 2012.

Une nouvelle installation serait préférée à une mise à niveau si la version précédente du système d'exploitation Windows rencontrait des problèmes de corruption de fichiers ou d'autres problèmes de performances. Si aucune volonté de conserver les applications ou les paramètres de la version précédente du système d'exploitation Windows n'est affirmée, préférez généralement une nouvelle installation plutôt qu'une mise à niveau ou une migration.

Question : Quels problèmes sont susceptibles de se poser lors de l'installation de Windows Server 2012 ?

Réponse : Les réponses peuvent varier.

Documentation supplémentaire

Windows ADK

Documentation supplémentaire: Pour obtenir une liste complète des chemins de recherche valides, accédez à la section Recherche implicite d'un fichier de réponses dans la page Méthodes d'exécution du programme d'installation Windows à l'adresse http://go.microsoft.com/fwlink/?LinkID=277144.

Démonstration

Démonstration : Préparation de l'image Windows Server 2012

Procédure de démonstration

1. Basculez vers LON-SVR1.
2. Dans la barre des tâches, cliquez sur **Explorateur de fichiers**.
3. Dans l'Explorateur de fichiers, dans le volet de navigation, développez **Ordinateur**, cliquez sur le lecteur **Allfiles (E:)**, cliquez avec le bouton droit sur le volet d'informations, cliquez sur **Nouveau**, puis sur **Dossier**.
4. Dans la zone **Nouveau dossier**, tapez **Images**, et appuyez sur Entrée.
5. Dans l'Explorateur de fichiers, dans le volet de navigation, double-cliquez sur **Images**, cliquez avec le bouton droit sur le volet d'informations, cliquez sur **Nouveau**, puis sur **Dossier**.

6. Dans la zone **Nouveau dossier**, tapez **Custom Images**, et appuyez sur Entrée.
7. Sur l'hôte, dans la fenêtre 22413B-LON-SVR1, dans la barre d'outils, cliquez sur **Support**, pointez sur **Lecteur de DVD**, puis cliquez sur **Insérer un disque**.
8. Dans la boîte de dialogue **Ouvrir**, dans la zone **Nom de fichier**, tapez **C:\Program Files\Microsoft Learning\22413\Drives\windows2012_RTM.ISO**, puis cliquez sur **Ouvrir**.
9. Copiez **D:\sources\install.wim** dans le dossier **E:\Images\Custom Images**.
10. Dans l'Explorateur de fichiers, cliquez avec le bouton droit sur **E:\Images**, puis cliquez sur **Propriétés**.
11. Cliquez sur l'onglet **Partage**, puis cliquez sur **Partage avancé**.
12. Dans la boîte de dialogue **Partage avancé**, activez la case à cocher **Partager ce dossier**.
13. Cliquez sur **Autorisations**, puis sur **Ajouter**.
14. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemple) :** tapez **Administrateur**, puis cliquez sur **OK**.
15. Dans la boîte de dialogue **Autorisations pour Images**, cliquez sur **Administrateur (ADATUM\Administrateur)**, sous **Autoriser**, activez la case à cocher **Contrôle total**, puis cliquez sur **OK**.
16. Dans la boîte de dialogue **Partage avancé**, cliquez sur **OK**, puis sur **Fermer**.
17. Dans l'Explorateur de fichiers, cliquez avec le bouton droit sur **Ordinateur**, puis cliquez sur **Connecter un lecteur réseau**.
18. Dans la boîte de dialogue **Connecter un lecteur réseau**, dans la zone **Lecteur**, vérifiez que le lecteur **Z:** s'affiche, dans la zone **Dossier**, tapez **\\lon-svr1\Images**, puis cliquez sur **Terminer**.
19. Sur LON-SVR1, déplacez le curseur de la souris vers le coin inférieur droit de la barre des tâches, cliquez sur **Rechercher**, puis tapez **cmd.exe**.
20. Dans la liste **Applications**, cliquez avec le bouton droit sur **cmd.exe**, puis cliquez sur **Exécuter comme administrateur**.
21. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
Mkdir c:\mounted
```

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

```
Dism /get-imageinfo /imagefile:"z:\Custom Images\install.wim"
```

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

```
Dism /mount-wim /wimfile:"z:\Custom Images\install.wim" /index:4 /mountdir:c:\mounted
```

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

```
Dism /image:c:\mounted /get-features
```

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

```
Dism /image:c:\mounted /get-featureinfo /featurename:IIS-WebServerRole
```

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

```
Dism /image:c:\mounted /enable-feature /featurename:IIS-WebServerRole –all
```

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

