Microsoft

PRODUIT OFFICIEL MICROSOFT LEARNING

22744B

Sécurisation de Windows Server 2016

Contenu d'accompagnement

Numéro de produit : 22744B

Date de publication : 05/2018

TERMES DU CONTRAT DE LICENCE D'UN ENVIRONNEMENT VIRTUEL QUI INCLUT LES LOGICIELS MICROSOFT SUIVANTS :

MICROSOFT ENHANCED MITIGATION EXPERIENCE TOOLKIT (EMET)
SYSINTERNALS
MICROSOFT LOCAL ADMINISTRATOR PASSWORD SOLUTION
MICROSOFT MESSAGE ANALYZER
MICROSOFT WINDOWS IDENTITY FOUNDATION 1.0
MICROSOFT WINDOWS MANAGEMENT FRAMEWORK 3.0
MICROSOFT SYNC FRAMEWORK RUNTIME 1.0 SP1
MICROSOFT SQL SERVER 2008 R2 NATIVE CLIENT SP1
MICROSOFT WCF DATA SERVICES 5.0
MICROSOFT ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES CLIENT 2.0
MICROSOFT APPFABRIC 1.1 POUR WINDOWS SERVER
MISE A JOUR CUMULATIVE 1 POUR MICROSOFT APPFABRIC 1.1 POUR WINDOWS SERVER
MICROSOFT IDENTITY EXTENSIONS 1.0
MICROSOFT .NET FRAMEWORK VERSION 4.5 POUR SYSTEME D'EXPLOITATION MICROSOFT WINDOWS ET MODULES LINGUISTIQUES ASSOCIES
MICROSOFT SHAREPOINT FOUNDATION 2013
MICROSOFT SQL SERVER 2014 ENTERPRISE SERVER/CAL EDITION
MICROSOFT SECURITY COMPLIANCE MANAGER VERSION 4.0
MICROSOFT SQL SERVER 2008 R2 EXPRESS
MICROSOFT ADVANCED THREAT ANALYTICS

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 s'appliquent à votre utilisation des différents logiciels visés ci-dessus ainsi qu'à la documentation, au contenu, au guide de préparation de la classe, aux fichiers de support et de configuration, aux services en ligne et aux exemples d'applications fournis en tant que parties intégrantes de l'environnement virtuel (tous collectivement désignés sous le terme « **Environnement Virtuel** ») y compris le support sur lequel vous l'avez reçu, le cas échéant. Les présents termes s'appliquent également aux mises à jour, suppléments, services Internet et d'assistance technique pour les composants de l'Environnement Virtuel.

Les images de disque dur virtuel du logiciel Microsoft pour l'Environnement Virtuel peuvent vous être fournies sur un ou plusieurs disques durs virtuels. Les différents logiciels visés ci-dessus sont normalement concédés sous licence séparément, mais vous sont fournis selon les présentes conditions de licence consolidées dans un souci de commodité.

COMME DÉCRIT CI-DESSOUS, EN UTILISANT L'ENVIRONNEMENT VIRTUEL VOUS CONSENTEZ À CE QUE MICROSOFT RECUEILLE CERTAINES INFORMATIONS DE VOTRE ORDINATEUR PENDANT L'ACTIVATION, LA VALIDATION ET POUR DES SERVICES INTERNET.

EN ACCÉDANT À QUELQUE PARTIE QUE CE SOIT DE L'ENVIRONNEMENT VIRTUEL, VOUS ACCEPTEZ CES CONDITIONS. SI VOUS NE LES ACCEPTEZ PAS, N'ACCÉDEZ À ET N'UTILISEZ AUCUN COMPOSANT DE L'ENVIRONNEMENT VIRTUEL.

VOTRE DROIT D'UTILISER L'ENVIRONNEMENT VIRTUEL OU D'Y OFFRIR L'ACCÈS EST LIMITÉ À UNE PÉRIODE SPÉCIFIQUE. REPORTEZ-VOUS À LA SECTION 8 POUR PLUS D'INFORMATIONS.

Dans le cadre des présents termes du contrat de licence, vous disposez des droits stipulés ci-dessous pour autant que vous disposiez d'une licence valable pour l'Environnement Virtuel.

1. DÉFINITIONS.

1.1. « **Centre de Formation Agréé** » désigne un Partenaire de Formation, un Membre du Programme Microsoft IT Academy ou toute autre entité que Microsoft peut désigner par écrit.

1.2. « **Session de Formation Agréée** » désigne le Cours Microsoft avec formateur agréé Microsoft dispensé par un MCT pour un Centre de Formation Agréé dans ses installations de formation.

1.3. « **Dispositif de la Classe** » désigne un ordinateur personnel dédié qu'un Centre de Formation Agréé possède ou contrôle, qui se trouve dans les installations de formation du Centre de Formation Agréé où la Session de Formation Agréée est assurée et qui répond ou est supérieur au niveau matériel spécifié pour le Cours Microsoft concerné.

1.4. « **Utilisateur Final** » désigne une personne dûment inscrite et qui participe à une Session de Formation Agréée.

1.5. « **Partenaire de Formation** » désigne un membre actif du programme Microsoft Partner Network qui a et conserve le statut Learning Competency.

1.6. « **MCT** » ou « **Microsoft Certified Trainer** » désigne une personne qui est (i) engagée par un Centre de Formation Agréé pour donner sa Session de Formation Agréée ; (ii) actuellement Formateur Agréé Microsoft actif dans le cadre du Programme de Certification Microsoft, et (iii) détentrice actuelle d'une Certification Microsoft pour la technologie objet de la Session de Formation Agréée.

