Microsoft

PRODUIT OFFICIEL DE FORMATION MICROSOFT

22741A

Mise en réseau avec Windows Server 2016

Contenu complémentaire

Numéro de produit : 22741A

Date de publication : 03/2017

TERMES DU CONTRAT DE LICENCE MICROSOFT
COURS MICROSOFT AVEC FORMATEUR

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

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

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

1. DÉFINITIONS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    Cette limitation concerne :

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

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

Dernière mise à jour : septembre 2012.

Module 1

Planification et implémentation d'un réseau IPv4

Sommaire :

Leçon 1

Planification de l’adressage IPv4

Sommaire :

Questions et réponses

Question : Sélectionnez le masque de sous-réseau pour créer les plus petits réseaux qui permettent à 172.168.32.223 et 172.168.35.19 d'être sur le même réseau.

( ) /20

( ) /21

( ) /22

( ) /23

( ) /24

Réponse :

( ) /20

( ) /21

(√) /22

( ) /23

( ) /24

Commentaire :

L'option 1 et l'option 2 placent les deux adresses sur le même réseau, mais rendent les réseaux beaucoup plus larges que nécessaire. L'option 4 et l'option 5 forcent les deux adresses à être sur des réseaux distincts.

Question : Quel est l'équivalent décimal du masque de sous-réseau correct pour la question précédente ?

Réponse : 255.255.252.0

Vue d'ensemble des paramètres IPv4

Question : Convertissez les valeurs suivantes

Binaire	Notation décimale séparée par des points
00001010 00001110 00011011 00100000	
	172.16.34.22
	192.168.87.19
10101100 00010000 01100010 00010111	
11000000 10101000 01010111 00111000	
	10.17.22.99

Réponse :

Binaire	Notation décimale séparée par des points
00001010 00001110 00011011 00100000	10.14.27.32
10101100 00010000 00100010 00010110	172.16.34.22

Binaire	Notation décimale séparée par des points
11000000 10101000 01010111 00010011	192.168.87.19
10101100 00010000 01100010 00010111	172.16.98.23
11000000 10101000 01010111 00111000	192.168.87.56
00001010 00010001 00010110 01100011	10.17.22.99

Définition des sous-réseaux

Question : Comment la communication réseau est-elle affectée si une passerelle par défaut est mal configurée ?

Réponse : Un hôte avec une passerelle par défaut incorrecte n'est pas capable de communiquer avec des hôtes sur un réseau à distance. Les communications sur le réseau local ne sont pas affectées.

Question : Votre organisation utilise-t-elle un réseau simple ou complexe ?

Réponse : Les réponses varient. La plupart des petites entreprises utilisent des réseaux simples pour faciliter la configuration. Les grandes entreprises ayant des spécialistes réseau sont plus susceptibles d'utiliser des réseaux complexes.

Discussion : définition de la notation et traduction IPv4

Question : Laquelle ou lesquelles des adresses suivantes sont une classe d'adresses IP et laquelle ou lesquelles ne le sont pas ?

- 10.14.27.32/8
- 172.16.34.22/26
- 192.168.87.19 masque de sous-réseau 255.555.555.0
- 172.16.98.23 masque de sous-réseau 255.240.0.0
- 192.168.87.56/24
- 10.17.22.99/12

Réponse :

- 10.14.27.32/8 (à classes)
- 172.16.34.22/26 (sans classe)
- 192.168.87.19 masque de sous-réseau 255.555.555.0 (à classes)
- 172.16.98.23 masque de sous-réseau 255.240.0.0 (sans classe)
- 192.168.87.56/24 (à classes)
- 10.17.22.99/12 (sans classe)

Question : identifiez l'ID de réseau pour chacune des adresses suivantes.

- 10.25.12.100/24
- 10.25.12.100/16
- 172.168.20.66/24
- 172.168.20.66/26
- 192.168.52.98 masque de sous-réseau 255.255.255.0

- 192.168.52.98 masque de sous-réseau 255.255.255.240

  Réponse :

  - 10.25.12.100/24 (ID réseau 10.25.12.0)
  - 10.25.12.100/16 (ID réseau 10.25.0.0)
  - 172.168.20.66/24 (ID réseau 172.168.20.0)
  - 172.168.20.66/26 (ID réseau 172.168.20.64)
  - 192.168.52.98 masque de sous-réseau 255.255.255.0 (ID réseau 192.168.52.0)
  - 192.168.52.98 masque de sous-réseau 255.255.255.240 (ID réseau 192.168.52.96)

Question : Pour le réseau dans lequel chacune de ces adresses réside, identifiez la première adresse utilisable et l'adresse de diffusion.

- 10.25.12.100/24
- 10.25.12.100/16
- 172.168.20.66/24
- 172.168.20.66/26
- 192.168.52.98 masque de sous-réseau 255.255.255.0
- 192.168.52.98 masque de sous-réseau 255.255.255.240

  Réponse :

  - 10.25.12.100/24 (première adresse utilisable 10.25.12.1, adresse de diffusion 10.25.12.255)
  - 10.25.12.100/16 (première adresse utilisable 10.25.12.1, adresse de diffusion 10.25.255.255)
  - 172.168.20.66/24 (première adresse utilisable 172.168.20.1, adresse de diffusion 172.168.20.255)
  - 172.168.20.66/26 (première adresse utilisable 172.168.20.65, adresse de diffusion 172.168.20.127)
  - 192.168.52.98 masque de sous-réseau 255.255.255.0 (première adresse utilisable 192.168.52.1, adresse de diffusion 192.168.52.255)
  - 192.168.52.98 masque de sous-réseau 255.255.255.240 (première adresse utilisable 192.168.52.97, adresse de diffusion 192.168.52.111)

Discussion : Création d'un système de sous-réseau pour un nouveau bureau

Question : Combien de sous-réseaux sont nécessaires ?

> **Réponse :** Cinq sous-réseaux sont nécessaires dans ce scénario. Parmi ceux-ci, quatre sous-réseaux sont nécessaires pour les bâtiments et un est nécessaire pour le centre de données. Il s'agit du nombre minimum de sous-réseaux requis par les exigences du scénario.

Question : Combien de bits sont nécessaires pour créer ce nombre de sous-réseaux ?

> **Réponse :** Les sous-réseaux sont calculés en utilisant la formule 2^n, où « n » est le nombre de bits. Comme on le voit dans le tableau ci-dessous, trois bits sont nécessaires pour créer cinq sous-réseaux, parce que deux bits ne fournissent que 4 sous-réseaux et trois bits permettent la création de huit sous-réseaux. Comme les imprimantes dans ce scénario ont une capacité de mise en réseau, il vous revient de leur attribuer des adresses IP.

Bits de sous-réseau	Formule	Sous-réseaux
1	2^1	2

Bits de sous-réseau	Formule	Sous-réseaux
2	2^2	4
3	2^3	8
4	2^4	16
5	2^5	32
6	2^6	64

Question : Combien d'hôtes disponibles sont nécessaires sur chaque sous-réseau ?

Réponse : Puisque chaque sous-réseau doit prendre en charge jusqu'à 700 utilisateurs et 14 imprimantes, 714 adresses utilisables doivent être disponibles sur chaque sous-réseau.

Question : Combien de bits sont nécessaires pour prendre en charge ce nombre de sous-réseaux ?

Réponse : Le nombre d'hôtes utilisables dépend du nombre de bits. La formule est (2^n)-2, « n » étant le nombre de bits. 9 bits hôtes prennent en charge 510 hôtes, ((2^9) - 2 = 510). Dix bits ((2^10) - 2 = 1022) fournissent jusqu'à 1 022 hôtes.

Question : Quel masque de sous-réseau peut satisfaire ces exigences ?

Réponse : Plusieurs masques de sous-réseau peuvent fournir un nombre minimal de réseaux et un nombre minimal d'hôtes :

- 255.255.224.0 (3 bits de sous-réseau, 13 bits d'hôte)
- 255.255.240.0 (4 bits de sous-réseau, 12 bits d'hôte)
- 255.255.248.0 (5 bits de sous-réseau, 11 bits d'hôte)
- 255.255.252.0 (6 bits de sous-réseau, 10 bits d'hôte)

Leçon 2

Configuration d'un hôte IPv4

Sommaire :

Questions et réponses

Question : Quelle serait la meilleure façon de configurer les adresses IP pour une succursale qui comprendrait seulement 50 ordinateurs de bureau ?

> **Réponse :** Les réponses varient. Certains étudiants peuvent suggérer qu'on utilise les adresses IP statiques comme Serveur DHCP, puisque les systèmes de bureau ne passent généralement pas d'un emplacement (type ordinateur portable) à l'autre et que le réseau ne comporte pas de serveur. D'autres peuvent suggérer d'utiliser le Serveur DHCP et d'envoyer les requêtes DHCP à un Serveur DHCP dans le réseau domestique.

Question : En quoi votre réponse changerait s'il y avait un mélange d'ordinateurs portables et ordinateurs de bureau ?

> **Réponse :** Les réponses varient. Les stagiaires qui ont suggéré le DHCP ne varieront sans doute pas. Tous les utilisateurs qui suggèrent des adresses statiques proposent probablement un DHCP pour soutenir l'itinérance d'un ordinateur portable.

Vérifier les paramètres IPv4.

Question : Les ordinateurs ou les périphériques de votre organisation ont-ils des adresses IP statiques ?

> **Réponse :** Dans la plupart des cas, les serveurs ont des adresses IP statiques. D'autres périphériques réseau tels que les imprimantes ont aussi généralement des adresses IP statiques.

Outils pour configurer IPv4

Question : Quels sont les outils qui permettent d'attribuer des adresses IPv4 multiples à un serveur ?

> **Réponse :** Les Propriétés Internet Protocol Version 4 (TCP/IPv4), Paramètres avancés TCP/IP constituent l'outil le plus simple pour accomplir cette tâche.

Ressources

 **Lectures supplémentaires :** Pour plus d'informations sur les net TCP/IP cmdlets dans Windows PowerShell, accédez à http://aka.ms/L50hb6

Démonstration : Configuration d'IPv4

Procédure de démonstration

Configuration IPv4 à l'aide de l'interface utilisateur

1. Sur **LON-SVR1**, cliquez sur l'icône **Démarrer**, puis cliquez sur **Paramètres**.
2. Dans la fenêtre **Paramètres**, cliquez sur **Réseau et Internet**.
3. Dans la fenêtre **Réseau et Internet**, dans le volet de navigation, cliquez sur **Ethernet**.
4. Dans la fenêtre **Réseau et Internet**, dans le volet des résultats, cliquez sur **Centre de réseau et partage**.
5. Dans la fenêtre **Centre Réseau et partage**, dans le volet de navigation, cliquez sur **Modifier les paramètres de l'adaptateur**.
6. Cliquez avec le bouton droit sur **Ethernet**, puis cliquez sur **Propriétés**.
7. Sélectionnez **Internet Protocol Version 4 (TCP/IPv4)**, puis cliquez sur **Propriétés**.
8. Remplacez **l'adresse IP par 172.16.0.111**, cliquez sur **OK**, puis fermez toutes les fenêtres ouvertes.

Configuration IPv4 à l'aide de Windows PowerShell

1. Cliquez sur le bouton **Démarrer**, puis sur **Windows PowerShell**.
2. Vérifiez que l'adresse IP a été changée en tapant la commande suivante, puis appuyez sur Entrée.

```
Get-NetIPAddress -InterfaceAlias "Ethernet"
```

3. Vérifiez l'adresse IP en tapant la commande suivante, puis appuyez sur Entrée.

```
Remove-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 172.16.0.111
```

4. Lorsque vous êtes invité à **Confirmer**, entrez **y**, puis appuyez sur Entrée.
5. Vérifiez que l'adresse IP a été changée en tapant la commande suivante, puis appuyez sur Entrée.

```
Get-NetIPAddress -InterfaceAlias "Ethernet"
```

6. Notez l'adresse IP attribuée à l'interface.
7. Ajoutez l'adresse IP **172.16.0.11** à l'interface **Ethernet** en tapant la commande suivante, puis appuyez sur Entrée.

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 172.16.0.11 -PrefixLength 24
```

8. Fermez toutes les fenêtres actives, puis minimisez tous les ordinateurs virtuels.

Leçon 3

Gestion et résolution de la connectivité réseau IPv4

Sommaire :

Questions et réponses

Question : Quel est le résultat de l'application d'un masque de sous-réseau erroné à un système ?

Réponse : Les communications seront perturbées.

Question : Si un client ne parvient pas à se connecter à un serveur, quelles sont, parmi les étapes suivantes, celles qui permettraient de résoudre le problème ?

( ) Redémarrez le serveur.

( ) Vérifiez que le client dispose d'une adresse IP valide.

( ) Vérifiez que le client a reçu l'adresse APIPA appropriée.

( ) Vérifiez la configuration IP des serveurs auxquels le client tente de se connecter.

( ) Tout ce qui précède.

Réponse :

( ) Redémarrez le serveur.

(√) Vérifiez que le client dispose d'une adresse IP valide.

( ) Vérifiez que le client a reçu l'adresse APIPA appropriée.

( ) Vérifiez la configuration IP des serveurs auxquels le client tente de se connecter.

( ) Tout ce qui précède.

Méthodologie de résolution de IPv4

Question : Quelles mesures supplémentaires pourriez-vous utiliser pour résoudre les problèmes de connectivité réseau ?

Réponse : Les réponses varient. Certains stagiaires peuvent surveiller les pare-feu si le problème est lié à la connectivité Internet. Les stagiaires peuvent également utiliser les journaux d'applications lors de la résolution de la connectivité à un programme spécifique.

Ressources

Qu'est-ce que Microsoft Message Analyzer ?

Liens de référence : Pour plus d'informations sur Microsoft Message Analyzer, consultez le Guide d'utilisation de Microsoft Message Analyzer sur http://aka.ms/Jzc3pk
Pour télécharger Microsoft Message Analyzer, rendez-vous sur http://aka.ms/S20hr4

Démonstration : Dépannage IPv4

Procédure de démonstration

Utilisation de Get-NetIPAddress et ipconfig

1. Sur **LON-SVR1**, cliquez sur le bouton **Démarrer**, puis sur **Windows PowerShell**.
2. Cliquez sur le bouton **Démarrer**, saisissez **cmd**, puis appuyez sur Entrée.
3. Sur **LON-SVR1**, cliquez avec le bouton droit sur la barre des tâches, puis cliquez sur **Afficher les fenêtres côte à côte**.
4. Dans la fenêtre Windows PowerShell, tapez la commande suivante et appuyez sur Entrée.

```
Get-NetIPAddress -InterfaceAlias “Ethernet”
```

5. À l’invite de commandes Administrateur, tapez la commande suivante et appuyez sur Entrée :

```
ipconfig
```

6. Discutez des similitudes et des différences dans la sortie de chaque commande.

Utilisation de Test-NetConnection et ping

1. Sur **LON-SVR1**, dans la fenêtre Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée.

```
Test-NetConnection 172.16.0.1
```

2. À l’invite de commandes Administrateur, tapez la commande suivante et appuyez sur Entrée :

```
Ping 172.16.0.1
```

3. Discutez des similitudes et des différences entre les résultats des différentes commandes.

Utilisation de Test-NetConnection -TraceRoute et tracert

1. Sur **LON-SVR1**, dans la fenêtre Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée.

```
Test-NetConnection - Détermination d’itinéraire 172.16.18.20
```

2. Dans la fenêtre de l’invite de commandes, entrez la commande suivante et appuyez sur Entrée.

```
Tracert 172.16.18.20
```

3. Discutez des similitudes et des différences entre les résultats des différentes commandes.

Démonstration : Utilisation de Microsoft Message Analyzer

Procédure de démonstration

Nouvelle Capture/Trace dans Microsoft Message Analyzer

1. Connectez-vous à **LON-SVR2**, si vous ne l’avez pas déjà fait, enregistrez-vous en tant que **Adatum\Administrator** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur Démarrer puis cliquez sur l’icône **Windows PowerShell**.
3. À l’invite Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Clear-DnsClientCache
```

4. Cliquez sur **Démarrer**, puis sur **Toutes les applications**, développez **Microsoft Message Analyzer**, puis cliquez sur **Microsoft Message Analyzer**.
5. Dans le volet de navigation, cliquez sur **Démarrer le traçage local**.

Capture de paquets à partir d’une requête ping

1. Dans la barre des tâches, cliquez sur la session Windows PowerShell.
2. À l’invite Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Test-NetConnection LON-DC1.adatum.com
```

3. Patientez pendant que la commande se termine, puis dans la barre des tâches, cliquez sur **Microsoft Message Analyzer**.
4. Dans Microsoft Message Analyzer, sur la barre d'outils, cliquez sur **Arrêter**.

Analysez le trafic réseau capturé

1. Dans Microsoft Message Analyzer, dans le volet des résultats, sous la colonne **Module**, sélectionnez le premier groupe de paquets **ICMP**.
2. Dans le volet des résultats, cliquez sur le signe plus **+** à côté du groupe de paquets sélectionné.
3. Montrez que le groupe de paquets comprend les paquets **Echo Request** et **Echo Reply** en raison de la requête ping exécutée lors de l'exécution de l'applet **Test-NetConnection**.
4. Regardez les adresses IP source et de destination pour chaque paquet.

Filtrez le trafic réseau

1. Sur la barre d'outils de Microsoft Message Analyzer, dans la section **Voir le filtre**, dans la boîte **Filtre**, tapez la commande suivante, puis cliquez sur **Appliquer** :