```
Dism /unmount-wim /mountdir:c:\mounted /commit
```

Contrôle des acquis et éléments à retenir

Méthode conseillée

Meilleures pratiques	Description
Toujours installer les dernières mises à jour de sécurité sur l'ordinateur de référence.	Démarrer avec un ordinateur de référence à jour diminue le niveau de vulnérabilité des nouveaux ordinateurs mis en ligne.
Implémenter les contrôles d'accès pour protéger les supports de démarrage.	Lorsque vous créez un support de démarrage, veillez à lui allouer un mot de passe et à en contrôler l'accès physique.
Utiliser des points de service PXE uniquement sur des segments réseau sécurisés.	Un point de service PXE nécessite que les ports UDP soient ouverts sur des commutateurs et des serveurs
Si vous devez déployer des systèmes d'exploitation à un ordinateur inconnu, implémentez des contrôles d'accès pour éviter que des ordinateurs non-autorisés ne se connectent au réseau.	La mise en service d'ordinateurs inconnus peut être un moyen pratique d'ajouter plusieurs ordinateurs à la demande, mais cela peut permettre également à un utilisateur malveillant de devenir un client de confiance sur votre réseau.
Réduire la taille de l'image de démarrage pour accélérer la vitesse de téléchargement TFTP	Vérifiez que cette image a été préparée avec **PEIMG.exe /prep**. La meilleure pratique consiste à utiliser la commande **ImageX /export** pour exporter l'image de démarrage sur un nouveau fichier .wim avant d'ajouter l'image au serveur Services de déploiement Windows.

Question(s) de contrôle des acquis

Question : Dans votre organisation, aucune version de serveur n'est identique. Vous avez choisi d'utiliser des images personnalisées pour optimiser le déploiement. Pensez-vous utiliser des images épaisses ou fines ?

Réponse : Les images fines seraient les plus appropriées. Utilisez la stratégie de groupe et des scripts pour automatiser le déploiement d'applications une fois les serveurs déployés. Pour ce scénario, les images épaisses contiennent trop de personnalisation.

Question : De quels outils avez-vous besoin pour automatiser des déploiements avec un degré important d'intervention (High-touch) à l'aide de supports commercialisés ?

Réponse : Vous pouvez utiliser des supports commercialisés, Windows ADK et des supports amovibles.

Question : Votre organisation souhaite implémenter une stratégie de déploiement de type Lite-touch. Outre l'utilisation de MDT 2012, quels outils vous seront utiles pour effectuer des déploiements de type Lite-touch ?

Réponse : Vous pouvez utiliser les outils suivants :

- la boîte à outils MAP ;
- la boîte à outils ACT ;
- le support de licence en volume ;
- MDT
- Windows ADK
- des supports d'installation ou services de déploiement Windows pour démarrer les ordinateurs client pendant le déploiement.

Problèmes réels et scénarios

Bien que les services de déploiement Windows offrent la possibilité de déployer des systèmes d'exploitation Windows, les moyennes et grandes entreprises doivent envisager d'implémenter MDT afin de personnaliser des scénarios de migration plus complexes. Pour une implémentation de type Zero-touch, Configuration Manager 2012 fournit un environnement de déploiement fiable, évolutif, et contrôlé. Configuration Manager permet également des déploiements de système d'exploitation Windows et fournit une gestion continue d'ordinateurs déjà installés.

Outils

Outil	Utilisé pour	Emplacement
Application Compatibility Toolkit	Vérifier la compatibilité des applications avec Windows 8	http://go.microsoft.com/fwlink/?LinkID=277145
Windows ADK	Évaluer et déployer les systèmes d'exploitation Windows	http://go.microsoft.com/fwlink/?LinkID=277146
Windows SIM	Créer et modifier les fichiers de réponses	Windows ADK
ImageX	Créer, modifier et appliquer les fichiers .wim à base d'image	Windows ADK
USMT	Effectuer la migration des paramètres utilisateur	Windows ADK
DISM	Effectuer la maintenance des fichiers .wim à base d'image	Windows ADK

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

Atelier pratique A : Planification et implémentation d'une infrastructure de déploiement de serveur

Questions et réponses

Question : Pour quelle approche avez-vous opté pour le plan de conception ?

Réponse : Les réponses varient.

Question : Votre plan de conception est-il différent de la solution suggérée ?

Réponse : Les réponses varient.

Question : En quoi la conception de l'atelier pratique diffère-t-elle des méthodes de déploiement Windows Server 2012 mises en œuvre dans votre organisation ?

Réponse : Les réponses varient.

Question : Si vous n'aviez pas à tenir compte des considérations budgétaires, en quoi votre conception serait-elle différente ?

Réponse : Si les organisations n'avaient pas à tenir compte des considérations budgétaires, la plupart d'entre elles envisageraient un déploiement de type Zero-touch avec System Center 2012 Configuration Manager SP1, dont l'objectif central est un déploiement de bout en bout des systèmes d'exploitation Windows Server 2012. Bien que l'implémentation de Configuration Manager SP1 représente un certain investissement initial, vous en constaterez le retour sur investissement rapidement. L'utilisation de Configuration Manager SP1 est justifiée, car elle réduira probablement les coûts de déploiement de Windows Server 2012 lors de l'acquisition des deux nouvelles entreprises par A. Datum. En outre, lors du déploiement des serveurs des sociétés nouvellement acquises, le déploiement d'image déjà testé avec Configuration Manager SP1 pourra être utilisé. Les modifications des séquences de tâches de ce déploiement seront donc mineures voire inexistantes.

Module 3

Conception et gestion d'une solution de gestion d'adresses et de configuration IP

Table des matières :

Leçon 1

Conception et implémentation de DHCP

Table des matières :

Questions et réponses

Discussion : Sélection d'un modèle d'adressage IP

Question : À votre avis, combien de sous-réseaux cette région requiert-elle ?

Réponse : Cette région compte 300 ordinateurs. Les spécifications stipulent que vous devez déployer environ 50 ordinateurs hôtes dans chaque sous-réseau. Vous devez également prévoir une croissance d'environ 25 %. Six sous-réseaux sont requis dans la région pour héberger les ordinateurs, mais vous devez planifier un sous-réseau supplémentaire pour chaque emplacement afin d'anticiper l'hébergement d'un nombre croissant d'ordinateurs. Cela signifie que vous devez disposer d'un total de neuf sous-réseaux.

Question : Combien d'hôtes déploierez-vous dans chaque sous-réseau ?

Réponse : Les spécifications stipulent que vous devez déployer un maximum de 50 ordinateurs hôtes pour chaque sous-réseau.

Question : Quel masque de sous-réseau utiliserez-vous pour chaque filiale ?

Réponse : L'adresse réseau actuelle de la région est 172.16.16.0/20. Cela laisse 12 bits à allouer aux sous-réseaux et aux hôtes. Pour exprimer neuf sous-réseaux, vous avez besoin de quatre bits, car trois bits permettent de fournir uniquement huit sous-réseaux. Quatre bits permettent de fournir 16 sous-réseaux, ce qui est largement suffisant. Il s'agit d'un masque décimal de 255.255.255.0.

Question : Quelles sont les adresses de sous-réseau pour chaque filiale ?

Réponse : Filiale 1 :

172.16.16.0/24

172.16.17.0/24

172.16.18.0/24

Filiale 2 :

172.16.19.0/24

172.16.20.0/24

172.16.21.0/24

Filiale 3 :

172.16.22.0/24

172.16.23.0/24

172.16.24.0/24

Question : Quelle est la plage d'adresses d'hôte dans chaque filiale ?

Réponse : Filiale 1 :

172.16.16.1–172.16.16.254

172.16.17.1–172.16.17.254

172.16.18.1–172.16.18.254

Filiale 2 :

172.16.19.1–172.16.19.254

172.16.20.1–172.16.20.254

172.16.21.1–172.16.21.254

Filiale 3 :

172.16.22.1–172.16.22.254

172.16.23.1–172.16.23.254

172.16.24.1–172.16.24.254

Question : Ce scénario requiert-il des adresses IP publiques ?

Réponse : Non, ce scénario ne requiert pas d'adresses IP publiques. Toutes les communications s'effectuent au sein de l'intranet de l'entreprise.

Question : Quelles autres adresses IP privées pouvez-vous utiliser ?

Réponse : Les plages d'adresses privées sont indiquées dans le tableau suivant.

Classe	Masque	Plage
A	10.0.0.0/8	10.0.0.0–10.255.255.255
B	172.16.0.0/12	172.16.0.0–172.31.255.255
C	192.168.0.0/16	192.168.0.0–192.168.255.255

Question : Quelles autres recommandations pouvez-vous formuler concernant l'allocation des adresses IP ?

Réponse : Allouez des adresses IP manuelles avec parcimonie. Lorsque vous allouez des adresses IP manuelles, allouez la même plage dans chaque sous-réseau. Attribuez toujours la même adresse de sous-réseau au même périphérique. Par exemple, attribuez au routeur l'adresse .1, puis au contrôleur de domaine l'adresse .2. Cette stratégie permet de simplifier le processus d'installation et peut aider à la résolution des problèmes.

Démonstration

Démonstration : Implémentation du basculement DHCP

Procédure de démonstration

1. Connectez-vous à LON-SVR1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le volet de résultats du Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Cliquez sur **Suivant** à trois reprises.
4. Dans la page **Sélectionner des rôles de serveurs**, sélectionnez le rôle **Serveur DHCP**, puis cliquez sur **Ajouter des fonctionnalités**.
5. Cliquez sur **Suivant** à trois reprises, puis cliquez sur **Installer**.
6. Lorsque le rôle est installé, cliquez sur **Fermer**.
7. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP** dans la liste déroulante.
8. Développez et cliquez avec le bouton droit sur **lon-svr1.adatum.com**, puis cliquez sur **Autoriser**.
9. Basculez vers LON-DC1.
10. Connectez-vous à LON-DC1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
11. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP** dans la liste déroulante.
12. Dans la console DHCP, développez **lon-dc1.adatum.com**, sélectionnez et cliquez avec le bouton droit sur **IPv4**, puis cliquez sur **Configurer un basculement**.
13. Dans l'Assistant de configuration du basculement, cliquez sur **Suivant**.
14. Dans la page **Spécifier le serveur partenaire à utiliser pour le basculement**, dans le champ **Serveur partenaire**, tapez **172.16.0.21**, puis cliquez sur **Suivant**.
15. Dans la page **Créer une relation de basculement**, dans le champ **Nom de la relation**, tapez **Basculement Adatum**.
16. Dans le champ **Délai de transition maximal du client (MCLT)**, définissez les heures sur **0**, et les minutes sur **10**.
17. Vérifiez que le champ **Mode** est défini sur **Équilibrage de charge**.
18. Vérifiez que les deux valeurs du champ **Pourcentage d'équilibrage de charge** sont définies sur **50 %**.
19. Activez la case à cocher **Intervalle de basculement d'état**. Laissez la valeur par défaut de **60 minutes**.
20. Activez la case à cocher **Activer l'authentification du message**, puis dans le champ **Secret partagé**, tapez **Pa$$w0rd**, puis cliquez sur **Suivant**.

21. Cliquez sur **Terminer**, puis sur **Fermer**.
22. Basculez vers LON-SVR1. Notez que le nœud IPv4 est actif. Si tel n'est pas le cas, cliquez sur **lon-svr1.adatum.com**, puis dans la barre d'outils cliquez sur **Actualiser**.
23. Développez le nœud **IPv4**, puis développez **Étendue [172.16.0.0] Adatum**.
24. Cliquez sur **Pool d'adresses** et notez que le pool d'adresses est configuré.
25. Cliquez sur **Options d'étendue** et notez que les options d'étendue sont configurées.
26. Fermez la console DHCP sur LON-DC1 et LON-SVR1.

Leçon 3

Planification et implémentation d'une stratégie d'approvisionnement IPAM

Table des matières :

Démonstration

Démonstration : Implémentation d'IPAM

Procédure de démonstration

Installer IPAM

1. Connectez-vous à LON-SVR2 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le volet de résultats du 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. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
7. Dans la page **Sélectionner des fonctionnalités**, activez la case à cocher **Serveur de gestion des adresses IP (IPAM)**.
8. Dans la boîte de dialogue contextuelle **Ajouter les fonctionnalités requises pour Serveur de gestion des adresses IP (IPAM)**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
9. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Quand l'Assistant Ajout de rôles et de fonctionnalités a terminé, cliquez sur Fermer.

Configurer IPAM

1. Dans le volet de navigation du Gestionnaire de serveur, cliquez sur **IPAM**.
2. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Se connecter au serveur IPAM**. Sélectionnez **LON-SVR2.Adatum.com**, puis cliquez sur **OK**.
3. Cliquez sur **Configurer le serveur IPAM**.
4. Dans l'Assistant Approvisionner IPAM, cliquez sur **Suivant**.
5. Dans 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**, tapez **IPAM**, puis cliquez sur **Suivant**.
6. Dans la page **Confirmer les paramètres**, cliquez sur **Appliquer**. La configuration prend quelques instants.
7. Une fois l'approvisionnement terminé, 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 serveurs**, cliquez sur **Ajouter**, puis 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 la valeur du champ État de l'accès IPAM est Bloqué pour les deux serveurs. 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. À l'invite Windows PowerShell, tapez la commande suivante, puis 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, tapez **O**, puis appuyez sur Entrée. Cette commande demande quelques minutes pour s'exécuter.
15. Fermez Windows PowerShell.
16. Basculez vers le Gestionnaire de serveur.
17. Dans le volet d'informations sur IPv4, cliquez avec le bouton droit sur **LON-DC1**, puis cliquez sur **Modifier le serveur**.
18. Dans la boîte de dialogue **Ajouter ou modifier un serveur**, définissez le champ **État de gérabilité** sur **Géré**, puis cliquez sur **OK**.
19. Dans le volet d'informations sur IPv4, cliquez avec le bouton droit sur **lon-svr1**, puis cliquez sur **Modifier le serveur**.
20. Dans la boîte de dialogue **Ajouter ou modifier un serveur**, définissez le champ **État de gérabilité** sur **Géré**, puis cliquez sur **OK**.
21. Basculez vers **LON-DC1**.
22. Dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
23. À l'invite de Windows PowerShell, tapez **Gpupdate /force**, puis appuyez sur Entrée.
24. Fermez la fenêtre Windows PowerShell.
25. Basculez vers **LON-SVR1**.
26. Dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
27. À l'invite de commandes, tapez **Gpupdate /force**, puis appuyez sur Entrée.
28. Fermez la fenêtre Windows PowerShell.
29. Rebasculez vers LON-SVR2.
30. Dans le Gestionnaire de serveur, cliquez avec le bouton droit sur **LON-DC1**, puis cliquez sur **Actualiser l'état de l'accès serveur**. Répétez cette étape pour **LON-SVR1**.
31. Une fois la découverte terminée, actualisez IPv4 en cliquant sur l'icône **Actualiser**. La modification de l'état peut prendre jusqu'à 5 minutes. Lorsque l'état de la récupération de données indique Terminé(e), vous pouvez continuer.
32. Dans le volet Vue d'ensemble d'IPAM, cliquez sur **Récupérer les données des serveurs gérés**. L'exécution de cette action prend quelques minutes.

Contrôle des acquis et éléments à retenir

Question(s) de contrôle des acquis

Question : Votre entreprise dispose de deux sous-réseaux et vous souhaitez utiliser DHCP pour allouer des adresses aux ordinateurs clients sur les deux sous-réseaux. Vous ne souhaitez pas déployer deux serveurs DHCP. De quels facteurs devez-vous tenir compte ?

Réponse : Le routeur qui interconnecte les deux sous-réseaux doit prendre en charge le relais DHCP ou vous devez installer un agent de relais sur le sous-réseau qui n'héberge pas le serveur DHCP. En outre, vous devez réfléchir à l'incidence sur la disponibilité du service en cas de défaillance de votre unique serveur DHCP.

Question : Votre entreprise s'est développée et votre étendue IPv4 est presque à court d'adresses. Que pouvez-vous faire ?

Réponse : Vous pouvez implémenter une étendue globale en combinant l'étendue existante et une nouvelle étendue.

Question : De quelles informations avez-vous besoin pour configurer une réservation DHCP ?

Réponse : Vous avez besoin de l'adresse MAC du client qui louera la réservation.

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

Atelier pratique A : Conception et gestion d'une solution de gestion d'adresses IP et de configuration IP

Questions et réponses

Question : Pour quelle approche avez-vous opté lors des exercices de planification et de conception IP ?

Réponse : Les réponses varient.

Question : Pour quelle approche avez-vous opté lors des exercices de planification d'un déploiement IPAM ?

Réponse : Les réponses varient.

Question : En quoi la conception du modèle d'adressage IP pour Contoso est-il comparable au modèle d'adressage IP de votre organisation ?

Réponse : Les réponses varient.

Module 4

Conception et implémentation de la résolution de noms

Table des matières :

Leçon 1

Conception d'une stratégie d'implémentation de serveurs DNS

Table des matières :

Démonstration

Démonstration : Installation du rôle de serveur DNS

Procédure de démonstration

1. Basculez vers LON-SVR1.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans le volet de résultats du Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
4. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Sélectionner un serveur du pool de serveurs**, puis cliquez sur **Suivant**.
7. Dans la page **Sélectionner des rôles de serveurs**, dans la liste **Rôles**, activez la case à cocher **Serveur DNS**, cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant**.
8. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Dans la page **Serveur DNS**, cliquez sur **Suivant**.
10. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. Lorsque le rôle a été ajouté correctement, cliquez sur **Fermer**.

Leçon 3

Conception et implémentation de zones DNS

Table des matières :

Questions et réponses

Discussion : Conception d'une stratégie de zone DNS

Question : Comment modifieriez-vous la conception du système DNS pour ce scénario ?

Réponse : Pensez à déployer des serveurs DNS supplémentaires dans les succursales. Toutefois, cela affecterait la configuration de transfert de zone DNS.

Question : Où placeriez-vous les serveurs de noms supplémentaires, le cas échéant ?

Réponse : Pour atténuer les effets d'un échec dans une liaison WAN, chaque site doit avoir d'autres moyens d'effectuer une résolution DNS que d'utiliser les serveurs DNS du siège social. Pensez à déployer au moins un serveur DNS sur chaque site et davantage pour les grands sites.

Question : Quels rôles serveurs DNS proposeriez-vous de déployer ?

Réponse : Les petites succursales peuvent gérer les serveurs cache uniquement, ce qui permet d'éviter les transferts de zone. Les grandes succursales doivent avoir des zones secondaires northwindtraders.priv. Toutefois, si les zones intégrées à Active Directory sont prises en compte, tous les serveurs DNS peuvent être promus contrôleurs de domaine. Cela augmente la résilience de réseau et garantit que les transferts de zone sont effectués automatiquement et en toute sécurité dans le cadre de la réplication AD DS.

Question : À supposer que toute la connectivité Internet passe par le siège social, comment proposez-vous de concevoir le transfert ?

Réponse : Vous pourriez configurer tous les serveurs DNS pour qu'ils utilisent un serveur DNS du siège social comme redirecteur. Cela garantit également que vous pouvez suivre la direction du trafic de requête DNS.

Question : Comment concevriez-vous les zones DNS ?

Réponse : La zone existante northwindtraders.priv est suffisante. Toutefois, le basculement vers une zone intégrée à Active Directory serait avantageuse.

Question : Les zones Active Directory sont-elles indiquées ?

Réponse : Les zones Active Directory sont éventuellement indiquées.

Question : Comment concevriez-vous des transferts de zone ?

Réponse : Vous pouvez concevoir des transferts de zone en utilisant des zones AD DS comme indiqué. Si vous utilisez des zones intégrées à Active Directory, vérifiez que tous les serveurs DNS des succursales sont également des contrôleurs de domaine AD DS. Cela garantit que les transferts de zone sont traités dans le cadre de la réplication AD DS normale.

Question : Northwind Traders vient d'être racheté par Contoso, Ltd. Cela affecte-t-il vos décisions de conception DNS ?

Réponse : Oui, cela affecte vos décisions de conception DNS. La redirection conditionnelle peut être avantageuse pour le domaine Contoso.com.

Démonstration

Démonstration : Création de zones DNS

Procédure de démonstration

Créer une zone de recherche inversée principale

1. Basculez vers LON-DC1, puis connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **DNS**.
3. Dans DNS, développez **LON-DC1**, puis développez **Zones de recherche inversée**.
4. Cliquez avec le bouton droit sur **Zones de recherche inversée**, puis cliquez sur **Nouvelle zone**.
5. Dans l'Assistant Nouvelle zone, cliquez sur **Suivant**.
6. Dans la page **Type de zone**, cliquez sur **Zone principale**, puis cliquez sur **Suivant**.
7. Dans la page **Étendue de la zone de réplication de Active Directory**, cliquez sur **Suivant**.
8. Dans la page **Nom de la zone de recherche inversée**, cliquez sur **Zone de recherche inversée IPv4**, puis cliquez sur **Suivant**.
9. Dans la page **Nom de la zone de recherche inversée**, dans la zone **ID réseau**, tapez **172.16.0**, puis cliquez sur **Suivant**.
10. Dans la page **Mise à niveau dynamique**, cliquez sur **Suivant**.
11. Dans la page **Fin de l'Assistant Nouvelle zone** , cliquez sur **Terminer**.

Créer une nouvelle zone de recherche directe secondaire

1. Basculez vers LON-SVR1.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **DNS**.
3. Dans DNS, développez **LON-SVR1**, puis développez **Zones de recherche directes**.
4. Cliquez avec le bouton droit sur **Zones de recherche directes**, puis cliquez sur **Nouvelle zone**.
5. Dans l'Assistant Nouvelle zone, cliquez sur **Suivant**.
6. Dans la page **Type de zone**, cliquez sur **Zone secondaire**, puis cliquez sur **Suivant**.
7. Dans la page **Nom de la zone**, dans la zone **Nom de la zone**, tapez **Adatum.com**, puis cliquez sur **Suivant**.
8. Dans la page **Serveurs DNS maîtres**, dans la liste **Serveurs maîtres**, tapez **172.16.0.10**, appuyez sur Entrée, puis cliquez sur **Suivant**.
9. Dans la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.

Leçon 4

Conception et configuration de la réplication et de la délégation de zone DNS

Table des matières :

Démonstration

Démonstration : Configuration de transferts de zones

Procédure de démonstration

Activer les transferts de zone sur une zone

1. Basculez vers LON-DC1.
2. Dans la console DNS, développez **Zones de recherche directes**, puis cliquez sur **Adatum.com**.
3. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur l'onglet **Transferts de zone**.
5. Activez la case à cocher **Autoriser les transferts de zone**, cliquez sur **Uniquement vers les serveurs listés dans l'onglet Serveurs de noms**, puis cliquez sur **Notifier**.
6. Dans la boîte de dialogue **Notifier**, dans la liste **Les serveurs suivants**, tapez **172.16.0.21**, puis appuyez sur Entrée.
7. Cliquez sur **OK**, puis cliquez sur l'onglet **Serveurs de noms**.
8. Cliquez sur **Ajouter**, et dans la boîte de dialogue **Nouvel enregistrement de serveur de noms**, dans la zone **Nom de domaine complet (FQDN) du serveur**, tapez **LON-SVR1.Adatum.com**, cliquez sur **Résoudre**, puis cliquez deux fois sur **OK**.

Effectuez un transfert de zone

1. Basculez vers LON-SVR1, puis vers la console DNS.
2. Dans le volet de navigation, cliquez sur **Adatum.com**, puis dans la barre d'outils, cliquez sur **Actualiser**.