1.7. « **Cours Microsoft** » désigne la version kit-étudiant du cours avec formateur Microsoft qui est concédé sous licence par Microsoft et qui forme aux technologies Microsoft. Un Cours Microsoft peut être labellisé Cours Officiel Microsoft, Microsoft Dynamics ou Microsoft Business Group.

1.8. « **Membre du Programme Microsoft IT Academy** » désigne un établissement d'enseignement qui est membre actif du programme Microsoft IT Academy.

1.9. « **Vous** » désigne le Partenaire de Formation ou un MCT exerçant des droits dans le cadre de la présente licence.

2. INSTALLATION ET DROITS D'UTILISATION.

2.1. Annulation et remplacement de tous les autres termes du contrat de licence. Les termes du présent contrat de licence annulent et remplacent les termes de tout contrat de licence Microsoft que vous pouvez rencontrer dans tout Environnement Virtuel, même si l'installation ou l'utilisation de ce logiciel nécessite « l'acceptation » d'un contrat de licence distinct.

2.2. Droits d'utilisation limités. L'Environnement Virtuel n'est pas vendu mais concédé sous licence. L'Environnement Virtuel ne pouvant être utilisé que conjointement au Cours Microsoft associé à l'Environnement Virtuel, vous devez acheter une licence du Cours Microsoft associé à l'Environnement virtuel pour chaque Utilisateur Final qui accède à l'Environnement Virtuel et vous devez fournir à chaque Utilisateur Final sa propre copie concédée sous licence du Cours Microsoft. Vous trouverez ci-dessous deux sections sur les droits d'utilisation. Une seule section de droits d'utilisation vous est applicable.

a. **Si vous êtes un Partenaire de Formation**, pour chaque Session de Formation Agréée que vous assurez, vous êtes autorisé à :

   i. télécharger et installer uniquement les composants de l'Environnement Virtuel figurant dans le guide de préparation de la classe pour le Cours Microsoft qui est l'objet de votre Session de Formation Agréée sur un (1) Dispositif hôte de la Classe exécutant une copie concédée sous licence de Microsoft Hyper-V pour créer l'Environnement Virtuel associé au Cours Microsoft ;

   ii. soit

      1. installer l'Environnement Virtuel sur (1) serveur interne situé dans les installations de formation de votre Centre de Formation Agréé où la Session de Formation Agréée est assurée, **OU**

      2. dupliquer l'Environnement Virtuel et installer une (1) instance de l'Environnement Virtuel sur un (1) des Dispositifs de votre Classe exécutant une copie concédée sous licence de Microsoft Hyper-V, à condition que vous n'installiez pas l'Environnement Virtuel sur plus de Dispositifs de la Classe que le nombre d'Utilisateurs Finaux inscrits à cette Session de Formation Agréée spécifique ; et

   iii. autoriser l'accès à l'Environnement Virtuel et son utilisation exclusivement via un Dispositif de la Classe et uniquement par :

1. un (1) Utilisateur Final qui a acheté une licence valable du Cours Microsoft associé à l'Environnement Virtuel uniquement pour effectuer les activités pratiques associées au Cours Microsoft et uniquement pendant leur participation à votre Session de Formation Agréée, et
2. un MCT pour préparer et assurer votre Session de Formation Agréée.

b. **Si vous êtes un MCT**, pour chaque Session de Formation Agréée que vous assurez, vous êtes autorisé à :

i. télécharger et installer uniquement les composants de l'Environnement Virtuel figurant dans le guide de préparation de la classe pour le Cours Microsoft qui est l'objet de la Session de Formation Agréée sur un (1) Dispositif hôte de la Classe exécutant une copie concédée sous licence de Microsoft Hyper-V pour créer l'Environnement Virtuel associé au Cours Microsoft ;

ii. soit

1. installer les composants de l'Environnement Virtuel sur (1) serveur interne situé dans les installations de formation du Centre de Formation Agréé où la Session de Formation Agréée est assurée, **OU**
2. dupliquer et installer une (1) instance des composants de l'Environnement Virtuel sur les Dispositifs de la Classe exécutant une copie concédée sous licence de Microsoft Hyper-V, à condition que vous n'installiez pas l'Environnement Virtuel sur plus de Dispositifs de la Classe que le nombre d'Utilisateurs Finaux inscrits à cette Session de Formation Agréée spécifique ; et

iii. dupliquer et installer une (1) instance de l'Environnement Virtuel sur un (1) ordinateur personnel qui vous appartient et exécutant une copie concédée sous licence de Microsoft Hyper-V, et ce uniquement pour vous préparer à assurer la Session de Formation Agréée.

2.3. Absence d'Autres Droits. L'accès à l'Environnement Virtuel et son utilisation sur une base autonome ne sont pas autorisés. L'accès et l'utilisation de l'Environnement Virtuel ne sont autorisés que conjointement à la Session de Formation Agréée présentant le Cours Microsoft associé à l'Environnement Virtuel. Vous n'êtes pas autorisé à utiliser l'Environnement Virtuel concédé au titre du présent contrat de licence dans un environnement d'exploitation ou de production. Vous n'êtes autorisé à distribuer, exécuter ou présenter en public ni l'Environnement Virtuel ni aucun de ses composants.

2.4. Dissociation de composants. L'Environnement Virtuel pour un Cours Microsoft peut inclure divers logiciels, contenus et autres composants susceptibles de vous être fournis sur plusieurs supports ou au moyen de plusieurs téléchargements. L'Environnement Virtuel vous est fourni et concédé sous licence sous la forme d'une seule unité devant être utilisée conformément à la Section 2.2. Vous n'êtes pas autorisé à dissocier les composants de l'Environnement Virtuel ni à les installer sur différents dispositifs ou serveurs.