```
*DestinationAddress == 172.16.0.10
```

2. Vérifiez que seuls les paquets qui correspondent au filtre sont affichés.
3. Fermez **Microsoft Message Analyzer** sans enregistrer.

Contrôle des acquis et éléments à retenir

Recommandations

Lors de la mise en œuvre d'IPv4, utilisez les recommandations suivantes :

- Permettre la croissance lors de la planification des sous-réseaux IPv4. Cela garantit que vous n'avez pas besoin de changer votre schéma de configuration IPv4.
- Définir des objectifs pour les gammes et les sous-réseaux d'adresses spécifiques. Cela vous permet à la fois d'identifier facilement les hôtes en fonction de leur adresse IP et d'utiliser des pare-feu pour accroître la sécurité.
- Utilisez des adresses dynamiques IPv4 pour les clients. Il est beaucoup plus facile de gérer la configuration IPv4 pour les ordinateurs des clients en utilisant DHCP qu'avec une configuration manuelle.
- Utilisez des adresses IPv4 statiques pour les serveurs. Lorsque les serveurs ont une adresse IPv4 statique, il est plus facile d'identifier où les services sont situés sur le réseau.

Questions de contrôle des acquis

Question : Vous occupez depuis peu un poste d'administrateur de serveur pour une petite organisation travaillant sur un site unique. L'organisation utilise la plage d'adresses 131.107.88.0/24 pour le réseau interne. Est-ce un problème ?

> **Réponse :** Oui, cela pose problème car ce sont des adresses Internet routables. La plupart des réseaux IPv4 utilisent des adresses privées avec la traduction d'adresses réseau (NAT) pour permettre l'accès à Internet. Si cette organisation ne possède pas le réseau 131.107.88.0/24, ils ne seront pas en mesure d'accéder aux ressources sur le réseau 131.107.88.0/24 sur Internet parce que tous les clients penseront que ces adresses sont locales.

Question : Vous travaillez pour une organisation qui fournit des services d'hébergement web à d'autres organisations. Vous avez un seul réseau /24 à partir de votre FAI pour les hébergeurs web. Vous n'avez presque plus d'adresses IPv4 et vous avez demandé à votre FAI une plage d'adresses supplémentaire. Vous souhaitez créer un sur-réseau avec le réseau existant et le nouveau réseau. Existe-t-il des exigences spécifiques concernant le sur-réseau ?

> **Réponse :** Oui. Pour réaliser le supernetting, les deux réseaux doivent être consécutifs. En outre, les réseaux doivent vous permettre de supprimer un seul bit du masque de sous-réseau et d'identifier les deux comme un seul et même réseau.

Question : Vous avez installé un nouveau site programme en ligne qui fonctionne sur un numéro de port non standard. Un collègue teste l'accès au nouveau programme en ligne et indique qu'il ne peut pas s'y connecter. Quelles sont les causes les plus probables de son problème ?

> **Réponse :** Quand un programme de serveur fonctionne sur un port non standard, vous devez fournir le programme client avec le numéro de port auquel il doit être connecté, par exemple *http://servername:port*. Il est également possible que votre collègue tente de se connecter en utilisant http, alors qu'il devrait utiliser https.

Outils

Le tableau suivant répertorie les outils référencés par ce module.

Outil	Fonction	Emplacement
Microsoft Message Analyzer	Capture et analyse du trafic réseau	Téléchargeable sur le site Web de Microsoft

Outil	Fonction	Emplacement
Get-NetIPAddress	Accès à la liste des adresses IP configurées pour les interfaces	Windows PowerShell
Test-NetConnection	Affichage des éléments suivants : • Résultats d'une recherche DNS • Liste des interfaces IP • Option pour tester une connexion TCP • Règles de sécurité du protocole Internet (IPsec) • Confirmation d'établissement de connexion	Windows PowerShell
Ipconfig	Voir la configuration réseau	Invite de commandes
Ping	Vérifier la connectivité réseau	Invite de commandes
Tracert	Vérifier le chemin réseau entre les hôtes	Invite de commandes
Pathping	Vérifier le chemin réseau et la fiabilité entre les hôtes	Invite de commandes
Route	Voir et configurer la table de routage locale	Invite de commandes
Telnet	Tester la connectivité à un port spécifique	Invite de commandes
Netstat	Voir les informations de connectivité réseau	Invite de commandes
Moniteur de ressources	Voir les informations de connectivité réseau	Outils dans le Gestionnaire de serveur
Diagnostics réseau de Windows	Diagnostiquer un problème avec une connexion réseau	Propriétés de la connexion réseau
Observateur d'événements	Voir les événements système liés au réseau	Outils dans le Gestionnaire de serveur

Problèmes courants et conseils de dépannage

Problème courant	Conseil pour la résolution du problème
Conflits de propriété intellectuelle	Dans la plupart des cas, les ordinateurs qui exécutent des systèmes d'exploitation Windows affichent un message lorsqu'ils ont un conflit d'IP avec un autre périphérique réseau. Cependant, certains périphériques réseau ne le font pas. Lorsque vous effectuez une capture de paquets, des accusés de réception TCP en duplicata peuvent indiquer que deux périphériques ont la même adresse IP et que les deux sont en train de répondre à des tentatives de

Problème courant	Conseil pour la résolution du problème
	connexion. Pour éviter les conflits d'IP, mentionnez clairement les adresses IPv4 utilisées sur votre réseau et n'attribuez pas de nouvelles adresses IPv4 sans vérifier la documentation.
Passerelles multiples par défaut définies	Sur les hôtes ayant plusieurs cartes réseau, une seule d'entre elles doit avoir une passerelle par défaut définie. Windows Server est conçu pour fonctionner avec une passerelle par défaut uniquement. Lorsque plusieurs passerelles par défaut sont définies, la communication réseau peut s'avérer imprévisible. Vous pouvez vérifier qu'une passerelle par défaut unique est configurée en utilisant l'applet de commande **Get-NetRoute.**
Configuration IPv4 incorrecte	Des informations de configuration IPv4 incorrectes résultent le plus souvent d'une erreur de configuration manuelle. Pour s'assurer que ceci n'affecte pas un environnement de production, vous devez tester intégralement la connectivité réseau pour identifier, le cas échéant, les nouveaux serveurs que vous placez dans la production. Vous devrez également effectuer des tests après avoir effectué des modifications de la configuration du réseau.

Questions et réponses sur les ateliers pratiques

Atelier pratique A : Planification d'un réseau IPv4

Questions et réponses

Question : Combien de passerelles par défaut sont nécessaires ?

Réponse : Chaque sous-réseau nécessite une passerelle par défaut. Pour utiliser sept sous-réseaux, il faut sept passerelles par défaut.

Question : Quels autres facteurs prenez-vous en considération lors de la conception d'un réseau ?

Réponse : Les réponses varient, il est possible d'envisager la répartition des bureaux. Par exemple, vous ne voulez utiliser que deux sous-réseaux pour les connexions câblées à Houston, mais les installations sont aménagées de telle manière qu'il est impossible de n'utiliser que deux sous-réseaux.

Atelier pratique B : Planification et dépannage d'un réseau IPv4.

Questions et réponses

Question : Lors de la résolution d'un problème, quelle est la première étape que vous devez effectuer ?

Réponse : Les réponses varient. Beaucoup de gens prennent différentes approches de dépannage. La première étape, très importante, consiste à reproduire le problème.

Question : Quel applet de commande Windows PowerShell pouvez-vous utiliser pour afficher la table de routage local d'un ordinateur au lieu d'utiliser **route print** ?

Réponse : Vous pouvez utiliser l'applet de commande **Get-NetRoute** pour consulter la table de routage local d'un ordinateur.

Module 2

Implémentation de DHCP

Sommaire :

Leçon 1

Présentation du rôle serveur DHCP

Sommaire :

Questions et réponses

Question : S'il existe plusieurs serveurs DHCP répondant aux demandes des clients, comment est-ce que le client choisit quelle offre DHCP accepter ?

Réponse : Le client n'a pas de préférence. Il acceptera la première offre qu'il reçoit.

Question : Tous les systèmes d'exploitation Windows sont configurés pour être des clients DHCP après l'installation initiale du système d'exploitation.

( ) Vrai

( ) Faux

Réponse :

(√) Vrai

( ) Faux

Commentaire :

Même les systèmes d'exploitation de serveur commencent comme clients DHCP. Vous devez configurer une adresse statique si c'est ce que vous souhaitez.

Leçon 2

Déploiement de DHCP

Sommaire :

Questions et réponses

Question : Tout administrateur de domaine peut autoriser un Serveur DHCP.

( ) Vrai

( ) Faux

Réponse :

( ) Vrai

(√) Faux

Commentaire :

Seul un administrateur d'entreprise peut autoriser un Serveur DHCP.

Question : Dans le cas d'un conflit entre les options DHCP, quel niveau prévaudra ?

( ) Niveau de serveur

( ) Niveau de classe

( ) Niveau d'étendue

( ) Niveau de la réservation du client

Réponse :

( ) Niveau de serveur

( ) Niveau de classe

( ) Niveau d'étendue

(√) Niveau de la réservation du client

Commentaire :

Les options attribuées aux réservations des clients annuleront toutes les options contradictoires.

Ressources

Attribution et gestion des adresses IPv4 avec DHCP

 **Lectures supplémentaires :** Pour plus d'informations sur les applets de Serveur DHCP dans Windows PowerShell, reportez-vous à « applets de Serveur DHCP dans Windows PowerShell » : http://aka.ms/Blsmzw

 **Lectures supplémentaires :** Pour les applets Windows PowerShell pour DHCP ajoutés dans Windows Server 2012 R2, reportez-vous à « Quoi de neuf dans DHCP ? » : http://aka.ms/Hfgoye

Démonstration : Installez un Serveur DHCP et exécutez des tâches de post-installation

Procédure de démonstration

Installez le rôle Serveur DHCP

1. Vous connecter à **LON-SVR1** en tant que **Adatum\Administrator** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur **Démarrer**, puis sur la vignette **Gestionnaire de serveur**.
3. Sur le tableau de bord **Gestionnaire de serveur**, allez sur **Ajouter des rôles et des fonctionnalités**.

4. Sur la page **Avant de commencer**, faites **Suivant**.
5. Dans la page **Sélectionner le type d'installation**, appuyez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
7. Sur la page **Sélectionner les rôles de serveur**, sélectionnez **Serveur DHCP**.
8. Dans **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
9. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
10. Dans la page **Serveur DNS**, cliquez sur **Suivant**.
11. Dans la page **Confirmer les sélections d'installation**, faites **Installer**. Cette installation prend quelques minutes.
12. Une fois l'installation terminée, pressez sur **Fermer**.

Effectuez les tâches post-installation

1. Cliquez sur l'icône **Notifications** (triangle orange) dans la barre de menu supérieure, puis sur le lien **Réaliser la configuration DHCP**.
2. Dans l'**Assistant Configuration post-installation DHCP**, sur la page **Description**, lisez le texte, puis cliquez sur **Suivant**.
3. Sur la page **Autorisation**, faites **Valider**.
4. Lisez le texte sur la page **Résumé**, puis faites **Fermer**.
5. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Services**.
6. Sélectionnez le service **Serveur DHCP**, puis cliquez sur le lien **Redémarrer**.
7. Fermez la console Services Microsoft Management (MMC).

Démonstration : Configuration d'un Serveur DHCP

Procédure de démonstration

Créer une étendue DHCP

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP**.
2. Dans le volet de gauche, cliquez pour sélectionner **lon-svr1.adatum.com**. Cela ouvrira le nœud **IPv4**.
3. Cliquez pour sélectionner le nœud **IPv4**. Dans le volet **Actions**, cliquez sur **Plus d'actions**, puis sur **Nouvelle étendue**.
4. Dans l'**Assistant Nouvelle étendue**, cliquez sur **Suivant**.
5. Sur la page **Nom de l'étendue** dans la zone **Nom**, tapez **Adatum**, puis cliquez sur **Suivant**.
6. Sur la page **Plage d'adresses IP**, dans la zone de texte **Adresse IP de début**, tapez **10.0.0.100** et dans la zone de texte **Adresse IP de fin**, tapez **10.0.0.150**.

   Remarque : Notez que le champ de masque de sous-réseau se remplit automatiquement en fonction du masque de sous-réseau par défaut pour une plage d'adresses de classe **A**.

7. Modifiez le masque de sous-réseau sur **255.255.255.0**, puis cliquez sur **Suivant**.

8. Sur la page **Ajouter des exclusions et un délai**, cliquez sur **Suivant**.
9. Sur la page **Durée du bail**, modifiez la valeur du champ **Jours** à **1**, puis cliquez sur **Suivant**.
10. Sur la **Configurer les options DHCP**, sélectionnez **Non, je vais configurer ces options plus tard**, faites sur **Suivant**, puis **Terminer**.

Remarque : Notez que le dossier Étendue a une flèche rouge vers le bas pour indiquer que l'étendue n'est pas activée.

Configurer les options DHCP

1. Développez le nœud **IPv4**, puis le dossier **Étendue [10.0.0.0] Adatum**.
2. Cliquez pour sélectionner le dossier **Options d'étendue**. Cliquez avec le bouton droit sur le dossier, puis faites **Configurer les options**.
3. Dans la zone de texte **Options d'étendue**, sélectionnez **Routeur 003**. Dans la zone **Adresse IP**, tapez **10.0.0.1**, puis cliquez sur **Ajouter**.
4. Sélectionnez **Serveurs DNS 006**. Dans la zone de texte **adresse IP**, tapez **172.16.0.10**, cliquez sur **Ajouter**, puis faites **OK.**
5. Cliquez avec le bouton droit sur le dossier **Étendue [10.0.0.0] Adatum**, puis appuyez sur **Activer**.
6. Notez que la **flèche rouge vers le bas** n'apparaît plus sur le dossier **Étendue**.

Créer une réservation DHCP

1. Cliquez pour sélectionner le dossier **Réservations**. Cliquez avec le bouton droit sur le dossier, puis cliquez sur **Nouvelle réservation**.
2. Dans la boîte de dialogue **Nouvelle réservation**, dans la zone de texte **Nom de réservation**, entrez **Sales Printer**.
3. Dans la zone **Adresse IP**, tapez **10.0.0.120**.
4. Dans la zone de texte **adresse MAC**, tapez **00-14-6D-01-73-6B**, cliquez sur **Ajouter**, puis sur **Fermer**.

Leçon 3

Gestion et dépannage DHCP

Sommaire :

Questions et réponses

Question : Comment pouvez-vous empêcher que les plages d'adresses du sous-réseau soient attribuées à des clients ?

> **Réponse :** Configurez les exclusions pour empêcher une ou plusieurs plages d'adresses du sous-réseau d'être distribuées.

Question : La différence de temps maximale qui peut exister entre deux serveurs DHCP dans une relation de basculement est de cinq minutes.

( ) Vrai

( ) Faux

> **Réponse :**
>
> ( ) Vrai
>
> (√) Faux
>
> **Commentaire :**
>
> La différence de temps maximale qui peut exister entre deux serveurs DHCP dans une relation de basculement est seulement d'une minute.

Ressources

Options avancées pour la configuration DHCP

 **Lectures supplémentaires :** Pour plus d'informations sur les politiques de DHCP pour les périphériques, reportez-vous à « Utilisation des politiques DHCP pour définir différentes durées de bail pour différents types de périphériques » : http://aka.ms/Ijz5m7

Démonstration : Configuration de la redondance DHCP

Procédure de démonstration

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DHCP** dans la liste déroulante.
2. Dans la console **DHCP**, développez **lon-dc1.adatum.com**, sélectionnez et cliquez avec le bouton droit sur **IPv4**, puis faites **Configurer un basculement**.
3. Dans l'Assistant de **configuration du basculement**, cliquez sur **Suivant**.
4. Dans la page **Spécifier le Serveur partenaire à utiliser pour le basculement**, dans la zone de texte **Serveur partenaire**, tapez **172.16.0.11**, puis cliquez sur **Suivant**.
5. Dans la page **Créer une relation de basculement**, dans la zone **Nom de la relation**, tapez **Adatum**.
6. Dans le champ **Délai de transition maximal du client**, définissez les **heures** sur **0**, puis les **minutes** sur **15**.
7. Vérifiez que le **Mode** est réglé sur **Équilibrer la charge**.
8. Vérifiez que le champ **Pourcentage d'équilibrage de charge** est réglé sur **50%**.
9. Activez la case à cocher **Intervalle de basculement d'état.** Laissez la valeur par défaut de **60** minutes.
10. Dans la zone de texte Activer le secret partagé de l'authentification du message, tapez Pa$$w0rd, puis cliquez sur Suivant.

11. Cliquez sur **Terminer**, puis sur **Fermer**.
12. Basculez vers **LON-SVR1**.
13. Actualisez le nœud **IPv4**, développez le nœud, puis développez **Étendue [172.16.0.0] Adatum**.
14. Cliquez sur **Pool d'adresses** et notez que le pool d'adresses est configuré.
15. Cliquez sur **Options d'étendue** et notez que les options d'étendues sont configurées.
16. Fermez la console DHCP sur LON-DC1 et LON-SVR1.

Révision du module et éléments à retenir

Bonnes Pratiques

Voici les meilleures pratiques pour travailler avec DHCP :

- Configurer les relations de basculement DHCP pour fournir une haute disponibilité.
- S'assurer que les périodes sont appropriées. Des périodes plus courtes sont généralement recommandées pour les réseaux sans fil en raison de la nature transitoire des clients sans fil.
- Créer des réserves pour les appareils qui ont besoin d'adresses IP qui ne changent pas.
- Activer la vérification DHCP pour suivre les tendances et l'historique.
- Activer la protection du nom.

Problèmes courants et conseils de dépannage

Problème courant	Conseil de dépannage.
Les clients sont en mesure d'obtenir les adresses IP	Vérifiez que l'étendue a des adresses disponibles et que le serveur est en ligne.

Questions et réponses sur les ateliers pratiques

Atelier pratique : Implémentation de DHCP

Questions et réponses

Question : Pourquoi les étendues créées dans l'exercice commencent à 172.16.x.2 et non à 172.16.x.1 ?

Réponse : La passerelle par défaut utilise l'adresse 172.16.x.1 dans tous les cas.

Question : Quel est l'emplacement par défaut de la base de données DHCP ?

Réponse : L'emplacement par défaut de la base de données DHCP est le dossier **%systemroot%\System32\Dhcp**.

Module 3

Implémentation d'IPv6

Sommaire :

Leçon 1

Vue d’ensemble de l’adressage IPv6

Sommaire :

Questions et réponses

Vue d'ensemble de l'adressage IPv6

Question : Utilisez l'application de la calculatrice sur votre ordinateur pour convertir l'adresse IPv6 suivante de binaire en hexadécimal. Ensuite, simplifiez l'adresse hexadécimale en utilisant la compression zéro.

Adresse IPv6 binaire :

0010 0000 0000 0001 0000 1101 0001 0001 0010 0010 0011 0100 0000 0000 0000 0000

0000 0011 1011 1011 0000 0000 1010 1100 1011 1100 0011 1011 1010 1101 0110 1011

Réponse : Adresse IPv6 au format hexadécimal : 2001:0D11:2234:0000:03BB:00AC:CD39:AD6B

Adresse IPv6 simplifiée en utilisant la compression zéro : 2001:D11:2234::3BB:AC:CD39:AD6B

Leçon 2

Configuration d'un hôte IPv6

Sommaire :

Questions et réponses

Question : Les serveurs de votre organisation sont configurés pour IPv6 et ils reçoivent des adresses IPv6 à partir d'un Serveur DHCPv6. Vous devez ajouter une adresse IPv6 à l'interface sur un de vos serveurs. Que devez-vous faire ?

Réponse : Si vous utilisez l'applet **New-NetIPAddress** pour ajouter une adresse IPv6 à une interface sur laquelle le DHCP est déjà activé, le DHCP est automatiquement désactivé. Par conséquent, vous devez soit :

1. Utiliser l'applet **Set-NetIPInterface** pour désactiver la configuration DHCP sur l'interface, puis **Set-NetIPAddress** et **New-NetIPAddress** pour configurer les adresses IPv6 sur l'interface.
2. Utiliser **New-NetIPAddress** pour désactiver la configuration DHCP sur l'interface, puis **New-NetIPAddress** pour configurer l'adresse IPv6 supplémentaire sur l'interface.

Ressources

Outils pour configurer IPv6

Lectures supplémentaires : Pour plus d'informations sur l'utilisation de Windows PowerShell, reportez-vous à la liste des applets de commande de configuration IPv6 sur : http://aka.ms/Sscfek

Lectures supplémentaires : Pour plus d'informations sur l'utilisation de Netsh, reportez-vous à la liste des commandes Netsh pour configurer IPv6 sur : http://aka.ms/Dley4n

Démonstration : Configuration d'IPv6

Procédure de démonstration

Afficher la configuration IPv6 à l'aide d'IPconfig

1. Sur LON-DC1, si nécessaire, ouvrez une invite de commandes **Windows PowerShell**.
2. À l'invite Windows PowerShell, entrez **ipconfig**, puis appuyez sur Entrée.

   Notez que ceci retourne une adresse IPv6 de liaison locale.
3. Tapez **Get-NetIPAddress** et appuyez sur Entrée.

Configurer IPv6 sur LON-DC1

1. Sur LON-DC1, dans le **Gestionnaire de serveur**, cliquez sur **Serveur local**.
2. Dans la boîte de dialogue **Propriétés du serveur local** en regard d'**Ethernet**, cliquez sur **172.16.0.10, Compatible IPv6**.
3. Dans la fenêtre Connexions réseau, cliquez avec le bouton droit sur **Ethernet**, puis cliquez sur **Propriétés**.
4. Cliquez sur **Protocole Internet version 6 (TCP/IPv6),** puis sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de Protocole Internet Version 6 (TCP/IPv6)** , cliquez sur **Utiliser l'adresse IPv6 suivante.**
6. Dans la zone Adresse IPv6, tapez **FD00:AAAA:BBBB:CCCC::A**
7. Dans la zone **Longueur du préfixe de sous-réseau**, tapez **64**.
8. Dans la zone **Serveur DNS préféré**, tapez **::1**, puis cliquez sur **OK**.

9. Dans la zone **Propriétés Ethernet**, cliquez sur **Fermer**.
10. Fermez la fenêtre **Connexions réseau**. Si la page **Réseau** s'ouvre, cliquez sur **Oui**.

Configurer IPv6 sur LON-SVR1

1. Sur LON-SVR1, dans le Gestionnaire de serveur, cliquez sur **Serveur local**.
2. Dans la boîte de dialogue **Propriétés du serveur local**, en regard d'**Ethernet**, cliquez sur **172.16.0.11**, **Compatible IPv6**.
3. Dans la fenêtre **Connexions réseau**, cliquez avec le bouton droit sur **Ethernet**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés Ethernet**, cliquez sur **Protocole Internet version 6 (TCP/IPv6)**, puis sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de Protocole Internet version 6 (TCP/IPv6)**, cliquez sur **Utiliser l'adresse IPv6 suivante**.
6. Dans la zone **Adresse IPv6**, tapez **FD00:AAAA:BBBB:CCCC::15**.
7. Dans la zone **Longueur du préfixe de sous-réseau**, tapez **64**.
8. Dans la zone **Serveur DNS préféré**, tapez **FD00:AAAA:BBBB:CCCC::A**, puis cliquez sur **OK**.
9. Dans la boîte de dialogue **Propriétés Ethernet**, cliquez sur **Fermer**.
10. Fermez la fenêtre **Connexions réseau**.

Vérifier que la communication IPv6 est fonctionnelle

1. Sur LON-SVR1, cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
2. À l'invite Windows PowerShell, entrez **ipconfig**, puis appuyez sur Entrée.

   Notez que l'adresse IPv6 de liaison locale et l'adresse IPv6 que vous avez configurées s'affichent toutes les deux.
3. À l'invite de commandes, tapez **ping -6 lon-dc1**, puis appuyez sur Entrée.
4. Tapez **ping -4 lon-dc1**, puis appuyez sur Entrée.

 **Remarque :** Laissez tous les ordinateurs virtuels dans leur état actuel pour la prochaine démonstration de ce module.

Démonstration : Configuration DHCP pour IPv6

Procédure de démonstration

Configurer une étendue et des options d'étendue dans DHCP

1. Sur LON-DC1, sur la barre des tâches, cliquez sur l'icône **Gestionnaire de serveur**, puis dans la fenêtre Gestionnaire de serveur, dans le coin supérieur droit, cliquez sur **Outils**, puis cliquez sur **DHCP**.
2. Dans la console DHCP, dans le volet de navigation, développez **LON-DC1.adatum.com**, développez **IPv6**, sélectionnez puis cliquez avec le bouton droit sur **IPv6** et cliquez sur **Nouvelle étendue**.
3. Dans l'**Assistant Nouvelle Étendue**, cliquez sur **Suivant**.
4. Sur la page **Nom de l'étendue**, dans la zone **Préfixe**, tapez **Headquarters IPv6**, puis cliquez sur **Suivant**.

5. Sur la page **Préfixe d'étendue**, dans la zone de texte **Préfixe**, tapez **fd00:0000:0000:0000::**, puis cliquez sur **Suivant**.
6. Sur la page **Ajouter des exclusions**, tapez ce qui suit, cliquez sur **Ajouter**, puis cliquez sur **Suivant** :
   - Adresse IPv6 de début : **0000:0000:0000:0000**
   - Adresse IPv6 de fin : **0000:0000:0000:00ff**
7. Sur la page **Bail d'étendue**, cliquez sur **Suivant**.
8. Sur la page **Fin de l'Assistant Nouvelle Étendue**, cliquez sur **Terminer**.

Configurer DNS avec un enregistrement de ressource hôte IPv6 (AAAA)

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Dans le Gestionnaire DNS, développez **LON-DC1**, développez **Zones de recherche directes**, puis cliquez sur **Adatum.com**.
3. Lisez les enregistrements répertoriés pour la zone et notez que LON-DC1 et LON-SVR1 ont enregistré leurs adresses IPv6 de manière dynamique avec le Serveur DNS.
4. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
5. Dans la fenêtre **Nouvel hôte**, dans la zone **Préfixe**, tapez **WebApp**.
6. Dans la zone **Adresse IP**, tapez **FD00:AAAA:BBBB:CCCC::A**, puis cliquez sur **Ajouter un hôte**.
7. Cliquez sur **OK** pour effacer le message de réussite.
8. Cliquez sur **Terminé** pour fermer la fenêtre **Nouvel hôte**.

Vérifier la résolution de noms pour un enregistrement de ressource hôte IPv6 (AAAA)

1. Sur LON-SVR1, depuis le menu **Démarrer**, cliquez sur **Windows PowerShell**.
2. À l'invite de commandes Windows PowerShell, saisissez **Test-NetConnection WebApp.adatum.com**, puis appuyez sur Entrée.

Leçon 3

Transition d'IPv4 à IPv6

Sommaire :

Ressources

Qu'est-ce qu'ISATAP ?

Lectures supplémentaires :

- Pour plus d'informations sur les applets de transition réseau dans Windows PowerShell, reportez-vous à « Applets de transition réseau dans Windows PowerShell » sur : http://aka.ms/Vzxldt
- Pour plus d'informations sur les Commandes Netsh pour l'interface ISATAP, reportez-vous à « Commandes Netsh pour l'interface ISATAP » sur : http://aka.ms/E5u3fk

Qu'est-ce que 6to4 ?

Lectures supplémentaires : Pour plus d'informations sur les commandes Netsh pour l'interface 6to4, reportez-vous à « commandes Netsh pour l'interface 6to4 » sur : http://aka.ms/Qqqgu7

Qu'est-ce que Teredo ?

Lectures supplémentaires : Pour plus d'informations sur les commandes Netsh pour l'interface Teredo, reportez-vous à « commandes Netsh pour l'interface Teredo » sur : http://aka.ms/Tsgd7b

Qu'est-ce que PortProxy ?

Lectures supplémentaires : Pour plus d'informations sur les technologies de transition IPv6, reportez-vous à « Technologies de transition IPv6 » sur http://aka.ms/E8c95o

Révision du module et éléments à retenir

Bonnes pratiques

Utilisez les meilleures pratiques suivantes lors de la mise en œuvre d'IPv6 :

- Ne désactivez pas IPv6 sur Windows Vista, Windows Server 2008 ainsi que les nouveaux clients Windows et les systèmes d'exploitation Windows Server.
- Activez la coexistence d'IPv4 et IPv6 dans votre organisation plutôt que d'utiliser les technologies de transition.
- Utilisez les adresses IPv6 locales uniques sur votre réseau interne.
- Utilisez Teredo pour mettre en œuvre la connectivité IPv6 sur Internet IPv4.

Questions de contrôle des acquis

Question : Quelle est la principale différence entre 6to4 et Teredo ?

> **Réponse :** Les deux protocoles permettent une connectivité IPv6 sur Internet IPv4. Cependant, seul Teredo peut fournir la connectivité via NAT.

Question : Comment pouvez-vous fournir un Serveur DNS à un hôte IPv6 de façon dynamique ?

> **Réponse :** Pour fournir un Serveur DNS à un hôte IPv6 dynamique, vous devez utiliser DHCPv6. Vous pouvez utiliser des annonces de routeur pour fournir la partie réseau d'une adresse IPv6, mais les annonces de routeur ne peuvent pas distribuer les adresses IP du Serveur DNS.

Question : Votre organisation envisage de mettre en œuvre IPv6 en interne. Après quelques recherches, vous avez identifié les adresses IPv6 locales uniques comme le type correct d'adresses IPv6 à utiliser pour le réseau privé. Pour utiliser les adresses IPv6 locales uniques, vous devez sélectionner un identificateur de 40 bits qui fait partie du réseau. Un collègue suggère que vous n'utilisiez que des zéros pour les 40 bits. Pourquoi n'est-ce pas une bonne idée ?

> **Réponse :** L'identifiant d'organisation 40 bit dans une adresse IPv6 locale doit être généré de manière aléatoire. Cela permet d'assurer avec la plus grande probabilité que deux organisations n'utilisent pas le même identificateur d'organisation. Si deux organisations utilisent le même identificateur d'organisation, les réseaux ne peuvent pas être reliés entre eux après une fusion.

Question : Avec combien d'adresses IPv6 un nœud IPv6 doit-il être configuré ?

> **Réponse :** Un nœud IPv6 n'est pas lié à un nombre spécifique d'adresses IPv6. Ceci dépend de la configuration de l'organisation. Chaque nœud IPv6 a une adresse IPv6 en liaison-locale. En outre, il pourrait également avoir une adresse IPv6 locale unique pour la connectivité interne et une adresse IPv6 unicast globale pour la connectivité Internet IPv6.

Questions et réponses sur les ateliers pratiques

Atelier pratique : Configuration et évaluation des technologies de transition IPv6

Questions et réponses

Question : Dans cet exercice, avez-vous configuré IPv6 en mode statique ou dynamique ?

Réponse : Vous avez configuré IPv6 dynamiquement dans cet exercice. Vous avez ajouté les deux réseaux IPv6 au routeur et les annonces de routeur ont configuré LON-DC1 et LON-CL1 avec l'adresse réseau correcte.

Question : Pourquoi n'avez-vous pas eu besoin de configurer EU-RTR avec l'adresse IPv4 du routeur ISATAP ?

Réponse : La configuration par défaut pour les systèmes d'exploitation client Windows est configurée pour résoudre l'ISATAP en utilisant le DNS pour localiser l'adresse IPv4 du routeur ISATAP. EU-RTR utilisait la configuration par défaut.

Module 4

Implémentation de DNS

Sommaire :

Leçon 1

Implémentation de serveurs DNS

Sommaire :

Questions et réponses

Classez l'activité

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

Éléments	
1	Contient une base de données des noms d'hôtes et les adresses IP
2	Possède des catégories de résolution avant et inversée
3	Est géré par le service client DNS
4	Répond aux demandes de clients
5	Contient des enregistrements de ressources
6	Génère des demandes de clients
7	S'il ne dispose pas des informations de cartographie nécessaire, envoyez les demandes vers d'autres serveurs DNS
8	Capacité de reproductibilité
9	Facilite la mise en cache des applications résolues dans un cache local du client pour une utilisation future

Catégorie 1		Catégorie 2		Catégorie 3
Serveur DNS		Zones DNS		Résolveur DNS

Réponse :

Catégorie 1		Catégorie 2		Catégorie 3
Serveur DNS		Zones DNS		Résolveur DNS
Contient une base de données des noms d'hôtes et les adresses IP Répond aux demandes de clients S'il ne dispose pas des informations de cartographie nécessaire, envoyez les demandes vers d'autres serveurs DNS		Possède des catégories de résolution avant et inversée Contient des enregistrements de ressources Capacité de reproductibilité		Est géré par le service client DNS Génère des demandes de clients Facilite la mise en cache des applications résolues dans un cache local du client pour une utilisation future

Ressources

Outils et techniques pour résoudre la résolution de noms

Lectures supplémentaires : Pour plus d'informations sur les paramètres de l'applet **Get-DnsServerStatistics**, reportez-vous à « Get-DnsServerStatistics » sur : http://aka.ms/U9442y

Liens de référence : Pour télécharger le package Dnslint.exe, reportez-vous à « Description de l'utilitaire DNSLint » sur : http://aka.ms/Vw9oyv

Démonstration : Installation et configuration du rôle de DNS

Procédure de démonstration

Installer le rôle serveur DNS

1. Sur **TOR-SVR1**, connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur **Démarrer**, puis cliquez sur **Gestionnaire de serveur**.
3. Dans le Gestionnaire de serveur, dans le volet de navigation, cliquez sur **Tableau de bord** puis, dans le volet **informations**, cliquez sur **Ajouter des rôles et fonctionnalités**.
4. Dans la fenêtre de dialogue **Assistant ajout de rôles et de fonctionnalités**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, assurez-vous que la case **TOR-SVR1.adatum.com** est cochée dans la zone **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**.
8. Dans la boîte de dialogue **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**.
9. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
10. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
11. Dans la page **Serveur DNS**, cliquez sur **Suivant**.
12. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
13. Après avoir installé le rôle, cliquez sur **Fermer**.

Activer les pings

1. Sur TOR-SVR1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Pare-feu Windows avec fonctions avancées de sécurité**.
2. Dans la console **Pare-feu Windows avec fonctions avancées de sécurité**, sélectionnez **Règles de trafic entrant**.
3. Dans le volet d'information des **Règles de trafic entrant**, faites défiler vers le bas et cliquez-droit sur l'élément **Partage des fichiers et de l'impression (Echo Request - ICMPv4-In)** et cliquez sur **Activer la règle**.
4. Cliquez-droit et activez l'élément intitulé **Partage des fichiers et de l'impression (Echo Request - ICMPv6-In).**

5. Fermez la console **Pare-feu Windows avec fonctions avancées de sécurité**.
6. Cliquez sur le bouton **Démarrer** et, dans le menu Démarrer, cliquez sur **Windows PowerShell**.
7. Dans **Windows PowerShell**, tapez la commande suivante, puis appuyez sur **Entrée** :

```
Ping 172.16.0.10
```

8. Vous devriez obtenir quatre réponses.
9. Fermez **Windows PowerShell**.
10. Basculez sur **LON-DC1**, puis cliquez sur le bouton **Démarrer** et, dans le menu Démarrer, cliquez sur **Windows PowerShell**.
11. Dans **Windows PowerShell**, tapez la commande suivante, puis appuyez sur **Entrée** :

```
Ping 172.16.18.20
```

12. Vous devriez obtenir quatre réponses.
13. Fermez **Windows PowerShell**.

Configurer le rôle serveur DNS

1. Sur **TOR-SVR1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Dans le Gestionnaire DNS, développez **TOR-SVR1**, sélectionnez et cliquez avec le bouton droit sur **TOR-SVR1**, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de TOR-SVR1**, cliquez sur l'onglet **Redirecteurs**.
4. Dans l'onglet **Redirecteurs**, cliquez sur **Modifier**. Dans la fenêtre **Modifier les transferts**, dans la zone de texte **Cliquez ici pour ajouter une adresse IP ou le nom du DNS**, entrez **172.16.0.10**, puis appuyez sur Entrée. En quelques minutes, l'adresse IP se confirmera, et vous obtiendrez une coche verte à côté de l'adresse.

   Remarque : Si vous obtenez une autre indication dans la colonne **adresse IP** avec un X rouge, qui dit **Le nom demandé** et une indication dans la colonne **Validé**, qui dit **Aucune adresse IPv6**, sélectionnez le message, puis cliquez sur le bouton **Supprimer**.

   Cliquez sur **OK**.
5. Dans la fenêtre **Propriétés de TOR-SVR1**, cliquez sur **OK**.
6. Dans l'arborescence de la **console DNS**, sélectionnez et cliquez-droit sur **Zones de recherche directes**, puis cliquez sur **Nouvelle zone**.
7. Dans l'**Assistant Nouvelle zone** qui s'ouvre, cliquez sur **Suivant**.
8. Sur la page **Type de zone**, cliquez sur **Suivant**.
9. Dans la page **Nom de la zone**, dans la zone de texte **Nom de la zone**, entrez **Contoso.com**, puis cliquez sur **Suivant**.
10. Sur la page **Fichier de zone**, cliquez sur **Suivant**.
11. Dans la page **Mise à niveau dynamique**, cliquez sur **Suivant**.
12. Dans la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.
13. Dans l'arborescence de la console, développez **Zones de recherche directes**, double-cliquez sur **Contoso.com**, cliquez-droit sur **Contoso.com**, puis sélectionnez **Nouvel hôte (A ou AAAA)**.

14. Dans la fenêtre **Nouvel hôte**, dans la zone de texte **Nom**, entrez **ATL-SVR1**, dans la zone de texte **Adresse IP**, entrez **172.16.18.125**, puis cliquez sur **Ajouter un hôte**.
15. Dans la fenêtre pop-up **DNS**, cliquez sur **OK**, puis dans la fenêtre **Nouvel hôte**, cliquez sur **Terminé**.

Démonstration : Résolution des problèmes liés à la résolution de noms

Procédure de démonstration

Utilisez les cmdlets de Windows PowerShell pour résoudre les DNS

1. Sur **LON-CL1**, sur la **barre de tâches**, dans le champ **Rechercher**, tapez **PowerShell** puis, dans la liste qui s'affiche, cliquez sur **Windows PowerShell.**
2. Dans la console **Windows PowerShell**, entrez les applets suivants, puis appuyez sur Entrée après chaque commande :

```
Get-DnsClientServerAddress
Clear-DnsClientCache
```

   Notez que l'adresse du serveur DNS affecté à London_Network IPv4 est **172.16.0.10**. C'est **LON-DC1**.
3. Notez les entrées marquées **London_Network** dans la colonne InterfaceAlias, et l'entrée marquée **IPv4** dans la colonne Famille d'adresses. Dans la colonne Interface Index, notez le numéro d'Interface Index qui se trouve sur la même ligne que London_Network et IPv4. Notez ce numéro. Vous utiliserez ce numéro spécifique d'Interface Index à une étape ultérieure.
4. Dans la console **Windows PowerShell**, entrez la commande suivante, puis appuyez sur Entrée :