 **Remarque :** Le transfert de zone n'a peut-être pas encore eu lieu, donc cette étape peut ne pas remplir la zone avec des enregistrements.

3. Basculez vers LON-DC1.
4. Dans DNS, cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel alias (CNAME)**.
5. Dans la boîte de dialogue **Nouvel enregistrement de ressource**, dans la zone **Nom de l'alias**, tapez **WWW**.
6. Dans la zone **Nom de domaine complet (FQDN) pour l'hôte de destination :**, tapez **LON-SVR1.Adatum.com**, puis cliquez sur **OK**.
7. Basculez vers LON-SVR1.
8. Dans la console DNS, cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Transfert à partir du maître**.

 **Remarque :** Si le nouvel enregistrement d'alias n'apparaît pas, dans le volet de navigation, cliquez sur **Zones de recherche directes**. Dans la barre d'outils, cliquez sur **Actualiser**. Cliquez sur **Adatum.com**, puis vérifiez la présence du nouvel enregistrement d'alias.

Leçon 6

Conception du système DNS pour la haute disponibilité et la sécurité

Table des matières :

Questions et réponses

Discussion : Instructions relatives à la conception de la sécurité DNS

Question : Comment pourriez-vous renforcer la sécurité d'une infrastructure DNS interne ?

Réponse : Vous pouvez renforcer la sécurité de l'infrastructure DNS interne en implémentant les zones intégrées à Active Directory.

Question : Quelles modifications de configuration seraient nécessaires pour soutenir vos propositions ?

Réponse : Vous devez promouvoir le serveur de noms déployé dans la succursale 1 dans un contrôleur de domaine. Vous devez également convertir la zone northwindtraders.priv en une zone intégrée à Active Directory. Vous devez également envisager de remplacer les serveurs de noms du siège social par des contrôleurs de domaine supplémentaires pour éviter d'utiliser les zones secondaires et les transferts de zone. Notez que vous devez renommer ces serveurs pour valider leurs rôles modifiés.

Question : Comment recommanderiez-vous de configurer des mises à jour sur votre serveur DNS ?

Réponse : Si vous utilisez des zones intégrées à Active Directory, vous pouvez configurer des mises à jour dynamiques uniquement sécurisées.

Question : Quel niveau de stratégie de sécurité DNS avez-vous choisi ?

Réponse : Vous devez choisir le niveau de stratégie de sécurité DNS Haut.

Question : Existe-t-il d'autres critères de sécurité liés à la conception de DNS ?

Réponse : Les réponses varieront selon les réponses aux questions précédentes.

Contrôle des acquis et éléments à retenir

Question(s) de contrôle des acquis

Question : Quelle est la différence entre un sous-domaine dans une zone DNS et une zone déléguée ?

Réponse : La différence entre un sous-domaine dans une zone DNS et une zone déléguée est qu'un sous-domaine dans une zone DNS n'a aucun serveur de noms en propre, alors qu'une zone déléguée a en propre les serveurs de noms faisant autorité.

Question : Contoso a créé un service Ventes régional. Une partie du personnel de vente se trouve dans les centres de ventes régionaux où il n'y a qu'environ 10 ordinateurs. Les ordinateurs du personnel de vente doivent pouvoir accéder aux mêmes applications et ressources que le reste du personnel Contoso. Comment implémenteriez-vous le service DNS dans ces petites succursales ?

Réponse : Il y a un certain nombre de solutions possibles, mais la plus logique serait de configurer un serveur cache uniquement dans ces succursales.

Question : Si la conception doit être tolérante aux défaillances de liaison entre les succursales et les sites hub, comment cela affecterait-il votre conception ?

Réponse : Un serveur cache uniquement présenterait un problème. En cas de liaison défaillante, le serveur de noms local ne pourrait fournir de réponses que pour les enregistrements déjà interrogés. Pour assurer la tolérance de pannes requise, utilisez un serveur DNS local avec une zone secondaire ou une zone intégrée à Active Directory, à condition que le serveur DNS soit également un contrôleur de domaine.

Question : Vrai ou faux ? Vous devez désactiver la récursivité sur tous les serveurs DNS internes.

Réponse : Faux. En général, les serveurs DNS internes ont besoin que la récursivité soit activée, alors qu'un serveur DNS qui héberge un espace de noms DNS externe doit généralement faire désactiver la récursivité. Cela empêche les clients Internet d'utiliser ce serveur pour résoudre les noms DNS.

Question : Pourquoi n'est-il pas recommandé de désactiver la rotation circulaire sur tous les serveurs DNS ?

Réponse : La rotation circulaire est un mécanisme d'équilibrage de la charge que les serveurs DNS utilisent pour partager et distribuer les charges de ressources réseau. Si plusieurs enregistrements de ressources sont trouvés, vous pouvez utiliser cette fonctionnalité pour permuter tous les types d'enregistrements de ressources qui sont contenus dans une réponse à une requête. Bien que la désactivation de cette fonctionnalité puisse réduire la charge de travail sur le processeur du serveur DNS, cette fonctionnalité dirigera tous les clients vers le même serveur de ressources pour une requête donnée.

Question : Quand configureriez-vous un serveur cache uniquement ?

Réponse : Les serveurs cache uniquement ne contiennent pas de données de zone et ne participent donc pas aux transferts de zone. Cela peut être utile lorsqu'une liaison WAN qui connecte à une succursale a une capacité disponible minimale pour prendre en charge le trafic de transfert de zone.

Question : Pour déterminer la résolution de noms NetBIOS, quand choisirez-vous WINS sur GNZ ?

Réponse : WINS assure une meilleure prise en charge de l'inscription, de la version et de la résolution de noms NetBIOS que le GNZ statique. Pour les réseaux d'entreprise qui dépendent plus des applications NetBIOS, WINS est le choix logique. Toutefois, lorsque l'utilisation de NetBIOS diminue et que les clients et les serveurs présentent des configurations IPv4 statiques, GNZ peut fournir tous les éléments requis pour prendre en charge la résolution de noms NetBIOS.

Question : Vous êtes préoccupé par la sécurité des données de zone lorsqu'elle sont en transit sur le réseau pendant un transfert de zone. Tous vos serveurs DNS sont également des contrôleurs de domaine. Quelles sont les deux stratégies que vous pouvez implémenter pour atténuer les menaces sur la sécurité perçues ?

Réponse : Une stratégie consiste à implémenter des zones intégrées à Active Directory. Les transferts de zone auront alors lieu dans le cadre de la réplication Active Directory à l'aide du chiffrement Active Directory standard sur la connexion. Sinon, vous pouvez implémenter une règle de sécurité de connexion (IPsec) pour chiffrer le trafic entre les serveurs maîtres et les supports configurés de zone secondaire.

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

Atelier pratique A : Conception et implémentation de la résolution de noms

Questions et réponses

Question : Pour quelle approche avez-vous opté lors des exercices de conception de DNS ?

Réponse : Les réponses varient.

Question : Votre conception est-elle différente de la solution suggérée ?

Réponse : Les réponses varient.

Question : En quoi la conception DNS pour Contoso est-elle comparable avec l'implémentation du service DNS dans votre organisation ?

Réponse : Les réponses varient.

Module 5

Conception et implémentation d'une infrastructure de forêt et de domaine pour les services de domaine Active Directory

Table des matières :

Leçon 1

Conception d'une forêt AD DS

Table des matières :

Questions et réponses

Discussion : Choix d'une conception de forêt adéquate

Question : Combien de forêts sont requises pour intégrer les deux organisations ?

Réponse : Deux forêts (celles qui existent déjà) sont requises. Modifier l'environnement de deux grandes organisations représenterait un projet de grande envergure, très long et bien trop onéreux.

Question : Comment recommanderiez-vous d'intégrer les deux organisations ?

Réponse : Vous utiliseriez des approbations de forêt pour intégrer les deux organisations.

Question : Quelle est la pertinence des modifications de schéma de la forêt de Tailspin Toys pour la conception que vous pouvez envisager ?

Réponse : Une raison majeure qui incite à implémenter plusieurs forêts est que tous les contrôleurs de domaine d'une même forêt partagent un schéma commun. En d'autres termes, deux forêts ont un schéma distinct et potentiellement différent. Puisque le scénario suggère que des modifications ont été apportées dans une organisation pour prendre en charge une application vitale pour l'entreprise, à moins que ces mises à jour de schéma ne soient pertinentes pour les deux organisations, elles doivent rester distinctes.

Question : Comment les noms de domaine externes existants utilisés affectent-ils votre conception ?

Réponse : Ce facteur n'affecte en rien la conception. Les noms externes n'ont pas besoin d'être liés de quelque façon que ce soit aux noms de domaine et de forêt AD DS internes.

Leçon 2

Conception et implémentation d'approbations de forêt AD DS

Table des matières :

Démonstration

Démonstration : Création d'une approbation de forêt

Procédure de démonstration

Définir les conditions préalables à la création d'une approbation de forêt

1. Basculez vers LON-DC1 et, si nécessaire, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
3. Dans DNS, dans le volet de navigation, développez **LON-DC1**, puis **Redirecteurs conditionnels**, cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez sur **Nouveau redirecteur conditionnel**.
4. Dans la boîte de dialogue **Nouveau redirecteur conditionnel**, dans la zone **Domaine DNS**, tapez **treyresearch.net**, puis cliquez sur la liste **Adresse IP**.
5. Tapez **172.16.10.10**, appuyez sur Entrée, puis cliquez sur **OK**.
6. Positionnez le pointeur de la souris dans l'angle inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
7. Tapez **cmd.exe**, puis appuyez sur Entrée.
8. À l'invite de commandes, tapez **nslookup trey-dc1.treyresearch.net**, puis appuyez sur Entrée. La requête doit aboutir et retourner l'adresse IP **172.16.10.10**.
9. Basculez vers TREY-DC1.
10. Au besoin, connectez-vous en tant que **Treyresearch\Administrateur** avec le mot de passe **Pa$$w0rd**.
11. Cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **DNS**.
12. Dans DNS, dans le volet de navigation, développez **TREY-DC1**, puis **Redirecteurs conditionnels**, cliquez avec le bouton droit sur **Redirecteurs conditionnels**, puis cliquez sur **Nouveau redirecteur conditionnel**.
13. Dans la boîte de dialogue **Nouveau redirecteur conditionnel**, dans la zone **Domaine DNS**, tapez **Adatum.com**, puis cliquez sur la liste **Adresse IP**.
14. Tapez **172.16.0.10**, appuyez sur Entrée, puis cliquez sur **OK**.
15. Cliquez sur **Démarrer**, dans la zone **Rechercher les programmes et fichiers**, tapez **cmd.exe**, puis appuyez sur Entrée.
16. À l'invite de commandes, tapez **nslookup lon-svr1.adatum.com**, puis appuyez sur Entrée. La requête doit aboutir et retourner l'adresse IP 172.16.0.21.

Créer une approbation de forêt

1. Basculez vers LON-DC1.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Domaines et approbations Active Directory**.
3. Dans la fenêtre Domaines et approbations Active Directory, cliquez sur **Adatum.com**, cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur l'onglet **Approbations**, puis sur **Nouvelle approbation**.
5. Dans la boîte de dialogue **Assistant Nouvelle approbation**, cliquez sur **Suivant**.
6. Dans la page **Nom d'approbation**, dans la zone **Nom**, tapez **treyresearch.net**, puis cliquez sur **Suivant**.
7. Dans la page **Type d'approbation**, cliquez sur **Approbation de forêt**, puis cliquez sur **Suivant**.
8. Dans la page **Direction de l'approbation**, cliquez sur **Bidirectionnel**, puis sur **Suivant**.
9. Dans la page **Sens de l'approbation**, cliquez sur **Ce domaine et le domaine spécifié**, puis sur **Suivant**.
10. Dans la page **Nom d'utilisateur et mot de passe**, dans la zone **Nom d'utilisateur**, tapez **Treyresearch\Administrateur**.
11. Dans la zone **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Suivant**.
12. Dans la page **Niveau d'authentification d'approbations sortantes--Forêt locale**, cliquez sur **Suivant**.
13. Dans la page **Niveau d'authentification d'approbations sortantes -- Forêt spécifiée**, cliquez sur **Suivant**.
14. Dans la page **Fin de la sélection des approbations**, cliquez sur **Suivant**.
15. Dans la page **Fin de la création de l'approbation**, cliquez sur **Suivant**.
16. Dans la page **Confirmer l'approbation sortante**, cliquez sur **Oui, confirmer l'approbation sortante**, puis sur **Suivant**.
17. Dans la page **Confirmer l'approbation entrante**, cliquez sur **Oui, confirmer l'approbation entrante**, puis cliquez sur **Suivant**.
18. Dans la page **Fin de l'Assistant Nouvelle approbation**, cliquez sur **Terminer**.
19. Dans la boîte de dialogue **Propriétés de : Adatum.com**, cliquez sur **OK**.

Leçon 3

Conception et implémentation de domaines AD DS

Table des matières :

Démonstration

Démonstration : Implémentation d'un domaine AD DS

Procédure de démonstration

Ajouter le rôle serveur AD DS

1. Basculez vers CON-SVR.
2. Connectez-vous en tant qu'**Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans le Gestionnaire de serveur, dans le volet d'informations, cliquez sur **Ajouter des rôles et des fonctionnalités**.
4. Dans l'Assistant Ajout de rôles et de fonctionnalités, dans la page **Avant de commencer**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
7. Dans la page **Sélectionner des rôles de serveurs**, dans la liste **Rôles**, activez la case à cocher **Services AD DS**.
8. Cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
9. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
10. Dans la page **Services de domaine Active Directory**, cliquez sur **Suivant**.
11. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
12. Une fois l'installation du rôle terminée, cliquez sur **Fermer**.

Créer un domaine dans une forêt existante

1. Dans le Gestionnaire de serveur, dans le volet de navigation, cliquez sur **AD DS**.
2. Dans le volet d'informations, cliquez sur **Autres...**
3. Dans la boîte de dialogue **Détails et notifications de la tâche Tous les serveurs**, cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.
4. Dans l'Assistant Configuration des services de domaine Active Directory, dans la page **Configuration de déploiement**, cliquez sur **Ajouter un nouveau domaine à une forêt existante**.
5. Dans la liste **Sélectionnez le type du domaine**, cliquez sur **Domaine de l'arborescence**.
6. Dans la zone **Nom de la forêt**, tapez **Adatum.com**.
7. Dans la zone **Nouveau nom de domaine**, tapez **contoso.com**, puis cliquez sur **Modifier**.
8. Dans la boîte de dialogue **Sécurité de Windows**, dans la zone **Nom d'utilisateur**, tapez **ADATUM\Administrateur**. Dans la zone **Mot de passe**, tapez **Pa$$w0rd**.
9. Cliquez sur **OK**, puis sur **Suivant**.
10. Dans la page **Options du contrôleur de domaine**, dans les zones **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Suivant**.

11. Dans la page **Options DNS**, cliquez sur **Suivant**.
12. Dans la page **Options supplémentaires**, cliquez sur **Suivant**.
13. Dans la page **Chemins d'accès**, cliquez sur **Suivant**.
14. Dans la page **Examiner les options**, cliquez sur **Suivant**.
15. Une fois les conditions préalables vérifiées, cliquez sur **Installer**.
16. Votre ordinateur redémarre. À l'invite, connectez-vous en tant que **Contoso\Administrateur** avec le mot de passe **Pa$$w0rd**.

Contrôle des acquis et éléments à retenir

Question(s) de contrôle des acquis

Question : Quel est le rôle du modèle de forêt basé sur les ressources ?

Réponse : Vous pouvez utiliser le modèle de forêt basé sur les ressources dans un environnement comportant une application, un dossier partagé ou tout autre ressource système particulièrement vitale ou sécurisée. Dans ce cas, les administrateurs créent une forêt spécifiquement pour les utilisateurs qui doivent accéder à cette ressource.

Question : Quel niveau fonctionnel de forêt devez-vous définir dans AD DS pour pouvoir établir une approbation de forêt ?

Réponse : Vous devez définir le niveau fonctionnel de forêt de Windows Server 2003 au minimum afin de pouvoir établir une approbation de forêt entre deux forêts. En outre, vous devez configurer DNS dans les deux forêts, de sorte que les clients puissent résoudre les noms de l'autre forêt.

Question : Si vous souhaitez intégrer plusieurs espaces de noms internes, quelles technologies devez-vous utiliser ?

Réponse : Vous devez utiliser des zones de stub et des enregistrements de délégation.

Question : Un utilisateur de Contoso tente d'accéder à un dossier partagé dans le domaine Tailspin Toys et reçoit une erreur d'accès refusé. Une relation d'approbation est établie entre ces deux domaines. Que devez-vous faire pour autoriser l'utilisateur à accéder au dossier ?

Réponse : Tout d'abord, vous devez vérifier la direction de l'approbation et vous assurer que l'authentification sélective est appliquée. Ensuite, vous devez vérifier la liste de contrôle d'accès (ACL) sur le dossier partagé.

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

Atelier pratique A : Conception et implémentation d'une infrastructure de forêt pour les services de domaine Active Directory

Questions et réponses

Question : Pour quelle approche avez-vous opté lors des exercices de conception de forêt AD DS ?

Réponse : Les réponses varient.

Question : Votre conception est-elle différente de la solution suggérée ?

Réponse : Les réponses varient.

Question : Si le coût n'importait pas, en quoi pourrait-elle affecter votre conception ?

Réponse : La réponse varie, mais peut se concentrer sur l'intérêt de fusionner toutes les organisations dans une forêt unique. Ce projet se révélerait onéreux, mais offrirait certains avantages (abordés dans le module).

Atelier pratique B : Conception et implémentation d'une infrastructure de domaine AD DS

Questions et réponses

Question : Pour quelle approche avez-vous opté lors des exercices de conception de domaine AD DS ?

Réponse : Les réponses varient.

Question : Votre conception est-elle différente de la solution suggérée ?

Réponse : Les réponses varient.

Question : Comment la conception de domaine rivalise-t-elle avec l'implémentation de domaine dans votre organisation ?

Réponse : Les réponses varient.

Module 6

Conception et implémentation d'une infrastructure d'unités d'organisation Active Directory

Table des matières :

Leçon 1

Planification du modèle de délégation des tâches d'administration Active Directory

Table des matières :

Documentation supplémentaire

Qu'est-ce qu'un modèle de délégation des tâches d'administration Active Directory ?

 **Documentation supplémentaire:** Pour plus d'informations sur les Méthode conseillée pour déléguer l'administration d'Active Directory, consultez les deux liens suivants :

- http://go.microsoft.com/fwlink/?linkid=279914
- http://go.microsoft.com/fwlink/?linkid=279915

Leçon 2

Conception de la structure d'unités d'organisation

Table des matières :

Questions et réponses

Stratégies de conception des unités d'organisation

Question : Quelle est la structure d'unités d'organisation que vous utilisez sur votre lieu de travail ? Pourquoi est-elle conçue ainsi ? Quels problèmes rencontrez-vous actuellement avec votre modèle d'unités d'organisation ?

Abordez ces questions avec les autres stagiaires et votre instructeur.

Réponse : <Ajoutez la réponse ici>

Protection des unités d'organisation contre des suppressions accidentelles

Question : Que pensez-vous de la structure d'unités d'organisation utilisée dans votre organisation ? Y a-t-il des choses que vous souhaitez modifier ?

Réponse : <Ajoutez la réponse ici>

Démonstration

Démonstration : Implémentation d'unités d'organisation

Procédure de démonstration

Créer une unité d'organisation

1. Basculez vers LON-DC1 et, si nécessaire, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
3. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Adatum (local)**.
4. Dans le volet Tâches, dans la section **Adatum (local)**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
5. Dans la boîte de dialogue **Créer Unité d'organisation**, dans la zone **Nom**, tapez **Contoso-IT**. Dans la zone **Description**, tapez **Unité d'organisation destinée à contenir des comptes/groupes à des fins administratives**.
6. Notez que la case à cocher **Protéger contre la suppression accidentelle** est activée.
7. Pour créer l'unité d'organisation et fermer la boîte de dialogue **Créer Unité d'organisation : Contoso-IT**, cliquez sur **OK**.

Vérifier que cette unité d'organisation est protégée contre des suppressions accidentelles

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans la console Utilisateurs et ordinateurs Active Directory, dans la barre de menus, cliquez sur **Affichage**, puis sur **Fonctionnalités avancées**.

3. Dans la console Utilisateurs et ordinateurs Active Directory, développez **Adatum.com**, puis cliquez sur **Adatum.com**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur **Contoso-IT**, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de : Contoso-IT**, cliquez sur l'onglet **Objet**. Assurez-vous que la case à cocher **Protéger l'objet des suppressions accidentelles** est activée, puis cliquez sur **OK**.
6. Fermez Utilisateurs et ordinateurs Active Directory.

Examiner les paramètres de sécurité par défaut de l'unité d'organisation

7. Revenez au Centre d'administration Active Directory.
8. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Adatum (local)**.
9. Dans le volet d'informations, cliquez sur l'unité d'organisation **Contoso-IT**.
10. Dans le volet Tâches, dans la section **Contoso-IT**, cliquez sur **Propriétés**.
11. Faites défiler l'écran vers le bas jusqu'à la section **Extensions**, puis cliquez sur l'onglet **Sécurité**.
12. Sous l'onglet **Sécurité**, cliquez sur **Avancé**.
13. Dans la boîte de dialogue **Paramètres de sécurité avancés pour Contoso-IT**, examinez les paramètres de sécurité par défaut, puis cliquez sur **Annuler**.

Supprimer une unité d'organisation protégée

1. Dans la boîte de dialogue **Contoso-IT**, désactivez la case à cocher **Protéger contre la suppression accidentelle**, puis cliquez sur **OK**.
2. Dans le Centre d'administration Active Directory, dans le volet Tâches, dans la section **Contoso-IT**, cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Supprimer la confirmation**, cliquez sur **Oui**.

Leçon 3

Conception et implémentation d'une stratégie de groupe Active Directory

Table des matières :

Questions et réponses

Groupes Active Directory dans Windows Server 2012

Question : Discutez avec les stagiaires de la stratégie de groupe utilisée dans votre organisation. Quels problèmes rencontrez-vous actuellement dans votre environnement par rapport à votre stratégie de groupe ?

Réponse : <Ajoutez la réponse ici>

Démonstration

Démonstration : Création et gestion de groupes

Procédure de démonstration

Créer une unité d'organisation

1. Sur LON-DC1, basculez vers le Centre d'administration Active Directory.
2. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Adatum (local)**.
3. Dans le volet Tâches, dans la section **Adatum (local)**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
4. Dans la boîte de dialogue Créer Unité d'organisation, dans la zone Nom, tapez SelfService. Dans la zone Description, tapez Unité d'organisation pour les groupes qui s'autogèrent, puis cliquez sur OK.