2.5. Absence d'Accès Réseau. Vous n'êtes pas autorisé à installer l'Environnement Virtuel sur des Dispositifs de la Classe ou des serveurs accessibles via d'autres réseaux, sauf autorisation explicite de Microsoft, tel qu'énoncé et spécifié dans le guide de préparation de la classe du Cours Microsoft associé.

2.6. Reproduction/Redistribution des Images de Disque Dur Virtuel du Logiciel Microsoft dans l'Environnement Virtuel. Vous reconnaissez et acceptez que :

a. l'Environnement Virtuel contient des images de disque dur virtuel du Logiciel Microsoft ;

b. les logiciels Microsoft qui vous sont fournis dans le cadre du présent contrat sont des actifs de valeur de Microsoft et que la duplication et la distribution non autorisées desdits logiciels priveraient Microsoft des revenus qui découlent normalement de la concession de licences de ces logiciels Microsoft ;

c. Microsoft vous fournit les logiciels Microsoft gratuitement aux seules fins d'aider les Utilisateurs Finaux à acquérir des compétences en utilisant des technologies Microsoft tel que décrit dans le présent contrat de licence ;

d. vous n'êtes pas autorisé à vendre, à louer, à transférer, à céder ni à concéder en sous-licence quelque partie que ce soit des logiciels ; et

e. vous n'êtes pas autorisé à concéder en sous-licence, à transférer ni à céder la présente licence ou le présent contrat de licence à un tiers.

2.7. Logiciel tiers. L'Environnement Virtuel peut inclure du code de tiers que Microsoft, et non le tiers, vous concède sous licence aux termes du présent contrat. Les mentions éventuelles relatives au code de tiers sont incluses pour votre information uniquement.

2.8. Services en ligne. Si Microsoft met à votre disposition des services en ligne dans le cadre du Cours Microsoft (« **Services en ligne** »), votre utilisation des Services en ligne est régie par la présente section et par les termes non contradictoires du contrat séparé des services qui vous sont présentés. Lors de l'utilisation de Services en ligne pendant un Cours Microsoft, vous reconnaissez (a) que les Services en ligne ne peuvent être utilisés que pour effectuer les activités pratiques associées au Cours Microsoft associé à l'Environnement Virtuel, (b) que les informations d'authentification que vous utilisez (ou que vos Utilisateurs Finaux utilisent) pour accéder aux Services en ligne ne doivent être liées à aucun compte « live », (c) que vous concédez sous licence à Microsoft, ses affiliés et tous les détenteurs de sous-licence requis tous les droits pour utiliser et traiter l'ensemble des textes, sons, images ou fichiers (« Données ») téléchargés, traités ou stockés à l'aide des Services en ligne, (d) que vous n'autoriserez pas vos Utilisateurs Finaux à entrer, télécharger, traiter ni stocker de Données contenant des informations personnelles identifiantes sur les Services en ligne, (e) qu'aucun dispositif d'Utilisateurs Finaux ne sera utilisé avec les Services en ligne ni enregistré sur ceux-ci, (f) que Microsoft peut supprimer toutes les Données à quelque moment que ce soit sans notification et sans responsabilité à votre égard, et (g) que Microsoft ne fournira aucun service d'assistance technique pour les Services en ligne.

3. CONDITIONS DE LICENCE ET DROITS D'UTILISATION SUPPLÉMENTAIRES.

3.1 Vous êtes autorisé à utiliser l'Environnement Virtuel uniquement si vous vous conformez aux conditions générales du présent contrat de licence ainsi qu'aux conditions de sécurité suivantes :

a. Vous pouvez accéder aux, installer et utiliser uniquement les composants répertoriés comme composants de l'Environnement Virtuel dans le guide de préparation de la classe pour le Cours Microsoft qui est l'objet de la Session de Formation Agréée prévue et vous ne pouvez utiliser l'Environnement Virtuel que pour assurer une Session de Formation Agréée qui présente le Cours Microsoft associé à l'Environnement Virtuel.

b. Vous ne pouvez utiliser les images de disque dur virtuel du logiciel accompagnant le présent contrat de licence que pour assembler l'Environnement Virtuel.

c. Vous devez assembler et configurer l'Environnement Virtuel conformément au guide de préparation de la classe pour le Cours Microsoft qui est l'objet de votre Session de Formation Agréée prévue. Vous n'êtes pas autorisé à inclure ni à utiliser aucun contenu ou logiciel tiers dans l'Environnement Virtuel, sauf autorisation explicite de Microsoft, tel qu'énoncé dans le guide de préparation de la classe du Cours Microsoft associé.

d. Vous n'êtes pas autorisé à installer l'Environnement Virtuel sur des Dispositifs de la Classe ou des serveurs accessibles via d'autres réseaux, sauf autorisation explicite de Microsoft, tel qu'énoncé dans le guide de préparation de la classe approprié pour le Cours Microsoft.

e. Avant le début de la Session de Formation Agréée, vous devez fournir à tous les Utilisateurs Finaux une copie imprimée de la déclaration suivante :

« En accédant à l'environnement virtuel et en l'utilisant de quelque manière que ce soit, vous reconnaissez et acceptez que (a) vous ne pouvez accéder à l'environnement virtuel et l'utiliser qu'à partir de ce dispositif de la classe et uniquement pour effectuer les activités pratiques de cette session de formation, (b) vous ne pouvez pas contourner les restrictions techniques contenues dans l'environnement virtuel, (c) vous ne pouvez pas télécharger, reproduire, transmettre ni transférer aucun logiciel ni composant de l'environnement virtuel sous quelque forme et par quelque moyen que ce soit sans l'autorisation écrite préalable de Microsoft, (d) vous ne pouvez pas entrer, télécharger, traiter ni stocker d'informations personnelles identifiantes dans l'environnement virtuel, (e) vous ne pouvez pas autoriser un tiers à utiliser l'environnement virtuel ni à y accéder, et (f) ces conditions annulent et remplacent celles de tout contrat de licence Microsoft que vous pouvez rencontrer dans tout Environnement Virtuel, même si l'installation ou l'utilisation de ce composant nécessite « l'acceptation » d'un contrat de licence distinct.