```
Resolve-DnsName lon-dc1
```

   Noter l'adresse retournée. Ne fermez pas Windows PowerShell.
5. Cliquez avec le bouton droit sur **Démarrer**, puis sur **Panneau de configuration**.
6. Dans le **Panneau de configuration**, cliquez sur le lien hypertexte **Réseau et Internet**.
7. Sur la page **Réseau et Internet**, cliquez sur le lien hypertexte **Centre de réseau et partage**.
8. Sur la page **Centre Réseau et partage**, cliquez sur le lien hypertexte **London_Network**.
9. Dans la fenêtre **London_Network Status**, cliquez sur **Détails**.
10. Sur la fenêtre contextuelle **Détails des connexions au réseau**, notez les informations affichées, puis cliquez sur **Fermer**.
11. Sur la page **London_Network Status**, cliquez sur **Propriétés**.
12. Faites défiler jusqu'à la section **Cette connexion utilise les éléments suivants**, sélectionnez **Internet Protocol Version 4 (TCP / IPv4)**, puis cliquez sur **Propriétés**.
13. Dans la boîte de dialogue **Propriétés : Internet Protocol Version 4 (TCP / IPv4)**, sélectionnez les boutons radio **Obtenir une adresse IP automatiquement** et **Obtenir l'adresse du serveur DNS automatiquement**, cliquez sur **OK**, puis cliquez deux fois sur **Fermer**.
14. Basculez sur la console **Windows PowerShell**, tapez les applets suivants en appuyant sur Entrée à chaque fois. *X* est le numéro d'Interface Index que vous avez noté à l'étape 3 :

```
Set-DnsClientServerAddress -InterfaceIndex X -ResetServerAddresses
Clear-DnsClientCache
Get-DnsClientServerAddress
```

Remarque : Notez qu'il n'y a pas d'adresse IP pour IPv4.

15. Dans la console **Windows PowerShell**, tapez l'applet suivant, où *X* est le numéro d'Interface Index que vous avez noté à l'étape 3, puis appuyez sur Entrée:

```
Set-DnsClientServerAddress –InterfaceIndex X –ServerAddress 172.16.0.10
```

16. Dans la console **Windows PowerShell**, entrez la commande suivante, puis appuyez sur Entrée :

```
Get-DnsClientServerAddress
```

Remarque : Notez qu'il existe désormais une adresse IPv4.

17. Dans la console **Windows PowerShell**, tapez l'applet suivant, appuyez sur Entrée, puis notez l'adresse qui s'affiche :

```
Resolve-DnsName lon-dc1
```

18. Retournez à la fenêtre **Centre Réseau et partage**, puis cliquez sur le lien hypertexte **Ethernet**.
19. Sur la page **état de London_Network**, cliquez sur **Propriétés**.
20. Sur la page **Propriétés Ethernet**, faites défiler vers la section **Cette connexion utilise les éléments suivants**, sélectionnez **Internet Protocol Version 4 (TCP / IPv4)**, puis cliquez sur **Propriétés**.
21. Dans la boîte de dialogue **Propriétés : Internet Protocol version 4 (TCP/IPv4)**, cliquez sur **Utiliser l'adresse IP suivante** et saisissez les données suivantes :
    - Adresse IP : 172.16.0.50
    - Masque de sous-réseau : 255.255.0.0
    - Passerelle par défaut : 172.16.0.1
22. Cliquez sur **OK**, puis cliquez sur **Fermer**.
23. Pour afficher le résultat des applets suivants, dans la console **Windows PowerShell**, tapez chacun des applets suivants, puis appuyez sur Entrée après chaque applet :

```
Get-DnsClientCache
Clear-DnsClientCache
Get-DnsClientCache
Get-DnsClientGlobalSetting
Inscrivez-DNSClient
```

24. Fermez les fenêtres **Windows PowerShell** et **Centre Réseau et partage**.

Utilisez des outils de ligne de commande pour résoudre les DNS

1. Sur **LON-CL1**, sur la **barre de tâches**, dans le champ **Rechercher**, tapez **cmd**. Dans la liste qui s'affiche, cliquez-droit sur **Invite de commandes**, puis cliquez sur **Exécuter en tant qu'administrateur**.
2. Dans la fenêtre de l'**invite de commandes**, entrez la commande suivante et appuyez sur Entrée :

```
ipconfig / all
```

3. Examinez le résultat qui s'affiche, et notez la section **Serveur DNS**.

4. Dans la fenêtre d'**Invite de commandes**, tapez la commande suivante et appuyez sur Entrée.

```
nslookup
```

Remarque : Vous devriez voir s'afficher l'adresse du serveur DNS de l'étape 3 ci-dessus. Notez la présence du signe **>**, qui montre que vous vous trouvez dans l'invite nslookup.

5. Dans la fenêtre d'**Invite de commandes**, tapez la commande suivante et appuyez sur Entrée.

```
LON-CL1
```

6. Dans la fenêtre de l'**invite de commandes**, entrez la commande suivante et appuyez sur Entrée :

```
exit
```

Remarque : Ne fermez aucune fenêtre ouverte.

7. Basculez vers **LON-DC1**.
8. Sur la **barre des tâches**, dans le champ **Rechercher**, tapez **cmd** puis, dans la liste qui s'affiche, cliquez-droit sur **Invite de commandes**, puis cliquez sur **Exécuter en tant qu'administrateur**.
9. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
dnscmd /?
```

Remarque : Utilisez le résultat pour examiner certaines des options dsncmd disponibles. Ne passez pas beaucoup de temps sur cette question car le second serveur DNS n'a pas été configuré.

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

```
ipconfig / displaydns
```

Remarque : Notez le résultat qui s'affiche.

11. À l'invite de commandes, saisissez les commandes ci-dessous, puis appuyez sur Entrée après chaque ligne :

```
ipconfig / flushdns
ipconfig / displaydns
```

Remarque : Notez qu'il n'y a plus de valeur de sortie.

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

```
ping LON-CL1.
```

Remarque : Notez que la commande ping a retourné le FQDN de **LON-CL1**. Faites remarquer aux stagiaires que ceci indique que la résolution de nom DNS a eu lieu avant même que le paquet ping n'ait été généré.

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

```
ipconfig / displaydns
```

Remarque : Notez que les informations sur l'enregistrement de ressources DNS LON-CL1 s'affichent.

14. Fermez toutes les fenêtres actives.

Démonstration : Test du serveur DNS

Procédure de démonstration

Testez le serveur DNS

1. Sur **TOR-SVR1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.
2. Dans le **Gestionnaire DNS**, développez **TOR-SVR1**, sélectionnez et cliquez avec le bouton droit sur **TOR-SVR1**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Avancé**. Sur cet onglet, vous pouvez configurer les options, y compris fixer le cache contre la pollution.
4. Cliquez sur l'onglet **Indications** de racine. Sur cet onglet, vous pouvez voir la configuration des serveurs d'indication de racines.
5. Cliquez sur l'onglet **Debug Logging**, puis sélectionnez la case **Paquets à déboguer** cochez la case. Sur cet onglet, vous pouvez configurer les options d'enregistrement de débogage.
6. Décochez la case **Enregistrer les paquets pour le débogage**, puis cliquez sur l'onglet **Enregistrement d'événement**.
7. Cliquez sur **Erreurs et avertissements**.
8. Cliquez sur l'onglet **Surveillance**. Vous pouvez effectuer des tests simples et récursifs du serveur en utilisant l'onglet **Surveillance**. Sélectionnez la case **Une simple requête sur ce serveur DNS**, puis cliquez sur **Tester maintenant**.
9. Dans la fenêtre **Propriétés de TOR-SVR1**, cliquez sur **OK**.
10. Cliquez sur **Démarrer**, puis cliquez sur **Windows PowerShell**.
11. Dans la console **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :

```
nslookup -d2 LON-DC1.Adatum.com
```

12. Passez en revue les informations fournies par Nslookup. Ceci fournit des informations de débogage détaillées.
13. Dans la console **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :

```
Test-DnsServer -AdresseIP 172.16.18.20
```

14. Observez les résultats.

15. Dans la console **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :

```
Get-DNSServerDiagnostics
```

16. Observez les résultats.
17. Laissez la fenêtre Windows PowerShell ouverte.

Utilisez la vérification et l'enregistrement des événements d'analyse

1. Sur **TOR-SVR1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **l'observateur d'événements**.
2. Agrandissez la console d'**Observateur d'événements**, puis attendez le chargement des informations d'Aperçu et de résumé, qui peut prendre quelques secondes.
3. Dans l'arborescence de la console, développez **Logs d'applications et de services**, développez **Microsoft**, développez **Fenêtres**, puis cliquez sur **Serveur DNS**.
4. Cliquez droit sur **Serveur DNS**, dirigez-vous vers **Afficher**, puis cliquez sur **Afficher les journaux analytiques et de débogage**. Le log d'analyse s'affiche.
5. Cliquez avec le bouton droit sur **Analytique**, puis cliquez sur **Propriétés**.
6. En-dessous de **Lorsque la taille maximale du log d'événements est atteinte**, sélectionnez **Ne pas remplacer les événements (Effacer les logs manuellement)**, sélectionnez **Activer la journalisation**, Puis cliquez sur **OK**. Dans la fenêtre **Voulez-vous activer ce log ?**, cliquez sur **OK**.
7. Basculez vers la console **Windows PowerShell**.
8. Dans la console **Windows PowerShell**, tapez les commandes suivantes, puis appuyez sur Entrée après chaque ligne :

```
Nslookup
Serveur tor-svr1.adatum.com
ATL-SVR1.contoso.com
```

9. Retournez à l'Observateur d'événements, et dans **Serveur DNS**, cliquez sur **Analytique**.
10. Cliquez-droit sur **Analytique**, puis cliquez sur **Actualiser**.
11. Le volet d'information de l'Observateur d'événements devrait désormais se remplir d'événements. Développez-en quelques-uns en expliquant les informations qu'ils vous fournissent. Vous devriez pouvoir identifier l'événement ayant retourné la requête réussie pour l'adresse **ATL-SVR1.contoso.com**, à l'étape 8 ci-dessus.
12. Fermez toutes les fenêtres actives. Ne vous déconnectez pas.

Leçon 2

La configuration des zones dans DNS

Sommaire :

Questions et réponses

Question : Un serveur DNS est autorisé pour une zone si :

( ) Il est défini sur Faisant autorité dans les propriétés du serveur DNS.

( ) Il héberge les enregistrements de ressources dans le fichier de zone qui est nommé pour la zone.

( ) Il contient plusieurs enregistrements de ressources CNAME.

( ) Il est défini sur Faisant autorité dans les propriétés de la zone.

( ) Il constitue le serveur de zone secondaire.

Réponse :

( ) Il est défini sur Faisant autorité dans les propriétés du serveur DNS.

(√) Il héberge les enregistrements de ressources dans le fichier de zone qui est nommé pour la zone.

( ) Il contient plusieurs enregistrements de ressources CNAME.

( ) Il est défini sur Faisant autorité dans les propriétés de la zone.

( ) Il constitue le serveur de zone secondaire.

Leçon 3

La configuration de la résolution de noms entre les zones DNS

Sommaire :

Questions et réponses

Question : Parmi les options suivantes, lesquelles constituent une zone souche (choisir deux réponses) ?

( ) L'adresse IP d'un ou de plusieurs serveurs maîtres que vous pouvez utiliser pour mettre à jour la zone.

( ) Les enregistrements de ressources ne figurent pas dans la zone d'un serveur DNS.

( ) Un cache de noms de domaines et les adresses IP associées des domaines les plus courants utilisés ou consultés par l'organisation.

( ) Les demandes de tous les noms Internet transmis à un serveur DNS via un fournisseur de services Internet (ISP).

( ) L'enregistrement de ressources de la zone déléguée Start of Authority, les enregistrements de ressources NS, et les enregistrements de ressources A.

Réponse :

(√) L'adresse IP d'un ou de plusieurs serveurs maîtres que vous pouvez utiliser pour mettre à jour la zone.

( ) Les enregistrements de ressources ne figurent pas dans la zone d'un serveur DNS.

( ) Un cache de noms de domaines et les adresses IP associées des domaines les plus courants utilisés ou consultés par l'organisation.

( ) Les demandes de tous les noms Internet transmis à un serveur DNS via un fournisseur de services Internet (ISP).

(√) L'enregistrement de ressources de la zone déléguée Start of Authority, les enregistrements de ressources NS, et les enregistrements de ressources A.

Leçon 4

Configuration de l'intégration de DNS avec AD DS

Sommaire :

Questions et réponses

Que sont les zones intégrées à Active Directory ?

Question : Existe-t-il des inconvénients à stocker des informations DNS dans AD DS ?

> **Réponse :** Si vous souhaitez répliquer les données DNS vers d'autres serveurs DNS non-Microsoft, vous ne devriez pas les stocker dans AD DS.

Démonstration : Configuration des zones AD DS intégrées

Procédure de démonstration

Promouvoir un serveur comme contrôleur de domaine

1. Sur **TOR-SVR1**, ouvrez le **Gestionnaire de serveur**, puis cliquez sur **Ajouter des rôles et fonctionnalités**.
2. Sur 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**, assurez-vous que **TOR-SVR1.Adatum.com** est sélectionné, puis cliquez sur **Suivant**.
5. Sur la page **Sélectionnez les rôles du serveur**, cliquez sur **Services du domaine Active Directory**.
6. Lorsque la fenêtre **Assistant Ajout de rôles et de fonctionnalités** apparaît, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
7. Dans la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Dans la page **Services de domaine Active Directory**, cliquez sur **Suivant**.
9. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Sur la page **Progression de l'installation**, lorsque le message **Installation réussie** apparaît, cliquez sur **Fermer**.
11. Dans la console **Gestionnaire de serveur**, sur la page de navigation, cliquez sur **AD DS**.
12. Dans la barre de titre où l'on voit **Configuration requise pour les services de domaine Active Directory sur TOR-SVR1**, cliquez sur **Plus**.
13. Dans la page **Tous les détails et notifications de la tâche Tous les serveurs**, cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.
14. Dans l'**Assistant de configuration des services de domaine Active Directory**, sur la page **Configuration de déploiement**, veillez à ce que la mention **Ajouter un contrôleur de domaine à un domaine existant** soit sélectionnée, puis cliquez sur **Suivant**.
15. Sur la page **Options de contrôleur de domaine**, assurez-vous que les options **Domain Name System (DNS)** et **Catalogue mondial (GC)** sont toutes les deux sélectionnés.
16. Dans les zones de texte **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa$$w0rd**, puis cliquez sur **Suivant**.
17. Dans la page **Options DNS**, cliquez sur **Suivant**.
18. Dans la page **Options supplémentaires**, cliquez sur **Suivant**.
19. Dans la page **Chemins d'accès**, cliquez sur **Suivant**.
20. Dans la page **Examiner les options**, cliquez sur **Suivant**.

21. Dans la page **Confirmer les conditions préalables**, cliquez sur **Installer**.
22. Sur la barre d'applications **Vous êtes sur le point d'être déconnecté**, cliquez sur **Fermer**.

Remarque : Le serveur redémarre automatiquement dans le cadre de la procédure.

23. Après le redémarrage de **TOR-SVR1**, connectez-vous en tant qu'**Adatum\Administrateur** à l'aide du mot de passe **Pa$$w0rd**.

Créer une zone intégrée à Active Directory

1. Sur **LON-DC1**, ouvrez le **Gestionnaire de serveur**.
2. Cliquez sur **Outils**, puis sur **DNS**.
3. Dans la console **Gestionnaire DNS**, cliquez, puis cliquez-droit sur **LON-DC1**, et enfin sur **Nouvelle zone**.
4. Dans l'**Assistant Nouvelle zone**, cliquez sur **Suivant**.
5. Sur la page **Type de Zone**, cliquez sur **zone principale**, veillez à ce que l'option **Conserver la zone dans Active Directory** soit sélectionnée, puis cliquez sur **Suivant**.

Remarque : Faites remarquer que cette option permet de confirmer que la zone est dans AD DS.

6. Sur la page **Zone Active Directory : étendue de la réplication**, passez en revue les options disponibles, puis, sans apporter de modifications, cliquez sur **Suivant**.
7. Sur la page **Zone de recherche directe ou inversée**, sélectionnez **Zone de recherche directe**, puis cliquez sur **Suivant**.
8. Dans la page **Nom de la zone**, dans la zone de texte **Nom de la zone**, entrez **TreyResearch.net**, puis cliquez sur **Suivant**.
9. Sur la page **Mise à jour dynamique**, consultez les options disponibles, sélectionnez **Autoriser uniquement les mises à jour dynamiques sécurisées**, puis cliquez sur **Suivant**.
10. Sur la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.
11. Dans la console **Gestionnaire DNS**, développez **Zones de recherche directes**, cliquez sur **TreyResearch.net**, puis examinez les enregistrements créés automatiquement.

Créer un enregistrement

1. Dans la console **Gestionnaire DNS**, développez **LON-DC1**, développez **Zones de recherche directes**, puis cliquez sur **TreyResearch.net**.
2. Cliquez avec le bouton droit sur **TreyResearch.net**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
3. Dans la fenêtre **Nouvel hôte**, dans la zone de texte **Nom**, entrez **www**, dans la zone de texte **Adresse IP**, entrez **172.16.0.100**, puis cliquez sur **OK**.
4. Cliquez sur **Terminer**.

Vérifier la réplication vers un second serveur DNS

1. Sur **TOR -SVR1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.

2. Dans la console **Gestionnaire DNS**, développez **TOR-SVR1**, développez **Zones de recherche directes**, puis cliquez sur **TreyResearch.net**.
3. Vérifiez que l'enregistrement de ressource **www** existe. L'enregistrement pourrait mettre quelques minutes à s'afficher, et vous pourriez être obligé de rafraîchir l'affichage de la console.

Leçon 5

Configuration des paramètres DNS avancés

Sommaire :

Ressources

Stratégies DNS

Lectures supplémentaires : Pour plus d'informations sur les sinkholes DNS, reportez-vous à « Application de filtres aux requêtes DNS en utilisant les politiques de serveur Windows DNS » sur : http://aka.ms/Efxdlc

Démonstration : Configuration de la zone GlobalNames

Procédure de démonstration

1. Sur **LON-DC1**, cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
2. Pour créer une zone de recherche directe intégrée à Active Directory nommée **Fabrikam.com**, à l'invite de commande Windows PowerShell, saisissez la cmdlet suivante, puis appuyez sur Entrée :

```
Add-DnsServerPrimaryZone -Name Fabrikam.com -ReplicationScope Forêt
```

3. Pour permettre la prise en charge des zones GlobalNames, sur l'invite de commandes Windows PowerShell, tapez la commande suivante et appuyez sur Entrée :

```
Set-DnsServerGlobalNameZone -AlwaysQueryServer $ true
```

4. Pour créer une zone de recherche directe intégrée à Active Directory nommée **GlobalNames**, à l'invite de commande Windows PowerShell, saisissez la commande suivante, puis appuyez sur Entrée :

```
Add-DnsServerPrimaryZone -Name GlobalNames -ReplicationScope Forêt
```

5. Fermez la fenêtre **Windows PowerShell**.
6. Dans la **barre des tâches**, restaurez la console **Gestionnaire DNS**.
7. Dans le **Gestionnaire DNS**, cliquez sur **Action**, puis sur **Actualiser**.
8. Dans la console **Gestionnaire DNS**, développez **Zones de recherche directes**, cliquez sur la zone **Fabrikam.com**, cliquez avec le bouton droit sur **Fabrikam.com**, puis cliquez sur **Nouvel hôte (A ou AAAA)**.
9. Dans la boîte de dialogue **Nouvel hôte**, dans la zone de texte **Nom**, tapez **App1**.

   Remarque : Le champ **Nom** utilise le nom de domaine parent si ce champ est vide.

10. Dans le champ **Adresse IP**, tapez **172.16.0.200**, puis cliquez sur **Ajouter un hôte**.
11. Cliquez sur **OK**, puis sur **Fin**.
12. Sélectionnez puis cliquez-droit sur la zone **GlobalNames**, puis cliquez sur **Nouvel alias (CNAME)**.
13. Dans la boîte de dialogue **Nouvel enregistrement de ressource**, dans la zone **Nom de l'alias**, tapez **App1**.
14. Dans le champ **Nom de domaine complet (FQDN) pour l'hôte cible**, tapez **App1.Fabrikam.com**, puis cliquez sur **OK**.
15. Fermez le Gestionnaire DNS.

Démonstration : Configurer des stratégies DNS

Procédure de démonstration

Créer un enregistrement d'hôte www.adatum.com et une résolution de test

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Dans la console **Gestionnaire DNS**, développez **LON-DC1**, développez **Zones de recherche directes**, puis cliquez sur **Adatum.com**.
3. Cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Nouvel alias (CNAME)...**.
4. Dans la fenêtre **Nouvel enregistrement de ressource**, dans la zone de texte **Nom d'alias**, saisissez **www** et dans la zone de texte **Nom de domaine complet (FQDN) pour l'hôte de destination**, saisissez **LON-DC1.adatum.com**, puis cliquez sur **OK**.
5. Basculez vers **TOR-SVR1**.
6. Sur **TOR-SVR1**, cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell**.
7. Dans la console **Windows PowerShell**, entrez les deux commandes suivantes, puis appuyez sur Entrée après chaque commande :

```
ipconfig / flushdns
nslookup www.adatum.com
```

8. Vérifiez que la dernière commande renvoie l'adresse IP **172.16.0.10**.

Remarque : Vous pouvez recevoir une réponse qui ressemble à ce qui suit :

```
Le requête DNS a expiré.
    Le délai d'attente était de 2 secondes.
Serveur :  Inconnu
Adresse :  172.16.0.10
Nom :    lon-dc1.adatum.com
Adresses :  fd00::10
          172.16.0.10
Alias : www.adatum.com
```

Expliquez aux stagiaires que la première moitié du résultat ressemble à une erreur, mais que ceci est normal s'il n'y a pas de zone de recherche inversée. Il n'y a pas de zone de recherche inversée sur LON-DC1 et le nslookup du client transmet la requête au serveur DNS préféré dans les propriétés TCP/IP qui, dans ce cas, est 172.16.0.10. La requête n'a pas de nom d'hôte à transmettre avec l'adresse IP du serveur et, par conséquent, indique avec le temps de requête DNS et le serveur : Ligne inconnue.

9. Basculez vers **LON-CL1**.
10. Cliquez droit sur l'icône **Démarrer** et sélectionnez **Invite de commandes (Admin)**.
11. Dans la fenêtre **Administrateur** : Dans la console **Invite de commandes**, tapez les deux commandes ci-dessous, et appuyez sur **Entrée** après chacune :

```
ipconfig / flushdns
nslookup www.adatum.com
```

12. Vérifiez que le nom aboutit à une adresse IP **172.16.0.10**.

Configurer la stratégie DNS

Remarque : Il y existe un fichier texte situé sur LON-DC1 dans E:\Labfiles\Mod04 nommé ConfigurePolicies.txt qui a toutes les cmdlets ci-dessous que vous pouvez utiliser pour copier et coller les cmdlets ci-dessous dans Windows PowerShell afin d'éliminer la dactylographie excessive.

1. Sur **LON-DC1**, cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
2. À l'invite de commandes Windows PowerShell, entrez les applets suivant, puis appuyez sur Entrée après chacun d'entre eux :

```
Add-DnsServerClientSubnet -Name "UKSubnet" -IPv4Subnet "172.16.0.0/24"
Add-DnsServerClientSubnet -Name "CanadaSubnet" -IPv4Subnet "172.16.18.0/24"
Add-DnsServerZoneScope -ZoneName "Adatum.com" -Name "UKZoneScope"
Add-DnsServerZoneScope -ZoneName "Adatum.com" -Name "CanadaZoneScope"
Add-DnsServerResourceRecord -ZoneName "Adatum.com" -A -Name "www" -IPv4Address
"172.16.0.41" -ZoneScope "UKZoneScope"
Add-DnsServerResourceRecord -ZoneName "Adatum.com" -A -Name "www" -IPv4Address
"172.16.18.17" -ZoneScope "CanadaZoneScope"
Add-DnsServerQueryResolutionPolicy -Name "UKPolicy" -Action PERMETTRE -ClientSubnet
"eq, UKSubnet" -ZoneScope "UKZoneScope, 1" -ZoneName "Adatum.com"
Add-DnsServerQueryResolutionPolicy -Name "CanadaPolicy" -Action PERMETTRE -
ClientSubnet "eq, CanadaSubnet" -ZoneScope "CanadaZoneScope, 1" -ZoneName Adatum.com
```

3. Basculez vers **LON-CL1**.
4. Pour vérifier que les modifications ci-dessus ont fonctionné, dans la fenêtre Invite de commandes administrateur, tapez les commandes suivantes et appuyez sur **Entrer** après chacune d'entre elles :

```
Ipconfig /flushdns
Nslookup www.adatum.com
```

5. Vous devriez obtenir le résultat **172.16.0.41**.
6. Sur **TOR-SVR1**, cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
7. Dans la fenêtre **Windows PowerShell**, entrez les applets suivants, puis appuyez sur **Entrée** après chaque commande :

```
Ipconfig /flushdns
Nslookup www.adatum.com
```

8. Vous devriez obtenir un résultat de **172.16.18.17**.

Démonstration : Configuration du DNSSEC

Procédure de démonstration

1. Sur **LON-DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **DNS**.
2. Dans la console **Gestionnaire DNS**, développez **LON-DC1**, développez **Zones de recherche directes**, puis cliquez sur **Adatum.com**.
3. Dans le menu contextuel, cliquez sur **DNSSEC**, puis sur **Signer la zone**.
4. Dans l'**Assistant de connexion** à la zone, cliquez sur **Suivant**.
5. Cliquez sur **Personnalisez les paramètres de signature de zone**, puis sur **Suivant**.

6. Sur la page **Maître des clés**, cliquez sur **Le serveur DNS LON-DC1 est le maître des clés**, puis sur **Suivant**.
7. Sur la page **Clé KSK**, cliquez sur **Suivant**.
8. Sur la page **Clé KSK**, cliquez sur **Ajouter**.
9. Sur la page **Nouvelle clé KSK**, cliquez sur **OK**.
10. Sur la page **Clé KSK**, cliquez sur **Suivant**.
11. Sur la page **Clé ZSK**, cliquez sur **Suivant**.
12. Sur la page **Clé ZSK**, cliquez sur **Ajouter**.
13. Sur la page **Nouvelle clé KSK**, cliquez sur **OK**.
14. Sur la page **Clé ZSK**, cliquez sur **Suivant**.
15. Sur la page **Next Secure** cliquez sur **Suivant.**
16. Sur la page **Trust Anchors (TA)**, sélectionnez **Activer la distribution des trust anchors pour cette zone**, puis cliquez sur **Suivant**.
17. Sur la page **paramètres de signature et d'interrogation**, cliquez sur **Suivant**.
18. Sur la page **Extensions de sécurité DNS**, cliquez sur **Suivant**, puis sur **Terminer**.
19. Dans le Gestionnaire DNS, développez **Points de confiance**, développez **com**, puis cliquez sur **Adatum**. Assurez-vous que les enregistrements de ressources DNSKEY existent, et que leur statut est valide.
20. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
21. Dans la **Console de gestion de stratégie de groupe (GPMC)**, développez **Forêt : Adatum.com**, déroulez les **Domaines**, déroulez **Adatum.com**, cliquez droit sur **Stratégie de domaine par défaut**, puis cliquez sur **Modifier**.
22. Dans l'Éditeur de gestion des politiques du groupe, dans **Configuration de l'ordinateur**, développez **Politiques**, développez **Paramètres Windows**, puis cliquez sur le dossier **Politique de résolution du nom**.
23. Dans la section **Créer des règles**, dans le champ **Suffixe**, tapez **Adatum.com** pour appliquer la règle au suffixe de l'espace-nom.
24. Sélectionnez **Activer DNSSEC dans cette règle**, sélectionnez **Exiger que les clients DNS vérifient que les données de nom et d'adresse ont été validées par le serveur DNS**, puis cliquez sur **Créer**.
25. Fermez toutes les fenêtres actives.

Révision du module et éléments à retenir

Bonnes Pratiques

Lorsque vous implémentez le DNS, utilisez les meilleures pratiques suivantes :

- Utilisez toujours des noms d'hôte au lieu de noms NetBIOS.
- Utilisez des transferts plutôt que des indications de racine.
- Soyez conscient des problèmes de mise en cache potentiels lorsque vous résolvez la résolution de noms.
- Utilisez des zones intégrées à Active Directory au lieu de zones primaires et secondaires.
- Utilisez la zone GlobalNames lorsque vous devez disposer d'entités à nom unique.
- Utilisez les stratégies DNS pour affiner la résolution de nom du client et les transferts de zone.