Créer un groupe et configurer la gestion de ce groupe

1. Dans le Centre d'administration Active Directory, dans le volet d'informations, double-cliquez sur l'unité d'organisation **SelfService**.
2. Dans le volet Tâches, dans la section **SelfService**, cliquez sur **Nouveau**, puis sur **Groupe**.
3. Dans la boîte de dialogue **Créer Groupe :** dans la zone **Nom du groupe**, tapez **SportsInLondon**. Dans la zone **Adresse de messagerie**, tapez **SportsInLondon@adatum.com**.
4. Dans la zone **Description**, tapez **Groupe local de domaine autogéré qui contiendra les membres de la communauté Sports in London**, puis cliquez sur **OK**.
5. Dans le Centre d'administration Active Directory, dans l'unité d'organisation SelfService, cliquez sur le groupe **SportsInLondon**.
6. Dans le volet Tâches, dans la section **SportsInLondon**, cliquez sur **Propriétés**.
7. Dans la boîte de dialogue **SportsInLondon**, dans la section **Géré par**, cliquez sur **Modifier**.
8. Dans la boîte de dialogue **Sélectionnez un utilisateur, un contact ou un groupe**, dans la zone **Entrez le nom de l'objet à sélectionner (exemples)**, tapez **SportsInLondon**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
9. Dans la boîte de dialogue **SportsInLondon**, dans la section **Géré par**, activez la case à cocher **Le gestionnaire peut mettre à jour la liste des membres**, puis cliquez sur **OK**.

Ajouter un utilisateur dans le groupe

1. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Adatum (local)**.
2. Dans le volet d'informations, double-cliquez sur l'unité d'organisation **Marketing**.
3. Dans le volet d'informations, cliquez sur **Adam Barr**.
4. Dans le volet Tâches, dans la section **Adam Barr**, cliquez sur **Ajouter au groupe**.
5. Dans la boîte de dialogue **Sélectionnez des groupes**, dans la zone **Entrez les noms des objets à sélectionner (exemples)**, tapez **SportsInLondon**, cliquez sur **Vérifier les noms**, puis sur **OK**.

Vérifier que le groupe communautaire peut s'autogérer

1. Déconnectez-vous de LON-DC1.
2. Reconnectez-vous à LON-DC1 en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans l'écran d'accueil, cliquez sur la vignette **Outils d'administration**.
4. Dans Outils d'administration, double-cliquez sur **Centre d'administration Active Directory**.
5. Dans le Centre d'administration Active Directory, dans la page **Vue d'ensemble**, dans la zone **RECHERCHE GLOBALE**, tapez **Pat**, puis cliquez sur **Rechercher**.
6. Dans le volet d'informations, cliquez sur **Pat Coleman**.
7. Dans le volet Tâches, dans la section **Pat Coleman**, cliquez sur **Ajouter au groupe**.
8. Dans la boîte de dialogue **Sélectionnez des groupes**, dans la zone **Entrez les noms des objets à sélectionner**, tapez **SportsInLondon**, cliquez sur **Vérifier les noms**, puis sur **OK**.
9. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Adatum (local)**.
10. Dans le volet d'informations, double-cliquez sur l'unité d'organisation **SelfService**, puis cliquez sur le groupe **SportsInLondon**.
11. Dans le volet Tâches, dans la section **SportsInLondon**, cliquez sur **Propriétés**.
12. Dans la boîte de dialogue **SportsInLondon**, dans la section **Membres**, vérifiez que Pat Coleman est membre du groupe, puis cliquez sur **Annuler**.
13. Déconnectez-vous de LON-DC1.

Contrôle des acquis et éléments à retenir

Méthode conseillée

- Utilisez le modèle AG(U)DLP lors de la conception de votre stratégie de groupe. Les comptes sont regroupés en groupes globaux correspondant aux rôles métier. Si nécessaire, vous pouvez consolider ces groupes sur plusieurs domaines dans un groupe universel. Les groupes de rôles sont alors attribués par l'intermédiaire de groupes locaux de domaine qui accordent l'accès à la ressource spécifique.
- Concevez votre modèle de tâches d'administration Active Directory en ayant à l'esprit les privilèges minimaux. Comme meilleure pratique, dressez la liste des tâches dans votre organisation, puis attribuez chaque tâche à une équipe spécifique. Si une équipe souhaite les autorisations, elle est responsable des tâches correspondantes.
- Utilisez des scripts pour implémenter votre conception. Passez en revue les applets de commande Windows PowerShell et l'outil dsacls permettant de définir des autorisations.

Question(s) de contrôle des acquis

Question : Pourquoi est-il judicieux d'implémenter les privilèges minimaux requis lors de la délégation des tâches d'administration ?

Réponse : Lorsque vous déléguez des tâches d'administration à d'autres groupes d'administration, vous limitez également ce que le personnel délégué peut voir dans l'interface utilisateur. Par exemple, si quelqu'un dispose uniquement des droits permettant de créer des objets utilisateur dans une unité d'organisation conçue pour des objets utilisateur, l'utilisateur ne peut pas éviter les stratégies de groupe en créant par erreur des objets d'ordinateur dans l'unité d'organisation. En outre, évitez d'utiliser le groupe Account Operators par défaut. Si ce groupe est requis, vous pouvez créer un groupe personnalisé doté des mêmes droits, mais seulement pour les objets appropriés (pour les ordinateurs dans leur unité d'organisation, pour les utilisateurs dans l'unité d'organisation utilisateur et pour les groupes dans l'unité d'organisation de groupe). Les personnes à qui vous déléguez des tâches doivent être qualifiées pour accomplir ces tâches. AD DS peut être très complexe, notamment en ce qui concerne les modifications globales, comme celles des paramètres de schéma et de configuration.

Question : Pourquoi est-il préférable d'utiliser des comptes administratifs et de les enregistrer dans un emplacement différent des comptes d'utilisateurs standard ?

Réponse : Lorsqu'un utilisateur dispose de privilèges de compte administratif, les codes malveillants qu'il peut recevoir dans un message électronique ou en naviguant sur Internet sont susceptibles de s'exécuter ou d'installer des binaires. Par conséquent, nous recommandons d'utiliser un compte administratif dédié et personnalisé à des fins d'administration uniquement. En outre, les comptes administratifs restreints sont protégés contre la délégation. Ce mécanisme de protection peut provoquer des problèmes imprévisibles avec certaines applications, telles que le courrier et la télécopie mobiles. En outre, vous pouvez déléguer des tâches d'administration dans votre structure d'unités d'organisation à un stade ultérieur. Par conséquent, il est important de placer vos administrateurs dans une structure d'unités d'organisation distincte, de sorte que vous ne puissiez pas déléguer par erreur leur contrôle ni permettre à un administrateur délégué de détourner un compte et d'obtenir des autorisations plus élevées.

Question : Que devez-vous prendre en compte lorsque vous souhaitez migrer votre structure d'unités d'organisation vers un nouveau modèle ?

Réponse : La nouvelle structure d'unités d'organisation ne doit pas endommager la structure existante. Assurez-vous que la délégation fonctionne correctement avant de déplacer les objets. Assurez-vous que les objets de stratégie de groupe sont liés correctement pour configurer les utilisateurs et les ordinateurs. En outre, il peut être nécessaire de reconfigurer les applications prenant en charge le protocole LDAP (Lightweight Directory Access Protocol), par exemple pour configurer à quel point elles recherchent des comptes d'utilisateurs. Cela peut également affecter le matériel non basé sur ordinateur, tel que les imprimantes multifonctionnelles et les systèmes téléphoniques. Cela peut également affecter les applications de réseau de périmètre, telles que les analyseurs de courrier, qui utilisent l'annuaire pour fournir des numéros de téléphone ou pour vérifier qu'un utilisateur dispose d'un compte de messagerie avant d'autoriser l'entrée d'un message électronique dans le système de messagerie de l'organisation.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Lorsque vous utilisez l'Assistant Délégation de sécurité pour définir des autorisations, quand l'Assistant s'ouvre à nouveau, les autorisations ne s'affichent pas.	Utilisez l'Assistant Délégation de sécurité dans Utilisateurs et ordinateurs Active Directory pour configurer les tâches de délégation courantes. Les paramètres obtenus sont enregistrés dans les propriétés **Sécurité** de l'unité d'organisation, mais ne s'afficheront pas dans l'Assistant. Pour vérifier les autorisations, utilisez la boîte de dialogue **Sécurité** et la boîte de dialogue **Sécurité avancée** permettant de passer en revue les paramètres.
Comment déterminer quels attributs doivent être délégués ?	Consultez le livre blanc Best Practices for Delegating Active Directory Administration (en anglais) et son annexe. Vous pouvez également modifier une valeur sur un objet utilisateur, puis utiliser l'éditeur d'attributs pour trouver la valeur. Vous pouvez utiliser LDIFDE.exe pour créer un vidage des attributs de l'objet avant et après la modification, puis comparer les fichiers.
Comment pouvez-vous modifier les paramètres de sécurité d'un attribut qui n'est pas affiché dans la boîte de dialogue **Sécurité avancée** ?	Certains attributs sont masqués dans la boîte de dialogue **Sécurité avancée**. La meilleure pratique consiste à utiliser DSAcls.exe pour modifier les paramètres de sécurité.

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

Atelier pratique A : Conception et implémentation d'une infrastructure et d'un modèle de délégation d'unités d'organisation Active Directory

Questions et réponses

Question : Quelle conception d'unités d'organisation avez-vous suggérée ? Quelles sont les raisons sous-tendant vos décisions de conception ?

Réponse : Les réponses varient. Selon le temps dont vous disposez, incitez les stagiaires à discuter de leurs conceptions.

Question : L'atelier pratique vous a fait utiliser Windows PowerShell pour déplacer des objets utilisateur selon un certain attribut. Pouvez-vous imaginer d'autres manières de procéder ?

Réponse : Dans Utilisateurs et ordinateurs Active Directory, vous pouvez utiliser la fonctionnalité des requêtes enregistrées pour créer une requête personnalisée, sélectionner tous les résultats, puis les déplacer. Dans le Centre d'administration Active Directory, vous pouvez également effectuer une recherche globale (via le filtre LDAP), puis sélectionner tous les objets obtenus et les déplacer immédiatement. Toutefois, nous vous recommandons d'utiliser des scripts via Windows PowerShell ou une invite de commandes, en utilisant les commandes dsquery / dsmove, puis de valider vos scripts dans un environnement de test avant de les exécuter.

Question : Bill a suggéré l'autogestion pour certains groupes. Comment l'implémenteriez-vous ? Quels sont les avantages et les risques associés à cette recommandation ?

Réponse : L'autogestion des groupes qui ne sont pas concernés par la sécurité est une bonne idée. On peut citer comme exemple le cas de groupes communautaires ou de certaines listes de distribution auxquels les utilisateurs sont libres d'adhérer ou non, comme ils le veulent. Ces groupes sont des groupes pour lesquels les autorisations de sécurité sont définies de sorte que le groupe lui-même puisse gérer son attribut « member ». Vous pouvez également utiliser la propriété **Géré par** dans les propriétés de l'objet de groupe. Après avoir implémenté l'autogestion, les membres du groupe peuvent ajouter d'autres utilisateurs ou s'extraire du groupe. Si l'extension messagerie est activée pour le groupe, les membres du groupe peuvent utiliser Office Outlook sans avoir à utiliser d'outils d'administration d'ordinateur client.

Module 7

Conception et implémentation d'une stratégie d'objet de stratégie de groupe

Table des matières :

Leçon 1

Collecte des informations requises pour la conception d'un objet de stratégie de groupe

Table des matières :

Questions et réponses

Question : Comment la stratégie de groupe est-elle utilisée dans votre organisation ? Quels sont les problèmes que vous rencontrez ou avez rencontrés dans votre organisation en matière de stratégie de groupe ? Présentez les paramètres ou les tâches que vous n'arrivez pas à gérer avec les objets de stratégie de groupe.

Réponse : Les réponses varient.

Leçon 2

Conception et implémentation des objets de stratégie de groupe

Table des matières :

Démonstration

Démonstration : Implémentation d'objets de stratégie de groupe

Procédure de démonstration

Créer un utilisateur du service DSRM

1. Basculez vers LON-DC1 et, si nécessaire, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
3. Dans le Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Adatum (local)**, puis double-cliquez sur le conteneur **Users**.
4. Dans le volet des tâches, dans la section **Users**, cliquez sur **Nouveau**, puis sur **Utilisateur**.
5. Dans la boîte de dialogue **Créer Utilisateur**, dans la zone de texte **Nom complet**, tapez **srv_dsrm**.
6. Dans la zone de texte **SamAccountName de l'utilisateur**, tapez **ADATUM\srv_dsrm**.
7. Dans les zones de texte **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa$$w0rd**.
8. Dans **Options de mot de passe**, sélectionnez **Autres options de mot de passe**, cliquez sur **Le mot de passe n'expire jamais**, puis cliquez sur **OK**.
9. Dans le Centre d'administration Active Directory, dans le volet d'informations du conteneur **Users**, cliquez sur le nouvel utilisateur **srv_dsrm**.

Dans le volet des tâches, dans la section **srv_dsrm**, cliquez sur **Désactiver**.

Créer une stratégie de groupe

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la Console de gestion des stratégies de groupe, dans le volet de navigation, développez **Forêt : Adatum.com**, développez **Domaines**, développez **Adatum.com**, puis cliquez sur **Objets de stratégie de groupe**.
3. Cliquez avec le bouton droit sur le nœud **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
4. Dans la boîte de dialogue **Nouvel objet GPO**, dans la zone **Nom**, tapez **DSRM_Pwd**, puis cliquez sur **OK**.

Créer une tâche planifiée à l'aide des préférences de stratégie de groupe

1. Cliquez avec le bouton droit sur **DSRM_Pwd**, puis cliquez sur **Modifier**.
2. Dans l'Éditeur de gestion des stratégies de groupe, développez **Configuration ordinateur**, développez **Préférences**, développez **Paramètres du Panneau de configuration**, puis cliquez sur **Tâches planifiées**.
3. Cliquez avec le bouton droit sur le nœud **Tâches planifiées**, pointez sur **Nouveau**, puis cliquez sur **Tâche planifiée (au minimum Windows 7)**.
4. Dans la boîte de dialogue **Nouvelles propriétés de Tâche (au minimum Windows 7)**, sous l'onglet **Général**, dans la liste **Action**, cliquez sur **Créer**.
5. Dans la zone de texte **Nom**, tapez **Synchroniser le mot de passe DSRM**.

6. Dans la section **Options de sécurité**, cliquez sur **Utilisateur ou groupe**.
7. Dans la boîte de dialogue **Sélectionnez un utilisateur ou un groupe**, dans la zone **Entrez le nom de l'objet à sélectionner (exemples) :** tapez **Système**, cliquez sur **Vérifier les noms**, puis sur **OK**.
8. Dans la boîte de dialogue **Nouvelles propriétés de Tâche (au minimum Windows 7)**, cliquez sur **Exécuter même si l'utilisateur n'est pas connecté**.
9. Dans la boîte de dialogue **Planificateur de tâches (Windows 7)**, cliquez sur **Annuler**.
10. Activez les cases à cocher **Ne pas stocker le mot de passe. La tâche n'aura accès qu'aux ressources locales** et **Exécuter avec les privilèges les plus élevés**.
11. Sous l'onglet **Déclencheurs**, cliquez sur **Nouveau**.
12. Dans la boîte de dialogue **Nouveau déclencheur**, dans la section **Paramètres**, sélectionnez l'option **Tous les jours**, dans la section **Paramètres avancés**, activez la case à cocher **Répéter la tâche toutes les**, puis cliquez sur **OK**.
13. Dans la boîte de dialogue **Nouvelles propriétés de Tâche (au minimum Windows 7)**, sous l'onglet **Actions**, cliquez sur le bouton **Nouveau**.
14. Dans la boîte de dialogue **Nouvelle action**, dans la section **Paramètres**, dans la zone de texte **Programme/script**, tapez **c:\Windows\System32\ntdsutil.exe**.
15. Dans la zone de texte **Ajouter arguments (facult.)**, tapez **"set dsrm password" "sync from domain account srv_dsrm" quit quit**, puis cliquez sur **OK** à deux reprises.

Liez la stratégie à l'unité d'organisation Domain Controllers

1. Dans la Console de gestion des stratégies de groupe, dans le volet de navigation, cliquez sur **Domain Controllers**.
2. Cliquez avec le bouton droit sur **Domain Controllers**, puis cliquez sur **Lier un objet de stratégie de groupe existant**.
3. Dans la boîte de dialogue **Sélectionner un objet GPO**, sous **Objets de stratégie de groupe**, cliquez sur **DSRM_Pwd**, puis sur **OK**.

Leçon 3

Conception du traitement des objets de stratégie de groupe

Table des matières :

Questions et réponses

Question : Comment pensez-vous remodeler votre infrastructure de stratégie de groupe en tenant compte des informations des trois dernières leçons ? Quels problèmes vous attendez-vous à rencontrer lors de l'implémentation de ces modifications ?

Réponse : Les réponses varient.

Leçon 4

Planification de la gestion des stratégies de groupe

Table des matières :

Démonstration

Démonstration : Gestion des objets de stratégie de groupe

Procédure de démonstration

Créer une sauvegarde de tous les objets de stratégie de groupe

1. Sur LON-DC1, dans la barre des tâches, démarrez Windows PowerShell®.
2. À l'invite de commandes Windows PowerShell, tapez **New-Item c:\GPO-Backups –ItemType Directory**, puis appuyez sur Entrée.
3. Basculez vers Gestion des stratégies de groupe.
4. Dans la Console GPMC, dans le volet de navigation, cliquez sur **Objets de stratégie de groupe**.
5. Cliquez avec le bouton droit sur **Objets de stratégie de groupe**, puis cliquez sur **Sauvegarder tout**.
6. Dans la boîte de dialogue **Sauvegarde de l'objet GPO**, dans la zone de texte **Emplacement**, tapez **C:\GPO-Backups**, puis cliquez sur **Sauvegarder**.
7. Une fois la sauvegarde effectuée, cliquez sur **OK**.

Remarque : Vous pouvez également utiliser l'applet de commande Windows PowerShell suivante pour sauvegarder les objets de stratégie de groupe : **Backup-GPO –All –Path c:\GPO-Backups**

8. Dans la Console GPMC, cliquez avec le bouton droit sur **Objets de stratégie de groupe**, puis cliquez sur **Gérer les sauvegardes**.
9. Dans la boîte de dialogue **Gérer les sauvegardes**, examinez les options, puis cliquez sur **Fermer**.

Documenter les paramètres d'objet de stratégie de groupe

1. Dans la Console GPMC, sous **Objets de stratégie de groupe**, cliquez sur **DSRM_Pwd**.
2. Cliquez avec le bouton droit sur **DSRM_Pwd**, puis cliquez sur **Enregistrer le rapport**.
3. Dans la boîte de dialogue **Enregistrer le rapport sur les objets GPO**, dans le volet de navigation, cliquez sur **Allfiles (E:)**, puis cliquez sur **Enregistrer**.
4. Dans la barre des tâches, cliquez sur **Explorateur de fichiers**.
5. Dans le volet de navigation, cliquez sur **Allfiles (E:)**.
6. Dans le volet d'informations, double-cliquez sur **DSRM_Pwd.htm**.
7. Affichez les sections **Liens** et **Filtrage de sécurité**, affichez **Délégation**, puis affichez les paramètres spécifiques.

Remarque : Vous pouvez également utiliser l'applet de commande Windows PowerShell suivante pour documenter les paramètres des objets de stratégie de groupe : **Get-GPOReport –Name** *GPO-Name* **–ReportType HTML –Path E:\GPOReports\GPOReport1.html**

Contrôle des acquis et éléments à retenir

Méthode conseillée

Activez le magasin central des modèles d'administration de stratégie de groupe si plusieurs administrateurs modifient les stratégies de groupe et si vous modifiez les objets de stratégie de groupe de différents ordinateurs.

Évitez d'utiliser des stratégies de groupe liées aux sites.

Planifiez soigneusement votre stratégie de sauvegarde et de récupération des stratégies de groupe.

Planifiez le test des stratégies de groupe avant d'appliquer des objets de stratégie de groupe aux utilisateurs et ordinateurs dans un environnement de production.

Limitez le nombre d'objets de stratégie de groupe qui s'appliquent aux utilisateurs et aux ordinateurs. Utilisez des objets de stratégie de groupe de haut niveau pour les paramètres usuels et essayez de limiter les paramètres individuels dans les objets de stratégie de groupe individuels. Un grand nombre d'objets de stratégie de groupe accroît les délais de démarrage et de connexion.

Prenez régulièrement le temps de documenter (ou de mettre à jour) vos objets de stratégie de groupe, leurs paramètres et les emplacements où ils sont liés dans la structure d'unités d'organisation.

Question(s) de contrôle des acquis

Question : Quelles sont les différentes options possibles pour appliquer des objets de stratégie de groupe à certains utilisateurs ou ordinateurs ?

Réponse : Vous pouvez lier des objets de stratégie de groupe à un domaine, à un site ou à n'importe quelle unité d'organisation dans le domaine Active Directory. Vous pouvez utiliser le filtrage de sécurité pour définir des autorisations en fonction des groupes, ou des filtres WMI pour identifier certains matériels, certaines configurations de système d'exploitation ou d'autres aspects relatifs à la gestion de l'ordinateur. En outre, vous pouvez appliquer ou bloquer l'héritage afin d'ajuster le mode d'héritage des objets de stratégie de groupe.

Question : Que devez-vous prendre en compte lorsque vous appliquez un objet de stratégie de groupe à un site ?

Réponse : Les objets de stratégie de groupe sont liés aux objets Active Directory, et certaines options de configuration sont enregistrées dans AD DS. Toutefois, les paramètres de stratégie de groupe sont basés sur des fichiers de SYSVOL, qui est répliqué automatiquement dans un domaine spécifique. Les sites AD DS ne correspondent pas nécessairement à la structure du domaine. Par exemple, un domaine peut s'étendre sur plusieurs sites et un site peut contenir des contrôleurs de domaine de plusieurs domaines. Pour vous assurer que les paramètres de stratégie de groupe ne sont pas transférés vers le réseau étendu (WAN), il est important de créer l'objet de stratégie de groupe dans un domaine qui a suffisamment de contrôleurs de domaine pour traiter les demandes de connexion des utilisateurs sur le site où vous souhaitez appliquer l'objet de stratégie de groupe.

Problèmes courants et conseils relatifs à la résolution des problèmes

Problème courant	Conseil relatif à la résolution des problèmes
Une stratégie récemment modifiée n'est pas encore appliquée.	Exécutez **gpupdate /force** à partir d'une ligne de commande ou **Invoke-GPUpdate –force** dans Windows PowerShell.
Le filtrage de sécurité ne fonctionne pas comme prévu.	Dans la Console GPMC, sous l'onglet **Délégations**, cliquez sur **Avancé**. Dans la boîte de dialogue **Sécurité**, cliquez sur **Avancé** de nouveau. Dans la boîte de dialogue **Sécurité avancée**, sous l'onglet **Autorisations effectives**, résolvez les problèmes d'autorisation de sécurité des utilisateurs indiqués.

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

Atelier pratique A : Conception et implémentation d'une stratégie d'objet de stratégie de groupe

Questions et réponses

Question : Quelle conception d'objets de stratégie de groupe avez-vous suggérée ?

Réponse : Les réponses varient. Selon le temps dont vous disposez, incitez les stagiaires à discuter de leur conception d'objets de stratégie de groupe.

Question : Vous avez utilisé des autorisations **Refuser** pour garantir que certains objets de stratégie de groupe ne s'appliquent pas aux administrateurs informatiques. Existe-t-il d'autres méthodes permettant de répondre à la même exigence ?