En utilisant l'environnement virtuel, vous acceptez de respecter ces conditions. Si vous n'acceptez pas ces conditions, n'utilisez pas l'environnement virtuel.

Cet environnement virtuel est fourni « En l'État ». Microsoft n'accorde aucune garantie expresse ou implicite.

f. Vous ne pouvez donner accès à l'Environnement Virtuel et à son utilisation qu'aux Utilisateurs Finaux qui ont accepté d'être liés par la déclaration du paragraphe 3.1e ci-avant.

g. Avant le début de chaque Session de Formation Agréée, vous devez fournir à chaque Utilisateur Final sa propre copie concédée sous licence du Cours Microsoft qui est l'objet de la Session de Formation Agréée.

h. Vous n'êtes pas autorisé à laisser d'autres personnes accéder à l'Environnement Virtuel, à le transférer, le copier ou le télécharger.

i. Vous devez respecter strictement toutes les instructions Microsoft relatives à l'installation, à l'activation, à l'utilisation, à la désactivation et à la sécurité de l'Environnement Virtuel.

j. Vous n'êtes pas autorisé à modifier l'Environnement Virtuel ni aucun de ses composants, sauf autorisation explicite de Microsoft, tel qu'énoncé dans le guide de préparation de la classe du Cours Microsoft associé.

k. Si vous êtes un Partenaire de Formation, vous devez supprimer toutes les copies de l'Environnement Virtuel de votre serveur interne et tous les Dispositifs de la Classe à la fin de la Session de Formation Agréée.

l. Si vous êtes un MCT, vous devez supprimer toutes les copies de l'Environnement Virtuel (1) sur votre ordinateur personnel, et (2) installées par vous sur le serveur interne du Partenaire de Formation et tous les Dispositifs de la Classe à la fin de la Session de Formation Agréée.

3.2 Si l'Environnement Virtuel inclut un logiciel de système d'exploitation qui est désactivé, vous devrez obtenir de Microsoft une clé de produit pour activer le logiciel avant de configurer le logiciel de l'Environnement Virtuel. Des instructions spécifiques sur l'obtention du logiciel et son activation à l'aide d'une clé de produit Microsoft figurent dans le guide de préparation de la classe du Cours Microsoft. Vous êtes responsable de l'utilisation des clés de produit qui vous sont attribuées. Vous n'êtes pas autorisé à partager vos clés de produit avec des tiers ni utiliser des clés de produit attribuées à des tiers.

L'activation associe l'utilisation du logiciel à un dispositif spécifique. Pendant l'activation, le logiciel envoie des informations sur le logiciel et le dispositif à Microsoft. Ces informations incluent la version, la langue et la clé de produit du logiciel, l'adresse IP du dispositif et des informations dérivées de la configuration matérielle du dispositif. **EN UTILISANT LE LOGICIEL, VOUS CONSENTEZ A LA TRANSMISSION DE CES INFORMATIONS**. Si la licence du logiciel est valide, vous êtes autorisé à utiliser la version du logiciel installée pendant le processus d'installation jusqu'au terme de la période d'activation prévue. **À MOINS QUE LE LOGICIEL NE SOIT ACTIVE, VOUS N'ETES PAS AUTORISE A UTILISER LE LOGICIEL AU-DELA DE LA PERIODE D'ACTIVATION SPECIFIEE.** Ceci vise à empêcher son utilisation sans licence. **VOUS N'ETES PAS AUTORISE A PASSER OUTRE OU A CONTOURNER LE PROCESSUS D'ACTIVATION**. Si le dispositif est connecté à Internet, le logiciel peut se connecter automatiquement à Microsoft pour être activé. Vous pouvez également activer le logiciel manuellement par Internet ou téléphone. Dans ce cas, des frais de communication peuvent s'appliquer. Il est possible que vous deviez réactiver le logiciel si vous modifiez vos composants informatiques ou le logiciel. **CELUI-CI AFFICHERA UN RAPPEL D'ACTIVATION JUSQU'A CE QU'IL SOIT ACTIVE.**

3.3 Si l'Environnement Virtuel inclut un logiciel de système d'exploitation qui ne nécessite pas de clé de produit, vous devez vérifier l'état du système d'exploitation après installation du logiciel dans l'Environnement Virtuel. Si le système d'exploitation est en mode « Notification », vous devez réarmer le logiciel pour changer l'état du système d'exploitation avant la Session de Formation Agréée.