Questions de contrôle des acquis

Question : Vous résolvez une résolution de noms DNS à partir d'un ordinateur client. Que devez-vous penser à faire avant chaque test ?

Réponse : Vous devez vider le cache de résolution avant de démarrer le dépannage.

Question : Vous déployez les serveurs DNS dans un domaine Active Directory et votre client exige que l'infrastructure soit résistante à des points de défaillance uniques. Que devez-vous prendre en considération lors de la planification de la configuration DNS ?

Réponse : Vous devez déployer plus d'un contrôleur de domaine AD DS avec le rôle de serveur DNS installé.

Question : Quels sont les avantages que vous obtenez en utilisant les transferts ?

Réponse : Les transferts sont utilisés lorsque votre serveur DNS local ne peut pas résoudre la requête d'un client en utilisant ses propres zones locales. On configure généralement les transferts pour résoudre les noms Internet. Cependant, vous pouvez également utiliser les transferts pour optimiser la performance, optimiser l'utilisation du lien Internet sur votre serveur DNS local, ainsi que pour renforcer la sécurité.

Outils

Nom de l'outil	Utilisé pour	Emplacement
Console du gestionnaire DNS	Gérer le rôle serveur DNS	Outils d'administration
Nslookup	Résoudre le DNS	Outil en ligne-de commande
Ipconfig	Résoudre le DNS	Outil en ligne-de commande
Les applets de commande Windows PowerShell	Gérer et résoudre le DNS	Windows PowerShell
Stratégies DNS	Divers scénarios impliquant les aspects de résolution du nom du client et du transfert de zone	Windows PowerShell

Nom de l'outil	Utilisé pour	Emplacement
WDK : Comprend Tracelog.exe	Suivi des événements pour les applications grand public Windows (ETW)	Vous pouvez « Télécharger WDK, WinDbg et les outils associés » sur : http://aka.ms/Dbocr6

Problèmes courants et conseils de dépannage

Problème courant	Conseil pour la résolution du problème
Les clients mettent parfois en cache des enregistrements DNS invalides.	Effacez le cache DNS.
Le serveur DNS fonctionne lentement.	Utilisez l'analyseur de performances pour mesurer la charge sur le DNS.

Questions et réponses sur les laboratoires

Atelier pratique A : La planification et l'implémentation de la résolution de noms en utilisant DNS

Questions et réponses

Question : Pouvez-vous installer le rôle de serveur DNS sur un serveur qui n'est pas un contrôleur de domaine ? Si oui, est-ce qu'il y a des limites ?

Réponse : Oui, vous pouvez installer le rôle de serveur DNS sur un serveur qui n'est pas un contrôleur de domaine. Cependant, il est impossible de créer des zones intégrées à Active Directory sur un serveur DNS qui n'est pas un contrôleur de domaine.

Question : Quel est le moyen le plus commun pour mener à bien la résolution de noms Internet sur un DNS local ?

Réponse : Les organisations configurent généralement leur DNS local avec un redirecteur. Ce dernier est le plus souvent un serveur DNS de leur FAI.

Question : Comment pouvez-vous parcourir le contenu du cache de résolution DNS sur un serveur DNS ?

Réponse : Vous pouvez parcourir le contenu du cache de résolution DNS sur un serveur DNS en activant la vue **Avancée** dans la console **Gestionnaire DNS** ou à l'aide des cmdlets Windows PowerShell.

Atelier pratique B : Intégration de DNS avec AD DS

Questions et réponses

Question : Pourquoi avez-vous promu **SYD-SVR1** à un contrôleur de domaine ?

Réponse : Lorsque vous hébergez le rôle de serveur DNS sur un contrôleur de domaine, la base de données DNS est répliquée sur chaque contrôleur de domaine AD DS du domaine, créant ainsi une réplication multi-maître automatique et une redondance pour votre environnement DNS. Il veille également à ce que chaque contrôleur de domaine de votre environnement puisse résoudre les requêtes DNS, ce qui constitue un aspect important de la fonctionnalité AD DS.

Atelier pratique C : Configuration des paramètres DNS avancés

Questions et réponses

Question : Quels deux paramètres le cmdlet Windows PowerShell Add-DnsServerZoneScope exige-t-il ?

Réponse : Le Nom de zone pour identifier la zone à laquelle le champ est ajouté et le paramètre Nom pour donner un nom au champ.

Module 5

Implémentation et gestion d'IPAM

Sommaire :

Leçon 1

Vue d’ensemble d’IPAM

Sommaire :

Questions et réponses

Question : Pour gérer IPv6 avec IPAM, vous devez activer IPv6 sur le serveur IPAM.

( ) Vrai

( ) Faux

Réponse :

(√) Vrai

( ) Faux

Commentaire :

Pour gérer IPv6 avec IPAM, vous devez activer IPv6 sur le serveur IPAM.

Ressources

Qu'est-ce qu'IPAM ?

Lectures supplémentaires : Pour plus d'informations, consultez : http://aka.ms/Sezy6m

Intégration IPAM avec Virtual Machine Manager

Lectures supplémentaires : Pour plus d'informations sur la façon de configurer l'intégration IPAM Virtual Machine Manager, reportez-vous à : http://aka.ms/o3vpkc

Leçon 2

Déploiement d'IPAM

Sommaire :

Questions et réponses

Question : Quels objets de stratégie de groupe (GPO) sont créés lorsque vous déployez IPAM ? À quoi servent-ils ?

Réponse : Les GPO créés sont :

- <Prefix>_DHCP. Ce GPO applique les paramètres qui permettent à l'IPAM de surveiller, gérer et collecter des informations auprès des serveurs DHCP gérés sur le réseau. Il met en place les tâches planifiées d'approvisionnement IPAM et ajoute des règles entrantes de pare-feu Windows pour Gestion à distance des journaux des événements/la gestion à distance des journaux d'événements (RPC-EMAP et RPC), la gestion des services à distance (RPC-EMAP et RPC), et le serveur DHCP (RPCSS-In et RPC-In).
- <Prefix>_DNS. Ce GPO applique les paramètres qui permettent à l'IPAM de surveiller, gérer et collecter des informations auprès des serveurs DNS gérés sur le réseau. Il met en place les tâches planifiées d'approvisionnement IPAM et ajoute des règles entrantes de pare-feu Windows pour RPC (TCP, entrant), Mappeur de point de terminaison RPC (TCP, entrant), Gestion à distance des journaux des événements/la gestion à distance des journaux d'événements (RPC-EMAP et RPC), et la gestion des services à distance (RPC-EMAP et RPC).
- <Prefix>_DC_NPS. Ce GPO applique les paramètres qui permettent à l'IPAM de recueillir des informations auprès des contrôleurs de domaine et des NPS gérés sur le réseau à des fins de suivi de l'adresse IP. Il met en place les tâches planifiées d'approvisionnement IPAM et ajoute des règles entrantes de pare-feu Windows pour Gestion à distance des journaux des événements/la gestion à distance des journaux d'événements (RPC-EMAP et RPC) et la gestion des services à distance (RPC-EMAP et RPC).

Ressources

Processus de mise en œuvre IPAM

Lectures supplémentaires : Pour plus d'informations, consultez : http://aka.ms/Skefwm

Démonstration : Installation et approvisionnement du rôle IPAM

Étapes de la démonstration

Installer IPAM

1. Basculez vers LON-SVR2.
2. Cliquez sur **Démarrer**, puis cliquez sur **Gestionnaire de serveur**.
3. Dans le **Gestionnaire de serveur**, dans le volet de résultats, 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 **Suivant**.
6. Dans la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
7. Dans la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.
8. Dans la page **Sélectionner des fonctionnalités**, sélectionnez la case à cocher **Serveur de gestion des adresses IP (IPAM)**.
9. Dans la boîte de dialogue **Ajouter les fonctionnalités requises pour Serveur de gestion des adresses IP (IPAM)**, cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.

10. Dans la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. Quand l'**Assistant Ajout de rôles et de fonctionnalités** est terminé, fermez l'assistant.

Configurer IPAM

1. Dans le volet de navigation du Gestionnaire de serveur, cliquez sur **IPAM**.
2. Dans le volet **Vue d'ensemble 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. Sur la page **Configurer la base de données**, cliquez sur **Suivant**.
6. Sur la page **Choisir l'approvisionnement**, veillez à ce que **Basé sur la stratégie de groupe** soit sélectionné.
7. Dans la zone de texte **Préfixe du nom GPO**, entrez **IPAM**, puis cliquez sur **Suivant**.
8. Dans la page **Confirmer les paramètres**, cliquez sur **Appliquer**. La configuration prend quelques instants.
9. Une fois l'approvisionnement terminé, cliquez sur **Fermer**.
10. Dans le volet **Vue d'ensemble d'IPAM**, cliquez sur **Configurer la découverte de serveurs**.
11. Dans la boîte de dialogue **Configurer la découverte de serveurs**, cliquez sur **Obtenir les forêts**.
12. Dans la boîte de dialogue **Configurer la découverte de serveurs**, cliquez sur **OK**, puis encore sur **OK**.
13. Dans le volet **Vue d'ensemble d'IPAM**, cliquez sur **Configurer la découverte de serveurs**.
14. Dans la boîte de dialogue **Configurer la découverte de serveurs**, cliquez sur **Ajouter**, puis sur **OK**.
15. Dans le volet **Vue d'ensemble d'IPAM**, cliquez sur **Démarrer la découverte de serveurs**.

 **Remarque :** Le processus de découverte peut durer entre 5 et 10 minutes. La barre jaune indique quand la découverte est terminée.

16. 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 LON-DC1. Faites défiler l'écran jusqu'au volet **Détails** et notez le rapport d'état.

 **Remarque :** Le serveur IPAM n'a pas encore obtenu l'autorisation de gérer LON-DC1 par l'intermédiaire de la stratégie de groupe.

17. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (Admin)**.
18. À l'invite de commandes dans l'interface de ligne de commande Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée :

```
Invoke-IpamGpoProvisioning –Domain Adatum.com –GpoPrefixName IPAM –IpamServerFqdn
LON-SVR2.adatum.com –DelegatedGpoUser Administrateur
```

19. Quand vous êtes invité à confirmer l'action, tapez **Y**, puis appuyez sur Entrée.

Remarque : Cette commande prend quelques minutes.

20. Fermez Windows PowerShell.
21. Basculez vers le **Gestionnaire de serveur**.
22. Dans le volet d'**informations sur IPv4**, cliquez avec le bouton droit sur **lon-dc1**, puis cliquez sur **Modifier le serveur**.
23. Dans la boîte de dialogue **Ajouter ou modifier un serveur**, définissez le champ **État de gérabilité** sur **Géré**, puis cliquez sur **OK**.

Remarque : Si une erreur d'objet de stratégie de groupe (GPO) apparaît, remettez le serveur sur **Non spécifié**, redémarrez LON-DC1, puis redémarrez LON-SVR2. Connectez-vous aux deux serveurs en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.

24. Basculez vers LON-DC1.
25. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (Admin)**.
26. À l'invite de commandes Windows PowerShell, entrez la commande suivante, puis appuyez sur Entrée.

```
Gpupdate /force
```

27. Fermez la fenêtre Windows PowerShell.
28. Rebasculez vers LON-SVR2.
29. Dans le **Gestionnaire de serveur**, cliquez avec le bouton droit sur **LON-DC1**, puis cliquez sur **Actualiser l'état de l'accès au serveur**.
30. Une fois terminé, actualisez IPv4 en cliquant sur **Actualiser**.

Remarque : La modification du statut peut prendre jusqu'à cinq minutes. Lorsque l'**État de la récupération de données** indique **Terminé**, vous pouvez continuer.

31. Cliquez de nouveau sur le volet **Vue d'ensemble d'IPAM**. Dans le volet **Vue d'ensemble d'IPAM**, cliquez sur **Récupérer les données des serveurs gérés**.

Remarque : Cette action prend quelques minutes.

Démonstration : Administrer IPAM

Étapes de la démonstration

Ajouter un groupe de rôles personnalisé

1. Sur LON-SVR2, dans le **Gestionnaire de serveur**, dans le volet de **navigation IPAM**, cliquez sur **CONTRÔLE D'ACCÈS**. Décrivez les rôles intégrés disponibles.
2. Cliquez avec le bouton droit sur **Rôles**, puis cliquez sur **Ajouter un rôle utilisateur**.
3. Dans la boîte de dialogue **Ajouter ou modifier un rôle**, dans la zone **Nom**, tapez **Rôle de gestion Adatum DHCP et DNS**.

4. Dans la liste **Opérations**, sélectionnez les cases à cocher suivantes, puis cliquez sur **OK** :
   - Opérations de serveur DHCP
   - Opérations de zone DNS
   - Opérations de serveur DNS

Ajouter une étendue personnalisée

1. Dans le volet de navigation, cliquez avec le bouton droit sur **Étendues d'accès**, puis cliquez sur **Ajouter une étendue d'accès**.
2. Dans la boîte de dialogue **Ajouter une étendue d'accès**, dans la liste **Sélectionner l'étendue d'accès parente**, cliquez sur **Globale**, puis cliquez sur **Nouveau**.
3. Dans la zone de texte **Nom**, tapez **Londres**, cliquez sur **Ajouter**, puis cliquez sur **OK**.

Ajouter une stratégie d'accès IPAM

1. Dans le volet de navigation, cliquez avec le bouton droit sur **Stratégies d'accès**, puis cliquez sur **Ajouter une stratégie d'accès**.
2. Dans la boîte de dialogue **Ajouter une stratégie d'accès**, sous **Paramètres utilisateur**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Sélectionner un utilisateur ou un groupe**, cliquez sur **Emplacements**.
4. Dans la boîte de dialogue **Emplacements**, développez **Tout l'annuaire**, développer **Adatum.com**, cliquez sur **IT**, puis cliquez sur OK.
5. Dans la boîte de dialogue **Sélectionner un utilisateur ou un groupe**, saisissez **IT**, cliquez sur **Vérifier les noms**, puis cliquez sur OK.
6. Dans la boîte de dialogue **Ajouter une stratégie d'accès**, sous **Paramètres d'accès**, cliquez sur **Nouveau**.
7. Dans la liste **Sélectionnez un rôle**, cliquez sur **Rôle de gestion A Datum DHCP et DNS**.
8. Dans la liste **Sélectionner l'étendue d'accès pour le rôle**, cliquez sur **Londres**, puis sur **OK**.
9. Dans le volet de navigation, cliquez sur **Stratégies d'accès**. La stratégie nouvellement créée apparaît dans la liste.

Définir l'étendue d'accès

1. Dans le volet de navigation, cliquez sur **Serveurs DNS et DHCP**.
2. Dans le volet de détails, cliquez avec le bouton droit sur le rôle DNS pour LON-DC1.Adatum.com, puis cliquez sur **Définir l'étendue d'accès**.
3. Dans la boîte de dialogue **Définir l'étendue d'accès**, décochez la case **Étendue d'accès héritée du parent**.
4. Dans la liste **Sélectionner l'étendue d'accès**, cliquez sur **Londres**, puis sur **OK**.
5. Dans le volet de détails, cliquez avec le bouton droit sur le rôle DHCP pour LON-DC1.Adatum.com, puis cliquez sur **Définir l'étendue d'accès**.
6. Dans la boîte de dialogue **Définir l'étendue d'accès**, décochez la case **Étendue d'accès héritée du parent**.
7. Dans la liste **Sélectionner l'étendue d'accès**, cliquez sur **Londres**, puis sur **OK**.

Démonstration : Gestion de DNS à l'aide d'IPAM

Étapes de la démonstration

Ajouter un redirecteur conditionnel

1. Dans **Gestionnaire de serveur**, dans IPAM, sur l'onglet **Serveurs DNS et DHCP**, cliquez droit sur le rôle de serveur DNS pour LON-DC1.Adatum.com, puis cliquez sur **Créer un redirecteur conditionnel DNS**.
2. Dans la zone de dialogue **Créer un redirecteur conditionnel DNS**, dans la zone de texte **Domaine DNS**, saisissez **TreyResearch.net**.
3. Dans la zone de texte **FQDN ou adresse IP**, tapez **172.16.0.11**, cliquez sur **Ajouter**, puis cliquez sur **OK.**

Créer une zone DNS

1. Dans l'onglet **Serveur DNS et DHCP**, dans le volet d'informations, cliquez avec le bouton droit sur le rôle de serveur DNS pour LON-DC1.Adatum.com, puis cliquez sur **Créer une zone DNS**.
2. Dans la boîte de dialogue **Créer une zone DNS**, dans la zone de texte **Nom de la zone**, saisissez **Contoso.com**, puis cliquez sur **OK**.

Ajouter un enregistrement DNS

1. Dans le volet de navigation, sur l'onglet **Zones DNS**, dans le volet d'informations, faites un clic droit sur **Contoso.com**, puis cliquez sur **Ajouter un enregistrement de ressource DNS**.
2. Dans la boîte de dialogue **Ajouter des enregistrements de ressources DNS**, cliquez sur **Nouveau**.
3. Dans la liste **Type d'enregistrement de ressource**, cliquez sur **A.**
4. Dans la zone de texte **Nom**, saisissez **Contoso1**.
5. Dans le champ **Adresse IP**, saisissez **172.32.0.99**, puis cliquez sur **Ajouter un enregistrement de ressource**.
6. Dans la boîte de dialogue **Ajouter des enregistrements de ressource DNS**, cliquez sur **OK**.
7. Dans l'onglet **Serveur DNS et DHCP** du volet de navigation, cliquez avec le bouton droit sur le rôle de serveur DNS pour LON-DC1.Adatum.com, puis cliquez sur **Lancer la console MMC**.
8. Dans la boîte de dialogue **Gestionnaire DNS**, développez **LON-DC1.Adatum.com**, développez **Zones de recherche directes**, puis cliquez sur **Contoso.com**. Vérifiez la présence de la zone et de l'enregistrement que vous avez créés.
9. Dans le volet de navigation, cliquez sur **Redirecteurs conditionnels**. Vérifiez la présence de l'enregistrement de redirecteur conditionnel que vous avez établi.
10. Fermez la console **Gestionnaire DNS**.

Démonstration : Gestion des étendues DHCP à l'aide d'IPAM

Étapes de la démonstration

1. Dans **Gestionnaire de serveur**, dans le volet de **navigation IPAM**, sur l'onglet **Serveurs DNS et DHCP**, faites un clic-droit sur le rôle de serveur DHCP pour LON-DC1.Adatum.com, puis cliquez sur **Créer une étendue DHCP**.
2. Dans la boîte de dialogue **Créer une étendue DHCP**, dans l'onglet **Propriétés générales**, dans la zone de texte **Nom de l'étendue**, saisissez **Contoso**.
3. Dans la zone de texte **Adresse IP de début**, saisissez **172.32.0.100**.

4. Dans la zone de texte **Adresse IP de fin**, saisissez **172.32.0.200**.
5. À côté de l'option **Activer l'étendue à la création**, cliquez sur **Non**.
6. En dessous de **Options d'étendue DHCP**, cliquez sur **Nouveau**.
7. Dans la section **Nouvelle configuration**, dans la liste **Option**, cliquez sur **006 Serveurs DNS**.
8. Dans la zone de texte **Nom du serveur**, saisissez **LON-DC1.Adatum.com**, cliquez sur **résoudre**, cliquez sur **Ajouter une configuration**, puis cliquez sur **OK**.
9. Dans l'onglet **Serveur DNS et DHCP** du volet de navigation, cliquez avec le bouton droit sur le rôle de serveur DHCP pour LON-DC1.Adatum.com, puis cliquez sur **Lancer la console MMC**.
10. Dans la boîte de dialogue **DHCP**, développez **LON-DC1.Adatum.com**, développez **IPv4**, puis cliquez sur **Étendue [172.32.0.0] Contoso.com**. Cliquez sur **Pool d'adresses**, Puis cliquez sur **Options d'étendue** pour vérifier la configuration de l'étendue.
11. Fermer la **console DHCP**.

Leçon 3

Gestion des espaces d'adresses IP à l'aide d'IPAM

Sommaire :

Questions et réponses

Question : Quelle est la différence entre un bloc d'adresses IP et une plage d'adresses IP dans IPAM ?

> **Réponse :** Un bloc d'adresses IP est un ensemble d'adresses IP qui ne font pas partie d'une étendue DHCP gérée par IPAM. Des plages d'adresses IP correspondent à un espace d'adressage IP géré. Vous créez généralement un bloc d'adresses IP pour maintenir un inventaire pour une plage d'adresses IP statiques.

Ressources

Utilisation d'IPAM pour gérer les adresses IP

Lectures supplémentaires : Pour plus d'informations, consultez : http://aka.ms/Rg40h1

Démonstration : Gestion des adresses IP à l'aide d'IPAM

Étapes de la démonstration

Ajouter un bloc d'adresse dans IPAM

1. Sur LON-SVR2, dans **Gestionnaire de serveur**, dans le volet de **navigation IPAM**, cliquez sur **Blocs d'adresses IP**.
2. Dans le volet **IPv4**, à côté de **Vue actuelle**, cliquez sur **Plages d'adresses IP**.
3. Dans le coin supérieur droit de la fenêtre, cliquez sur **Tâches**, puis cliquez sur **Ajouter un bloc d'adresses IP**.
4. Dans la boîte de dialogue **Ajouter ou modifier un bloc d'adresses IPv4**, tapez ce qui suit dans les zones de texte, puis cliquez sur **OK** :
   - ID réseau : **172.16.18.0**
   - Longueur du préfixe : **24**
   - Adresse IP de début : **172.16.18.0**
   - Adresse IP de fin : **172.16.18.255**
   - Description : **Sous-réseau de Toronto**
5. Dans le volet IPv4, à côté de la **Vue actuelle**, cliquez sur **Blocs d'adresses IP**. Notez le bloc d'adresses nouvellement créé pour Toronto.

Créer une réservation d'adresse IP

1. Dans **Gestionnaire de serveur**, sur la page **Configuration IPAM**, dans le volet de navigation, cliquez sur **Blocs d'adresses IP**.
2. Dans le volet **IPv4**, à côté de **Vue actuelle**, cliquez sur **Plages d'adresses IP**.
3. Faites un clic-droit sur **172.16.0.0/16**, puis cliquez sur **Modifier la plage d'adresses IP.**
4. Dans la fenêtre **Modifier la plage d'adresses IP**, cliquez sur **Réservations**.
5. Dans la zone de texte **Réservation**, saisissez **172.16.0.170**, cliquez sur **Ajouter**, puis cliquez sur **OK**.

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Pourquoi voudriez-vous récupérer une adresse IP dans IPAM ?

> **Réponse :** En règle générale, vous récupérez une adresse IP dans la liste des adresses IP disponibles, car elle a été allouée en vue d'une utilisation à un autre emplacement de votre environnement et n'est plus disponible.

Question : Est-ce que IPAM fournit des avantages si vous ne configurez pas ou ne gérez pas de manière centralisée votre environnement d'adressage IP ?

> **Réponse :** Oui. IPAM peut toujours assurer la surveillance centralisée de l'environnement d'adressage IP à partir d'une seule console.

Questions et réponses sur les ateliers pratiques

Atelier pratique : Implémentation d'IPAM

Questions et réponses

Question : Pourquoi avez-vous exécuté l'applet de commande **Invoke-IpamGpoProvisioning** ?

> **Réponse :** Vous avez exécuté la cmdlet **Invoke-IpamGpoProvisioning** pour définir les autorisations de serveur IPAM afin de gérer les serveurs dans le domaine. Lorsque vous exécutez la commande, elle crée trois GPO qui sont liés au domaine. Ces GPO appliquent des autorisations pour la gestion du contrôleur de domaine, DNS et les serveurs DHCP du domaine.

Question : Pourquoi seules les adresses et les plages IP de Houston, de la ville de Mexico et de Portland apparaissent dans la console IPAM ? Où sont les adresses IP de Londres, Toronto et Sydney ?

> **Réponse :** IPAM affiche uniquement des informations d'adresse IP pour les adresses IP et les plages d'adresses attribuées par DHCP. Il ne réalise pas spécifiquement l'inventaire, le suivi ou la gestion des adresses IP attribuées statiquement

Module 6

Accès à distance à Windows Server 2016

Sommaire :

Leçon 1

Vue d’ensemble de l’accès à distance

Sommaire :

Questions et réponses

Question : Quel genre de stratégies pouvez-vous configurer sur un serveur de stratégie réseau et pour quoi sont-elles utilisées ?

> **Réponse :** Vous pouvez configurer deux types de politiques sur un serveur de stratégie réseau : les stratégies de réseau et des politiques de demande de connexion. Vous pouvez utiliser des stratégies de réseau pour gérer et contrôler l'authentification et l'autorisation de tentatives de connexion d'accès à distance. Vous pouvez utiliser des stratégies de demande de connexion pour transmettre les tentatives de connexion d'accès à distance à un autre serveur RADIUS (Network Policy Server) à des fins de traitement.

Question : Lorsque vous installez d'abord le rôle de la stratégie réseau et des services d'accès, toutes les connexions vers le serveur d'accès à distance sont autorisées.

( ) Vrai

( ) Faux

> **Réponse :**
>
> ( ) Vrai
>
> (√) Faux
>
> **Commentaire :**
>
> Lorsque vous déployez d'abord le rôle de la politique et d'accès réseau, les deux stratégies réseau par défaut refusent l'accès à distance à toutes les tentatives de connexion. Vous devez configurer au moins une stratégie pour permettre l'accès.

Discussion : Quand utiliser l'accès à distance ?

Question : Avez-vous autorisé des utilisateurs à se connecter à vos ressources réseau à distance ? Et si oui, comment ?

> **Réponse :** Les réponses peuvent varier, mais peuvent inclure :
>
> - Accès au serveur VPN de l'entreprise.
> - Accès aux ressources de l'entreprise via DirectAccess.
> - Accès aux ressources de l'entreprise en utilisant RDS.

Question : Quels sont vos impératifs professionnels pour utiliser l'accès à distance ?

> **Réponse :** Les réponses peuvent varier, mais peuvent inclure :
>
> - Permet à vos administrateurs de travailler à domicile.
> - Résolution des problèmes qui surviennent pendant le week-end.
> - Permet aux utilisateurs d'accéder aux ressources de l'entreprise tout en voyageant.

Ressources

Gestion de l'accès à distance dans Windows Server 2016

 **Lectures supplémentaires :** Pour plus d'informations, reportez-vous aux applets de commande de l'accès à distance : http://aka.ms/Fp4ry6

Stratégies de serveur de politique réseau

Lectures supplémentaires : Pour plus d'informations, consultez RADIUS Proxy : http://aka.ms/Oy16cb

Démonstration : Installation et gestion du rôle de serveur d'accès à distance

Étapes de la démonstration

Installer le rôle de serveur d'accès à distance

1. Sur LON-SVR1, cliquez sur le bouton **Démarrer**, puis cliquez sur la vignette **Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
3. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner les rôles du serveur**, cliquez sur **Accès distant**, puis cliquez sur **Suivant**.
7. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
8. Sur la page **Accès distant**, cliquez sur **Suivant**.
9. Sur la page **Sélectionnez les services de rôle**, cliquez **DirectAccess et VPN (accès à distance)**, puis dans la boîte de dialogue **Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**.
10. Vérifiez que **DirectAccess et VPN (RAS)** est sélectionné et sur la page **Sélectionnez les services de rôle**, cliquez sur **Suivant**.
11. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
12. Une fois l'installation terminée, cliquez sur **Fermer**.

Gérez le rôle de serveur d'accès à distance

1. Dans la console **Gestionnaire de serveur**, dans la partie supérieure droite de la console, cliquez sur **Outils**, puis cliquez sur **Gestion de l'accès à distance**.
2. Dans la **console Gestion de l'accès à distance**, vérifiez les options de configuration et de gestion de l'accès à distance.
3. Dans la console **Gestionnaire de serveur**, dans la partie supérieure droite de la console, cliquez sur **Outils**, puis cliquez sur **Routage et Accès à distance**.
4. Dans la console **Routage et accès à distance**, vérifiez les options de configuration et de gestion de l'accès à distance.