Réponse : Il convient d'implémenter les autorisations **Refuser** avec prudence, car elles sont toujours prioritaires sur les autorisations **Autoriser** et peuvent conduire à des résultats non désirés. Toutefois, le refus de certains objets de stratégie de groupe pour les administrateurs est un scénario classique et valide. La seule autre voie possible pour atteindre cet objectif est d'appliquer la stratégie à chaque autre groupe de service, puis de supprimer le groupe Utilisateurs authentifiés. Cela peut comporter des risques pour les utilisateurs qui ne sont pas encore affectés à leur groupe de service ou pour tout nouveau groupe de service que vous ajoutez ultérieurement mais que vous oubliez d'ajouter à la stratégie.

Module 8

Conception et implémentation d'une topologie de services de domaine Active Directory

Table des matières :

Leçon 1

Conception et implémentation des sites AD DS

Table des matières :

Démonstration

Démonstration : Création d'objets de site

Procédure de démonstration

Créer un nouveau site AD DS

1. Basculez vers LON-DC1, puis connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Sites et services Active Directory**.
3. Dans la console Sites et services Active Directory, développez **Sites**, puis cliquez sur **Default-First-Site-Name**.
4. Cliquez avec le bouton droit sur **Default-First-Site-Name**, puis cliquez sur **Renommer**.
5. Tapez **LondonHQ**, puis appuyez sur Entrée.
6. Dans le volet de navigation, cliquez avec le bouton droit sur **Sites**, puis cliquez sur **Nouveau site**.
7. Dans la boîte de dialogue **Nouvel objet – Site** , dans la zone de texte **Nom**, tapez **Paris**.
8. Sélectionnez **DEFAULTIPSITELINK**, puis cliquez sur **OK**.
9. Dans la boîte de dialogue **Services de domaine Active Directory**, cliquez sur **OK**.

Créer un nouveau sous-réseau AD DS

1. Dans le volet de navigation, cliquez avec le bouton droit sur **Subnets**, puis cliquez sur **Nouveau sous-réseau**.
2. Dans la boîte de dialogue **Nouvel objet – Sous-réseau**, dans la zone de texte **Préfixe**, tapez **172.16.0.0/24**.
3. Sous **Sélectionnez un objet du site pour ce préfixe**, cliquez sur **LondonHQ**, puis cliquez sur **OK**.
4. Dans le volet de navigation, cliquez avec le bouton droit sur **Subnets**, puis cliquez sur **Nouveau sous-réseau**.
5. Dans la boîte de dialogue **Nouvel objet – Sous-réseau**, dans la zone de texte **Préfixe**, tapez **172.16.1.0/24**.
6. Sous **Sélectionnez un objet du site pour ce préfixe**, cliquez sur **Paris**, puis cliquez sur **OK**.

Contrôle des acquis et éléments à retenir

Question(s) de contrôle des acquis

Question : Dans une entreprise multisite, pourquoi est-il important d'identifier et d'associer tous les sous-réseaux à un site ?

Réponse : Vous pouvez 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 l'adresse IP de l'ordinateur client et en fonction de la définition des sous-réseaux. Si un ordinateur client a une adresse IP qui n'appartient pas à un site, l'ordinateur client lance une requête pour tous les contrôleurs de domaine dans le domaine, qui n'est pas efficace du temps. En fait, un ordinateur client unique peut effectuer des actions sur les contrôleurs de domaine de différents sites. Si ces modifications ne sont pas encore répliquées, cela peut produire des résultats indésirables. Il est important que chaque ordinateur client sache dans quel site il réside. Pour cela, vérifiez que les contrôleurs de domaine peuvent identifier les ordinateurs clients par site.

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

Réponse : Le serveur tête de pont est responsable de toute la réplication dans le site et en dehors pour une partition. Au lieu de répliquer tous les contrôleurs de domaine d'un site avec tous les contrôleurs de domaine dans un autre site, les serveurs tête de pont gèrent la réplication intersite.

Question : Quel protocole pouvez-vous utiliser comme alternative à la réplication Active Directory ? Quel est l'inconvénient lié à son utilisation ?

Réponse : Vous pouvez utiliser le protocole SMTP, mais il ne permet pas de répliquer une partition de domaine.

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

Atelier pratique A : Conception et implémentation d'une topologie physique de services de domaine Active Directory

Questions et réponses

Question : Quelle démarche avez-vous adoptée pour la conception de site Active Directory et sa réplication ?

Réponse : Les réponses varient.

Question : Comment avez-vous abordé l'exercice de planification de contrôleur de domaine Active Directory ?

Réponse : Les réponses varient.

Question : Comment cette conception des services AD DS physiques est-elle comparable à l'implémentation d'AD DS de votre organisation ?

Réponse : Les réponses varient.

Module 9

Planification et implémentation du stockage

Table des matières :

Leçon 2

Planification et implémentation des réseaux SAN iSCSI

Table des matières :

Documentation supplémentaire

Serveur cible iSCSI et initiateur iSCSI

Documentation supplémentaire: Pour plus d'informations sur l'introduction de cibles iSCSI dans Windows Server 2012, consultez http://go.microsoft.com/fwlink/?linkid=279916.

Démonstration

Démonstration : Implémentation d'iSCSI

Procédure de démonstration

Ajouter le service de rôle de serveur cible iSCSI

1. Dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
2. Dans l'Assistant Ajout de rôles et de fonctionnalités, dans la page **Avant de commencer**, cliquez sur **Suivant**.
3. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
5. Dans la page **Sélectionner des rôles de serveurs**, développez **Services de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, activez la case à cocher **Serveur cible iSCSI**, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
8. Une fois l'installation terminée, cliquez sur **Fermer**.
9. Lorsque vous êtes invité à redémarrer l'ordinateur, cliquez sur **Redémarrer maintenant**.
10. Connectez-vous à LON-DC1 avec le nom d'utilisateur **ADATUM\Administrateur** et le mot de passe **Pa$$w0rd**.

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, dans la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur **C:**, puis sur **Suivant**.

5. Dans la page **Indiquer le nom du disque dur virtuel iSCSI**, tapez **iSCSIDisk1**, puis cliquez sur **Suivant**.
6. Dans la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone **Taille**, tapez **5**, vérifiez que **Go** est sélectionné dans la zone de liste déroulante, puis cliquez sur **Suivant**.
7. Dans la page **Affecter la cible iSCSI**, cliquez sur **Nouvelle cible iSCSI**, puis sur **Suivant**.
8. Dans la page **Indiquer le nom de la cible**, dans la zone **Nom**, tapez **LON-SVR1**, puis cliquez sur **Suivant**.
9. Dans 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**, tapez **172.16.0.21**, puis cliquez sur **OK**.
11. Dans la page **Indiquer les serveurs d'accès**, cliquez sur **Suivant**.
12. Dans la page **Activer l'authentification**, cliquez sur **Suivant**.
13. Dans la page **Confirmer les sélections**, cliquez sur **Créer**.
14. Dans 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 liste déroulante **TÂCHES**, cliquez sur **Nouveau disque virtuel iSCSI**.
16. Dans l'Assistant Nouveau disque virtuel iSCSI, dans la page **Sélectionner l'emplacement du disque virtuel iSCSI**, sous **Emplacement de stockage**, cliquez sur **C:**, puis sur **Suivant**.
17. Dans la page **Indiquer le nom du disque dur virtuel iSCSI**, tapez **iSCSIDisk2**, puis cliquez sur **Suivant**.
18. Dans la page **Indiquer la taille du disque dur virtuel iSCSI**, dans la zone **Taille**, tapez **5**, vérifiez que **Go** est sélectionné dans la zone de liste déroulante, puis cliquez sur **Suivant**.
19. Dans la page **Affecter la cible iSCSI**, cliquez sur **lon-svr1**, puis sur **Suivant**.
20. Dans la page **Confirmer les sélections**, cliquez sur **Créer**.
21. Dans la page **Afficher les résultats**, attendez que la création soit terminée, puis cliquez sur **Fermer**.

Se connecter à la cible iSCSI

1. Sur LON-SVR1, 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 **Cible**, tapez **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-dc1-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-SVR1, dans le Gestionnaire de serveur, dans le menu **Outils**, cliquez sur **Gestion de l'ordinateur**.
2. Dans la console Gestion de l'ordinateur, sous le nœud **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.

Contrôle des acquis et éléments à retenir

Question(s) de contrôle des acquis

Question : Tailspin Toys doit décider comment implémenter divers aspects de son infrastructure de stockage. La société devra stocker les fichiers partagés dans un emplacement central, mais ils ne souhaitent pas implémenter un serveur de fichiers complet pour le moment. Quel type de stockage recommanderiez-vous ?

Réponse : Les réponses varieront, mais peuvent comprendre des solutions de stockage NAS ou SAN.

Question : Tailspin Toys envisage d'implémenter plusieurs serveurs de base de données et souhaite fournir de l'espace disque pour les bases de données. La société préfèrerait créer une baie de disques unique et gérée de manière centralisée pour toutes les bases de données. Quel type de stockage recommanderiez-vous ?

Réponse : Les réponses varieront, mais peuvent comprendre des solutions de stockage NAS ou SAN.

Question : Quels sont les principaux avantages d'une solution de stockage SAN par rapport à une solution de stockage DAS ?

Réponse : Les principaux avantages d'une solution de stockage SAN sont les suivants : elle est hautement efficace au niveau du partage des ressources, offre une meilleure utilisation du stockage et fournit une disponibilité et une consolidation du matériel.

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

Atelier pratique A : Planification et implémentation du stockage

Questions et réponses

Question : Pour quelle approche avez-vous opté pour l'exercice de planification du stockage ?

Réponse : Les réponses varient.

Question : Comment votre organisation implémente-t-elle le stockage ?

Réponse : Les réponses varient.

Module 10

Planification et implémentation des services de fichiers

Table des matières :

Leçon 1

Planification et implémentation du système de fichiers DFS

Table des matières :

Démonstration

Démonstration : Déploiement et configuration du système de fichiers DFS

Procédure de démonstration

Installer le rôle DFS

1. Sur LON-SVR1, 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, cliquez sur **Suivant**.
3. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner des rôles de serveurs**, développez **Services de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, puis activez la case à cocher **Espaces de noms DFS**.
6. Dans la fenêtre contextuelle Ajouter des rôles et fonctionnalités, cliquez sur **Ajouter des fonctionnalités**.
7. Activez la case à cocher **Réplication DFS**, puis cliquez sur **Suivant**.
8. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Une fois l'installation terminée, cliquez sur **Fermer**.

Créer un espace de noms

1. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion du système de fichiers distribués DFS**.
2. Dans la console Gestion du système de fichiers distribués DFS, cliquez sur **Espaces de noms**.
3. Cliquez avec le bouton droit sur **Espaces de noms**, puis cliquez sur **Nouvel espace de noms**.
4. Dans l'Assistant Nouvel espace de noms, dans la page **Serveur d'espaces de noms**, sous **Serveur**, tapez **LON-SVR1**, puis cliquez sur **Suivant**.
5. Dans la page **Nom et paramètres de l'espace de noms**, sous **Nom**, tapez **Research**, puis cliquez sur **Suivant**.
6. Dans la page **Type d'espace de noms**, assurez-vous que **Espace de noms de domaine** et **Activer le mode Windows Server 2008** sont sélectionnés, puis cliquez sur **Suivant**.
7. Dans la page **Revoir les paramètres et créer l'espace de noms**, cliquez sur **Créer**.
8. Dans la page **Confirmation**, vérifiez que la tâche de création de l'espace de noms a réussi, puis cliquez sur **Fermer**.
9. Dans la console, développez le nœud **Espace de noms**, puis cliquez sur **\\Adatum.com\Research**. Présentez les quatre onglets du volet d'informations aux stagiaires.
10. Dans la console, cliquez avec le bouton droit sur **\\Adatum.com\Research**, puis cliquez sur **Propriétés**. Vérifiez les options des onglets **Général**, **Références** et **Avancée**.
11. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : \\Adatum.com\Research**.

Créer un dossier et une cible de dossier

1. Sur LON-SVR1, dans la console Gestion du système de fichiers distribués DFS, cliquez avec le bouton droit sur **\\Adatum.com\Research**, puis cliquez sur **Nouveau dossier**.
2. Dans la boîte de dialogue **Nouveau dossier**, dans la zone **Nom**, tapez **Proposals**.
3. Dans la boîte de dialogue **Nouveau dossier**, sous **Cibles de dossier**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Ajouter une cible de dossier**, tapez **\\LON-SVR1\Proposal_docs**, puis cliquez sur **OK**.
5. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
6. Dans la boîte de dialogue **Créer un partage**, configurez les paramètres suivants, puis cliquez sur **OK**.
    i. Chemin d'accès local du dossier partagé : **C:\Proposal_docs**
    ii. Chemin d'accès local du dossier partagé : **Les administrateurs ont un accès total, les autres ont un accès en lecture/écriture**
7. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
8. Cliquez sur **OK** pour fermer la boîte de dialogue **Nouveau dossier**.
9. Dans la console, développez **\\Adatum.com\Research**, puis cliquez sur **Proposals**. Remarquez qu'actuellement, il n'existe qu'une seule cible de dossier. (Pour fournir la redondance, vous devez ajouter une deuxième cible de dossier avec la **réplication DFS** configurée.)
10. Pour tester l'espace de noms, cliquez sur l'icône de l'Explorateur de fichiers dans la barre des tâches.
11. Dans la barre d'adresses de l'Explorateur de fichiers, tapez **\\Adatum.com\Research**, puis appuyez sur Entrée. Le dossier Proposals s'affiche.

Créer une cible de dossier pour la réplication

1. Basculez vers LON-DC1.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Basculez vers le Gestionnaire de serveur.
4. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
5. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
6. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
7. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
8. Dans la page **Sélectionner des rôles de serveurs**, développez **Services de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, puis activez la case à cocher **Espaces de noms DFS**.
9. Dans la boîte de dialogue Ajouter des rôles et fonctionnalités, cliquez sur **Ajouter des fonctionnalités**.
10. Activez la case à cocher **Réplication DFS**, puis cliquez sur **Suivant**.
11. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.

12. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
13. Une fois l'installation terminée, cliquez sur **Fermer**.
14. Fermez le Gestionnaire de serveur.
15. Basculez vers LON-SVR1.
16. Dans Gestion du système de fichiers distribués DFS, cliquez avec le bouton droit sur le dossier **Proposals**, puis cliquez sur **Ajouter une cible de dossier**.
17. Dans la boîte de dialogue **Nouvelle cible de dossier**, tapez **\\LON-DC1\Proposal_docs**, puis cliquez sur **OK**.
18. Pour créer le dossier partagé, dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
19. Dans la boîte de dialogue **Créer un partage**, dans le champ **Chemin d'accès local du dossier partagé**, tapez **C:\Proposal_docs**.
20. Dans le champ **Autorisations du dossier partagé**, sélectionnez **Les administrateurs ont un accès total, les autres ont un accès en lecture/écriture**, puis cliquez sur **OK**.
21. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
22. Dans la boîte de dialogue **Réplication**, cliquez sur **Oui**. L'Assistant Réplication de dossier démarre.

Créer un groupe de réplication

1. Dans l'Assistant Réplication de dossier, dans la page **Nom du groupe de réplication et du dossier répliqué**, acceptez les paramètres par défaut, puis cliquez sur **Suivant**.
2. Dans la page **Éligibilité de réplication**, notez que **LON-DC1** et **LON-SVR1** sont tous deux éligibles comme membres de la réplication DFS, puis cliquez sur **Suivant**.
3. Dans la page **Membre principal**, sélectionnez **LON-SVR1** comme membre principal, puis cliquez sur **Suivant**.
4. Dans la page **Sélection de topologie**, laissez la sélection par défaut **Maille pleine**. (Cette option répliquera toutes les données entre tous les membres du groupe de réplication.)
5. Après vérification de toutes les sélections, cliquez sur **Suivant**.
6. Dans la page **Planification du groupe de réplication et bande passante**, laissez la sélection par défaut **Répliquer en continu à l'aide de la bande passante spécifiée**, puis configurez le paramètre pour utiliser la **complète bande passante**. Notez que vous pouvez également choisir une planification spécifique pour effectuer la réplication au cours des jours et des heures spécifiés.
7. Cliquez sur **Suivant**.
8. Dans la page **Vérifier les paramètres et créer le groupe de réplication**, cliquez sur **Créer**.
9. Dans la page **Confirmation**, vérifiez que toutes les tâches ont réussi, puis cliquez sur **Fermer**. Notez l'avertissement Délai de réplication, puis cliquez sur **OK**.
10. Dans la console, développez **Réplication**.
11. Sous **Réplication**, cliquez sur **adatum.com\research\proposals**.
12. Cliquez et examinez chacun des onglets dans le volet de détails.

Leçon 2

Planification et implémentation de BranchCache

Table des matières :

Questions et réponses

Discussion : Réplication DFS ou BranchCache ?

Question : Vous devez fournir un mécanisme pour permettre aux utilisateurs dans les succursales de votre organisation d'avoir un accès plus rapide aux fichiers stockés sur les serveurs du siège. Certaines des succursales disposent de serveurs de fichiers, et d'autres pas. Les succursales disposent d'une combinaison de systèmes d'exploitation clients, notamment Windows 7 et Windows 8. Est-il préférable d'implémenter la réplication DFS ou la fonctionnalité BranchCache ? Pourquoi ?

Réponse : Vous devez implémenter BranchCache. car sa principale fonction est de fournir un accès plus rapide aux fichiers distants pour les utilisateurs des succursales via la mise en cache. L'absence de serveurs de fichiers pose un problème pour implémenter la réplication DFS.

Question : Votre service commercial utilise des fichiers dans ses bureaux de vente distants. Ces fichiers doivent être regroupés dans un emplacement unique à la fin de chaque jour. Les utilisateurs du service commercial utilisent des ordinateurs portables Windows 7 ou Windows 8. Quelle technologie, réplication DFS ou BranchCache, est la mieux adaptée pour ce scénario ?

Réponse : La réplication DFS est plus appropriée. Cependant, elle requiert un serveur de fichiers dans chaque succursale. La fonctionnalité BranchCache ne convient pas, car elle ne regroupe pas les fichiers dans un emplacement central.

Démonstration

Démonstration : Implémentation de la fonctionnalité BranchCache

Procédure de démonstration

Ajouter BranchCache pour le service de rôle Fichiers réseau

1. Basculez vers LON-DC1 et, si nécessaire, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Dans la barre des tâches, cliquez sur **Gestionnaire de serveur**.
3. Dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
4. Dans l'Assistant Ajout de rôles et de fonctionnalités, dans la page **Avant de commencer**, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné, puis cliquez sur **Suivant**.
7. Dans la page **Sélectionner des rôles de serveurs**, développez **Services de fichiers et de stockage (Installé)**, développez **Services de fichiers et iSCSI (Installé)**, activez la case à cocher **BranchCache pour fichiers réseau**, puis cliquez sur **Suivant**.
8. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Une fois l'installation terminée, cliquez sur **Fermer**.

Configurer BranchCache dans l'Éditeur de stratégie de groupe locale

1. Sur LON-DC1, suspendez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
2. Sur l'écran d'accueil, tapez **gpedit.msc**, puis appuyez sur Entrée.
3. Développez **Configuration ordinateur**, développez **Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local**, développez **Réseau**, cliquez sur **Serveur Lanman**, puis 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**, cliquez sur **Autoriser la publication de hachages uniquement pour les dossiers partagés dans lesquels BranchCache est activé**, puis 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 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**, tapez **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 actives.

Leçon 3

Planification et implémentation du contrôle d'accès dynamique

Table des matières :

Démonstration

Démonstration : Création de règles et de stratégies d'accès centralisées pour le contrôle d'accès dynamique

Procédure de démonstration

1. Sur LON-DC1, dans la barre des tâches, cliquez sur **Gestionnaire de serveur**.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory**.
3. Dans la console Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**.
4. Double-cliquez sur **Claim Types**.
5. Dans le volet des tâches, cliquez sur **Nouveau**, puis sur **Type de revendication**.
6. Dans la fenêtre Créer Type de revendication de la section Attribut source, cliquez sur l'attribut **department**.
7. Dans la zone de texte **Nom complet**, tapez **Service de société**.
8. Activez les cases à cocher **Utilisateur** et **Ordinateur**, puis cliquez sur **OK**.
9. Dans le volet des tâches, cliquez sur **Nouveau**, puis sur **Type de revendication**.
10. Dans la fenêtre Créer Type de revendication, dans la section Attribut source, cliquez sur l'attribut **employeetype**.
11. Dans la zone de texte **Nom complet**, tapez le **Type d'employé**.
12. Activez les cases à cocher **Utilisateur** et **Ordinateur**, puis cliquez sur **OK**.
13. Cliquez sur **Contrôle d'accès dynamique**.
14. Dans le volet central, double-cliquez sur **Resource Properties**.
15. Dans la liste **Resource Properties**, recherchez et cliquez avec le bouton droit sur **Department**, puis cliquez sur **Activer**.
16. Dans la console Centre d'administration Active Directory, dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**.
17. Double-cliquez sur **Central Access Rules**.
18. Dans le volet des tâches, cliquez sur **Nouveau**, puis sur **Règle d'accès central**.
19. Dans la boîte de dialogue **Créer Règle d'accès central**, dans la zone **Nom**, tapez **Correspondance de service**.
20. Dans la section Ressources cibles, cliquez sur **Modifier**.
21. Dans la fenêtre Règle d'accès central, cliquez sur **Ajouter une condition**.
22. Définissez une condition comme suit, puis cliquez sur OK :
Ressource-Department-Est égal à-Valeur-Research and Development.

23. Dans la section Autorisations, cliquez sur **Utiliser les autorisations suivantes en tant qu'autorisations actuelles**, puis cliquez sur **Modifier**.
24. Cliquez sur **Administrateurs (ADATUM\Administrateurs)**, puis sur **Supprimer**.
25. Dans les **Paramètres de sécurité avancés pour Autorisations**, cliquez sur **Ajouter**.
26. Dans la boîte de dialogue **Autorisations pour Autorisations**, cliquez sur **Sélectionnez un principal**.
27. Dans la boîte de dialogue **Sélectionnez un utilisateur, un ordinateur, un compte de service ou un groupe**, tapez **Utilisateurs authentifiés**, cliquez sur **Vérifier les noms**, puis sur **OK**.