4. SERVICES INTERNET. Microsoft peut fournir des services Internet avec le logiciel de l'Environnement Virtuel. Microsoft peut les modifier ou les interrompre à tout moment. Si l'Environnement Virtuel contient des logiciels en version précommerciale, certains de leurs services Internet peuvent être activés par défaut. Cela ne signifie pas qu'ils le seront également dans la version commercialisée. La fonction de

transmission via Internet d'un logiciel peut toutefois être activée. Le cas échéant, les conditions suivantes s'appliquent :

a. Consentement pour les Services Internet. Certains des logiciels peuvent inclure des fonctionnalités qui se connectent aux systèmes informatiques de Microsoft ou de prestataires de services via Internet. Dans certains cas, vous ne recevrez pas de notification de connexion distincte. Dans certains cas, vous pouvez désactiver ces fonctionnalités ou ne pas les utiliser. **EN UTILISANT CES FONCTIONNALITÉS, VOUS CONSENTEZ À LA TRANSMISSION DE CES INFORMATIONS ET C'EST À VOUS QU'IL INCOMBE D'OBTENIR LE CONSENTEMENT NÉCESSAIRE DE TOUS LES UTILISATEURS FINAUX POUR LA TRANSMISSION DE CES INFORMATIONS À MICROSOFT**. Microsoft n'utilise pas ces informations pour vous identifier ou vous contacter.

b. Informations sur l'ordinateur. Ces fonctionnalités appelées Services Internet utilisent des protocoles Internet qui transmettent des informations aux systèmes appropriés, telles que l'adresse IP, le type de système d'exploitation, le navigateur, le nom et la version du logiciel que vous utilisez ainsi que le code de langue du dispositif sur lequel vous exécutez le logiciel. Microsoft utilise ces informations pour mettre à votre disposition les services Internet.

c. Utilisation d'informations. Microsoft est autorisé à utiliser les informations et les rapports pour améliorer son logiciel et ses services. Nous pouvons également être amenés à les partager avec des tiers, tels que des fournisseurs de matériels et de logiciels. Ceux-ci peuvent utiliser ces informations pour améliorer le fonctionnement de leurs produits avec le logiciel Microsoft.

d. Utilisation inappropriée des services Internet. Vous n'êtes pas autorisé à utiliser ces services de quelque manière que ce soit qui pourrait leur porter atteinte ou perturber leur utilisation par un autre utilisateur. Vous n'êtes pas autorisé à tenter d'accéder de façon non autorisée aux services, données, comptes ou réseaux de toute autre manière.

5. CHAMP D'APPLICATION DE LA LICENCE. L'Environnement Virtuel n'est pas vendu, mais concédé sous licence. Le présent contrat ne fait que vous conférer certains droits d'utilisation de l'Environnement Virtuel. 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 l'Environnement Virtuel qu'en conformité avec les termes du présent contrat de licence. Ce faisant, vous devez vous conformer aux restrictions techniques contenues dans les composants de l'Environnement Virtuel qui ne vous permettent de l'utiliser que d'une certaine façon. Vous ne pouvez pas, ni autoriser d'autres personnes à :

a. créer ou installer sur des Dispositifs de la classe un nombre de copies de l'Environnement Virtuel supérieur au nombre d'Utilisateurs Finaux participant à la Session de Formation Agréée ;

b. autoriser l'accès à l'Environnement Virtuel à un nombre de Dispositifs de la classe supérieur au nombre d'Utilisateurs Finaux participant à la Session de Formation Agréée ;

c. autoriser l'accès à l'Environnement Virtuel ou son utilisation à qui que soit si ce n'est aux Utilisateurs Finaux qui ont acheté une licence valable du Cours Microsoft qui est l'objet de la Session de Formation Agréée et uniquement lorsqu'ils participent à la Session de Formation Agréée présentant le Cours Microsoft associé à l'Environnement Virtuel ;

d. transmettre, publier, créer des liens vers, présenter en public ou transférer l'Environnement Virtuel ou l'utiliser de quelque autre manière non autorisée ou interdite ;

e. reproduire, utiliser, télécharger, donner accès à ou distribuer l'Environnement Virtuel, excepté conformément à ce qu'autorise de manière expresse le présent contrat ;

f. louer, vendre ou prêter l'Environnement Virtuel ou le reproduire sur un serveur ou à quelque autre emplacement à des fins de reproduction ou d'accès, excepté conformément à ce qu'autorise de manière expresse le présent contrat ;

g. accéder au logiciel ou à l'Environnement Virtuel ou l'utiliser pour (i) des services d'hébergement commercial, (ii) des besoins professionnels d'ordre général ou (iii) quelque fin pour laquelle vous n'avez pas obtenu d'autorisation expresse de Microsoft dans le cadre du présent contrat ;

h. ajouter du contenu, altérer, changer, adapter, modifier ou créer des œuvres dérivées basées sur l'Environnement Virtuel ;

i. utiliser l'environnement virtuel dans un autre système d'exploitation physique ou dans une application exécutant un autre système d'exploitation ;

j. contourner les restrictions techniques contenues dans l'Environnement Virtuel ; ou

k. reconstituer la logique de l'Environnement Virtuel, le décompiler ou le désassembler de quelque manière que ce soit.

Les droits d'accès à l'Environnement Virtuel sur un dispositif quelconque ne vous autorisent pas à exploiter des brevets appartenant à Microsoft ou tous autres droits de propriété intellectuelle de Microsoft dans l'Environnement Virtuel et sur des dispositifs qui accèdent à cet Environnement Virtuel.

6. **DROITS RÉSERVÉS ET PROPRIÉTÉ**. Microsoft et ses fournisseurs se réservent les droits de propriété, droits d'auteur et autres droits de propriété intellectuelle sur l'Environnement Virtuel et ses composants.