Démonstration : Configuration des stratégies du serveur de polices réseau

Étapes de la démonstration

1. Sur l'EU-RTR, ouvrez **Gestionnaire de serveur** puis sur le menu **Outils**, cliquez sur **Serveur NPS (Network Policy Server)**.
2. Dans la console **Serveur de stratégies de réseau**, dans le volet de navigation, développez **Stratégies**, cliquez avec le bouton droit sur **Stratégies réseau**, puis cliquez sur **Nouveau**.

3. Dans l'assistant **Nouvelle stratégie réseau**, dans **Nom de la stratégie**, saisissez **Adatum IT VPN**.
4. Dans la liste déroulante **Type de serveur d'accès au réseau**, cliquez sur **Serveur d'accès distant (VPN-Dial up)**, puis cliquez sur **Suivant**.
5. Sur la page **Spécifier les conditions**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Sélectionner une condition**, cliquez sur **Groupes de Windows**, puis cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Groupes Windows**, cliquez sur **Ajouter des groupes**.
8. Dans la boîte de dialogue **Sélectionner un groupe**, dans la zone **Entrer le nom de l'objet à sélectionner (exemples)**, saisissez **IT**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
9. Cliquez à nouveau sur **OK**, puis sur **Suivant**.
10. Sur la page **Spécifier l'autorisation d'accès**, vérifiez que l'**Accès autorisé** est sélectionné, puis cliquez sur **Suivant**.
11. Sur la page **Configurer les méthodes d'authentification**, décochez la case **Authentification cryptée Microsoft (MS-CHAP)**.
12. Pour ajouter les **Types d'EAP**, cliquez sur **Ajouter**.
13. Sur la page **Ajouter des protocoles EAP**, cliquez sur **Mot de passe sécurisé Microsoft (EAP-MSCHAP v2)**, puis cliquez sur **OK**.
14. Pour ajouter les **Types d'EAP**, cliquez sur **Ajouter**.
15. Sur la page **Ajouter EAP**, cliquez sur **Microsoft : Carte à puce ou autre certificat**, cliquez sur **OK**, puis cliquez sur **Suivant**.
16. Sur la page **Configurer des contraintes**, cliquez sur **Suivant**.
17. Sur la page **Configurer des paramètres**, cliquez sur **Suivant**.
18. Sur la page **Fin de la configuration de la nouvelle stratégie réseau**, cliquez sur **Terminer**.
19. Fermez toutes les fenêtres ouvertes.

Leçon 2

Implémentation du proxy d'application Web

Sommaire :

Questions et réponses

Question : Le rôle du Proxy de l'application Web exigence AD FS.

( ) Vrai

( ) Faux

Réponse :

(√) Vrai

( ) Faux

Commentaire :

Vous devez installer AD FS dans votre environnement si vous prévoyez d'utiliser le Proxy de l'application Web dans Windows Server 2016. Ceci est une exigence, même si vous prévoyez d'utiliser uniquement l'authentification unique.

Question : Quels types de préauthentification le proxy d'application web prend-il en charge ?

Réponse : Le proxy d'application web prend en charge deux types de préauthentification : la préauthentification AD FS et la préauthentification Pass-through.

Ressources

Publication d'applications avec le proxy d'application web

 **Lectures supplémentaires :** Pour plus d'informations, reportez-vous à la rubrique Publication d'applications dans SharePoint, Exchange et DGR : http://aka.ms/Qopw7d

Démonstration : Publication d'un site web sécurisé

Étapes de la démonstration

Déplacer le client vers Internet

1. Pour déplacer le client à partir du réseau interne vers Internet, dans LON-CL1, cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Connexion réseau**.
2. Dans **Connexions de réseau**, cliquez avec le bouton droit sur **London_Network**, puis cliquez sur **Désactiver**.
3. Cliquez avec le bouton droit sur **Internet**, puis cliquez sur **Activer**.
4. Dans la barre des tâches, cliquez sur l'icône de **Microsoft Edge**.
5. Dans **Microsoft Edge**, dans le champ **Rechercher ou saisir une adresse web**, saisissez **https://lon-svr1.adatum.com**, puis appuyez sur Entrée. Notez qu'un message d'erreur réseau apparaît.
6. Cliquez avec le bouton droit sur le bouton **Démarrer** et cliquez sur **Exécuter**. Dans la boîte de dialogue **Exécuter**, saisissez **mstsc**, puis appuyez sur Entrée.
7. Dans l'application **Connexion Bureau à distance**, dans la zone **Ordinateur**, saisissez **lon-dc1**, puis appuyez sur Entrée. Notez que vous ne pouvez pas vous connecter à lon-dc1, car l'ordinateur ne peut pas être trouvé sur le réseau.
8. Fermez toutes les fenêtres ouvertes.

Remarque : Vous êtes incapable d'ouvrir le site Web interne en cours d'exécution sur LON-SVR1 et de vous connectez à lon-dc1 en utilisant le Bureau à distance car le client ne peut pas accéder au réseau interne.

Installer le service de rôle du proxy d'application web

1. Basculez vers EU-RTR.
2. Cliquez sur le bouton **Démarrer**, puis cliquez sur la vignette du **Gestionnaire de serveur**.
3. Sur la page **Tableau de bord**, cliquez sur **Ajouter des rôles et fonctionnalités**.
4. Dans l' **Assistant Ajout de rôles et fonctionnalités**, sur la page **Avant de commencer**, cliquez sur **Suivant**, sur la page **Sélectionnez le type d'installation**, cliquez sur **Suivant**, puis sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Sur la page **Sélectionnez les rôles du serveur**, déroulez le menu **Accès distant**, cliquez sur **Proxy d'application web**, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
8. Sur la page **Progression de l'installation**, vérifiez que l'installation est réussie, puis cliquez sur **Fermer**.

Obtenir un certificat pour la ferme ADFSWAP

1. Sur EU-RTR, cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell**.
2. Dans la fenêtre **Windows PowerShell**, saisissez **mmc**, puis appuyez sur Entrée.
3. Dans le MMC, dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
4. Dans la fenêtre **Ajouter/supprimer un composant logiciel enfichable**, cliquez sur **Certificats**, sur **Ajout**, sur **Compte d'ordinateur**, puis sur **Suivant**.
5. Vérifiez que l'**Ordinateur local** est sélectionné, cliquez sur **Terminer** puis cliquez sur **OK**.
6. Dans le MMC, déroulez le menu **Certificats (ordinateur local)**, cliquez avec le bouton droit sur **Personnel**, cliquez sur **Toutes les tâches**, puis sur **Demander un nouveau certificat**.
7. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner la stratégie d'inscription du certificat**, cliquez sur **Suivant**.
9. Sur la page **Demander des certificats**, cliquez sur **Certificat Web Adatum**, puis cliquez sur **L'inscription pour obtenir ce certificat nécessite des informations supplémentaires.** Lien **Cliquez ici pour configurer les paramètres**.
10. Dans la section **Nom du sujet**, dans le menu déroulant **Type**, sélectionnez **Nom commun**, dans la zone de texte **Valeur**, saisissez **adfswap.adatum.com**, puis cliquez sur **Ajouter**.
11. Dans la liste **Autre nom**, dans le champ **Type**, cliquez sur la liste déroulante, puis sélectionnez **DNS**. Dans la zone **Valeur**, saisissez **adfswap.adatum.com**, puis cliquez sur **Ajouter**.
12. Dans la liste **Autre nom**, cliquez sur **DNS**, dans la case **Valeur**, saisissez **rdgw.adatum.com**, puis cliquez sur **Ajouter**.
13. Dans la liste **Autre nom**, cliquez sur **DNS**, dans la case **Valeur**, saisissez **lon-svr1.adatum.com**, puis cliquez sur **Ajouter**.
14. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés du certificat**.

15. Cliquez sur **Inscrire** afin de procéder avec le certificat d'inscription.
16. Cliquez sur **Terminer** pour fermer la boîte de dialogue **Inscription du certificat**.

Configurer le proxy d'application web

1. Dans le **Gestionnaire de serveur**, depuis le menu **Outils**, ouvrez la **Console de gestion de l'accès à distance**.
2. Dans le volet de navigation, cliquez sur **Proxy d'application Web**.
3. Dans le volet central, cliquez sur **Exécuter l'Assistant Configuration du proxy d'application Web**.
4. Dans l'**Assistant Configuration du Proxy d'application Web**, sur la page **Bienvenue**, cliquez sur **Suivant**.
5. Sur la page **Serveur de fédération**, effectuez les étapes suivantes :
   a. Dans la case **Nom du service de fédération**, saisissez **adfswap.adatum.com**, qui est le FQDN du service de fédération.
   b. Dans la zone **Nom d'utilisateur**, saisissez **Administrateur**, dans la zone **Mot de passe**, saisissez **Pa$$w0rd**, puis cliquez sur **Suivant**.
6. Sur la page **Certificat proxy AD FS**, dans la liste des certificats installés sur le serveur proxy d'application Web, cliquez sur **adfswap.adatum.com**, puis cliquez sur **Suivant**.
7. Sur la page **Confirmation**, vérifiez les paramètres. Si nécessaire, vous pouvez copier l'applet de commande Windows PowerShell pour automatiser les installations supplémentaires. Cliquez sur **Configurer**.
8. Sur la page **Résultats**, vérifiez que la configuration est réussie, puis cliquez sur **Fermer**.

Remarque : Si vous recevez un message d'erreur, vérifiez si LON-SVR2 a démarré et si le service AD FS s'exécute sur LON-SVR2. Ensuite, retournez à l'étape 2 pour exécuter l'assistant de configuration du proxy d'application web à nouveau.

Publiez le site Web interne

1. Sur le serveur proxy d'application Web, dans la console **Gestion de l'accès à distance**, dans le volet de navigation, cliquez sur **Proxy d'application web**, puis, dans le volet **Tâches**, cliquez sur **Publier**.
2. Dans l'**Assistant Publier une nouvelle application**, sur la page **Bienvenue**, cliquez sur **Suivant**.
3. Sur la page **préauthentification**, cliquez sur **Pass-through**, puis sur **Suivant**.
4. Sur la page **Paramètres de publication**, effectuez les étapes suivantes :
   a. Dans la zone **Nom**, saisissez **App Adatum LOB Web LOB (LON-SVR1)**.
   b. Dans la zone **URL externe**, saisissez **https://lon-svr1.adatum.com**.
   c. Dans la liste **Certificat externe**, cliquez sur **adfswap.adatum.com**.
   d. Dans la zone **URL du serveur principal**, assurez-vous que **https://lon-svr1.adatum.com** est répertorié, puis cliquez sur **Suivant**.

   Remarque : La valeur de l'**URL du serveur principal** est automatiquement saisie lorsque vous saisissez l'URL externe.

5. Sur la page **Confirmation**, vérifiez les paramètres, puis cliquez sur **Publier**. Vous pouvez copier la commande Windows PowerShell pour configurer d'autres applications publiées.
6. Sur la page **Résultats**, assurez-vous que l'application est publiée avec succès, puis cliquez sur **Fermer**.

Configurer l'authentification du site Web interne

1. Basculez vers LON-SVR1.
2. Cliquez sur le bouton **Démarrer**, puis cliquez sur la vignette du **Gestionnaire de serveur**. Cliquez sur le menu **Outils**, puis cliquez sur le **Gestionnaire des services Internet (IIS)**.
3. Dans la console **Gestionnaire des services Internet (IIS)**, déroulez le menu **LON-SVR1 (ADATUM\administrateur)**.
4. Développez **Sites**, puis cliquez sur **Site Web par défaut**.
5. Dans la console **Services Internet (IIS)**, dans le volet **Accueil du site Web par défaut**, double-cliquez sur **Authentification**.
6. Dans la console **Services Internet (IIS)**, dans le volet **Authentification**, cliquez avec le bouton droit sur **Authentification Windows**, puis cliquez sur **Activer**.
7. Dans la console **Services Internet (IIS)**, dans le volet **Authentification**, cliquez avec le bouton droit sur **Authentification anonyme**, puis cliquez sur **Désactiver**.
8. Fermez la console **Gestionnaire des services Internet (IIS)**.

Vérifier l'accès au site Web interne

1. Basculez vers LON-CL1.
2. Dans la barre des tâches, cliquez sur l'icône de **Microsoft Edge**.
3. Dans le champ **Rechercher ou entrer une adresse web**, saisissez **https://lon-svr1.adatum.com**, puis appuyez sur Entrée.
4. Lorsque vous y êtes invité, dans la boîte de dialogue **Microsoft Edge**, saisissez **adatum\logan** pour le nom d'utilisateur et **Pa$$w0rd** pour le mot de passe, puis cliquez sur **OK**.
5. Vérifiez que la page Web par défaut IIS 9.0 pour LON-SVR1 s'ouvre.

Contrôle des acquis et éléments à retenir

Méthode conseillée

Rappelez-vous qu'AD FS est nécessaire lors de la mise en œuvre du rôle Web Application Proxy. Si vous envisagez d'utiliser uniquement l'authentification directe avec le proxy d'application Web, vous devez uniquement installer AD FS et exécutez l'assistant de configuration AD FS. Vous n'avez pas à configurer quoi que ce soit d'autre.

Pour faciliter le déploiement, envisagez d'utiliser des certificats SSL publics pour votre serveur de proxy d'application web, le serveur de passerelle Bureau à distance et les serveurs d'applications web.

Questions de contrôle des acquis

Question : Quelles sont les solutions d'accès à distance que vous pouvez déployer à l'aide de Windows Server 2016 ?

> **Réponse :** Dans Windows Server 2016, vous pouvez déployer les solutions d'accès à distance suivantes : DirectAccess, VPN, routage et proxy d'application web.

Question : Quel type de solutions d'accès à distance pouvez-vous fournir en utilisant le VPN dans Windows Server 2016 ?

> **Réponse :** Vous pouvez configurer les solutions d'accès à distance suivantes à l'aide de VPN dans Windows Server 2016 :
>
> - Accès distant sécurisé aux ressources réseau internes pour les utilisateurs situés sur Internet. Les utilisateurs jouent le rôle de clients VPN qui se connectent à Windows Server 2016, qui sert de serveur VPN.
> - Communication sécurisée entre les ressources réseau qui se trouvent à des emplacements géographiques ou sur des sites différents. Cette solution est appelée *VPN de site à site*. Sur chaque site, Windows Server 2016 agit comme un serveur VPN qui chiffre la communication entre les sites.

Question : Quel type d'applications pouvez-vous publier en utilisant le proxy d'application web dans Windows Server 2016 ?

> **Réponse :** Le proxy d'application Web dans Windows Server 2016 est un service de rôle que vous pouvez utiliser pour publier des applications Web ou des serveurs de passerelle Bureau à distance. Vous pouvez choisir entre deux types de préauthentification pour les applications Web :
>
> - La préauthentification Active Directory Federation Services (AD FS), qui utilise AD FS pour les applications Web qui utilisent l'authentification basée sur les revendications.
> - La préauthentification directe, où un utilisateur se connecte à l'application Web par le biais d'un proxy d'application Web et l'application Web authentifie l'utilisateur.

Outils

Outil	Utilisation	Emplacement
Console de gestion d'accès à distance	Gestion de DirectAccess et du VPN	Gestionnaire de serveur/Outils
Console de routage et d'accès à distance	Gestion du VPN et du routage	Gestionnaire de serveur/Outils
Assistant de démarrage de l'accès à distance	Un outil graphique qui simplifie la configuration de	Console du gestionnaire de serveur/outils/gestion de l'accès

Outil	Utilisation	Emplacement
	DirectAccess.	à distance
Proxy d'application web	Applications web de publication	Gestionnaire de serveur/outils
Dnscmd.exe	Un outil de ligne de commande utilisé pour la gestion du DNS.	Exécuter à partir de ligne de commande
Services.msc	Aide à la gestion des services Windows.	Gestionnaire de serveur/Outils
Gpedit.msc	Aide à l'édition de la stratégie de groupe locale.	Exécuter à partir de ligne de commande
IPconfig.exe	Outil en ligne de commande qui affiche la configuration actuelle du réseau TCP/IP.	Exécuter à partir de ligne de commande
Console du gestionnaire DNS	Aide à la configuration de la résolution de noms.	Gestionnaire de serveur/Outils
Mmc.exe	Crée une MMC personnalisée pour la gestion des rôles du système d'exploitation, des caractéristiques et des paramètres.	Exécuter à partir de ligne de commande
Gpupdate.exe	Aide à la gestion de l'application Stratégie de groupe.	Exécuter à partir de ligne de commande
Utilisateurs et ordinateurs Active Directory	Utile pour la configuration de l'appartenance à un groupe pour les ordinateurs clients qui seront configurés avec DirectAccess.	Gestionnaire de serveur/Outils

Questions et réponses sur l'atelier pratique

Atelier pratique : Implémentation du proxy d'application Web

Questions et réponses

Question : Où devriez-vous déployer le serveur de proxy d'application web ?

Réponse : Vous devez déployer le serveur de proxy d'application web entre le réseau d'entreprise et Internet.

Question : Que faut-il pour que les clients accèdent à une application Web publiée ?

Réponse : Pour que les clients accèdent à une application Web publiée, ils doivent être en mesure de résoudre l'adresse externe de l'application qui est publiée par Web Application Proxy.

Module 7

Mise en œuvre de DirectAccess

Sommaire :

Leçon 1

Vue d’ensemble de DirectAccess

Sommaire :

Ressources

Composants de DirectAccess

Lectures supplémentaires : Pour plus d'informations, consultez IPv6 - Vue d'ensemble de la technologie : http://aka.ms/I43ird

Lectures supplémentaires : Pour plus d'informations, consultez Vue d'ensemble de l'accès à distance : http://aka.ms/Rlc58t

Options de protocoles de tunneling DirectAccess

Lectures supplémentaires : Pour plus d'informations, consultez Technologies de transition IPv6 : http://aka.ms/Hn3u61

Lectures supplémentaires : Pour plus d'informations, consultez Vue d'ensemble de Teredo : http://aka.ms/Jdw9r8

Lectures supplémentaires : Pour plus d'informations, consultez 3[MS-IPHTTPS] : protocole IP over HTTPS (IP-HTTPS) : http://aka.ms/Bcviz1

Gestion de l'accès à distance dans Windows Server 2016

Lectures supplémentaires : Pour obtenir une liste complète des applets de commande d'accès à distance dans Windows PowerShell, consultez Applets de commande d'accès à distance : http://aka.ms/Ar09tz

Démonstration : Installation du rôle de serveur Accès à distance

Procédure de démonstration

Installez le rôle de serveur Accès à distance

1. Sur LON-SVR1, cliquez sur **Démarrer**, **Gestionnaire de serveur**, **Gérer**, puis **Ajouter des rôles et fonctionnalités**.
2. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner les rôles de serveur**, cliquez sur **Accès à distance**, puis sur **Suivant**.
6. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
7. Sur la page **Accès à distance**, cliquez sur **Suivant**.
8. Sur la page **Sélectionner des services de rôle**, cliquez sur **DirectAccess et VPN (RAS)**.
9. Dans la boîte de dialogue **Assistant Ajout de rôles et fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**, puis vérifiez que **DirectAccess et VPN (RAS)** est sélectionné.
10. Sur la page **Sélectionner des services de rôle**, cliquez sur **Suivant**.
11. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
12. Une fois l'installation terminée, cliquez sur **Fermer**.

Leçon 2

Mise en œuvre de DirectAccess à l'aide de l'Assistant de démarrage

Sommaire :

Questions et réponses

Question : Combien d'objets de stratégie de groupe l'assistant de démarrage crée-t-il ?

( ) 1

( ) 2

( ) 3

( ) 4

( ) 5

Réponse :

( ) 1

(√) 2

( ) 3

( ) 4

( ) 5

Commentaire :

L'Assistant de démarrage crée deux objets de stratégie de groupe : Réglages du serveur DirectAccess et Paramètres du client DirectAccess.

Question : Vous souhaitez déployer un serveur de localisation de réseau dédié. Seriez-vous capable d'utiliser l'assistant de démarrage pour cela ?

Réponse : Non. Si vous utilisez l'Assistant de démarrage, le serveur d'emplacement réseau et le serveur DirectAccess constitueront le même ordinateur. Vous devrez configurer le serveur d'emplacement réseau manuellement à partir de la console **Gestion de l'accès à distance**.

Ressources

Obtention des changements de configuration de l'assistant de démarrage

Lectures supplémentaires : Pour plus d'informations, consultez DirectAccess les Configurations non prises en charge : http://aka.ms/R3r2ec

Démonstration : Exécution de l'assistant de démarrage

Procédure de démonstration

Créer un groupe de sécurité pour les ordinateurs clients de DirectAccess

1. Sur LON-DC1, dans le **Gestionnaire de serveur**, cliquez dans le coin supérieur droit sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory.**
2. Dans l'arborescence de la console **Utilisateurs et ordinateurs Active Directory**, cliquez à l'aide du bouton droit sur **Adatum.com**, cliquez sur **Nouveau**, puis cliquez sur **Unité organisationnelle**.
3. Dans la boîte de dialogue **Nouvel objet - Unité organisationnelle**, dans la zone de texte **Nom**, entrez **Comptes spéciaux**, 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 **Comptes spéciaux**, cliquez sur **Nouveau**, puis sur **Groupe**.

5. Dans la boîte de dialogue **Nouvel objet - groupe**, dans la zone de texte **Nom de groupe**, entrez **DirectAccessClients**.
6. Dans le champ d'application **Groupe**, veillez à ce que **Global** soit sélectionné. Dans le type **Groupe**, veillez à ce que **Sécurité** soit sélectionné, puis cliquez sur **OK**.
7. Dans le volet d'informations, cliquez avec le bouton droit sur **DirectAccessClients**, puis cliquez sur **Propriétés**.
8. Dans la boîte de dialogue **Propriétés de DirectAccessClients**, cliquez sur l'onglet **Membres**, puis sur **Ajouter**.
9. Dans la boîte de dialogue **Sélectionner les utilisateurs, contacts, ordinateurs, comptes de service ou groupes**, cliquez sur **Types d'objets**, sélectionnez la case à cocher **Ordinateurs**, puis cliquez sur **OK**.
10. Dans le champ **Entrez le nom de l'objet à sélectionner (exemples)**, entrez **LON-CL1**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
11. Vérifiez que **LON-CL1** s'affiche sous **Membres**, puis cliquez sur **OK**.
12. Fermez la console **Utilisateurs et ordinateurs Active Directory**.

Configurer DirectAccess en exécutant l'assistant de démarrage

1. Basculez vers **EU-RTR**.
2. Cliquez sur **Démarrer**, puis sur la mosaïque **Gestionnaire de serveur**.
3. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion de l'accès à distance**.
4. Dans la console **Gestion de l'accès à distance**, sous **Configuration**, cliquez sur **DirectAccess et VPN**, puis sur **Exécuter l'Assistant de démarrage**.
5. Dans l' **Assistant de démarrage**, sur la page **Configurer l'accès à distance**, cliquez sur **Déployer DirectAccess seulement**.
6. Sur la Page **Topologie de réseau**, vérifiez que **Edge** est sélectionné, et dans la zone de texte **Saisir le nom ou l'adresse IPv4 publique utilisée par les clients pour se connecter au serveur d'accès à distance**, entrez **131.107.0.10**, puis cliquez sur **Suivant**.
7. Sur la page **Configurer l'accès à distance**, cliquez sur le lien **ici**.

Remarque : Assurez-vous de cliquer sur le lien **ici**, car cette opération permettra d'afficher une fenêtre supplémentaire pour la configuration des paramètres d'objet de stratégie de groupe (GPO) et des groupes Active Directory qui réunira les ordinateurs qui seront affectés par les paramètres DirectAccess.

8. Sur la page **Vérification de l'accès à distance**, vérifiez que deux objets objets de stratégie de groupe ont été créés : **Paramètres du serveur DirectAccess** et **Paramètres client de DirectAccess**.
9. À côté de **Clients à distance**, cliquez sur le lien **Changer**.
10. Cliquez sur **Ordinateurs du domaine (ADATUM\Ordinateurs du domaine)**, puis cliquez sur **Retirer**.
11. Cliquez sur **Ajouter**. Dans le champ **Entrez le nom de l'objet à sélectionner (exemples)**, entrez **direct**, puis cliquez sur **Vérifier les noms**. Vérifiez que **DirectAccessClients** s'affiche, puis cliquez sur **OK**.
12. Désactivez la case à cocher **Activer DirectAccess pour les ordinateurs portables uniquement**, puis cliquez sur **Suivant**.

13. Sur la page **Configuration du client de DirectAccess**, remplissez les informations suivantes, puis cliquez sur **Terminer** :
    - Adresse e-mail du service d'assistance : **DAHelp@adatum.com**
    - Nom de connexion de DirectAccess : **A. Datum DirectAccess**

    Remarque : Indiquez aux stagiaires que même s'il n'est pas nécessaire de fournir une adresse e-mail Helpdesk, nous le recommandons vivement. Si aucune adresse e-mail n'est renseignée, l'utilisateur ne sera pas en mesure de collecter les fichiers journaux client DirectAccess s'il y a un problème.

14. Dans la fenêtre **Vérification de l'accès à distance**, cliquez sur **OK**.
15. Sur la page **Configurer l'accès à distance**, cliquez sur **Terminer** et attendez que la configuration soit terminée.
16. Dans la boîte de dialogue **Appliquer les paramètres de l'assistant de démarrage**, vérifiez que l'importation s'est déroulée avec succès, puis cliquez sur **Fermer**.

Démonstration : Identifier les paramètres Assistant de démarrage

Procédure de démonstration

Passer en revue les modifications de configuration dans la console Gestion de l'accès à distance

1. Basculez vers la console **Gestion de l'accès à distance** sur EU-RTR.
2. Dans la fenêtre **Configuration de l'accès à distance**, sous l'image de l'ordinateur client nommé **Étape 1 : Clients distants**, cliquez sur **modifier**.
3. Dans la fenêtre **Configuration du client DirectAccess**, cliquez sur **Scénario de déploiement** et passez en revue les paramètres par défaut.
4. Cliquez sur **Sélectionner des groupes** et enregistrez les paramètres par défaut.
5. Cliquez sur **Assistant Connectivité réseau**, puis enregistrez les paramètres par défaut.
6. Cliquez sur **Annuler**, puis sur **OK**.
7. Dans la fenêtre **Configuration de l'accès à distance**, sous l'image de l'ordinateur client nommé **Étape 2 : Serveur d'accès à distance**, cliquez sur **Modifier**.
8. Dans la fenêtre **Configuration du serveur d'accès à distance**, cliquez sur **Topologie de réseau** et enregistrez les paramètres par défaut.
9. Cliquez sur **Adaptateurs réseau** et enregistrez les paramètres par défaut.
10. Cliquez sur **Authentification** et enregistrez les paramètres par défaut.
11. Cliquez sur **Annuler**, puis sur **OK**.
12. Dans la fenêtre **Configuration de l'accès à distance**, sous l'image de l'ordinateur client nommé **Étape 3 : Serveurs d'infrastructure**, cliquez sur **modifier**.
13. Dans la fenêtre **Configuration des serveurs d'infrastructure**, cliquez sur **Serveur d'emplacement réseau** et enregistrez les paramètres par défaut.
14. Cliquez sur **DNS** et passez en revue les paramètres par défaut.
15. Cliquez sur **Liste de recherche de suffixes DNS** et enregistrez les paramètres par défaut.

16. Cliquez sur **Gestion** et passez en revue les paramètres par défaut.
17. Cliquez sur **Annuler**, puis sur **OK**.
18. Dans la fenêtre **Configuration de l'accès à distance**, sous l'image de l'ordinateur client nommé **Étape 4 : Serveurs d'applications**, cliquez sur **Modifier**.
19. Dans la fenêtre **Installation du serveur d'applications DirectAccess**, passez en revue les paramètres par défaut. Cliquez sur **Annuler**, puis sur **OK**.
20. Fermez toutes les fenêtres actives.