28. Dans la section Autorisations de base, cliquez sur **Modification**, **Lecture et exécution**, **Lecture** et **Écriture**.
29. Cliquez sur **Ajouter une condition**.
30. Dans la liste déroulante **Groupe**, cliquez sur **Service de société**.
31. Dans la liste déroulante **Valeur**, cliquez sur **Ressource**.
32. Dans la dernière liste déroulante, cliquez sur **Department**.

 **Remarque :** En conséquence, vous devez avoir **Utilisateur-Service de société-Est égal à-Ressource-Department**.

33. Cliquez trois fois sur **OK**.
34. Dans la console Centre d'administration Active Directory, cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur **Central Access Policies**.
35. Dans le volet des tâches, cliquez sur **Nouveau**, puis sur **Stratégie d'accès central**.
36. Dans la zone **Nom**, tapez **Correspondance de service**, puis cliquez sur **Ajouter**.
37. Cliquez sur la règle **Correspondance de service**, puis sur l'icône **Autre** (>>).
38. Cliquez sur **OK** à deux reprises.

Contrôle des acquis et éléments à retenir

Question(s) de contrôle des acquis

Question : Quel est le principal avantage d'un espace de noms DFS basé sur un domaine ?

Réponse : Le principal avantage d'un espace de noms DFS basé sur un domaine est que vous pouvez assurer la tolérance de pannes de l'espace de noms sans devoir implémenter le clustering du rôle de services de fichiers.

Question : En quoi la fonctionnalité BranchCache diffère-t-elle du système de fichiers 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 aux autres utilisateurs, ce qui force le fichier à être à nouveau téléchargé via la liaison WAN. Par conséquent, vous utiliserez probablement le mode de cache hébergé lorsqu'un ordinateur qui exécute le système d'exploitation Windows Server 2012 est disponible dans la succursale.

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

Réponse : Une *revendication* désigne les informations qu'AD DS énonce au sujet d'un objet spécifique, généralement un utilisateur ou un ordinateur. Les revendications fournissent des informations provenant d'une source sûre au sujet d'une entité.

Question : Quel est le rôle d'une stratégie d'accès centralisée ?

Réponse : Une stratégie d'accès centralisée permet aux administrateurs de créer une stratégie qui est appliquée à un ou plusieurs serveurs de fichiers d'une entreprise. Une stratégie d'accès centralisée contient un ou plusieurs règles de stratégie d'accès centralisée. Chaque règle contient les paramètres qui déterminent l'applicabilité et les autorisations.

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

Atelier pratique A : Conception et implémentation des services de fichiers

Questions et réponses

Question : Pour quelle approche avez-vous opté lors de la conception de l'accès aux données ?

Réponse : Les réponses varient.

Question : Pour quelle approche avez-vous opté lors de la conception du contrôle d'accès dynamique ?

Réponse : Les réponses varient.

Question : Comment votre organisation implémente-elle l'accès aux données pour les succursales ?

Réponse : Les réponses varient.

Module 11

Conception et implémentation des services d'accès réseau

Table des matières :

Leçon 1

Conception et implémentation des services d'accès à distance

Table des matières :

Questions et réponses

Discussion : Conception de l'accès à distance

Question : Comment proposeriez-vous de prendre en charge le besoin des utilisateurs du service des ventes d'accéder à leur messagerie électronique ?

Réponse : Vous pouvez prendre en charge l'accès à la messagerie électronique à l'aide de tous les VPN existants, à condition de modifier toutes les stratégies réseau pour faciliter le trafic spécifique d'accès à la messagerie électronique. Exchange Server 2010 et Outlook 2010 prennent en charge les connexions qui utilisent RPC sur HTTPS. Cette méthode est un autre moyen pour les utilisateurs de communiquer avec leurs serveurs de messagerie. Elle présente certains avantages par rapport à l'utilisation de VPN, qui peut être donc conservé pour l'accès aux bases de données. Notamment, aucune modification de configuration n'est requise sur le pare-feu, et en outre, la façon dont les utilisateurs accèdent à leur messagerie électronique ne change pas lorsqu'ils se trouvent sur le réseau interne. Les utilisateurs n'ont pas besoin d'initialiser le VPN pour se connecter.

Question : De quels composants réseau supplémentaires avez-vous besoin pour prendre en charge votre conception, le cas échéant ?

Réponse : L'accès à distance à la messagerie électronique peut nécessiter des modifications de pare-feu, selon la solution choisie. En outre, il n'est pas recommandé de placer les serveurs de boîtes aux lettres dans un réseau de périmètre.

Question : Pour faciliter l'accès aux fichiers de base de données, quel type de tunnel VPN recommanderiez-vous ?

Réponse : Tous les types de clients prennent en charge le protocole SSTP, qui requiert la reconfiguration minimale du pare-feu. IKEv2 peut également être utilisé avec Windows 7 et Windows 8.

Demonstration

Démonstration : Implémentation d'un réseau privé virtuel (VPN)

Procédure de démonstration

Configurer un serveur VPN

1. Connectez-vous à LON-RTR en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Si besoin, cliquez sur l'icône **Gestionnaire de serveur** dans la barre des tâches.
3. Dans le volet d'informations, cliquez sur **Ajouter des rôles et des fonctionnalités**.
4. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
7. Dans la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services de stratégie et d'accès réseau**.
8. Cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant** à deux reprises.

9. Dans la page **Services de stratégie et d'accès réseau**, cliquez sur **Suivant**.
10. Dans la page **Sélectionner des services de rôle**, vérifiez que la case à cocher **Serveur NPS (Network Policy Server)** est activée, puis cliquez sur **Suivant**.
11. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
12. Vérifiez que l'installation a réussi, puis cliquez sur **Fermer**.
13. Fermez la fenêtre du Gestionnaire de serveur.
14. Positionnez le pointeur de la souris dans l'angle inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
15. Dans le menu **Accueil**, cliquez sur **Serveur NPS (Network Policy Server)**.
16. Dans le Gestionnaire de stratégies réseau, dans le volet de navigation, cliquez avec le bouton droit sur **NPS (local)**, puis cliquez sur **Inscrire un serveur dans Active Directory**.
17. Dans la boîte de message **Serveur NPS (Network Policy Server)**, cliquez sur **OK**.
18. Dans la boîte de dialogue **Serveur NPS (Network Policy Server)** suivante, cliquez sur **OK**.
19. Laissez la fenêtre de la console Serveur NPS ouverte.
20. Positionnez le pointeur de la souris dans l'angle inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
21. Dans Accueil, cliquez sur **Outils d'administration**, puis double-cliquez sur **Routage et accès distant**. Si l'Assistant Activation de DirectAccess s'ouvre, cliquez sur **Annuler**, puis sur **OK**.
22. Dans la console Routage et accès distant, cliquez avec le bouton droit sur **LON-RTR (local)**, puis cliquez sur **Désactiver le routage et l'accès à distance**.
23. Dans la boîte de dialogue, cliquez sur **Oui**.
24. Dans la console Routage et accès distant, cliquez avec le bouton droit sur **LON-RTR (local)**, puis cliquez sur **Configurer et activer le routage et l'accès à distance**.
25. Cliquez sur **Suivant**, sur **Accès à distance (connexion à distance ou VPN)**, puis sur **Suivant**.
26. Activez la case à cocher **VPN**, puis cliquez sur **Suivant**.
27. Cliquez sur l'interface réseau **Connexion au réseau local 2**, désactivez la case à cocher **Sécuriser l'interface sélectionnée en configurant des filtres de paquet statiques**, puis cliquez sur **Suivant**.
28. Dans la page **Attribution d'adresses IP**, cliquez sur **À partir d'une plage d'adresses spécifiée**, puis cliquez sur **Suivant**.
29. Dans la page **Assignation de plages d'adresses**, cliquez sur **Nouveau**. Dans le champ **Adresse IP de début**, tapez **172.16.0.100**, dans le champ **Adresse IP de fin**, tapez **172.16.0.110**, puis cliquez sur **OK**.
30. Vérifiez que 11 adresses IP ont été attribuées aux clients distants, puis cliquez sur **Suivant**.
31. Dans la page **Gestion de serveurs d'accès à distance multiples**, cliquez sur **Suivant**.
32. Cliquez sur **Terminer**.
33. Dans la boîte de dialogue **Routage et accès distant**, cliquez sur **OK**.
34. Si vous y êtes invité, cliquez une nouvelle fois sur **OK**.

Configurer un client VPN

1. Basculez vers LON-CL2.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans Démarrer, tapez **Panneau**.
4. Dans la liste **Applications**, cliquez sur **Panneau de configuration**.
5. Dans Panneau de configuration, cliquez sur **Réseau et Internet**, sur **Centre Réseau et partage**, puis sur **Configurer une nouvelle connexion ou un nouveau réseau**.
6. Dans la page **Choisir une option de connexion**, cliquez sur **Connexion à votre espace de travail**, puis sur **Suivant**.
7. Dans la page **Comment voulez-vous vous connecter ?**, cliquez sur **Utiliser ma connexion Internet (VPN)**.
8. Cliquez sur **Je configurerai une connexion Internet ultérieurement**.
9. Dans la page **Entrez l'adresse Internet à laquelle vous souhaitez vous connecter**, dans la zone **Adresse Internet**, tapez **10.10.0.1**.
10. Dans la zone **Nom de la destination**, tapez **VPN Adatum**.
11. Activez la case à cocher **Autoriser d'autres personnes à utiliser cette connexion**, puis cliquez sur **Créer**.
12. Dans la fenêtre Centre Réseau et partage, cliquez sur **Modifier les paramètres de la carte**.
13. Cliquez avec le bouton droit sur la connexion **VPN Adatum**, cliquez sur **Propriétés**, puis cliquez sur l'onglet **Sécurité**.
14. Dans l'onglet **Sécurité**, dans la liste **Type de réseau VPN**, cliquez sur **Protocole PPTP (Point to Point Tunneling Protocol)**.
15. Sous Authentification, cliquez sur **Autoriser ces protocoles**, puis cliquez sur **OK**.
16. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur la connexion **VPN Adatum**, puis cliquez sur **Connecter/Déconnecter**.
17. Dans la liste **Réseaux** de droite, cliquez sur **VPN Adatum**, puis sur **Connexion**.
18. Dans Authentification réseau, dans la zone de texte **Nom d'utilisateur**, tapez **ADATUM\Administrateur**.
19. Dans la zone de texte **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **OK**.
20. Attendez que la connexion VPN soit établie. Votre connexion échoue. Vous recevez une erreur 812 relative aux problèmes d'authentification.
21. Cliquez sur **Fermer**.

Créer une stratégie VPN basée sur la condition Groupes Windows

1. Basculez vers LON-RTR.
2. Basculez vers **Serveur NPS (Network Policy Server)**.

3. Dans Serveur NPS (Network Policy Server), développez **Stratégies**, puis cliquez sur **Stratégies réseau**.
4. Dans le volet d'informations, cliquez avec le bouton droit sur la première stratégie de la liste, puis cliquez sur **Désactiver**.
5. Dans le volet d'informations, cliquez avec le bouton droit sur la dernière stratégie de la liste, puis cliquez sur **Désactiver**.
6. Dans le volet de navigation, cliquez avec le bouton droit sur **Stratégies réseau**, puis cliquez sur **Nouveau**.
7. Dans l'Assistant Nouvelle stratégie réseau, dans la zone de texte **Nom de la stratégie**, tapez **Stratégie VPN Adatum**.
8. Dans la liste **Type de serveur d'accès réseau**, cliquez sur **Serveur d'accès à distance (VPN-Dial up)**, puis sur **Suivant**.
9. Dans la page **Spécifier les conditions**, cliquez sur **Ajouter**.
10. Dans la boîte de dialogue **Sélectionner une condition**, cliquez sur **Groupes Windows**, puis cliquez sur **Ajouter**.
11. Dans la boîte de dialogue **Groupes Windows**, cliquez sur **Ajouter des groupes**.
12. Dans la boîte de dialogue **Sélectionnez un groupe**, dans la zone de texte **Entrez le nom de l'objet à sélectionner (exemples)**, tapez **Admins du domaine**, puis cliquez sur **OK**.
13. Cliquez une nouvelle fois sur **OK**, puis cliquez sur **Suivant**.
14. Dans la page **Spécifier l'autorisation d'accès**, cliquez sur **Accès accordé**, puis sur **Suivant**.
15. Dans la page **Configurer les méthodes d'authentification**, cliquez sur **Suivant**.
16. Dans la page **Configurer des contraintes**, cliquez sur **Suivant**.
17. Dans la page **Configurer les paramètres**, cliquez sur **Suivant**.
18. Dans la page **Fin de la configuration de la nouvelle stratégie réseau**, cliquez sur **Terminer**.

Tester le VPN

1. Basculez vers LON-CL2.
2. Dans la liste **Réseaux** de droite, cliquez sur **VPN Adatum**, puis sur **Connexion**.
3. Dans Authentification réseau, dans la zone de texte **Nom d'utilisateur**, tapez **ADATUM\Administrateur**.
4. Dans la zone de texte **Mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **OK**.
5. Attendez que la connexion VPN soit établie.

Leçon 2

Conception de l'authentification RADIUS à l'aide de NPS

Table des matières :

Questions et réponses

Discussion : Conception d'une implémentation RADIUS

Question : Il existe trois serveurs VPN sur le réseau de périmètre pour fournir une capacité suffisante aux connexions d'accès à distance entrantes. Comment pouvez-vous simplifier la gestion et l'application de la stratégie réseau ?

Réponse : Vous devez envisager de déployer le rôle NPS et configurer ce serveur en tant que serveur RADIUS. Vous devez ensuite configurer les serveurs VPN qui exécutent RRAS en tant que clients RADIUS. Enfin, vous devez configurer des stratégies réseau sur le serveur NPS.

Question : Pouvez-vous fournir l'accès à la messagerie électronique à tous les utilisateurs sans avoir besoin de VPN ?

Réponse : Oui, techniquement, vous pouvez implémenter RPC sur HTTPS. Toutefois, avec les besoins des utilisateurs d'accéder à d'autres ressources, l'utilisation de VPN semble inévitable. Par conséquent, d'un point de vue pratique, vous aurez probablement besoin des VPN pour d'autres types d'accès. Sachant que les utilisateurs utilisent leurs ordinateurs personnels, la configuration n'est pas fixe (et les ordinateurs sont non gérés). Par conséquent, une solution VPN semble logique.

Question : Comment vos stratégies réseau changent-elles suite à l'ajout de la prise en charge permettant à tous les utilisateurs de se connecter à distance ?

Réponse : Vous devez configurer sur le serveur RADIUS des stratégies réseau supplémentaires qui identifient les utilisateurs spécifiques, puis filtrer ce à quoi ils peuvent accéder. Vous pouvez avoir besoin d'une stratégie différente pour chaque service. Pour ce faire, vous devez procéder à une analyse des besoins pour déterminer les ressources auxquelles les services ont besoin d'accéder. Il est important de vérifier que les stratégies réseau sont configurées dans l'ordre de traitement approprié.

Question : Quel type de VPN est suggéré ?

Réponse : SSTP ou IKEv2 serait approprié aux solutions VPN.

Question : Une stratégie de demande de connexion est-elle requise ?

Réponse : Un seul serveur RADIUS s'exécute. Par conséquent, des stratégies de demande de connexion ne sont pas requises. Les stratégies de demande de connexion sont des ensembles de conditions et de paramètres qui désignent les serveurs RADIUS qui authentifient et autorisent les demandes de connexion que le serveur NPS reçoit des clients RADIUS.

Question : Un proxy RADIUS est-il requis ?

Réponse : Là encore, il n'y a qu'un serveur RADIUS. Lorsque vous utilisez le serveur NPS en tant que proxy RADIUS, vous devez configurer des stratégies de demande de connexion. Ces stratégies spécifient, d'une part, les demandes de connexion transmises par le serveur NPS à d'autres serveurs RADIUS et, d'autre part, les serveurs RADIUS auxquels vous souhaitez transmettre les demandes de connexion. Vous pouvez également configurer le serveur NPS pour qu'il transmette les données de comptes à un ou plusieurs ordinateurs dans un groupe de serveurs RADIUS distants à des fins de journalisation. Dans ce scénario, un proxy RADIUS n'est pas requis.

Leçon 3

Conception d'un réseau de périmètre

Table des matières :

Questions et réponses

Discussion : Conception de la connectivité Internet

Question : Quel est le problème de la configuration actuelle ?

Réponse : Le réseau de périmètre ne devrait pas avoir de contrôleur de domaine, car il n'est pas sécurisé. Si vous avez besoin des services d'annuaire, envisagez d'implémenter un serveur AD LDS, puis configurez la réplication du sous-ensemble de données AD DS requis vers le serveur AD LDS. Par exemple, pour prendre en charge les services Edge Exchange Server 2010, vous pouvez déployer un serveur AD LDS sur le périmètre pour prendre en charge le rôle serveur de transport Edge Exchange. En outre, vous devez déplacer le serveur RADIUS dans le réseau privé pour assurer la sécurité supplémentaire. Vous pouvez configurer les clients RADIUS (les serveurs VPN) pour une connexion au serveur RADIUS à l'aide des caractéristiques du trafic définies, que vous pouvez configurer sur le pare-feu interne.

Question : Pour prendre en charge les communications par courrier électronique sortantes, quels serveurs supplémentaires devez-vous déployer sur le périmètre, le cas échéant ?

Réponse : Il est recommandé d'implémenter un serveur Edge (ou tout autre relais SMTP) sur le périmètre du réseau pour améliorer l'hygiène des messages. Toutefois, vous devez modifier le pare-feu interne pour prendre en charge le trafic spécifique utilisé dans ce scénario.

Question : Pour prendre en charge l'infrastructure VPN conçue précédemment, quelles modifications devez-vous apporter au pare-feu ?

Réponse : Northwind Traders souhaite implémenter les VPN L2TP/IPsec et SSTP. Les VPN SSTP utilisent le port TCP 443 pour toutes les communications. Ceci est généralement déjà autorisé via les pare-feu. Cependant, vous devez modifier le pare-feu pour prendre en charge le trafic L2TP à partir d'Internet. Pour les deux types de VPN, vous devez modifier le pare-feu interne pour permettre le type de trafic prévu.

Leçon 4

Planification et implémentation de DirectAccess

Table des matières :

Démonstration

Démonstration : Configuration d'un serveur DirectAccess avec l'Assistant Mise en route

Procédure de démonstration

Créer un groupe de sécurité dans Active Directory pour les ordinateurs clients DirectAccess

1. Sur LON-DC1, la console du Gestionnaire de serveur doit s'ouvrir automatiquement. Dans la console du Gestionnaire de serveur , dans le coin supérieur droit, cliquez sur **Outils**, puis cliquez sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur **Adatum.com**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
3. Dans la fenêtre Nouvel Objet – Unité d'organisation , dans la zone **Nom**, tapez **DA_Clients OU**, puis cliquez sur **OK**.
4. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, développez **Adatum.com**, cliquez avec le bouton droit sur **DA_Clients OU**, cliquez sur **Nouveau**, puis cliquez sur **Groupe**.
5. Dans la boîte de dialogue **Nouvel objet – Groupe**, dans la zone **Nom du groupe**, tapez **DA_Clients**.
6. Sous **Étendue du groupe**, vérifiez que **Globale** est sélectionné, et sous **Type de groupe**, vérifiez que **Sécurité** est sélectionné, puis cliquez sur **OK**.
7. Dans le volet d'informations, cliquez avec le bouton droit sur **DA_Clients**, puis cliquez sur **Propriétés**.
8. Dans la boîte de dialogue **Propriétés de : DA_Clients**, cliquez sur l'onglet **Membres**, puis cliquez sur **Ajouter**.
9. Dans la boîte de dialogue **Sélectionnez des utilisateurs, des contacts, des ordinateurs, des comptes de service ou des groupes**, cliquez sur **Types d'objets**, activez la case à cocher **des ordinateurs**, puis cliquez sur **OK**.
10. Dans la zone **Entrez les noms des objets à sélectionner (exemples)** , tapez **LON-CL1**, puis cliquez sur **OK**.
11. Vérifiez que **LON-CL1** s'affiche correctement sous **Membres**, puis cliquez sur **OK**.
12. Fermez la console Utilisateurs et ordinateurs Active Directory.

Configurer DirectAccess

1. Basculez vers LON-RTR.
2. Suspendez votre pointeur de la souris dans le coin inférieur gauche de l'affichage, puis cliquez sur **Accueil**.
3. Cliquez sur **Panneau de configuration**.
4. Dans le Panneau de configuration, cliquez sur **Réseau et Internet**.
5. Dans Réseau et Internet, cliquez sur **Centre Réseau et partage**.

6. Dans Centre Réseau et partage, cliquez sur **Modifier les paramètres de la carte**.
7. Cliquez avec le bouton droit sur **Connexion au réseau local 2**, puis cliquez sur **Propriétés**.
8. Dans la boîte de dialogue **Propriétés de Connexion au réseau local 2**, double-cliquez sur **Protocole Internet version 4 (TCP/IPv4)**.
9. Dans la zone **Adresse IP**, tapez **131.107.0.21**.
10. Dans la zone **Masque de sous-réseau**, tapez **255.255.0.0**, puis cliquez sur **OK**.
11. Dans la boîte de dialogue **Propriétés de Connexion au réseau local 2**, cliquez sur **OK**.
12. Suspendez votre pointeur de la souris dans le coin inférieur droit de l'écran, puis cliquez sur **Paramètres**, cliquez sur **Marche/Arrêt**, puis sur **Redémarrer**.
13. Cliquez sur **Continuer**.
14. Lorsque le serveur est redémarré, connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
15. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de l'accès à distance**.
16. Dans la console Gestion de l'accès à distance, cliquez sur **Exécuter l'Assistant Mise en route**.
17. Dans la page **Configuration de l'accès distant**, cliquez sur **Déployer DirectAccess uniquement**.
18. Vérifiez que **Périmètre** est sélectionné, puis dans **Tapez le nom public ou l'adresse IPv4 utilisée par les clients pour se connecter au serveur d'accès à distance**, tapez **131.107.0.21**, puis cliquez sur **Suivant**.
19. Dans la page de l'**Assistant Prise en main**, cliquez sur le lien **ici**.
20. Dans la page **Vérification de l'accès DirectAccess**, à côté de **Clients distants**, cliquez sur le lien **Modifier**.
21. Cliquez sur **Ordinateurs du domaine (ADATUM\Ordinateurs du domaine)**, puis cliquez sur **Supprimer**.
22. Cliquez sur **Ajouter**, dans la zone, tapez **DA_Clients**, puis cliquez sur **OK**.
23. Désactivez la case à cocher **Activer DirectAccess pour les ordinateurs portables uniquement**, puis cliquez sur **Suivant**.
24. Dans l'Assistant Connectivité réseau, cliquez sur **Terminer**.
25. Dans la page **Vérification de l'accès DirectAccess**, cliquez sur **OK**.
26. Dans Configurer l'accès à distance, cliquez sur **Terminer** pour fermer l'Assistant DirectAccess.
27. Dans la zone **Application des paramètres de l'Assistant Mise en route**, cliquez sur **Fermer**.

Contrôle des acquis et éléments à retenir

Question(s) de contrôle des acquis

Question : Quel type de stratégie pouvez-vous appliquer pour déterminer si une tentative de connexion réseau sera réussie ?

Réponse : Vous pouvez utiliser une stratégie réseau, mais pas une stratégie de demande de connexion.

Question : Lors de la configuration d'ordinateurs privés pour permettre un accès à la messagerie de l'entreprise, laquelle des propositions suivantes constitue généralement la meilleure démarche : RPC sur HTTPS, ou un VPN ?

Réponse : Dans ce scénario, un VPN constitue la meilleure méthode, car chaque ordinateur privé est non géré et il est probable que la configuration de chacun sera différente. Il est également peu probable qu'Outlook 2010 soit installé sur l'ordinateur, car beaucoup d'ordinateurs personnels utilisent d'autres applications de messagerie électronique.