7. **LOGICIEL TEMPORAIRE**. Après le lancement initial, certains des logiciels de l'Environnement Virtuel peuvent cesser de fonctionner à la date indiquée pour le logiciel concerné dans le guide de préparation de la classe du Cours Microsoft. Vous ne recevrez aucune autre notification. Vous pourrez peut-être utiliser la commande de réarmement pour réinitialiser le logiciel de l'Environnement Virtuel afin de l'exécuter pendant une période supplémentaire. Le nombre de jours pendant lequel le logiciel fonctionnera par lancement et le nombre de fois que vous pouvez exécuter la commande de réarmement varie comme indiqué dans le guide de préparation de la classe du Cours Microsoft.

   Vous devez arrêter d'accéder à l'Environnement Virtuel et de l'utiliser si un logiciel présent dans celui-ci cesse de fonctionner et si vous avez épuisé tous les réarmements (le cas échéant). Vous ne pourrez plus accéder aux données du logiciel ou de l'Environnement Virtuel, les utiliser ou les récupérer une fois que le logiciel cessera de fonctionner.

8. **DURÉE ET RÉSILIATION**. Le présent contrat sera automatiquement et immédiatement résilié selon la date la plus proche (a) à la date d'expiration la plus proche du logiciel comme indiqué dans le guide de préparation de la classe et lorsque tous les réarmements ont été épuisés (le cas échéant) ; (b) à la résiliation du présent contrat par Microsoft ; (c) (i) à l'expiration ou à la résiliation de votre statut Learning Competency dans le cadre du programme Microsoft Partner Network si vous êtes un Partenaire de Formation, ou (ii) à l'expiration ou à la résiliation de votre statut de MCT si vous êtes un MCT ; ou (d) au terme le plus proche de la durée de la bêta de tout logiciel en version précommerciale inclus dans l'Environnement Virtuel (le cas échéant).

   Microsoft peut résilier immédiatement le présent contrat si nous avons des raisons de penser que vous n'en avez pas respecté une des conditions générales.

   Dès la résiliation du présent contrat pour quelque raison que ce soit, tous les droits qui vous ont été accordés dans le cadre du présent contrat prendront immédiatement fin et vous devrez arrêter tout accès à l'Environnement Virtuel et toute utilisation de celui-ci, et effacer et détruire définitivement toutes les copies de l'Environnement Virtuel et de ses composants en votre possession ou sous votre contrôle.

9. **COMMENTAIRES**. Si vous faites part de vos commentaires concernant l'Environnement Virtuel à Microsoft, vous concédez gracieusement à Microsoft le droit d'utiliser, de partager et de commercialiser vos commentaires de quelque façon que ce soit et à toute fin. Vous concédez également à des tiers, à titre gratuit, tout droit de brevet sur leurs produits, technologies et services, nécessaires pour utiliser ou interfacer des parties spécifiques d'un logiciel 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, des produits, ses technologies, ses services ou sa documentation à des tiers parce que nous y incluons vos commentaires. Ces droits survivent au présent contrat.

10. **RESTRICTIONS A L'EXPORTATION**. Le logiciel de l'Environnement Virtuel 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 concernant le logiciel. Ces réglementations comprennent des restrictions sur les pays destinataires, les utilisateurs finaux et les utilisations finales. Des informations supplémentaires sont disponibles sur le site www.microsoft.com/exporting.

11. **SERVICE D'ASSISTANCE TECHNIQUE**. L'Environnement Virtuel étant fourni « en l'état », Microsoft ne peut pas fournir de services d'assistance relatifs à ce produit.

12. **INTEGRALITE DES ACCORDS**. Le présent contrat (y compris la garantie ci-dessous) ainsi que les termes concernant les suppléments, les mises à jour, les Services en ligne (le cas échéant) et les services d'assistance technique que vous utilisez constituent l'intégralité des accords en ce qui concerne l'Environnement Virtuel et les services d'assistance technique.

13. **REGLEMENTATION APPLICABLE**.
    a. États-Unis. Si vous avez acquis les composants de l'Environnement Virtuel 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 de l'État 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 les composants de l'Environnement Virtuel dans un autre pays, les lois de ce pays s'appliquent.

14. **EFFET JURIDIQUE**. Le présent contrat décrit certains droits légaux. Vous pouvez bénéficier d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

15. **EXCLUSIONS DE GARANTIE**. **L'ENVIRONNEMENT VIRTUEL, CHACUN DE DES COMPOSANTS ET LES SERVICES EN LIGNE SONT CONCEDES SOUS LICENCE « EN L'ETAT ». VOUS ASSUMEZ TOUS LES RISQUES LIES A LEUR UTILISATION. MICROSOFT N'ACCORDE AUCUNE GARANTIE OU CONDITION EXPRESSE. VOUS POUVEZ BENEFICIER DE DROITS DES CONSOMMATEURS SUPPLEMENTAIRES DANS LE CADRE DU DROIT LOCAL, QUE CE CONTRAT NE PEUT MODIFIER. LORSQUE CELA EST AUTORISE PAR VOTRE LEGISLATION LOCALE, MICROSOFT EXCLUT LES GARANTIES IMPLICITES DE QUALITE, D'ADEQUATION A UN USAGE PARTICULIER ET D'ABSENCE DE VIOLATION.**

    POUR L'AUSTRALIE – LA LOI AUSTRALIENNE SUR LA CONSOMMATION (AUSTRALIAN CONSUMER LAW) VOUS ACCORDE DES GARANTIES STATUTAIRES QU'AUCUN ELEMENT DU PRESENT ACCORD NE PEUT AFFECTER.