Examiner les changements d'infrastructure dans la console Gestion des stratégies de groupe

1. Sur **EU-RTR**, cliquez sur **Démarrer**, puis cliquez sur la vignette **Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
3. Dans la **consolede Gestion des stratégies de groupe**, développez **Forêt: Adatum.com**, puis **Domaines** et enfin **Adatum.com**. Mettez en évidence les deux nouveaux objets de stratégie de groupe qui ont été créés :
   - **Paramètres du client DirectAccess**
   - **Paramètres du serveur DirectAccess**
4. Dans le volet de navigation, cliquez sur l'objet de stratégie de groupe **Réglages du serveur DirectAccess**.
5. Dans la boîte de dialogue **Console de gestion des stratégies de groupe**, cliquez sur **OK**, puis sur l'onglet **Paramètres** dans le volet d'informations.
6. Dans le volet d'informations, sous Configuration ordinateur (activée), sur la ligne **Paramètres de sécurité**, cliquez sur le lien **Afficher** sur le côté droit, puis sur la ligne **Pare-feu Windows avec fonctions avancées de sécurité**, cliquez sur le lien **Afficher**.
7. Mettez en évidence qu'il existe trois groupes de paramètres de pare-feu configurés pour les serveurs de DirectAccess : **Paramètres globaux**, **Règles de trafic entrant**, et **Paramètres de sécurité de la connexion**.
8. Sur la ligne **Paramètres globaux**, cliquez sur le lien **Afficher**, puis passez en revue le paramètre **Exception IPsec ICMP**.
9. Sur la ligne **Règles de trafic entrant**, cliquez sur le lien **Afficher**, puis passez en revue les paramètres suivants :
   - **Réseau central – IPHTTPS (TCP-In)**. Notez que cette règle permet le trafic IP-HTTPS entrant pour fournir la connectivité à travers les proxies HTTP et les pare-feu.
   - **Serveur de noms de domaine (UDP-In)**, et **Serveur de noms de domaine (TCP-In)**. Expliquez que ces règles autorisent le trafic vers le serveur DNS64 qui est déployé sur le serveur d'accès à distance. Mettez en évidence l'adresse IPv6 dans les règles et expliquez qu'il s'agit de l'adresse de la carte London_Network sur EU-RTR qui peut être vérifiée en exécutant la commande **ipconfig /all** dans une fenêtre Windows PowerShell.
10. Sur la ligne Paramètres de sécurité de la connexion, cliquez sur le lien **Afficher**, puis sur la ligne **Règles**, cliquez sur le lien **Afficher**. Passez en revue les paramètres suivants :
    - **Stratégie DirectAccess-DaServerToCorpSimplified**. Passez en revue les préfixes d'adresse IPv6 et comparez-les avec les préfixes d'adresse IPv6 que vous avez enregistrés à l'étape 9 de la section précédente de cette démonstration. Remarquez qu'il s'agit des mêmes préfixes que vous avez configurés dans l'assistant de démarrage.

11. Sur la ligne **Règles**, cliquez sur le lien **Masquer**.
12. Sous la ligne Paramètres de sécurité de la connexion, sur la ligne Première authentification, cliquez sur le lien **Afficher**, puis passez en revue le paramètre d'authentification Kerberos.
13. Répétez l'étape 12 pour les paramètres **Seconde authentification**, **Échange de clés (Mode principal)** et **Protection des données (mode rapide)**.
14. Dans le volet de navigation, cliquez sur l'objet de stratégie de groupe **Paramètres du client DirectAccess**.
15. Dans la boîte de dialogue **Console de gestion des stratégies de groupe**, cliquez sur **OK**.
16. Dans le volet d'informations, cliquez sur l'onglet **Paramètres**.
17. Dans le volet d'informations, sous Configuration ordinateur (activée), sur la ligne Paramètre de sécurité, cliquez sur le lien **Afficher** sur le côté droit. Sur la ligne Stratégies de clé publique/Autorités de certification de racine de confiance, cliquez sur le lien **Afficher**, puis sur la ligne Certificats, cliquez sur le lien **Afficher**. Notez que l'objet de stratégie de groupe configure les ordinateurs clients DirectAccess de sorte qu'il fasse confiance aux certificats auto-signés portant l'adresse IP 131.107.0.10 et le nom DirectAccess-NLS**.**Adatum.com.
18. Dans le volet d'informations, sous Configuration ordinateur (activée), sur les lignes Paramètre de sécurité et Pare-feu Windows avec fonctions avancées de sécurité, cliquez sur le lien **Afficher**.
19. Notez qu'il existe trois groupes de paramètres de pare-feu configurés pour les clients DirectAccess : **Paramètres globaux**, **Règles de trafic sortant** et **Paramètres de sécurité de la connexion**.
20. Sur la ligne **Paramètres globaux**, cliquez sur le lien **Afficher**, puis passez en revue le paramètre Exception IPsec ICMP.
21. Sur la ligne **Règles de trafic sortant**, cliquez sur le lien **Afficher**, puis passez en revue les paramètres suivants :
    - **Réseau central - IP-HTTPS (TCP-Out)**. Cette règle permet le trafic IP-HTTPS sortant pour fournir la connectivité à travers les proxies HTTP et les pare-feu.
22. Sur la ligne **Paramètres de sécurité de la connexion**, cliquez sur le lien **Afficher**, puis sur la ligne Règles, cliquez sur le lien **Afficher**.
23. Passez en revue les trois règles, puis comparez les préfixes d'adresse IPv6 avec les préfixes d'adresse IPv6 que vous avez enregistrés à l'étape 9 dans la section précédente de cette démonstration. Remarquez qu'il s'agit des mêmes préfixes qu'ils ont configurés avec l'Assistant de démarrage.
24. Sur la ligne **Règles**, cliquez sur le lien **Masquer**.
25. Sous la ligne **Paramètres de sécurité de la connexion**, sur la ligne Première authentification, cliquez sur le lien **Afficher**, puis passez en revue le paramètre d'authentification Kerberos.
26. Répétez l'étape 25 pour les lignes suivantes : **Seconde authentification**, **Échange de clés (Mode principal)** et **Protection des données (mode rapide)**.
27. Fermez la **Console de gestion des stratégies de groupe**.
28. Sur LON-DC1, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS**.
29. Dans la console **Gestionnaire DNS**, dans le volet de navigation, développez **Zones de recherche**, puis **Adatum.com**.
30. Passez en revue les enregistrements A et AAAA pour les hôtes suivants :
    - **DirectAccess-corpConnectivityHost**
    - **DirectAccess-NLS**
    - **DirectAccess-WebProbeHost**.

    Ces enregistrements sont créés par l'Assistant de démarrage.

Leçon 3

Mise en œuvre et gestion d'une infrastructure DirectAccess avancée

Sommaire :

Questions et réponses

Question : Que devez-vous configurer pour utiliser les ordinateurs fonctionnant sous Windows 7 en tant que clients de DirectAccess ?

> **Réponse :** Vous devez configurer votre déploiement DirectAccess pour qu'il utilise des certificats afin de prendre en charge Windows 7 en tant que client DirectAccess.

Question : Que devez-vous configurer sur le serveur DirectAccess afin que le bouton Collecter les journaux soit visible pour les utilisateurs ?

> **Réponse :** Vous devez renseigner le champ **Adresse de messagerie du support technique** lors de la configuration du serveur DirectAccess.

Ressources

Équilibrage de charge et des options de haute disponibilité

 **Lectures supplémentaires :** Pour plus d'informations, consultez Planifier un déploiement de Cluster à charge équilibrée : http://aka.ms/H2edc3

Soutenir plusieurs endroits

 **Lectures supplémentaires :** Pour plus d'informations, consultez Déployer plusieurs serveurs d'accès à distance dans un déploiement Multisite : http://aka.ms/Jz1esb

 **Lectures supplémentaires :** Pour plus d'informations, consultez Planifier le déploiement Multisite DirectAccess : http://aka.ms/T6qfvh

Intégration d'une PKI avec DirectAccess

 **Lectures supplémentaires :** Pour plus d'informations, consultez Services de certificats Active Directory : http://aka.ms/T8xtn9

Mise en œuvre des certificats clients pour DirectAccess

 **Lectures supplémentaires :** Pour plus d'informations, consultez Configurer DirectAccess avec l'authentification unique : http://aka.ms/Ax93rb

Options de configuration de réseau interne

 **Lectures supplémentaires :** Pour plus d'informations, reportez-vous à l'étape 2 : Planifier les déploiements de DirectAccess : http://aka.ms/Ttfwyn

Démonstration : Modification de l'infrastructure de DirectAccess

Procédure de démonstration

Configurez le rôle serveur d'accès à distance

1. Sur **EU-RTR**, dans **Gestionnaire de serveur**, dans le menu **Outils**, cliquez sur **Gestion de l'accès à distance**.
2. Dans la console **Gestion de l'accès à distance**, cliquez sur **Accès direct et VPN**.
3. Sous Étape 1, cliquez sur **Modifier** pour sélectionner les clients qui utiliseront DirectAccess.
4. Sur la page **Scénario de déploiement**, cliquez sur **Suivant**.
5. Sous **Sélectionner des groupes**, cliquez sur **Suivant**.
6. Dans la page **Assistant Connectivité réseau**, dans la colonne Ressource, supprimer l'enregistrement existant en cliquant droit sur la flèche, puis en cliquant sur **Effacer**.
7. Dans la page **Assistant Connectivité réseau**, dans la colonne Ressource, double-cliquez sur la ligne vide.
8. Dans la boîte de dialogue **Configurer des ressources d'entreprise pour NCA**, vérifiez que **HTTP** est sélectionné, puis dans la zone de texte à côté de **HTTP**, entrez **https://lon-svr1.adatum.com**.
9. Cliquez sur **Valider**, puis sur **Ajouter**.
10. Dans la page **Assistant Connectivité réseau**, cliquez sur **Terminer**.
11. Sous Étape 2, cliquez sur **Modifier**.
12. Sur la Page **Topologie de réseau**, vérifiez que **Edge** est sélectionné. Entrez **131.107.0.10**, puis cliquez sur **Suivant**.
13. Sur la page **Adaptateurs réseau**, assurez-vous que la case à cocher **Utiliser un certificat auto-signé créé automatiquement par DirectAccess** est sélectionnée. Vérifiez que **CN=131.107.0.10** est utilisé comme certificat pour authentifier les connexions IP-HTTPS, puis cliquez sur **Suivant**.
14. Sur la page **Authentification**, cliquez sur **Utiliser les certificats d'ordinateur**, puis sur **Parcourir**, **AdatumCA** et enfin sur **OK**.
15. Cliquez sur **Permettre aux ordinateurs clients Windows 7 de se connecter via DirectAccess**, puis cliquez sur **Terminer**.
16. Dans le volet **Configuration de l'accès à distance**, sous Étape 3, cliquez sur **Modifier**.
17. Sur la page **Serveur d'emplacement réseau**, sélectionnez **Le serveur d'emplacement réseau est déployé sur un serveur Web distant (recommandé)**, entrez **https://lon-svr1.adatum.com**, cliquez sur **Valider**, puis sur **Suivant**.
18. Sur la page **DNS**, cliquez sur **Suivant**.
19. Sur la page **Liste de recherche de suffixes DNS**, cliquez sur **Suivant**.
20. Dans la page **Gestion**, cliquez sur **Terminer**.
21. Sous Étape 4, cliquez sur **Modifier**.
22. Sur la page **Installation du serveur d'applications DirectAccess**, cliquez sur **Terminer**.
23. Cliquez sur **Terminer** pour enregistrer les modifications.
24. Sur la page **Vérification de l'accès à distance**, cliquez sur **Annuler**.

Remarque : La configuration de DirectAccess n'est pas appliquée car des conditions préalables doivent être configurées, telles que la configuration AD DS, les paramètres de pare-feu et le déploiement de certificats.

Démonstration : Surveillance et dépannage de la connectivité de DirectAccess

Procédure de démonstration

Vérifier les paramètres de configuration de la stratégie de groupe de DirectAccess pour les clients Windows 10

1. Basculez vers LON-CL1.
2. Redémarrez LON-CL1 et connectez-vous en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
3. Ouvrez une fenêtre **Invite de commandes**, puis tapez les commandes ci-dessous, en appuyant sur Entrée à la fin de chaque ligne :

```
gpupdate /force
gpresult /R
```

4. Vérifiez que l'objet de la stratégie de groupe **Paramètres du client DirectAccess** s'affiche dans la liste des objets de stratégie appliqués pour les paramètres de l'ordinateur.
5. Fermez la fenêtre **Invite de commandes**.

Déplacer l'ordinateur client vers le réseau virtuel Internet

1. Pour déplacer le client à partir de l'Intranet vers le réseau public, sur LON-CL1, cliquez droit sur **Démarrer**, puis cliquez sur **Connexions réseau**.
2. Dans la fenêtre **Connexions réseau**, cliquez avec le bouton droit sur **London_Network**, et cliquez ensuite sur **Désactiver**.
3. Cliquez avec le bouton droit sur **Internet**, puis cliquez sur **Activer**.
4. Fermez la fenêtre **Connexions réseau**.

Vérification de la connectivité au serveur DirectAccess

1. Sur **LON-CL1**, ouvrez une fenêtre **Invite de commandes**.
2. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
Ipconfig
```

   Remarquez l'adresse IPv6 qui commence par 2002. Ceci est une adresse IP-HTTPS.

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

```
Nom Netsh show effectivepolicy
```

4. Cliquez sur **Démarrer**, puis sur **Paramètres**.
5. Dans **Paramètres**, sélectionnez **Réseau et Internet**, puis cliquez sur **DirectAccess**.
6. Vérifiez que **Votre PC est correctement configuré pour un seul site DirectAccess** est affiché sous **Emplacement**.
7. Remarquez le bouton **Collecter** sous **Informations de résolution**.

Suivi de la connectivité de DirectAccess

1. Basculez vers **EU-RTR**.
2. Sur **EU-RTR**, ouvrez la console **Gestion de l'accès à distance**, puis dans le volet de gauche, cliquez sur **Tableau de bord**.
3. Passez en revue les informations dans le volet central, sous **DirectAccess et statut du client VPN**.
4. Dans le volet de gauche, cliquez sur **Statut du client à distance**, puis dans le volet central, passez en revue les informations dans la liste **Clients connectés**.
5. Si aucune information ne s'affiche dans la liste **Clients connectés**, redémarrez **LON-CL1** et répétez l'étape 4.
6. Dans le volet de gauche, cliquez sur **Création d'un rapport**, puis dans le volet central, cliquez sur **Configurer la comptabilisation**.
7. Dans la fenêtre **Configurer la comptabilisation**, sous **Sélectionner la méthode de comptabilisation**, cliquez sur **Utiliser la comptabilisation de la boîte de réception**, puis sur **Appliquer** et enfin sur **Fermer**.
8. Dans le volet central, sous **Rapports d'accès à distance**, passez en revue les options pour le suivi des données historiques.
9. Fermez la **Console de gestion de l'accès à distance.**

Contrôle des acquis et éléments à retenir

Bonnes Pratiques

- Windows Server 2016, Windows 10, Windows 8.1 et Windows 8 incluent des fonctionnalités pour une meilleure maniabilité, facilité de déploiement et pour une échelle et une performance améliorées.
- Vous pouvez surveiller l'environnement DirectAccess à l'aide de Windows PowerShell et des outils de l'interface graphique, et la connectivité réseau Assistant du côté du client.
- DirectAccess peut maintenant accéder aux serveurs IP4 de votre réseau. En outre, vos serveurs ne nécessitent pas que vous implémentiez des adresses IPv6 par DirectAccess, puisque votre serveur DirectAccess agit comme un proxy.
- Envisagez d'intégrer DirectAccess à votre solution d'accès à distance existante. Windows Server 2016 peut mettre en œuvre un serveur DirectAccess derrière le périphérique NAT, qui est la solution la plus commune d'accès à distance pour les organisations.

Questions de contrôle des acquis

Question : Quels sont les principaux avantages de l'utilisation de DirectAccess pour fournir une connectivité à distance ?

Réponse : Les principaux avantages de l'utilisation de DirectAccess pour fournir une connectivité à distance sont les suivants :

- Connectivité toujours activée. Lorsque l'utilisateur est connecté à Internet, ce dernier est également connecté à l'Intranet.
- Les utilisateurs disposent de la même expérience indépendamment du fait qu'ils soient connectés localement ou à distance.
- Accès bidirectionnel. Lorsque l'ordinateur client accède à l'Intranet, l'ordinateur peut être géré par les administrateurs.
- Sécurité optimisée. Les administrateurs peuvent définir et contrôler les ressources de l'Intranet qui sont accessibles via DirectAccess.

Question : Comment configurer les clients DirectAccess ?

Réponse : Pour configurer les clients DirectAccess, utilisez la stratégie de groupe. Lorsque vous utilisez l'Assistant d'accès à distance pour configurer DirectAccess, deux objets de stratégie de groupe sont créés et liés au domaine. Ces deux objets de stratégie de groupe définissent les paramètres liés à DirectAccess et sont appliqués aux clients DirectAccess.

Question : Comment l'ordinateur client DirectAccess détermine-t-il s'il est connecté au réseau Intranet ou à Internet ?

Réponse : Lors de la configuration du serveur DirectAccess, vous devez déterminer l'ordinateur qui servira de serveur de localisation de réseau. Le serveur de localisation de réseau doit être un serveur Web hautement disponible. Selon la réponse de ce serveur Web, le client DirectAccess détermine s'il est connecté au réseau Intranet ou à Internet.

Question : À quoi sert une table NRPT ?

Réponse : La table de stratégie de résolution de noms enregistre une liste d'espaces de noms DNS et leurs paramètres de configuration correspondants. Ces paramètres définissent le serveur DNS à contacter, ainsi que le comportement du client DNS pour cet espace de noms.

Outils

Outil	Utilisation	Emplacement
Console de Gestion de l'accès distant	Gestion de DirectAccess et du VPN	Gestionnaire de serveur/Outils
Assistant de démarrage de l'accès à distance	Un outil graphique qui simplifie la configuration de DirectAccess	Console du gestionnaire de serveur/outils/gestion de l'accès à distance
Dnscmd.exe	Un outil de ligne de commande utilisé pour la gestion de DNS	Exécuter depuis la ligne de commande
Services.msc	Aide à la gestion des services Windows	Gestionnaire de serveur/Outils
Gpedit.msc	Aide à l'édition de la stratégie de groupe locale	Exécuter depuis la ligne de commande
IPconfig.exe	Outil en ligne de commande qui affiche la configuration actuelle du réseau TCP/IP	Exécuter depuis la ligne de commande
Console du gestionnaire DNS	Aide à la configuration de la résolution de noms	Gestionnaire de serveur/Outils
Mmc.exe	Crée une MMC personnalisée pour la gestion des rôles du système d'exploitation, des caractéristiques et des paramètres.	Exécuter depuis la ligne de commande
Gpupdate.exe	Aide à la gestion des applications de la stratégie de groupe	Exécuter depuis la ligne de commande
Utilisateurs et ordinateurs Active Directory	Utile pour la configuration de l'appartenance à un groupe pour les ordinateurs clients qui seront configurés avec DirectAccess	Gestionnaire de serveur/outils

Problèmes courants et conseils de dépannage

Problème courant	Conseil pour la résolution du problème
Vous avez configuré DirectAccess, mais les utilisateurs se plaignent de problèmes de connectivité. Vous voulez un moyen efficace pour résoudre leurs problèmes.	Le dépannage de base est intégré dans l'assistance Connectivité réseau, afin de montrer aux utilisateurs comment y accéder et déterminer ce qui empêche l'ordinateur client de communiquer avec le serveur DirectAccess.
L'ordinateur client DirectAccess tente de se connecter au serveur DirectAccess à l'aide d'IPv6 et IPsec, mais n'y parvient pas.	Si vous utilisez Teredo comme technologie de transition IPv6, vérifiez si vous disposez de deux adresses publiques sur la carte réseau externe du serveur DirectAccess. Ces dernières sont nécessaires pour l'établissement de deux tunnels IPsec.

Questions et réponses sur le contrôle des ateliers pratiques

Atelier pratique A : Mise en œuvre de DirectAccess à l'aide de l'Assistant de démarrage

Questions et réponses

Question : Pourquoi avez-vous créé le groupe DirectAccessClients ?

Réponse : Vous avez créé le groupe DirectAccessClients pour appliquer les paramètres de sécurité DirectAccess aux ordinateurs appartenant à ce groupe de sécurité.

Question : Comment allez-vous configurer l'adresse IPv6 pour les ordinateurs des clients exécutant Windows 10 pour utiliser DirectAccess ?

Réponse : Les adresses IPv6 unicast globales sont générées automatiquement en fonction de l'infrastructure réseau. Par conséquent, les clients Windows 10 peuvent se connecter au réseau Intranet de l'entreprise et à Internet via DirectAccess, sans qu'il soit nécessaire de configurer les adresses IPv6.

Atelier pratique B : Déploiement d'une solution DirectAccess avancée

Questions et réponses

Question : Pourquoi la liste de révocation des certificats est-elle disponible sur le serveur Edge ?

Réponse : Vous avez rendu la CRL accessible sur le serveur Edge afin que les clients DirectAccess se connectant via Internet puissent accéder à la CRL.

Question : Pourquoi avez-vous installé un certificat sur l'ordinateur du client ?

Réponse : Sans certificat, le serveur DirectAccess ne peut pas identifier et authentifier le client.

Module 8

Implémentation de VPN

Contenu :

Leçon 1

Planification de VPN

Contenu :

Questions et réponses

Question : Quels sont les noms des différents protocoles de tunnel que vous pouvez utiliser dans Windows Server 2016 ?

Réponse : Vous pouvez utiliser les protocoles de tunnel PPTP, L2TP, IKEv2 et SSTP dans Windows Server 2016.

Question : Quelles sont les exigences pour reconnecter le VPN ?

Réponse : Les conditions d'utilisation de VPN Reconnect stipulent que vous devez utiliser :

- Un ordinateur qui exécute Windows Server 2016, Windows Server 2012 ou Windows Server 2008 R2 en tant que serveur VPN.
- Un ordinateur exécutant un client Windows 10, Windows 8, Windows Server 2012, Windows 7 ou Windows Server 2008 R2.
- PKI, car VPN Reconnect requiert un certificat d'ordinateur pour une connexion à distance. Vous pouvez utiliser des certificats émis par une AC interne ou une AC publique.

Question : Vous pouvez utiliser le VPN déclenché par l'application avec les ordinateurs des membres du domaine.

( ) Vrai

( ) Faux

Réponse :

( ) Vrai

(√) Faux

Commentaire :

L'une des conditions d'utilisation d'un VPN déclenché par l'application est l'impossibilité pour l'ordinateur client d'être un membre de domaine.

Leçon 2

Implémentation de VPN

Contenu :

Questions et réponses

Question : Combien de cartes d'interface réseau sont nécessaires lors de la configuration d'un serveur VPN dans Windows Server 2016 ?

Réponse : Deux cartes d'interface réseau sont nécessaires. L'une doit être connecté au réseau interne et l'autre à Internet.

Question : Quelles méthodes pouvez-vous utiliser pour distribuer un profil VPN à vos utilisateurs finaux ?

Réponse : Vous pouvez distribuer des profils VPN à vos utilisateurs finaux via :

- System Center Configuration Manager
- Stratégie de groupe
- Un script de démarrage
- Un script de connexion

Question : Quel est le nombre maximal de ports que vous pouvez configurer pour SSTP ?

( ) 25

( ) 75

( ) 128

( ) 500

( ) 999

Réponse :

( ) 25

( ) 75

( ) 128

( ) 500

(√) 999

Commentaire :

Vous pouvez configurer un maximum de 999 ports SSTP sur un serveur d'accès distant qui exécute Windows Server 2016.

Ressources

Distribution de profils VPN

Lectures supplémentaires : Pour plus d'informations, reportez-vous à « Comment créer des profils VPN dans le Gestionnaire de configuration du centre système » à : http://aka.ms/Gmn5hp

Lectures supplémentaires : Pour plus d'informations, voir « Connexions VPN dans Microsoft Intune » à : http://aka.ms/vp3kds

Lectures supplémentaires : Pour plus d'informations, reportez-vous à « Déploiement de connexions VPN à l'aide de PowerShell et de la Politique de groupe » à l'adresse : http://aka.ms/Khk938

Démonstration : Configuration VPN

Procédure de démonstration

Préparer l'environnement

1. Sur LON-DC1, cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (Admin)**.
2. À l'invite de commandes Windows PowerShell, saisissez la commande suivante, puis appuyez sur Entrée :

```
cd E:\Labfiles\Mod08
```

3. À l'invite de commandes Windows PowerShell, saisissez la commande suivante, puis appuyez sur Entrée :

```
.\mod8.ps1
```

4. Patientez jusqu'à ce que le script soit terminé, ce qui devrait prendre environ 20 secondes.

Demande de certificat pour l'EU-RTR

1. Sur EU-RTR, cliquez sur **Démarrer**, puis saisissez **Invite de commandes**. Dans les résultats, cliquez sur Invite de commandes.
2. Dans la fenêtre de l'**Invite de commandes**, saisissez la commande suivante et appuyez sur Entrée :