Question : Dans un environnement client mixte qui requiert de forts niveaux de sécurité, lequel des types de tunnel VPN suivants choisiriez-vous ? PPTP, L2TP/IPsec, SSTP ou IKEv2 ?

Réponse : L2TP/IPsec fournit un chiffrement et une authentification forts et est pris en charge par la plupart des types de clients. IKEv2 n'est pris en charge que sur Windows 7 et Windows 8, et SSTP est seulement pris en charge sur Windows Vista®, Windows 7, et Windows 8.

Question : Vrai ou faux ? Le serveur NPS peut fonctionner en tant que client RADIUS.

Réponse : Faux. RRAS peut fournir cette fonctionnalité, mais vous ne pouvez configurer NPS qu'en tant que proxy RADIUS ou serveur RADIUS.

Question : Laquelle des propositions suivantes constitue la solution de pare-feu la plus sécurisée ? hôte bastion, pare-feu multirésident ou pare-feu dos à dos ?

Réponse : Les pare-feu dos à dos constituent la solution la plus sécurisée.

Question : Quelle est la fonction du NLS dans une solution DirectAccess ?

Réponse : Les clients DirectAccess utilisent le serveur d'emplacement réseau (NLS) pour déterminer leur emplacement. Si le client peut se connecter avec HTTPS, il suppose alors qu'il est sur l'intranet et il désactive les composants DirectAccess. S'il est impossible de contacter le serveur NLS, le client suppose alors qu'il est sur Internet. Vous installez le serveur NLS avec le rôle serveur Web.

Question : De quelles manières les clients DirectAccess peuvent-ils se connecter aux ressources réseau ?

Réponse : Les clients DirectAccess peuvent se connecter aux ressources réseau de plusieurs façons :

- directement, sur le réseau Internet IPv6 ;
- à l'aide de 6to4 ;
- à l'aide de Teredo ;
- à l'aide d'IP-HTTPS.

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

Atelier pratique A : Conception et implémentation des services d'accès réseau

Questions et réponses

Question : Pour quelle approche avez-vous opté lors de la conception du réseau privé virtuel (VPN) ?

Réponse : Les réponses varient.

Question : Pour quelle approche avez-vous opté lors de la conception DirectAccess ?

Réponse : Les réponses varient.

Question : Comment votre organisation prend en charge les utilisateurs distants ?

Réponse : Les réponses varient.

Module 12

Conception et implémentation de la protection réseau

Table des matières :

Leçon 1

Vue d'ensemble de la conception de la sécurité du réseau

Table des matières :

Questions et réponses

Discussion : À quelles menaces liées au réseau les organisations s'exposent-elles ?

Question : Quelles sont les dix menaces les plus courantes liées à la sécurité réseau que rencontrent les entreprises ?

Réponse : Les réponses varieront, mais elles peuvent inclure les éléments suivants :

- Virus et vers
- Chevaux de Troie
- Courrier indésirable
- Hameçonnage
- Détection de paquets
- Sites Web contenant du code malveillant
- Attaques de mot de passe
- Compromission de données via la perte physique de disques
- Utilisation d'ordinateurs partagés
- Ordinateurs zombies non détectés susceptibles de lancer certaines des attaques précédentes

Question : Quelles sont les mesures de correction ou solutions possibles pour contrer ces menaces ?

Réponse : Les réponses varieront, mais elles peuvent inclure les éléments suivants :

- Virus et vers. Formez les utilisateurs à la manipulation des messages électroniques et des pièces jointes. Implémentez des technologies telles que les antivirus qui assurent des messages propres.
- Chevaux de Troie. Formez les utilisateurs aux bonnes pratiques en ligne afin d'éviter les chevaux de Troie potentiels. Toutefois, cela peut ne pas être suffisant. Vous devez également implémenter des listes noires ou approuvées de sites Web afin à réduire le risque potentiel de chevaux de Troie.
- Courrier indésirable. Implémentez des technologies qui assurent un flux de messages propre. De plus, formez les utilisateurs aux meilleures pratiques d'utilisation des messages électroniques.
- Hameçonnage. Implémentez des technologies qui assurent un flux de messages propre. De plus, formez les utilisateurs aux meilleures pratiques d'utilisation des messages électroniques.
- Détection de paquets. Restreignez l'accès au réseau physique pour empêcher les pirates informatiques de connecter des périphériques de détection de réseau. Implémentez des paramètres sécurisés avec des réseaux sans fil. Informez vos utilisateurs sur la connexion à des zones d'accès sans fil publiques non sécurisées.
- Sites Web contenant du code malveillant. Implémentez un navigateur Web, tel que Internet Explorer® 10, capable d'identifier du code malveillant, et de bloquer les logiciels espions, les logiciels de publicité et les scripts intersites.

- Attaques de mot de passe Beaucoup d'attaques de mot de passe requièrent des chevaux de Troie ou l'accès physique à votre réseau pour leur mise en œuvre. La prévention des chevaux de Troie et la protection de votre réseau physique aideront à réduire les attaques de mot de passe. L'utilisation de mots de passe complexes permettent d'assurer une protection contre les attaques en force sur les mots de passe.
- Compromission de données via la perte physique de disques. Sensibilisez les utilisateurs à l'importance de protéger leurs ordinateurs portables et périphériques de stockage USB. Envisagez d'implémenter des technologies de chiffrement, telles que le chiffrement de lecteur BitLocker® Windows et BitLocker To Go® Windows.
- Utilisation d'ordinateurs partagés. Si vous devez autoriser l'utilisation d'ordinateurs partagés, tels que des ordinateurs faisant office de bornes, mettez en place des stratégies restrictives pour que l'utilisateur ne puisse effectuer que certaines tâches spécifiques. L'implémentation de plusieurs des solutions précédentes aidera également à protéger les ordinateurs partagés.
- Ordinateurs zombies non détectés susceptibles de lancer certaines des attaques précédentes. Ces ordinateurs ont été infectés par des chevaux de Troie, des virus ou des vers informatiques. Ils peuvent ensuite implémenter des attaques par hameçonnage ou de courrier indésirable. Par conséquent, l'implémentation des solutions précédentes doit empêcher vos ordinateurs d'être infectés et de propager de nouvelles attaques.

En résumé, les solutions suivantes sont utiles pour contrer les attaques réseau courantes :

- Sensibilisez les utilisateurs aux meilleures pratiques en ligne.
- Implémentez des technologies pour assurer la sécurité des messages électroniques.
- Limitez l'accès physique à votre réseau.
- Implémentez le chiffrement pour vos périphériques de stockage.

Leçon 3

Conception et implémentation d'une stratégie de Pare-feu Windows

Table des matières :

Questions et réponses

Discussion : Scénarios résolus par le Pare-feu Windows

Question : Quels sont les scénarios que le Pare-feu Windows peut aider à résoudre ?

Réponse : Les réponses peuvent varier, mais elles incluront les éléments suivants :

- protéger les serveurs contre les menaces internes en limitant la communication entrante à des plages spécifiques d'adresses IP ou à des ports spécifiques ;
- empêcher les logiciels malveillants (également appelés *malware*) de se propager en limitant les communications sortantes à certains ports ou à des applications spécifiques ;
- fournir l'authentification du trafic réseau avec IPsec ;
- fournir le chiffrement des données en transit via IPsec.

Démonstration

Démonstration : Configuration des règles de sécurité de connexion

Procédure de démonstration

Activer le trafic ICMP sur LON-SVR1

1. Basculez vers LON-SVR1.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité**.
4. Dans Pare-feu Windows avec fonctions avancées de sécurité, cliquez avec le bouton droit sur **Règles de trafic entrant**, puis cliquez sur **Nouvelle règle**.
5. Dans la boîte de dialogue **Assistant Nouvelle règle de trafic entrant**, cliquez sur **Personnalisée**, puis sur **Suivant**.
6. Dans la page **Programme**, cliquez sur **Suivant**.
7. Dans la page **Protocoles et ports**, dans la liste **Type de protocole**, cliquez sur **ICMPv4**, puis sur **Suivant**.
8. Dans la page **Étendue**, cliquez sur **Suivant**.
9. Dans la page **Action**, cliquez sur **Autoriser la connexion si elle est sécurisée**, puis sur **Suivant**.
10. Dans la page **Utilisateurs**, cliquez sur **Suivant**.
11. Dans la page **Ordinateurs**, cliquez sur **Suivant**.
12. Dans la page **Profil**, cliquez sur **Suivant**.
13. Dans la page **Nom**, dans la zone **Nom**, tapez **ICMPv4 autorisé**, puis cliquez sur **Terminer**.

Créer une règle de serveur à serveur sur des serveurs de connexion

1. Sur LON-SVR1, dans Pare-feu Windows avec fonctions avancées de sécurité, cliquez avec le bouton droit sur **Règles de sécurité de connexion**, puis cliquez sur **Nouvelle règle**.
2. Dans l'Assistant Nouvelle règle de sécurité de connexion, cliquez sur **Serveur à serveur**, puis cliquez sur **Suivant**.
3. Dans la page **Points de terminaison**, cliquez sur **Suivant**.
4. Dans la page **Configuration requise**, cliquez sur **Imposer l'authentification des connexions entrantes et sortantes**, puis cliquez sur **Suivant**.
5. Dans la page **Méthode d'authentification**, cliquez sur **Avancée**, puis sur **Personnaliser**.
6. Dans la boîte de dialogue **Personnaliser les méthodes d'authentification avancées**, sous **Premières méthodes d'authentification**, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Ajouter la première méthode d'authentification**, cliquez sur **Clé pré-partagée**, tapez **secret**, puis cliquez sur **OK**.
8. Dans la boîte de dialogue **Personnaliser les méthodes d'authentification avancées**, cliquez sur **OK**.
9. Dans la page **Méthodes d'authentification**, cliquez sur **Suivant**.
10. Dans la page **Profil**, cliquez sur **Suivant**.
11. Dans la page **Nom**, dans la zone **Nom**, tapez **Adatum-Serveur à serveur**, puis cliquez sur **Terminer**.

Créer une règle de serveur à serveur sur LON-CL1

1. Basculez vers LON-CL1.
2. Connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Sur l'écran d'accueil, tapez **Pare-feu Windows**, puis cliquez sur **Paramètres**.
4. Dans la liste **Paramètres**, cliquez sur **Pare-feu Windows**.
5. Dans le Pare-feu Windows, cliquez sur **Paramètres avancés**.
6. Sélectionnez, puis cliquez avec le bouton droit sur **Règles de sécurité de connexion**, puis cliquez sur **Nouvelle règle**.
7. Dans l'Assistant Nouvelle règle de sécurité de connexion, cliquez sur **Serveur à serveur**, puis cliquez sur **Suivant**.
8. Dans la page **Points de terminaison**, cliquez sur **Suivant**.
9. Dans la page **Configuration requise**, cliquez sur **Imposer l'authentification des connexions entrantes et sortantes**, puis cliquez sur **Suivant**.
10. Dans la page **Méthode d'authentification**, cliquez sur **Avancée**, puis sur **Personnaliser**.
11. Dans la boîte de dialogue **Personnaliser les méthodes d'authentification avancées**, sous **Premières méthodes d'authentification**, cliquez sur **Ajouter**.
12. Dans la boîte de dialogue **Ajouter la première méthode d'authentification**, cliquez sur **Clé pré-partagée**, tapez **secret**, puis cliquez sur **OK**.

13. Dans la boîte de dialogue **Personnaliser les méthodes d'authentification avancées**, cliquez sur **OK**.
14. Dans la page **Méthodes d'authentification**, cliquez sur **Suivant**.
15. Dans la page **Profil**, cliquez sur **Suivant**.
16. Dans la page **Nom**, dans la zone **Nom**, tapez **Adatum-Serveur à serveur**, puis cliquez sur **Terminer**.

Tester la règle

1. Placez le pointeur de votre souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
2. Sur l'écran d'accueil, tapez **cmd.exe**, puis appuyez sur Entrée.
3. À l'invite de commandes, tapez **ping 172.16.0.21**, puis appuyez sur Entrée.
4. Basculez vers Pare-feu Windows avec fonctions avancées de sécurité.
5. Développez successivement **Analyse**, puis **Associationsde sécurité**, puis cliquez sur **Mode principal**.
6. Dans le volet droit, double-cliquez sur l'élément répertorié.
7. Affichez les informations dans le mode principal, puis cliquez sur **OK**.
8. Cliquez sur **Mode rapide**.
9. Dans le volet droit, double-cliquez sur l'élément répertorié.
10. Affichez les informations dans le mode rapide, puis cliquez sur **OK**.

Leçon 4

Conception et implémentation d'une infrastructure de protection d'accès réseau (NAP)

Table des matières :

Démonstration

Démonstration : Implémentation de la protection d'accès réseau

Procédure de démonstration

Installer le rôle de serveur NPS

1. Basculez vers LON-DC1, puis connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Si nécessaire, dans la barre des tâches, cliquez sur **Gestionnaire de serveur**.
3. Dans le Gestionnaire de serveur, dans le volet d'informations, cliquez sur **Ajouter des rôles et des fonctionnalités**.
4. Dans l'Assistant Ajout de rôles et de fonctionnalités, cliquez sur **Suivant**.
5. Dans la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
7. Dans la page **Sélectionner des rôles de serveurs**, activez la case à cocher **Services de stratégie et d'accès réseau**.
8. Cliquez sur **Ajouter des fonctionnalités**, puis cliquez sur **Suivant** à deux reprises.
9. Dans la page **Services de stratégie et d'accès réseau**, cliquez sur **Suivant**.
10. Dans la page **Sélectionner des services de rôle**, vérifiez que la case à cocher **Serveur NPS (Network Policy Server)** est activée, puis cliquez sur **Suivant**.
11. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
12. Vérifiez que l'installation a réussi, puis cliquez sur **Fermer**.

Configurer le serveur NPS en tant que serveur de stratégie de contrôle d'intégrité NAP

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Serveur NPS (Network Policy Server)**.
2. Dans le volet de navigation, développez successivement **Protection d'accès réseau**, **Programmes de validation d'intégrité système**, **Programme de validation d'intégrité de la sécurité Windows**, puis cliquez sur **Paramètres**.
3. Dans le volet de droite, sous **Nom**, double-cliquez sur **Configuration par défaut**.
4. Dans le volet de navigation, cliquez sur **Windows 8/Windows 7/Windows Vista**.
5. Dans le volet d'informations, désactivez toutes les cases à cocher, puis activez la case à cocher **Un pare-feu est activé pour toutes les connexions réseau**.
6. Cliquez sur **OK** pour fermer la boîte de dialogue **Programme de validation d'intégrité de la sécurité Windows**.

Configurer les stratégies de contrôle d'intégrité

1. Dans le volet de navigation, développez **Stratégies**.
2. Cliquez avec le bouton droit sur **Stratégies de contrôle d'intégrité**, puis cliquez sur **Nouveau**.
3. Dans la boîte de dialogue **Créer une stratégie de contrôle d'intégrité**, sous **Nom de la stratégie**, tapez **Conforme**.
4. Sous **Contrôles du client par les programmes de validation d'intégrité système (SHV)**, vérifiez que la case à cocher **Réussite de tous les contrôles SHV pour le client** est activée.
5. Sous **Programmes de validation d'intégrité système (SHV) utilisés dans cette stratégie de contrôle d'intégrité**, activez la case à cocher **Programme de validation d'intégrité de la sécurité Windows**, puis cliquez sur **OK**.
6. Cliquez avec le bouton droit sur **Stratégies de contrôle d'intégrité**, puis cliquez sur **Nouveau**.
7. Dans la boîte de dialogue **Créer une stratégie de contrôle d'intégrité**, dans la zone **Nom de la stratégie**, tapez **Non conforme**.
8. Sous Contrôles du client par les programmes de validation d'intégrité système (SHV), cliquez sur **Échec d'un ou de plusieurs contrôles SHV pour le client**.
9. Sous Programmes de validation d'intégrité système (SHV) utilisés dans cette stratégie de contrôle d'intégrité, activez la case à cocher **Programme de validation d'intégrité de la sécurité Windows**, puis cliquez sur **OK**.

Configurer des stratégies réseau pour les ordinateurs conformes

1. Dans le volet de navigation, sous Stratégies, cliquez sur **Stratégies réseau**.
2. Important : vous devez désactiver les deux stratégies par défaut indiquées sous Nom de la stratégie en cliquant avec le bouton droit sur chacune d'elles, puis en cliquant sur **Désactiver**.
3. Cliquez avec le bouton droit sur **Stratégies réseau**, puis cliquez sur **Nouveau**.
4. Dans la page **Spécifier le nom de la stratégie réseau et le type de connexion**, sous **Nom de la stratégie**, tapez **Conforme-accès complet**, puis cliquez sur **Suivant**.
5. Dans la page **Spécifier les conditions**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Sélectionner une condition**, double-cliquez sur **Stratégies de contrôle d'intégrité**.
7. Dans la boîte de dialogue **Stratégies de contrôle d'intégrité**, sous **Stratégies de contrôle d'intégrité**, cliquez sur **Conforme**, puis sur **OK**.
8. Dans la page **Spécifier les conditions**, cliquez sur **Suivant**.
9. Dans la page **Spécifier l'autorisation d'accès**, cliquez sur **Suivant**.
10. Dans la page **Configurer les méthodes d'authentification**, désactivez toutes les cases à cocher, activez la case à cocher **Vérifier uniquement l'intégrité de l'ordinateur**, puis cliquez sur **Suivant**.
11. Cliquez à nouveau sur **Suivant**.
12. Dans la page **Configurer les paramètres**, cliquez sur **Contrainte de mise en conformité NAP**. Vérifiez que l'option **Autoriser un accès complet au réseau** est sélectionnée, puis cliquez sur **Suivant**.
13. Dans la page **Fin de la configuration de la nouvelle stratégie réseau**, cliquez sur **Terminer**.

Configurer des stratégies réseau pour les ordinateurs non conformes

1. Cliquez avec le bouton droit sur **Stratégies réseau**, puis cliquez sur **Nouveau**.
2. Dans la page **Spécifier le nom de la stratégie réseau et le type de connexion**, dans la zone **Nom de la stratégie**, tapez **Non conforme-restreint**, puis cliquez sur **Suivant**.
3. Dans la page **Spécifier les conditions**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Sélectionner une condition**, double-cliquez sur **Stratégies de contrôle d'intégrité**.
5. Dans la boîte de dialogue **Stratégies de contrôle d'intégrité**, sous **Stratégies de contrôle d'intégrité**, cliquez sur **Non conforme**, puis sur **OK**.
6. Dans la page **Spécifier les conditions**, cliquez sur **Suivant**.
7. Dans la page **Spécifier l'autorisation d'accès**, vérifiez que l'option **Accès accordé** est sélectionnée, puis cliquez sur **Suivant**.
8. Dans la page **Configurer les méthodes d'authentification**, désactivez toutes les cases à cocher, activez la case à cocher **Vérifier uniquement l'intégrité de l'ordinateur**, puis cliquez sur **Suivant**.
9. Cliquez à nouveau sur **Suivant**.
10. Dans la page **Configurer les paramètres**, cliquez sur **Contrainte de mise en conformité NAP**, puis sur **Autoriser un accès limité**. Désactivez la case à cocher **Activer la mise à jour automatique des ordinateurs clients**, cliquez sur **Suivant**, puis sur **Terminer**.

Configurer le rôle de serveur DHCP (Dynamic Host Configuration Protocol) pour la protection d'accès réseau

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP**.
2. Dans DHCP, développez successivement **lon-dc1.adatum.com** et **IPv4**, cliquez avec le bouton droit sur **Étendue [172.16.0.0] Adatum**, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de : Étendue [172.16.0.0] Adatum**, cliquez sur l'onglet **Protection d'accès réseau**, sur **Activer pour cette étendue**, puis sur **OK**.
4. Dans le volet de navigation, sous **Étendue [172.16.0.0] Adatum**, cliquez sur **Stratégies**.
5. Cliquez avec le bouton droit sur **Stratégies**, puis cliquez sur **Nouvelle stratégie**.
6. Dans l'Assistant Configuration de stratégie DHCP, dans la zone **Nom de la stratégie**, tapez **Stratégie NAP**, puis cliquez sur **Suivant**.
7. Dans la page **Configurer les conditions de la stratégie**, cliquez sur **Ajouter**.
8. Dans la boîte de dialogue **Ajouter/Modifier une condition**, dans la liste **Critères**, cliquez sur **Classe d'utilisateur**.
9. Dans la liste **Opérateur**, cliquez sur **Est égal à**.
10. Dans la liste **Valeur**, cliquez sur **Classe de protection d'accès réseau par défaut**, puis cliquez sur **Ajouter**.
11. Cliquez sur **OK**, puis sur **Suivant**.
12. Dans la page **Configurer les paramètres de la stratégie**, cliquez sur **Non**, puis sur **Suivant**.

13. Dans la page **Configurer les paramètres de la stratégie**, dans la liste **Classe de fournisseur**, cliquez sur **DHCP Standard Options**.
14. Dans la liste **Options disponibles**, activez la case à cocher **006 Serveurs DNS**.
15. Dans le champ **Adresse IP**, tapez **172.16.0.10**, puis cliquez sur **Ajouter**.
16. Dans la liste **Options disponibles**, activez la case à cocher **015 Nom de domaine DNS**.
17. Dans le champ **Valeur chaîne**, tapez **restricted.adatum.com**, puis cliquez sur **Suivant**.
18. Dans la page **Résumé**, cliquez sur **Terminer**.
19. Fermez DHCP.

Configurer les paramètres NAP du client

1. Basculez vers LON-CL1, puis connectez-vous en tant qu'**ADATUM\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Sur l'écran d'accueil, tapez **napclcfg.msc**, puis appuyez sur Entrée.
3. Dans NAPCLCFG – [Configuration du client NAP (Ordinateur local)], dans le volet de navigation, cliquez sur **Clients de contrainte**.
4. Dans le volet de résultats, cliquez avec le bouton droit sur **Client de contrainte de quarantaine DHCP**, puis cliquez sur **Activer**.
5. Fermez NAPCLCFG – [Configuration du client NAP (Ordinateur local)\Clients de contrainte].
6. Placez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
7. Sur l'écran d'accueil, tapez **Services.msc**, puis appuyez sur Entrée.
8. Dans Services, dans le volet de résultats, double-cliquez sur **Agent de protection d'accès réseau**.
9. Dans la boîte de dialogue **Propriétés de Agent de protection d'accès réseau (ordinateur local)**, dans la liste **Type de démarrage**, cliquez sur **Automatique**.
10. Cliquez sur **Accueil**, puis sur **OK**.
11. Placez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
12. Sur l'écran d'accueil, tapez **gpedit.msc**, puis appuyez sur Entrée.
13. Dans l'arborescence de la console, développez successivement **Stratégie Ordinateur local**, **Configuration ordinateur**, **Modèles d'administration**, **Composants Windows**, puis cliquez sur **Centre de sécurité**.
14. Double-cliquez sur **Activer le Centre de sécurité (ordinateurs appartenant à un domaine uniquement)**, cliquez sur **Activé**, puis sur **OK**.
15. Fermez la fenêtre de la console.
16. Placez le pointeur de votre souris dans le coin inférieur droit de la barre des tâches, puis cliquez sur **Paramètres**.

17. Dans la liste **Paramètres**, cliquez sur **Panneau de configuration**.
18. Dans le Panneau de configuration, cliquez sur **Réseau et Internet**.
19. Dans Réseau et Internet, cliquez sur **Centre Réseau et partage**.
20. Dans Centre Réseau et partage, dans le volet gauche, cliquez sur **Modifier les paramètres de la carte**.
21. Cliquez avec le bouton droit sur **Connexion au réseau local**, puis cliquez sur **Propriétés**.
22. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, double-cliquez sur **Protocole Internet version 4 (TCP/IPv4)**.
23. Dans la boîte de dialogue **Propriétés de : Protocole Internet version 4 (TCP/IPv4)**, cliquez sur **Obtenir une adresse IP automatiquement**.
24. Cliquez sur **Obtenir les adresses des serveurs DNS automatiquement**, puis sur **OK**.
25. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, cliquez sur **OK**.

Tester la protection d'accès réseau

1. Placez le pointeur de la souris dans le coin inférieur gauche de la barre des tâches, puis cliquez sur **Accueil**.
2. Sur l'écran d'accueil, tapez **cmd.exe**, puis appuyez sur Entrée.
3. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
Ipconfig
```