16. **LIMITATION ET EXCLUSION DE RECOURS ET DE DOMMAGES**. **VOUS POUVEZ OBTENIR DE MICROSOFT ET DE SES FOURNISSEURS UNE INDEMNISATION EN CAS DE DOMMAGES DIRECTS UNIQUEMENT, QUI NE SAURAIT EXCÉDER LE MONTANT QUE VOUS AVEZ EFFECTIVEMENT PAYÉ POUR L'ENVIRONNEMENT VIRTUEL OU 5 DOLLARS US (US $ 5,00), SI CE MONTANT EST PLUS ÉLEVÉ. VOUS NE POUVEZ PRETENDRE A AUCUNE INDEMNISATION POUR LES AUTRES DOMMAGES, Y COMPRIS LES DOMMAGES SPECIAUX, INDIRECTS, ACCESSOIRES OU INCIDENTS ET LES PERTES DE BENEFICES.**

    Cette limitation concerne :
    a. toute affaire liée à l'Environnement Virtuel, ses composants, les Services en ligne et le contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers ; et
    b. 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 ou aurait dû connaître l'éventualité de tels dommages. 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.

Module 1

Attaques, détection des violations de la sécurité et outils Sysinternals

Sommaire :

Leçon 1

Présentation des attaques

Sommaire :

Questions et réponses

Question : demandez aux stagiaires de décrire les attaques rencontrées par leur entreprise.

> **Réponse :** les réponses varient. Cette question a pour but d'amorcer une discussion sur les expériences des stagiaires avec les attaques.

Ressources

Chronologie des attaques

 **Lectures supplémentaires :** pour en savoir plus sur les attaques « pass the hash », consultez « Protection contre les attaques pass-the-hash » à l'adresse : http://aka.ms/yxwbip

Leçon 2

Détection des violations de la sécurité

Sommaire :

Questions et réponses

Question : discutez avec les stagiaires de leur expérience de détection de violations de la sécurité. Demandez-leur ce qu'ils recherchent en cas de suspicion de violation de la sécurité dans leur environnement.

Réponse : les réponses varient. Cette discussion poursuit celle commencée dans la leçon 1.

Leçon 3

Analyse de l’activité avec les outils Sysinternals

Sommaire :

Questions et réponses

Question : demandez aux stagiaires s'ils ont déjà utilisé un des outils Sysinternals et, le cas échéant, de quelle façon.

> **Réponse :** les réponses peuvent varier en fonction de l'expérience des stagiaires. Cette question permettra à l'instructeur de mieux jauger le niveau de connaissance de ces outils par les stagiaires.

Ressources

System Monitor

Lectures supplémentaires : pour en savoir plus sur Sysmon, consultez : « Sysmon v7.01 » à l'adresse : http://aka.ms/Tigm98

Autoruns

Lectures supplémentaires : pour en savoir plus sur l'outil Autoruns, consultez « Autoruns for Windows v13.82 » à l'adresse : http://aka.ms/Xnt6os

LogonSessions

Lectures supplémentaires : pour en savoir plus sur l'outil LogonSessions, consultez : « LogonSessions v1.4 » à l'adresse : http://aka.ms/Ugnyh8

Process Explorer

Lectures supplémentaires : pour en savoir plus sur l'outil Process Explorer, consultez « Process Explorer v16.21 » à l'adresse : http://aka.ms/usw7c8

Process Monitor

Lectures supplémentaires : pour en savoir plus sur l'outil Process Monitor, consultez « Process Monitor v3.50 » à l'adresse : http://aka.ms/Qc19u6

Sigcheck

Lectures supplémentaires : pour en savoir plus sur Sigcheck, consultez « Sigcheck v2.60 » à l'adresse : http://aka.ms/Lsef33

Démonstration : outils Sysinternals

Étapes de la démonstration

1. Démarrez **LON-DC1**. Une fois cet ordinateur virtuel démarré, lancez **LON-SVR1**.
2. Connectez-vous à **LON-SVR1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
3. Dans la barre des tâches, cliquez sur **Explorateur de fichiers**.

4. Dans l'Explorateur de fichiers, double-cliquez sur le volume **Allfiles (D:)**.
5. Double-cliquez sur le dossier **Labfiles**.
6. Double-cliquez sur le dossier **Mod01**.
7. Dans le dossier **Mod01**, cliquez avec le bouton droit sur **LogonSessions.zip**, puis cliquez sur **Extraire tout**.
8. Dans la boîte de dialogue **Extraire les dossiers compressés (zippés)**, désactivez la case à cocher **Afficher les dossiers extraits une fois l'opération terminée**, puis cliquez sur **Extraire**.
9. Répétez les étapes 7 et 8 pour **ProcessExplorer.zip** et **ProcessMonitor.zip**.
10. Fermez l'Explorateur de fichiers.
11. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Gestion de l'ordinateur**.
12. Dans la console **Gestion de l'ordinateur**, développez **Utilisateurs et groupes locaux**, cliquez avec le bouton droit sur **Utilisateurs**, puis cliquez sur **Nouvel utilisateur**.
13. Dans la boîte de dialogue **Nouvel utilisateur**, dans la zone de texte **Nom d'utilisateur**, saisissez **Attaquant**.
14. Dans les champs **Mot de passe** et **Confirmer le mot de passe**, tapez **Pa55w.rd**.
15. Désactivez la case à cocher **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**, cliquez sur **Créer**, puis sur **Fermer**.
16. Dans la liste **Utilisateurs**, cliquez avec le bouton droit sur **Attaquant**, puis cliquez sur **Propriétés**.
17. Dans la boîte de dialogue **Propriétés de Attaquant**, sous l'onglet **Membre de**, cliquez sur **Ajouter**.
18. Dans la boîte de dialogue **Sélectionner des groupes**, tapez **Administrateurs**, puis cliquez sur **OK**.
19. Pour fermer la boîte de dialogue **Propriétés de Attaquant**, cliquez sur **OK**.
20. Fermez la console **Gestion de l'ordinateur**.
21. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Exécuter**.
22. Dans la boîte de dialogue **Exécuter**, tapez **cmd.exe**, puis cliquez sur **OK**.
23. Dans la fenêtre **Administrator: C:\Windows\system32\cmd.exe**, tapez la commande suivante, puis appuyez sur Entrée :

```
runas /user:Attaquant cmd.exe
```