```
mmc
```

3. Dans la fenêtre **Console**, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
4. Dans la liste **Composants logiciels enfichables disponibles**, cliquez sur **Certificats**, puis sur **Ajouter**.
5. Dans la boîte de dialogue **Certificat du composant logiciel enfichable**, cliquez sur **Compte d'ordinateur**, puis cliquez sur **Suivant**.
6. Dans la boîte de dialogue **Sélectionner un ordinateur**, cliquez sur **Ordinateur local**, cliquez sur **Terminer**, puis cliquez sur **OK**.
7. Dans le composant logiciel enfichable **Certificats**, dans l'arborescence de la console du composant logiciel enfichable **Certificats**, accédez à **Certificats (Ordinateur local)\Personnel**.
8. Cliquez avec le bouton droit sur **Personnel**, pointez sur **Toutes les tâches**, puis cliquez sur **Demander un nouveau certificat**.
9. Sur la page Avant de commencer, cliquez sur Suivant, puis sur la page Sélectionner une politique d'inscription de certificats, cliquez sur Suivant.
10. Sur la page Demander des certificats, cliquez sur Certificat Web Adatum, puis cliquez sur De plus amples informations sont nécessaires pour s'inscrire à ce certificat. Cliquez ici pour configurer les paramètres.
11. Dans la boîte de dialogue **Propriétés du certificat**, dans l'onglet **Personne**, sous le **Nom de la personne**, en dessous de **Type**, sélectionnez **Nom commun**.
12. Dans la zone de texte **Valeur**, saisissez **131.107.0.10**, puis cliquez sur **Ajouter**.
13. Cliquez sur **OK**, sur **Inscrire**, puis cliquez sur **Terminer**.

14. Dans le composant logiciel enfichable **Certificats**, cliquez sur **Certificats,** puis dans le volet des **détails**, vérifier qu'un nouveau certificat avec le nom **131.107.0.10** est inscrit avec **Fins prévues** d'**Authentification du serveur**.
15. Fermer la fenêtre de console.
16. Lorsque vous êtes invité à enregistrer les paramètres, cliquez sur **Non**.

Changer les liaisons HTTPS

1. Sur EU-RTR, ouvrez le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire des services Internet (IIS).**
2. Dans la console Gestionnaire des services Internet (IIS), déroulez le menu EU-RTR (ADATUM\administrateur).
3. Dans Gestion des services Internet (IIS), dans l'arborescence de la console, déroulez Sites, puis cliquez sur Site web par défaut.
4. Dans le volet **Actions**, cliquez sur **Liaisons**, puis sur **Ajouter**.
5. Dans la boîte de dialogue **Ajouter des liaisons de site**, sous **Type** sélectionnez **https** et dans la liste **Certificat SSL**, cliquez sur le certificat**131.107.0.10**, cliquez sur **OK**, Puis cliquez sur **Fermer**.
6. Fermez la console du Gestionnaire des Services Internet (IIS).

Vérifier la configuration VPN par défaut

1. Sur EU-RTR, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Routage et accès à distance**.
2. Agrandissez la fenêtre **Routage et accès à distance**, cliquez avec le bouton droit sur **EU-RTR (local)**, puis sélectionnez **Désactiver le routage et l'accès à distance**.
3. Lorsque vous êtes invité, dans la boîte de dialogue **Routage et accès à distance**, cliquez sur **Oui**.
4. Cliquez avec le bouton droit sur **EU-RTR (local)**, puis sélectionnez **Configurer et activer le routage et l'accès à distance**.
5. Dans l'**Assistant de configuration d'accueil du routage et du serveur d'accès à distance**, cliquez sur **Suivant**.
6. Sur la page **Configuration**, sélectionnez **Configuration personnalisée**, puis cliquez sur **Suivant**.
7. Sur la page **Configuration personnalisée**, sélectionnez **Accès VPN** et **Routage LAN**, puis cliquez sur **Suivant**.
8. Sur la page **Fin de l'Assistant Installation d'un serveur Routage et accès distant**, cliquez sur **Terminer**.
9. Lorsque vous êtes invité, dans la boîte de dialogue **Routage et accès distant**, cliquez sur **Démarrer le service**.
10. Développez **EU-RTR (local)**, cliquez avec le bouton droit sur **Ports**, puis cliquez sur **Propriétés**.
11. Dans la boîte de dialogue **Propriétés** des **Ports**, vérifiez que cinq ports existent pour **Wan Miniport (SSTP)**, **Wan Miniport (IKEv2)**, **Wan Miniport (PPTP)** et **Wan Miniport (L2TP)**.
12. Double-cliquez sur **Miniport WAN (SSTP)**. Dans la zone de texte **Nombre maximum de ports**, saisissez **4**, puis cliquez sur **OK**.
13. Dans la boîte de message **Routage et accès distant**, cliquez sur **Oui**.
14. Répétez les étapes 12 et 13 pour IKEv2, PPTP et L2TP.
15. Pour fermer la boîte de dialogue **Propriétés des ports**, cliquez sur **OK**.

16. Cliquez avec le bouton droit sur **EU-RTR (local)**, puis cliquez sur **Propriétés**.
17. Dans la boîte de dialogue **Propriétés EU-RTR (locales)**, dans l'onglet **Général**, vérifiez que **Serveur d'accès distant IPv4** est sélectionné.
18. Cliquez sur l'onglet **Sécurité**, cliquez sur la flèche déroulante à côté de **Certificat**, puis sélectionnez **131.107.0.10**.
19. Cliquez sur **Méthodes d'authentification**, vérifiez que **EAP** est sélectionné comme protocole d'authentification, puis cliquez sur **OK**.
20. Cliquez sur l'onglet **IPv4** et vérifiez que le serveur VPN est configuré pour attribuer l'adresse IPv4 à l'aide du **Protocole DHCP**.
21. Pour fermer la boîte de dialogue **Propriétés EU-RTR (locales)**, cliquez sur **OK** et lorsque vous y êtes invité, cliquez sur **Oui**.

Configuration de stratégies d'un accès à distance

1. Sur EU-RTR, dans Gestionnaire de serveur, dans le menu **Outils**, cliquez sur **Serveur de stratégies réseau**.
2. Dans la console **Serveur de stratégies réseau**, dans le volet de navigation, développez les **Stratégies**, puis cliquez sur **Stratégies réseau**.
3. Dans le volet de **navigation**, cliquez avec le bouton droit sur **Stratégies réseau**, puis cliquez sur **Nouveau**.
4. Dans l'**Assistant Nouvelle stratégie réseau**, dans la zone de texte **Nom de la stratégie**, saisissez **VPN IT d'Adatum**.
5. Dans la liste déroulante **Type de serveur d'accès au réseau**, cliquez sur **Serveur d'accès distant (VPN-Dial up)**, puis cliquez sur **Suivant**.
6. Sur la page **Spécifier les conditions**, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Sélectionner une condition**, cliquez sur **Groupes de Windows**, puis cliquez sur **Ajouter**.
8. Dans la boîte de dialogue **Groupes de Windows**, cliquez sur **Ajouter des groupes**.
9. Dans la boîte de dialogue **Sélectionner un groupe**, dans la zone de texte **Saisir le nom de l'objet à sélectionner (exemples)**, saisissez **IT**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.
10. Cliquez à nouveau sur **OK**, puis sur **Suivant**.
11. Sur la page **Spécifier l'autorisation d'accès**, vérifiez qu'**Accès autorisé** est sélectionné, puis cliquez sur **Suivant**.
12. Sur la page **Configurer les méthodes d'authentification**, décochez la case **Authentification cryptée Microsoft (MS-CHAP)**.
13. Pour ajouter les **Types d'EAP**, cliquez sur **Ajouter**.
14. Sur la page **Ajouter l'EAP**, cliquez sur **Mot de passe sécurisé de Microsoft (EAP-MSCHAP v2)**, puis cliquez sur **OK**.
15. Pour ajouter les **Types d'EAP**, cliquez sur **Ajouter**.
16. Sur la page **Ajouter EAP**, cliquez sur **Microsoft : Carte à puce ou autre certificat**, cliquez sur **OK**, puis cliquez sur **Suivant**.
17. Sur la page **Configurer des contraintes**, cliquez sur **Suivant**.
18. Sur la page **Configurer des paramètres**, cliquez sur **Suivant**.

19. Sur la page **Fin de la configuration de la nouvelle stratégie réseau**, cliquez sur **Terminer**.
20. Fermer toutes les fenêtres actives.

Démonstration : Créer un profil de connexion

Procédure de démonstration

Installer CMAK

1. Au besoin, ouvrez une session sur l'ordinateur LON-CL1 en tant qu'**Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
2. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Programmes et fonctions**.
3. Dans la fenêtre **Programmes et fonctionnalités**, cliquez sur **Activer ou désactiver des fonctionnalités Windows**.
4. Dans la fenêtre **Fonctionnalités de Windows**, cochez **Kit d'administration du Gestionnaire des connexions RAS (CMAK)**, puis cliquez sur **OK**.
5. Cliquez sur **Fermer**.

Créer un profil de connexion

1. Cliquez avec le bouton droit sur **Démarrer**, puis sur **Panneau de configuration**.
2. Dans le **Panneau de configuration**, cliquez sur **Système et sécurité**, puis sur **Outils administratifs**.
3. Double-cliquez sur le **Kit d'administration du Gestionnaire des connexions**.
4. Sur la page **Bienvenue dans l'Assistant Kit d'administration du Gestionnaire des connexions**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le système d'exploitation cible**, cliquez sur **Windows Vista ou version ultérieure**, puis sur **Suivant**.
6. Sur la page **Créer ou modifier un profil Gestionnaire des connexions,** cliquez sur **Nouveau profil**, puis cliquez sur **Suivant**.
7. Sur la page **Spécifier les noms de service et de fichier**, dans la zone de texte **Nom du service**, saisissez **Adatum HQ**, dans la zone de texte **Nom de fichier**, saisissez **Adatum**, puis cliquez sur **Suivant**.
8. Sur la page **Spécifier un nom Realm**, cliquez sur **Ne pas ajouter de nom de domaine realm au nom d'utilisateur**, puis sur **Suivant**.
9. Sur la page **Fusionner des informations à partir d'autres profils**, cliquez sur **Suivant**.
10. Sur la page **Ajouter une prise en charge des connexions VPN**, sélectionnez **Annuaire téléphonique de ce profil**.
11. Dans la zone de texte **Nom de serveur VPN ou adresse IP**, saisissez **131.107.0.10**, puis cliquez sur **Suivant**.
12. Sur la page **Créer ou modifier une entrée VPN**, cliquez sur **Suivant**.
13. Sur la page **Ajouter un annuaire téléphonique personnalisé**, désactivez la case à cocher **Téléchargement automatique des mises à jour de l'annuaire téléphonique**, puis cliquez sur **Suivant**.
14. Sur la page **Configurer des entrées d'accès réseau à distance**, cliquez sur **Suivant**.
15. Sur la page **Spécifier des mises à jour de table de routage**, cliquez sur **Suivant**.

16. Sur la page **Configurer les paramètres proxy pour Internet Explorer**, cliquez sur **Suivant**.
17. Sur la page **Ajouter des actions personnalisées**, cliquez sur **Suivant**.
18. Sur la page **Afficher une image bitmap de connexion personnalisée**, cliquez sur **Suivant**.
19. Sur la page **Afficher une image bitmap d'annuaire téléphonique personnalisée**, cliquez sur **Suivant**.
20. Sur la page **Afficher des icônes personnalisées**, cliquez sur **Suivant**.
21. Sur la page **Inclure un fichier d'aide personnalisé**, cliquez sur **Suivant**.
22. Sur la page **Afficher des informations de support technique personnalisées**, cliquez sur **Suivant**.
23. Sur la page **Afficher un contrat de licence personnalisé**, cliquez sur **Suivant**.
24. Sur la page **Installer des fichiers supplémentaires avec le profil Gestionnaire des connexions**, cliquez sur **Suivant**.
25. Sur la page **Générer le profil Gestionnaire des connexions et son programme d'installation**, cliquez sur **Suivant**.
26. Sur la page **Votre profil Gestionnaire des connexions est terminé et prêt à être distribué**, cliquez sur **Terminer**.

Examiner le profil créé

1. Sur le **bureau**, dans la **barre des tâches**, cliquez sur l'icône **Explorateur de fichiers**.
2. Dans l'**Explorateur de fichiers**, développez **Ce PC**, **Disque local (C:)**, **Fichiers de programme**, **CMAK**, **Profils**, **Windows Vista et versions supérieures**, puis cliquez sur **Adatum**.
3. Dans le volet **détails**, examinez les dossiers affichés. Ce sont les fichiers que vous devez distribuer.
4. Fermer toutes les fenêtres actives.

Contrôle des acquis et éléments à retenir

Bonnes Pratiques

- Nous vous recommandons de ne pas utiliser PPTP pour l'accès à distance et les connexions VPN de site à site, car il est considéré comme non garanti. Vous devez utiliser L2TP, IKEv2 ou SSTP à la place. Si vous devez utiliser PPTP en raison de problèmes de capacité, vous devez l'utiliser avec MS- CHAP v2 et PEAP, à cause d'une faille de sécurité dans PPTP.
- Vous pouvez surveiller l'environnement du VPN en utilisant Windows PowerShell et la gestion de l'accès à distance.
- Vous devez utiliser DHCP pour attribuer des adresses IP à vos clients VPN, sauf si vous avez moins de 20 clients.
- Vous ne devez pas activer CHAP, SPAP ou les protocoles d'authentification PAP, car ils ne sont pas sécurisés.
- Vous pouvez limiter les connexions à votre serveur VPN par nom d'utilisateur ou adresse IP.

Questions de contrôle des acquis

Question : Quelles solutions d'accès à distance pouvez-vous déployer à l'aide de Windows Server 2016 ?

Réponse : Dans Windows Server 2016, vous pouvez déployer les solutions d'accès à distance suivantes : DirectAccess, VPN, routage et proxy d'applications web.

Question : Quel type de solutions d'accès à distance pouvez-vous fournir en utilisant le VPN dans Windows Server 2016 ?

Réponse : Vous pouvez configurer les solutions d'accès à distance suivantes en utilisant le VPN dans Windows Server 2016 :

- Accès distant sécurisé aux ressources réseau internes pour les utilisateurs situés sur Internet. Les utilisateurs se connectent à un serveur VPN exécutant Windows Server 2016.
- Communication sécurisée entre les ressources réseau qui se trouvent à des emplacements ou sur des sites géographiques différents. Cette solution est le *VPN site à site*. Dans chaque site, un serveur VPN qui exécute Windows Server 2016 chiffre la communication entre les sites.

Outils

Outil	Utilisation	Emplacement
Console de gestion d'accès à distance	Gestion de DirectAccess et du VPN	Gestionnaire de serveur/Outils
Console de routage et d'accès à distance	Gestion du VPN et du routage	Gestionnaire de serveur/Outils
Dnscmd.exe	Outil de ligne de commande pour la gestion du DNS	Exécuter à partir de ligne de commande
Services.msc	Aide à la gestion des services Windows.	Gestionnaire de serveur/Outils
Gpedit.msc	Aide à l'édition de stratégie de groupe locale.	Exécuter à partir de ligne de commande
IPconfig.exe	Outil en ligne de commande	Exécuter à partir de ligne de

Outil	Utilisation	Emplacement
	qui affiche la configuration actuelle du réseau TCP/IP.	commande
Console du gestionnaire DNS	Aide à la configuration de la résolution de noms.	Gestionnaire de serveur/Outils
Mmc.exe	Créer une MMC personnalisée pour la gestion du système d'exploitation des rôles, des fonctions et des paramètres.	Exécuter à partir de ligne de commande
gpupdate.exe	Aide à la gestion de l'application des stratégies de groupe.	Exécuter à partir de ligne de commande
Utilisateurs et ordinateurs Active Directory	Aider à configurer l'appartenance de groupe pour les ordinateurs clients que vous allez configurer avec DirectAccess	Gestionnaire de serveur/Outils

Questions et réponses sur les laboratoires

Atelier pratique : Implémentation de VPN

Questions et réponses

Question : Dans le laboratoire, vous avez configuré le serveur VPN pour attribuer des adresses IPv4 en utilisant le Protocole de configuration de l'hôte dynamique (DHCP). Existe-t-il d'autres options pour attribuer des adresses IPv4 aux clients ?

Réponse : Oui, vous pouvez utiliser un pool d'adresses statiques en spécifiant une plage d'adresses IPv4. Toutefois, n'oubliez pas d'exclure ces dernières dans DHCP.

Question : Dans la tâche 3 de l'exercice 1, vous avez configuré une stratégie réseau qui a permis aux membres du groupe informatique de se connecter au serveur du VPN d'A. Datum. Êtes-vous capable de vous connecter si vous n'avez pas créé cette stratégie ?

Réponse : Si vous n'aviez pas créé la stratégie réseau pour le groupe informatique, personne n'aurait pu se connecter. Deux stratégies par défaut existent et les deux refusent l'accès. Si aucune stratégie n'existe sur le serveur de stratégie réseau, personne ne peut se connecter au serveur VPN.

Question : Dans l'exercice de dépannage, vous avez importé le certificat racine AdatumCA manuellement dans le magasin de certificats Autorité de certification racine approuvée sur LON-CL1. Est-il possible d'automatiser ce processus ?

Réponse : Si l'ordinateur est membre d'un domaine, vous pouvez utiliser la stratégie de groupe pour distribuer des certificats racines. Si l'ordinateur est membre d'un groupe de travail, vous pouvez utiliser un script ou renvoyer les utilisateurs vers un site Web à partir duquel ils peuvent télécharger le certificat racine.

Module 9

Mise en oeuvre de la gestion réseau pour les succursales

Contenu :

Leçon 1

Fonctionnalités et considérations de la gestion réseau des succursales

Contenu :

Questions et réponses

Question : Discutez des différents facteurs qui peuvent déterminer la configuration appropriée pour une succursale.

Réponse :

- Sécurité. L'hébergement de services au sein d'une succursale peut introduire des risques de sécurité potentiels.
- Disponibilité et fiabilité des données. La qualité d'une liaison WAN entre la succursale et le siège ou le centre de données est généralement le facteur le plus important susceptible d' affecter la disponibilité et la fiabilité.
- Rendement et capacité. Le facteur déterminant pour l'emplacement d'un service ou d'une application peut être simplement constitué des exigences en matière de performances et de capacités.
- Les exigences légales et réglementaires. En fonction des affiliations géographiques et industrielles de votre organisation, des restrictions légales ou des exigences relatives à la conformité aux règlements peuvent avoir une incidence sur l'emplacement des services.
- Organisation informatique. Les ressources informatiques nécessaires pour gérer l' infrastructure locale au sein des sièges et des succursales sont souvent différentes.
- Considérations commerciales. La structure de propriété d'une organisation peut affecter le placement d'un service.
- Coût. La centralisation de l'infrastructure de serveur se traduit généralement par des économies plus importantes.

Scénarios pour les succursales

Question : Ces scénarios de succursales s'appliquent-ils à votre organisation ? Votre organisation fait-elle l'expérience d'autres scénarios liés au succursales ?

Réponse : Les réponses varient. Cette question est destinée à encourager la discussion sur les scénarios de succursale réels. Demandez aux stagiaires de décrire les scénarios de leurs filiales et d'identifier les problèmes rencontrés lors de la livraison d'applications et de la prestation de services à ces filiales.

Leçon 2

Implémentation de DFS dans les succursales.

Contenu :

Questions et réponses

Question : Quels types d'espaces de noms DFS peuvent être déployés dans une organisation ? Quel type est le mieux adapté à votre organisation ?

> **Réponse :** Vous pouvez créer un espace de noms de domaine ou un espace de noms autonome. Chaque stagiaire peut faire un choix différent selon l'infrastructure et les exigences de l'entreprise.

Question : Quels scénarios peuvent être traités avec des fonctionnalités DFS dans Windows Server 2016 ?

> **Réponse :** DFS peut être mis en œuvre pour accroître l'efficacité de différents scénarios d'utilisation de fichiers réseau dans les succursales :
>
> - Partage de fichiers sur toutes les succursales
> - Collecte des données des succursales
> - Distribution des données aux succursales

Scénarios de mise en œuvre DFS

Question : Pourquoi devriez-vous éviter d'utiliser DFS pour répliquer des bases de données de volume élevé basées sur des transactions ?

> **Réponse :** Les bases de données contenant un grand volume d'opérations laissent plusieurs fichiers de base de données ouverts afin de traiter ces dernières. DFS ne peut pas répliquer les fichiers s'ils sont maintenus ouverts par une application. Si vous utilisez DFS pour répliquer une base de données d'opérations en masse, les copies répliquées de la base de données ne seront donc pas conformes aux données.

Planification pour DFS

Question : Vous devez utiliser DFS pour vous assurer qu'un partage de fichier hébergé sur un serveur de fichiers utilisant Windows Server 2016 soit répliqué sur un autre serveur de fichiers utilisant Windows Server 2016 dans une succursale. Le partage de fichiers contient plusieurs fichiers virtuels de disque dur qui contiennent des versions légèrement différentes de la même image du système d'exploitation de base. La déduplication des données est-elle efficace dans cette situation ?

> **Réponse :** La déduplication des données fonctionne parfaitement avec les données en cours de réplication. Toutefois, si votre organisation compte encore des serveurs Windows Server 2008 R2, vous ne pouvez pas utiliser la déduplication des données dans ce scénario, car elle n'est pas disponible dans Windows Server 2008 R2.

Démonstration : Configuration des espaces de noms DFS et de la réplication

Procédure de démonstration

Installation du service de rôle de réplication DFS

1. Sur LON-SVR1, cliquez sur **Démarrer**, puis sur **Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, développez **Services de fichiers et de stockage (installés)**, **Services de fichiers et iSCSI**, puis activez la case à cocher **Espaces de noms DFS**.

7. Dans la fenêtre contextuelle **Ajouter des rôles et des fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**.
8. Activez la case à cocher **Réplication DFS**, puis cliquez sur **Suivant**.
9. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
10. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. Une fois l'installation terminée, cliquez sur **Fermer**.
12. Répétez les étapes 1 à 11 pour **TOR-SVR1**.

Création d'un espace de noms

1. Basculez vers LON-SVR1.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur Gestion **DFS**.
3. Dans la console **Gestion DFS**, cliquez sur **Espaces de noms**.
4. Cliquez avec le bouton droit sur **Espaces de noms**, puis cliquez sur **Nouvel espace de noms**.
5. Dans l'**Assistant nouvel espace de noms**, sur la page **Serveur d'espace de noms**, dans la section **Serveur**, tapez **LON-SVR1**, puis cliquez sur **Suivant**.
6. Sur la page **Nom d'espace de noms et Réglages**, dans la zone de texte **Nom**, tapez **Recherche**, puis cliquez sur **Suivant**.
7. Sur la page **Type d'espace de noms**, assurez-vous que **Espace de noms de domaine** et **Activer mode Windows Server 2008** soient sélectionnés, puis cliquez sur **Suivant**.
8. Sur la page **Vérifier réglages et Créer Espace de noms**, cliquez sur **Créer**.
9. Sur la page **Confirmation**, vérifiez que la tâche de création d'espace de noms est effectuée, puis cliquez sur **Fermer**.
10. Dans la console, développez le nœud **Espaces de noms**, puis cliquez sur **\\Adatum.com\Research**. Vérifiez les quatre onglets du panneau **détails**.
11. Dans la console, cliquez avec le bouton droit sur **\\Adatum.com\Research**, puis cliquez sur **Propriétés**. Passez en revue les options des onglets **Général**, **Parrainages** et **Avancé**.
12. Pour fermer la boîte de dialogue **\\Adatum.com\Research**, cliquez sur **OK**.

Créer un nouveau dossier et une cible de dossier

1. Dans la console **Gestion 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 de texte **Nom**, entrez **Propositions**.
3. Dans la boîte de dialogue **Nouveau dossier**, dans la section **Cibles de dossier**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Ajouter une cible de dossier**, entrez **\\LON-SVR1\Proposal_docs**, puis cliquez sur **OK**.
5. Pour créer le dossier partagé, dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
6. Dans la boîte de dialogue **Créer un partage**, fournissez les détails suivants, puis cliquez sur **OK** :
   - Chemin d'accès local du dossier partagé : **C:\Proposal_docs**
   - Autorisations de dossier partagé : **Les administrateurs ont un accès complet ; les autres utilisateurs disposent d'autorisations d'écriture et de lecture**
7. Pour créer le dossier, dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.

8. Pour fermer la boîte de dialogue **Nouveau dossier**, cliquez sur **OK**.
9. Dans la console, développez **\\Adatum.com\Research**, puis cliquez sur **Propositions**.

   Notez que pour le moment il n'y a qu'une seule cible de dossier**.** Pour assurer la redondance, une seconde cible de dossier peut être ajoutée avec **Réplication DFS** configurée.
10. Pour tester l'espace de noms, ouvrez l'**Explorateur de fichiers**, dans la barre d'adresses, entrez **\\Adatum.com\Research**, puis appuyez sur Entrée.

    Le dossier **Propositions** apparaît.

Créer une nouvelle cible de dossier pour la réplication

1. Dans la console **Gestion DFS**, cliquez avec le bouton droit sur le dossier **Propositions**, puis cliquez sur **Ajouter une cible de dossier**.
2. Dans la boîte de dialogue **Nouvelle cible de dossier**, sous **Chemin vers le dossier cible**, entrez **\\TOR-SVR1\Proposal_docs**, puis cliquez sur **OK**.
3. Pour créer le dossier partagé, dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
4. Dans la boîte de dialogue **Créer un partage**, dans la boîte **Chemin d'accès local du dossier partagé**, entrez **C:\Proposal_docs**.
5. Dans la boîte **Autorisations du dossier partagé**, cochez la case **Les administrateurs ont un accès complet ; les autres utilisateurs ont des autorisations d'écriture et de lecture**, puis cliquez sur **OK**.
6. Pour créer le dossier, dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.
7. Dans la boîte de dialogue **Réplication**, cliquez sur **Oui** pour créer un groupe de réplication. Démarrage de l'**Assistant de réplication de dossier**.

Création d'un nouveau groupe de réplication

1. Dans la console **Gestion DFS**, dans **Assistant de réplication de dossier**, sur la page **Groupe de réplication et Nom du dossier répliqué**, acceptez les paramètres par défaut, puis cliquez sur **Suivant**.
2. Sur la page **Éligibilité de réplication**, notez que LON-SVR1 et TOR-SVR1 sont tous deux éligibles en tant que membres de Réplication DFS, puis cliquez sur **Suivant**.
3. Sur la page **Membre principal**, sélectionnez **LON-SVR1** comme membre principal, puis cliquez sur **Suivant**.
4. Sur la page **Sélection Topologie**, laissez la sélection par défaut de **Maillage complet** qui reproduit toutes les données entre tous les membres du groupe de réplication.

   Si vous au minimum trois membres au sein du groupe de réplication, vous pouvez également choisir **Hub and spoke**, ce qui vous permet de configurer un scénario de publication dans lequel les données sont répliquées à partir d'un concentrateur commun vers le reste des membres. Vous pouvez également choisir **Aucune topologie**, ce qui vous permet de configurer la topologie ultérieurement.
5. Après avoir passé en revue toutes les sélections, cliquez sur **Suivant**.
6. Sur la page **Groupe de réplication Horaire et bande passante**, laissez la sélection par défaut **Répliquer en continu en utilisant la bande passante spécifiée**, puis configurez le paramètre pour utiliser **Bande passante complète**. Notez que vous pouvez également choisir une planification spécifique pour la réplication durant des jours et des heures précises. Cliquez sur **Suivant**.
7. Sur la page **Vérifier réglages et Créer groupe de réplication**, cliquez sur **Créer**.
8. Sur la page **Confirmation**, assurez-vous que toutes les tâches soient appliquées, puis cliquez sur **Fermer**. Prenez note de l'avertissement du **Délai de réplication**, puis cliquez sur **OK**.
9. Dans la console, développez **Réplication**.
10. Sous **Réplication**, cliquez sur **Adatum.com\research\proposals**. Cliquez et passez en revue chacun des onglets du volet détails.

Leçon 3

Implémentation de BranchCache dans les succursales

Contenu :

Questions et réponses

Question : Quels modes pouvez-vous configurer pour BranchCache ?

Réponse : Vous pouvez configurer BranchCache pour utiliser le mode de cache hébergé ou le mode de cache distribué.

Question : Quels types de serveurs utilisant BranchCache sont des serveurs de contenu BranchCache ?

Réponse : Il existe trois types de serveurs qui peuvent agir en tant que serveurs de contenu BranchCache :

- Serveurs Web
- Serveurs de fichiers
- Serveurs d'applications

Démonstration : Configuration de la fonctionnalité BranchCache

Procédure de démonstration

Ajout de BranchCache au service de rôle des fichiers réseau

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

Activer BranchCache pour le serveur

1. Sur LON-DC1, cliquez sur l'écran Démarrer.
2. Sur l'écran d'accueil, saisissez **gpedit.msc**, puis appuyez sur Entrée.
3. Développez **Configuration de l'ordinateur**, **Modèles d'administration**, **Réseau**, cliquez ensuite 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 boîte **Options**, sous **Actions de publication de hachages**, sélectionnez **Autoriser la publication de hachages uniquement pour les dossiers partagés dans lesquels BranchCache est activé**, puis cliquez sur **OK**.
6. Fermez l'Éditeur de stratégie de groupe locale.

Activer BranchCache pour un partage de fichiers

1. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
2. Dans la fenêtre de l'Explorateur de fichiers, cliquez sur **Disque local (C:)**.

3. Dans la **Barre d'outils Accès rapide** située sur le côté supérieur gauche de la fenêtre, cliquez sur **Nouveau dossier**, entrez **Partager**, puis appuyez sur Entrée.
4. Cliquez avec le bouton droit sur **Partager**, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés de partage**, cliquez sur l'onglet **Partage**, puis sur **Partage avancé**.
6. Dans la boîte de dialogue **Partage avancé**, cliquez sur **Partager ce dossier**, puis cliquez sur **Mise en cache**.
7. Dans la boîte de dialogue **Paramètres hors ligne**, sélectionnez 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.

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : Qu'est-ce qui fait de DFSR une plateforme de réplication plus efficace que le service de réplication de fichier (FRS) ?

Réponse : DFSR utilise une heuristique delta avancée, qui réplique uniquement le parties modifiées du système de fichiers, alors que le service de réplication de fichiers (FRS) réplique toujours le fichier complet. DFSR utilise également RDC pour réduire le trafic réseau basé sur la réplication.

Question : En quoi BranchCache diffère du DFS ?

Réponse : BranchCache met uniquement en cache les fichiers auxquels les utilisateurs d'un site distant ont accédé. DFS réplique les fichiers entre le siège social et un site distant de manière que tous les fichiers existent aux deux emplacements.

Question : Pourquoi voudriez-vous mettre en œuvre BranchCache en mode de cache hébergé au lieu du mode de cache distribué ?

Réponse : Lorsque vous utilisez le mode de cache distribué, le cache est distribué sur tous les ordinateurs exécutant Windows 8 ou un système d'exploitation plus récent. Toutefois, il se peut que es ordinateurs ou ordinateurs portables soient éteints ou retirés du bureau. Autrement dit, il est possible qu'un fichier mis en cache ne soit pas disponible, ce qui contraint le système à télécharger à nouveau le fichier sur la liaison réseau étendu. Cependant, si le mode de cache hébergé est utilisé, l'ordinateur exécutant Windows Server 2016 qui héberge le cache rend les fichiers mis en cache disponibles, même si les ordinateurs clients sont éteints ou retirés du bureau.

Questions et réponses de contrôle des acquis sur les ateliers pratiques

Atelier pratique B : Implémentation de BranchCache

Questions et réponses

Question : Dans cet atelier pratique, vous avez déplacé SYD-SVR1 vers sa propre unité d'organisation. Pourquoi ?

Réponse : Les paramètres de configuration des clients ont été configurés dans la stratégie de domaine par défaut, qui est liée à la racine du domaine. Ces paramètres de stratégie de groupe empêchent le mode de cache hébergé d'être configuré sur SYD-SVR1. En déplaçant SYD-SVR1 vers sa propre unité d'organisation, vous pouvez bloquer l'héritage de la stratégie de groupe pour cette unité d'organisation et empêcher l'application de ces paramètres à SYD-SVR1.

Question : Quand envisagez-vous de mettre en place BranchCache au sein de votre organisation ?

Réponse : Les réponses varient, mais BranchCache n'est important que dans le cas d'une succursale ou d'un site connecté au siège de votre organisation par une liaison à faible bande passante.

Module 10

Configuration des fonctionnalités réseau avancées

Contenu :

Leçon 1

Présentation des fonctionnalités de mise en réseau de haute performance

Contenu :

Questions et réponses

Classer une activité

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

Éléments	
1	Cela vous permet de regrouper jusqu'à 32 cartes réseau, puis de les utiliser comme une seule interface réseau.
2	Ceci est un ensemble de technologies qui vous permettent de répondre aux exigences de service de la charge de travail.
3	Vous pouvez configurer cela depuis le Gestionnaire de périphériques ou depuis Windows PowerShell.
4	Cette configuration peut être déployée avec une seule carte réseau, mais ne propose pas de tolérance de pannes.
5	Cela peut vous aider à mettre en œuvre la gestion de la bande passante.
6	Pour cela, vous pouvez attribuer plusieurs cœurs à un ordinateur virtuel grâce au réseau de pointe.
7	Pour l'utiliser, l'hôte doit avoir au moins deux commutateurs virtuels externes.
8	Vous pouvez l'utiliser pour prioriser le trafic de diffusion de la voix ou de la vidéo par exemple.
9	Pour l'utiliser, vous devez configurer un ordinateur virtuel pour utiliser plusieurs cœurs de processeur.

Catégorie 1		Catégorie 2		Catégorie 3
Association de cartes réseau		QoS		RSS

Réponse :

Catégorie 1		Catégorie 2		Catégorie 3
Association de cartes réseau		QoS		RSS
Cela vous permet de regrouper jusqu'à 32 cartes réseau, puis de les utiliser comme une seule interface réseau. Cette configuration peut être déployée avec une seule carte réseau, mais ne propose pas de tolérance de pannes. Pour l'utiliser, l'hôte doit avoir au moins deux commutateurs virtuels externes.		Ceci est un ensemble de technologies qui vous permettent de répondre aux exigences de service de la charge de travail. Cela peut vous aider à mettre en œuvre la gestion de la bande passante. Vous pouvez l'utiliser pour prioriser le trafic de diffusion de la voix ou de la vidéo par exemple.		Vous pouvez configurer cela depuis le Gestionnaire de périphériques ou depuis Windows PowerShell. Pour cela, vous pouvez attribuer plusieurs cœurs à un ordinateur virtuel grâce au réseau de pointe. Pour l'utiliser, vous devez configurer un ordinateur virtuel pour utiliser plusieurs cœurs de processeur.

Ressources

Mise en œuvre des dossiers partagés SMB 3.1.1

Lectures supplémentaires :
Pour plus d'informations, reportez-vous à Présentation des blocs de message serveur : http://aka.ms/obyww0

Qu'est-ce que RSC ?

Lectures supplémentaires : Pour plus d'informations sur les applets de commande Windows PowerShell précédentes, reportez-vous à « Applets de commande Adaptateur réseau dans Windows PowerShell » à l'adresse suivante : http://aka.ms/D40x84

Démonstration : Mise en œuvre de l'association de cartes réseau

Procédure de démonstration

1. Sur LON-HOST1, ouvrez le Gestionnaire de serveur puis, dans le menu **Outils**, cliquez sur **Gestionnaire Hyper-V.**
2. Si le Gestionnaire de serveur ne démarre pas, cliquez sur **Démarrer**, puis sur l'icône **Gestionnaire de serveur** pour démarrer le Gestionnaire de serveur.
3. Dans l'arborescence de la console **Gestionnaire de serveur**, cliquez sur le nœud **Serveur local**.
4. Dans le volet **Détails des propriétés**, en regard de l'option**Association de cartes réseau**, cliquez sur le lien hypertexte **Désactivé**.
5. Dans la boîte de dialogue **Association de cartes réseau**, dans le volet **Cartes et interfaces**, cliquez sur **Ethernet 2**, puis dans la liste **Tâches**, sélectionnez **Ajouter à la nouvelle association**.
6. Dans la boîte de dialogue **Ajouter à la nouvelle association**, dans la zone **Nom de l'association**, saisissez **Association de cartes réseau hôtes**, puis cliquez sur **OK**.

7. Dans la boîte de dialogue **Association de cartes réseau**, dans le volet **Associations**, notez les détails suivants :
   a. Équipe : **Hôte de l'association de cartes réseau**
   b. État : **OK**
   c. Mode d'association : **Commutation autonome**
   d. Équilibrage de charge : **Dynamique**
   e. Adaptateurs : **1**

Remarque : Expliquez que, comme indiqué précédemment, vous avez créé une association de cartes réseau avec une seule carte. Cette dernière ne prend pas en charge la tolérance de pannes, mais permet la séparation du trafic réseau lorsque vous utilisez également des VLAN.

Leçon 2

Configuration des fonctionnalités avancées de réseau Hyper-V

Contenu :

Questions et réponses

Question : Qu'est-ce que « l'effet ping-pong » ?

( ) L'effet ping-pong se produit lorsque plusieurs cartes réseau physiques de l'hôte sont adaptées à plusieurs cartes réseau virtuelles. Elles échangent en permanence des adresses physiques.

( ) L'effet ping-pong se produit lorsqu'une extension de commutateur virtuel applique la transmission réseau. Il contourne le renvoi par défaut, ce qui provoque une boucle des paquets réseau vers le routeur.

( ) L'effet ping-pong résulte d'une situation rare qui peut se produire dans un VMQ dynamique lorsqu'un cœur d'UC est utilisé et que le traitement arrive à générer une quantité importante de trafic entrant. À cause de cela, un autre cœur de processeur, moins occupé, est sélectionné de façon dynamique et, la charge de trafic n'ayant pas changé, le trafic revient au cœur du processeur d'origine ou à un autre cœur de processeur. Ce processus se poursuit.

( ) Lorsque vous utilisez l'accès direct à la mémoire à distance (RDMA), une carte réseau peut permuter à plusieurs reprises entre l'association intégrée au commutateur (SET) et la fonctionnalité RDMA.

( ) L'effet ping-pong se produit lorsqu'une association de cartes réseau permute à plusieurs reprises entre des cartes membres de l'association.

Réponse :

( ) L'effet ping-pong se produit lorsque plusieurs cartes réseau physiques de l'hôte sont adaptées à plusieurs cartes réseau virtuelles. Elles échangent en permanence des adresses physiques.

( ) L'effet ping-pong se produit lorsqu'une extension de commutateur virtuel applique la transmission réseau. Il contourne le renvoi par défaut, ce qui provoque une boucle des paquets réseau vers le routeur.

(√) L'effet ping-pong résulte d'une situation rare qui peut se produire dans un VMQ dynamique lorsqu'un cœur d'UC est utilisé et que le traitement arrive à générer une quantité importante de trafic entrant. À cause de cela, un autre cœur de processeur, moins occupé, est sélectionné de façon dynamique et, la charge de trafic n'ayant pas changé, le trafic revient au cœur de processeur d'origine ou à un autre cœur de processeur. Ce processus se poursuit.

( ) Lorsque vous utilisez l'accès direct à la mémoire à distance (RDMA), une carte réseau peut permuter à plusieurs reprises entre l'association intégrée au commutateur (SET) et la fonctionnalité RDMA.

( ) L'effet ping-pong se produit lorsqu'une association de cartes réseau permute à plusieurs reprises entre des cartes membres de l'association.

Démonstration : Configuration des fonctionnalités avancées de la carte réseau

Procédure de démonstration

Utiliser Windows PowerShell pour activer la protection DHCP

1. Assurez-vous d'avoir effectué les étapes de préparation.
2. Sur **LON-CL1**, dans la zone de notification de la barre des tâches, cliquez avec le bouton droit sur l'icône **Réseau**, puis cliquez sur **Ouvrir le centre de réseau et partage**.
3. Dans la fenêtre **Centre Réseau et partage**, cliquez sur le lien hypertexte **Ethernet**.
4. Dans la fenêtre **Statut Ethernet**, cliquez sur **Détails**. Notez qu'il possède à présent l'**adresse IP de serveur DHCP 172.16.0.10** (**LON-DC1**).

5. Sur **LON-HOST1**, cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
6. Dans l'invite Windows PowerShell, saisissez les commandes suivantes pour empêcher **LON-DC1** d'émettre un bail DHCP, puis appuyez sur Entrée après chaque ligne :