4. Basculez vers Services.
5. Dans Services, dans le volet de résultats, double-cliquez sur **Pare-feu Windows**.
6. Dans la boîte de dialogue **Propriétés de Pare-feu Windows (Ordinateur local)**, dans la liste **Type de démarrage**, cliquez sur **Désactivé**.
7. Cliquez sur **Arrêter**, puis sur **OK**.
8. Dans la zone de barre d'état système, cliquez sur la fenêtre contextuelle **Protection d'accès réseau**. Passez en revue les informations dans la boîte de dialogue **Protection d'accès réseau**, puis cliquez sur **Fermer**.

Remarque : Si la fenêtre contextuelle ne s'affiche pas, poursuivez la démonstration.

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

```
Ipconfig
```

10. Notez que l'ordinateur a un masque de sous-réseau de 255.255.255.255 et un suffixe DNS restricted.Adatum.com. Ne fermez aucune fenêtre.

Contrôle des acquis et éléments à retenir

Question(s) de contrôle des acquis

Question : Le programme de validation d'intégrité système Windows peut déterminer à la fois l'état du pare-feu (activé ou désactivé) et s'il est à jour.

( ) Vrai

( ) Faux

Réponse :

(√) Vrai

( ) Faux

Question : Citez quelques formes courantes d'attaques réseau.

Réponse : Les formes courantes d'attaques réseau comprennent l'écoute illicite, la modification de données, l'usurpation d'identité, le déni de service, et les attaques de la couche Application, par mot de passe, de type intercepteur et par clé compromise.

Question : Quel(s) rôle(s) serveur devez-vous déployer pour prendre en charge la protection d'accès réseau ?

Réponse : Vous devez déployer le rôle NPS et, si nécessaire, Active Directory® Certificate Services (AD CS). Si vous implémentez la contrainte de mise en conformité DHCP, vous devez déployer un serveur DHCP. La contrainte de mise en conformité VPN nécessite le service de rôle Routage et accès distant (qui fait partie du rôle NPS).

Question : Quelles sont les utilisations conseillées d'IPsec ?

Réponse : Les utilisations conseillées d'IPsec sont :

- Filtrage des paquets
- Sécurisation du trafic d'hôte à hôte
- Sécurisation du trafic vers les serveurs
- Protocole L2TP (Layer Two Tunneling Protocol)
- Tunneling de site à site (de passerelle à passerelle)
- Mise en œuvre de réseaux logiques

Problèmes réels et scénarios

Scénario : Tailspin Toys envisage d'implémenter la protection d'accès réseau dans le cadre de son infrastructure de sécurité globale. Ils souhaitent une méthode de mise en œuvre qui s'applique à tous les clients réseau, quelle que soit la façon dont ils se connectent. Une infrastructure à clé publique est en place. Quelle(s) méthode(s) de mise en œuvre recommanderiez-vous ?

Réponse : La contrainte de mise en conformité IPsec serait appropriée, de même que la contrainte de mise en conformité 802.1X, si les commutateurs et les points d'accès prennent en charge l'authentification 802.1X. La contrainte de mise en conformité DHCP serait inappropriée, car les clients avec une configuration IP affectée manuellement peuvent contourner la protection d'accès réseau. La contrainte de mise en conformité VPN serait également inappropriée, car tous les clients ne se connectent pas via VPN.

Scénario : Wingtip Toys souhaite implémenter la contrainte de mise en conformité NAP IPsec. Quels composants d'infrastructure doivent être en place pour prendre en charge cette méthode ?

Réponse : Outre les conditions générales requises pour la protection d'accès réseau, IPsec requiert également que le déploiement d'une Autorité HRA (Health Registration Authority) et d'une Infrastructure à clé publique (PKI) pour les certificats d'intégrité.

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

Atelier pratique A : Conception et implémentation de la protection réseau

Questions et réponses

Question : Pour quelle approche avez-vous opté lors de l'exercice de conception du pare-feu ?

Réponse : Les réponses varient.

Question : Pour quelle approche avez-vous opté lors de l'exercice de conception de la protection d'accès réseau ?

Réponse : Les réponses varient.

Question : En quoi la conception de l'accès réseau diffère-t-elle de l'implémentation de l'accès réseau dans votre organisation ?

Réponse : Les réponses varient.