```
Set-VMNetworkAdapter -VMName 22741A-LON-DC1-B -DhcpGuard Sur
Set-VMNetworkAdapter -VMName 22741A-LON-SVR1-B -DhcpGuard Off
```

7. Sur **LON-CL1**, cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Invite de commandes (Admin)**.
8. Dans la fenêtre **Invite de commandes**, tapez les commandes ci-dessous et appuyez sur Entrée après chacune :

```
Ipconfig/release
Ipconfig/renew
```

9. Dans la zone de notification de la barre des tâches, cliquez avec le bouton droit sur l'icône **Réseau**, puis cliquez sur **Ouvrir le centre de réseau et partage**.
10. Dans la fenêtre **Centre Réseau et partage**, cliquez sur le lien hypertexte **Ethernet**.
11. Dans la fenêtre **Statut Ethernet**, cliquez sur **Détails**. Notez qu'il possède à présent l'**adresse IP de serveur DHCP** de **LON-SVR1**.

Désactiver la protection DHCP (pour que l'atelier pratique suivant puisse fonctionner correctement)

- Sur l'ordinateur hôte physique, dans l'invite Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
Set-VMNetworkAdapter -VMName 22741A-LON-DC1-B -DhcpGuard Off
```

Rétablir les ordinateurs virtuels

Une fois l'atelier pratique terminé, rétablir l'état initial des ordinateurs virtuels.

1. Sur l'ordinateur hôte, démarrez le Gestionnaire Hyper-V.
2. Dans la liste **Ordinateurs virtuels**, cliquez avec le bouton -droit sur **22741A-LON-DC1-B**, puis cliquez sur **Rétablir**.
3. Dans la boîte de dialogue **Rétablir l'ordinateur virtuel**, cliquez sur **Rétablir**.
4. Répétez les étapes 2 et 3 pour **22741A-LON-SVR1-B** et **22741A-LON-CL1-B**.

Révision du module et Takeaways

Bonnes Pratiques

Lors de la mise en œuvre de caractéristiques avancées de réseau pour Hyper-V, utilisez les meilleures pratiques suivantes :

- Déployer plusieurs cartes réseau sur un hôte physique Hyper-V avant de configurer ces cartes en association. Cela permet d'assurer la conservation de la connectivité réseau si les adaptateurs réseau individuels ne fonctionnent pas. Configurer plusieurs associations avec des cartes réseau connectées à différents commutateurs, pour vous assurer que la connectivité perdure en cas de défaillance matérielle d'un commutateur.
- Utiliser la gestion de bande passante pour configurer une attribution de bande passante minimum et maximum par carte réseau virtuelle. Vous devez configurer l'allocation de bande passante pour garantir à chaque ordinateur virtuel une allocation de bande passante minimale. Cela aide à s'assurer que, si un autre ordinateur virtuel physiquement hébergé sur le même serveur Hyper-V connaît un pic de trafic, d'autres ordinateurs virtuels seront en mesure de communiquer normalement avec le réseau.
- Approvisionner à un hôte physique Hyper-V une carte réseau qui prend en charge VMQ. VMQ utilise le filtrage de paquets de matériel pour acheminer le trafic réseau directement à un ordinateur virtuel. Cela contribue à l'amélioration des performances, puisque le paquet n'a pas à être copié depuis le système d'exploitation de l'hôte physique vers l'ordinateur virtuel. Quand les ordinateurs virtuels ne sont pas configurés pour prendre en charge VMQ, le système d'exploitation de l'hôte physique peut se transformer en goulet d'étranglement lors du traitement de grandes quantités de trafic réseau.
- Si vous hébergez physiquement un grand nombre d'ordinateurs virtuels et que vous devez les isoler, il est recommandé d'utiliser la virtualisation de réseau plutôt que les VLAN. La virtualisation de réseau est compliquée à configurer, mais elle présente un avantage sur les VLAN, en ce qu'il n'est pas nécessaire de configurer les VLAN sur tous les commutateurs connectés à l'hôte physique Hyper-V. Vous pouvez effectuer toutes les configurations nécessaires lorsque vous avez besoin d'isoler les serveurs sur un hôte physique Hyper-V sans avoir besoin d'impliquer l'équipe réseau.

Question de contrôle des acquis

Question : Vous souhaitez déployer un disque dur virtuel d'ordinateur virtuel Windows Server 2016 Hyper-V sur un fichier partagé. Quel système d'exploitation le serveur de fichier doit-il exécuter pour supporter cette configuration ?

> **Réponse :** Vous pouvez déployer des disques durs virtuels uniquement sur des partages de fichiers utilisant au minimum SMB 3.0. Par ailleurs, seuls les systèmes d'exploitation Windows Server 2012 et Windows Server 2016 prennent en charge l'hébergement physique de partages de fichiers SMB 3.0 et SMB 3.1.1.

Questions et réponses sur les ateliers pratiques

Atelier pratique : Configuration des fonctionnalités avancées de réseau Hyper-V

Questions et réponses

Question : Dans la tâche « Association de cartes réseau », vous avez créé **Équipe LON-SVR1 NIC** sur la carte réseau Ethernet 2. Est-ce doté d'une tolérance de pannes ?

Réponse : Non. Même si vous pouvez créer une association de cartes réseau avec une seule carte réseau, cela vous permet d'assurer l'isolement du réseau, mais pas la tolérance de pannes.

Question : Dans la tâche nommée « Création de cartes réseau virtuelles dans la partition parente », vous avez dû arrêter l'ordinateur virtuel **LON-SVR1**. Pourquoi ?

Réponse : Vous étiez en train d'ajouter du matériel, plus particulièrement une carte réseau. Cette action ne peut pas être effectuée si un ordinateur virtuel est en cours d'exécution.

Module 11

Implémentation de la mise en réseau SDN (Software Defined Networking)

Contenu :

Leçon 1

Présentation de la mise en réseau SDN (Software Defined Networking)

Contenu :

Questions et réponses

Question : Dans une mise en réseau SDN (Software Defined Networking), chaque ordinateur hôte physique doit se voir assigner au moins une adresse IP depuis le réseau logique de gestion. Vous pouvez utiliser DHCP pour cette affectation.

( ) Vrai

( ) Faux

Réponse :

(√) Vrai

( ) Faux

Commentaire :

Dans une mise en réseau SDN (Software Defined Networking), chaque ordinateur hôte physique doit se voir assigner au moins une adresse IP depuis le réseau logique de gestion. Vous pouvez utiliser DHCP pour cette affectation.

Question : La complexité de l'infrastructure réseau de votre organisation nécessite-t-elle une mise en réseau SDN (Software Defined Networking) ?

Réponse : Les réponses varient en fonction de l'expérience des stagiaires et de l'infrastructure réseau de leur organisation.

Leçon 2

Implémentation de la virtualisation du réseau

Contenu :

Questions et réponses

Question : L'adresse client (AC) d'un ordinateur virtuel change-t-elle lorsque vous déplacez l'ordinateur virtuel entre les hôtes Hyper-V ?

> **Réponse :** Lorsque vous déplacez un ordinateur virtuel, son adresse client (AC) demeure la même. Seule son adresse fournisseur (AF), qui correspond à celle de l'hôte Hyper-V sur lequel il est exécuté, change. Vous devez mettre à jour la configuration de la virtualisation réseau sur les hôtes Hyper-V afin qu'ils soient informés du déplacement.

Question : Pourquoi les stratégies de virtualisation de réseau sont-elles nécessaires lors de l'utilisation de la virtualisation réseau ?

> **Réponse :** Les stratégies de virtualisation réseau définissent l'hôte Hyper-V sur lequel les ordinateurs virtuels sont exécutés. Hyper-V consulte les stratégies de virtualisation réseau lorsqu'il a besoin de former un paquet encapsulé NVGRE et de l'envoyer sur un réseau physique.

Leçon 3

Implémentation du Contrôleur du réseau

Contenu :

Questions et réponses

Question : Pour quelles raisons le Contrôleur de réseau utilise-t-il les API Northbound et Southbound ?

Réponse : Le contrôleur de réseau utilise l'API Sud pour communiquer avec les périphériques réseau, les services et les composants. Avec l'API Sud, le contrôleur de réseau peut :

- Découvrir les périphériques réseau ;
- Détecter les configurations de service ;
- Rassembler toutes les informations nécessaires sur le réseau ;
- Envoyer des informations à l'infrastructure réseau, par exemple les changements de configuration réalisés.

L'API Nord du contrôleur de réseau vous permet de configurer, surveiller, dépanner et déployer de nouveaux périphériques sur le réseau en utilisant :

- Windows PowerShell ;
- REST API ;
- Une application de gestion et une interface utilisateur graphique, System Center Virtual Machine Manager par exemple.

Ressources

Procédure de déploiement du Contrôleur de réseau

 **Lectures supplémentaires :** Pour plus d'informations sur la syntaxe de ces applets, reportez-vous à : http://aka.ms/Jforwt

 **Lectures supplémentaires :** Pour plus d'informations sur la syntaxe de cet applet, reportez-vous à : http://aka.ms/Yv09r3

Équilibrage de charge logicielle

 **Lectures supplémentaires :** Vous pouvez également utiliser les applets de commande Windows PowerShell. Pour plus d'informations sur les applets de commande Windows PowerShell que vous pouvez utiliser pour gérer le Contrôleur de réseau, reportez-vous à : http://aka.ms/Q9ih9a

Démonstration : Préparation du déploiement du Contrôleur de réseau

Procédure de démonstration

Créer des groupes de sécurité AD DS

1. Basculez vers LON-DC1.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
3. Dans **Utilisateurs et ordinateurs Active Directory**, développez **Adatum.com**, puis cliquez sur **IT**.
4. Cliquez avec le bouton droit sur **IT**, cliquez sur **Nouveau**, puis sur **Groupe**.
5. Dans la boîte de dialogue **Nouvel objet - Groupe**, dans la zone de texte **Nom de groupe**, entrez **Administrateurs du Contrôleur de réseau**, puis cliquez sur **OK**.

6. Dans le volet des détails, double-cliquez sur **Administrateurs du Contrôleur de réseau,** puis dans la boîte de dialogue **Propriétés des Administrateurs du Contrôleur de réseau**, dans l'onglet **Membres**, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Sélectionner les utilisateurs, les contacts, les ordinateurs, les comptes de service ou les groupes**, dans la zone **Entrer les noms des objets à sélectionner (exemples)**, entrez **administrateur; Beth**, puis cliquez sur **OK** deux fois.
8. Cliquez avec le bouton droit sur **IT**, cliquez sur **Nouveau**, puis sur **Groupe**.
9. Dans la boîte de dialogue **Nouvel objet - groupe**, dans la zone **Nom de groupe**, entrez **Opérateurs du Contrôleur de réseau**, puis cliquez sur **OK**.
10. Dans le volet des détails, double-cliquez sur **Opérateurs du Contrôleur de réseau** puis dans la boîte de dialogue **Propriétés des Opérateurs du Contrôleur de réseau**, sur l'onglet **Membres**, cliquez sur **Ajouter**.
11. Dans la boîte de dialogue **Sélectionner les utilisateurs, les contacts, les ordinateurs, les comptes de service ou les groupes**, dans la zone **Entrer les noms des objets à sélectionner (exemples)**, entrez **administrateur; Beth**, puis cliquez sur **OK** deux fois.
12. Fermez la fenêtre **Utilisateurs et ordinateurs Active Directory**.

Demander un certificat

1. Basculez vers LON-SVR2.
2. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Exécuter**.
3. Dans la boîte de dialogue **Exécuter**, entrez **mmc.exe**, puis appuyez sur Entrée.
4. Dans la fenêtre **Console1 – [Racine de la console]**, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
5. Dans la boîte de dialogue **Ajouter ou supprimer un composant logiciel enfichable**, dans la liste **Composants logiciels enfichables**, double-cliquez sur **Certificats**.
6. Cliquez sur **Compte d'ordinateur**, cliquez sur **Suivant**, puis cliquez sur **Terminer**.
7. Cliquez sur **OK**.
8. Dans le volet de navigation, développez **Certificats (ordinateur local)**, puis cliquez sur **Personnel**.
9. Cliquez avec le bouton droit sur **Personnel**, cliquez sur **Toutes les tâches**, puis sur **Demander un nouveau certificat**.
10. Dans la boîte de dialogue **Inscription du certificat**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
11. Sur la page **Sélectionner la stratégie d'inscription de certificat**, cliquez sur **Suivant**.
12. Cochez la case **Ordinateur**, puis cliquez sur **Inscrire**.
13. Cliquez sur **Terminer**.
14. Fermez la console de gestion sans enregistrer les modifications.

Démonstration : Déploiement du Contrôleur de réseau

Procédure de démonstration

Ajouter le rôle de Contrôleur de réseau

1. Sur LON-SVR2, cliquez sur **Démarrer**, puis sur **Gestionnaire de serveurs**.

2. Dans le **Gestionnaire de serveur**, dans le volet des détails, cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, sur la page **Avant de commencer**, cliquez sur **Suivant**.
4. Sur la page **Sélectionner le type d'installation**, cliquez sur **Suivant**.
5. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, dans la liste **Rôles**, cochez la case **Contrôleur du réseau**.
7. Cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**.
8. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
9. Sur la page **Contrôleur de réseau**, cliquez sur **Suivant**.
10. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
11. Lorsque le rôle est installé, cliquez sur **Fermer**.
12. Cliquez avec le bouton droit sur **Démarrer**, pointez vers **Arrêter ou se déconnecter**, puis cliquez sur **Redémarrer**.
13. Dans la boîte de dialogue **Choisir un motif qui justifie, selon vous, d'éteindre cet ordinateur**, cliquez sur **Continuer**.
14. Après le redémarrage de LON-SVR2, connectez-vous en tant qu'**Adatum\administrator** avec le mot de passe **Pa$$w0rd**.

Configurer le cluster du Contrôleur de réseau

1. Sur LON-SVR2, cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (Admin)**.
2. À l'invite de commandes Windows PowerShell (Admin), entrez la commande suivante, puis appuyez sur Entrée :

```
$node=New-NetworkControllerNodeObject -Name "Node1" -Server "LON-SVR2.Adatum.com" -
FaultDomain "fd:/rack1/host1" -RestInterface "Ethernet"
```

3. À l'invite de commandes Windows PowerShell (Admin), entrez la commande suivante, puis appuyez sur Entrée :

```
$Certificate = Get-Item Cert:\LocalMachine\My | Get-ChildItem | where {$_.Subject -
imatch "LON-SVR2" }
```

4. À l'invite de commandes Windows PowerShell (Admin), entrez la commande suivante, puis appuyez sur Entrée :

```
Install-NetworkControllerCluster -Node $node -ClusterAuthentication Kerberos -
ManagementSecurityGroup "Adatum\Network Controller Admins" -
CredentialEncryptionCertificate $Certificate
```

Configurer l'application du contrôleur de réseau

- À l'invite de commandes Windows PowerShell (Admin), entrez la commande suivante, puis appuyez sur Entrée :

```
Install-NetworkController -Node $node -ClientAuthentication Kerberos -
ClientSecurityGroup "Adatum\Opérateurs du Contrôleur de réseau" -RestIpAddress
"172.16.0.99/24" -ServerCertificate $Certificate
```

Valider le déploiement

1. À l'invite de commandes Windows PowerShell (Admin), entrez la commande suivante, puis appuyez sur Entrée :

```
$cred=New-Object Microsoft.Windows.Networkcontroller.credentialproperties
```

2. À l'invite de commandes Windows PowerShell (Admin), entrez la commande suivante, puis appuyez sur Entrée :

```
$cred.type="usernamepassword"
```

3. À l'invite de commandes Windows PowerShell (Admin), entrez la commande suivante, puis appuyez sur Entrée :

```
$cred.username="admin"
```

4. À l'invite de commandes Windows PowerShell (Admin), entrez la commande suivante, puis appuyez sur Entrée :

```
$cred.value="abcd"
```

5. À l'invite de commandes Windows PowerShell (Admin), entrez la commande suivante, puis appuyez sur Entrée :

```
New-NetworkControllerCredential -ConnectionUri https://LON-SVR2.Adatum.com -
Properties $cred –ResourceId cred1
```

6. Appuyez sur **Y**, puis appuyez sur Entrée lorsque vous y êtes invité.

7. À l'invite de commandes Windows PowerShell (Admin), entrez la commande suivante, puis appuyez sur Entrée :

```
Get-NetworkControllerCredential -ConnectionUri https://LON-SVR2.Adatum.com -
ResourceId cred1
```

Révision du module et Takeaways

Questions de contrôle des acquis

Question : Vous décidez de déployer le Contrôleur de réseau dans votre environnement de domaine AD DS. Quelles mesures faut-il prendre pour préparer le déploiement ?

Réponse : Les conditions de déploiement dans un environnement de domaine sont les suivantes :

- Vous ne pouvez déployer le Contrôleur de réseau qu'avec Windows Server 2016 édition Datacenter.
- Le client de gestion que vous utilisez doit être installé sur un ordinateur physique ou virtuel exécutant Windows 10, Windows 8.1 ou Windows 8.
- Vous devez configurer l'inscription DNS dynamique pour permettre l'inscription des enregistrements DNS requis pour le Contrôleur de réseau.
- Si les ordinateurs physiques ou virtuels qui exécutent le Contrôleur de réseau ou le client de gestion du Contrôleur de réseau sont reliés à un domaine, vous devez :
    - Créer un groupe de sécurité qui contient tous les utilisateurs qui ont la permission de configurer le Contrôleur de réseau ;
    - Créer un groupe de sécurité incluant tous les utilisateurs ayant l'autorisation de configurer et de gérer le réseau à l'aide du Contrôleur de réseau.

Question : Quelles sont les raisons d'envisager l'implémentation d'une mise en réseau SDN (Software Defined Networking) avec Windows Server 2016 ?

Réponse : La mise en réseau SDN fournit des ressources réseau :

- Flexibles. Vous pouvez déplacer le trafic de votre infrastructure locale à votre infrastructure de cloud privé ou public.
- Efficaces. Vous pouvez abstraire les composants matériels de votre infrastructure réseau avec des composants logiciels.
- Évolutives. Votre infrastructure locale a une capacité limitée. Votre infrastructure cloud a des limites beaucoup plus larges, vous permettant d'étendre votre infrastructure si nécessaire.

Question : Comment installer la fonction du Contrôleur de réseau dans Windows Server 2016 à l'aide de Windows PowerShell ?

Réponse : Pour déployer le Contrôleur de réseau avec Windows PowerShell, installez la fonctionnalité en exécutant l'applet de commande suivante :

Install-WindowsFeature -Name NetworkController -IncludeManagementTools

Questions et réponses sur les ateliers pratiques

Atelier pratique : Déploiement du Contrôleur de réseau

Questions et réponses

Question : Dans l'atelier pratique, vous avez utilisé Windows PowerShell pour gérer le Contrôleur de réseau. Quels autres outils pourriez-vous utiliser ?

Réponse : Vous pouvez également utiliser System Center Virtual Machine Manager et des outils de gestion autres que ceux de Microsoft pour gérer le Contrôleur de réseau.

Question : Dans l'atelier pratique, vous avez déployé le Contrôleur de réseau dans un environnement de domaine. Dans un environnement hors domaine, quelles mesures devez-vous prendre pour assurer l'authentification ?

Réponse : Dans un environnement hors domaine, les certificats assurent l'authentification. Vous devez configurer l'authentification par certificat en :

- Créant un certificat destiné à être utilisé sur le client de gestion. Le Contrôleur de réseau doit faire confiance à ce certificat.
- Créant un certificat sur le Contrôleur de réseau pour l'authentification de l'ordinateur.