24. À l'invite **Entrez le mot de passe de Attaquant :**, saisissez **Pa55w.rd**, puis appuyez sur Entrée.
25. Ancrez la fenêtre **cmd.exe (exécutée sous LON-SVR1\Attaquant)** sur le côté droit de l'écran.
26. Ancrez la fenêtre **Administrator:c:\Windows\system32\cmd.exe** sur le côté gauche de l'écran.
27. Sur le côté droit de l'écran, dans la fenêtre d'**invite de commandes LON-SVR1\Attaquant**, tapez la commande ci-après, puis appuyez sur Entrée :

```
ftp.exe
```

28. Sur le côté gauche de l'écran, dans la fenêtre **Administrator**, tapez les commandes suivantes en appuyant sur Entrée après chacune d'elles :

```
D:
Cd labfiles\Mod01\LogonSessions
Logonsessions -p
```

29. Dans la boîte de dialogue **LogonSessions License Agreement**, cliquez sur **Agree**.
30. Étudiez la sortie de l'outil LogonSessions.

Remarque : notez les processus et les ID en cours d'exécution dans la session ouverte de **ADATUM\Administrator**, ainsi que ceux en cours d'exécution dans la session ouverte de **LON-SVR1\Attaquant**. Vous devriez constater que ftp.exe est en cours d'exécution.

31. À l'invite de commandes **Administrator**, sur le côté gauche de l'écran, tapez les commandes suivantes et appuyez sur Entrée :

```
Cd D:\Labfiles\Mod01\ProcessExplorer
procexp
```

32. Dans la boîte de dialogue **Process Explorer License Agreement**, cliquez sur **Agree**.
33. Ancrez la fenêtre **Process Explorer** sur le côté gauche de l'écran.
34. Dans Process Explorer, sous le processus cmd.exe, localisez le processus ftp.exe.
35. Pour fermer la session ftp, dans la fenêtre **cmd.exe** à droite, à l'invite **ftp>**, tapez **bye**, puis appuyez sur Entrée.

Remarque : l'élément ftp.exe est supprimé de Process Explorer.

36. Dans la fenêtre **cmd.exe** à droite, tapez **notepad newfile1.txt**, appuyez sur Entrée, puis cliquez sur **Oui**.

Remarque : un nouvel élément notepad.exe apparaît dans Process Explorer.

37. Dans la fenêtre **Bloc-notes**, tapez n'importe quel texte et remarquez les changements dans la fenêtre Process Explorer. Fermez le Bloc-Notes sans enregistrer.
38. À l'invite de commandes **Administrator**, sur le côté gauche de l'écran, tapez les commandes suivantes et appuyez sur Entrée après chacune d'elles :

```
Cd D:\Labfiles\Mod01\ProcessMonitor
Procmon
```

39. Dans la boîte de dialogue **Process Monitor License Agreement**, cliquez sur **Agree**, puis ancrez la fenêtre **Process Monitor** sur le côté gauche de l'écran.
40. Dans la fenêtre de droite **cmd.exe**, tapez **ftp.exe**, puis appuyez sur Entrée.
41. Faites défiler la fenêtre **Process Monitor** pour afficher le nom de processus ftp.exe.
42. Cliquez avec le bouton droit sur le nom de processus **ftp.exe**, puis cliquez sur **Highlight 'ftp.exe'**.
43. Faites défiler la fenêtre **Process Monitor** et remarquez que toutes les instances du nom de processus ftp.exe sont en surbrillance.
44. Dans la barre d'outils **Process Monitor**, cliquez sur l'icône **Filter**.
45. Dans la boîte de dialogue **Process Monitor Filter**, cliquez sur le menu déroulant **Architecture**, puis sur **Process Name**.
46. Dans la zone de texte, tapez **ftp.exe**, cliquez sur **Add**, puis sur **OK**.

47. Dans la fenêtre **cmd.exe** à droite, à l'invite **ftp>**, saisissez **bye**, puis appuyez sur Entrée.
48. Examinez les changements dans la fenêtre **Process Monitor**.
49. Dans la barre d'outils **Process Monitor**, cliquez sur l'icône **Filter**.
50. Dans la liste des filtres, désactivez la case à cocher en regard de **Process Name is ftp.exe**, cliquez sur le menu déroulant **Architecture**, puis sur **Process Name**.
51. Dans la zone de texte, tapez **cmd.exe**, cliquez sur **Add**, puis sur **OK**.
52. Dans la fenêtre de droite **cmd.exe**, tapez **notepad newfile2.txt**, appuyez sur Entrée, cliquez sur **Oui**, tapez n'importe quel texte, puis fermez le fichier sans enregistrer.
53. Examinez l'activité supplémentaire enregistrée dans Process Monitor en fonction du filtre cmd.exe.
54. Cliquez sur le menu **File,** puis sur **Save**.
55. Dans la boîte de dialogue **Save To File**, acceptez les paramètres par défaut, puis cliquez sur **OK**.

Contrôle des acquis et éléments à retenir

Question de contrôle des acquis

Question : quels types d'attaque de ce module avez-vous constatés dans votre environnement ?

Réponse : les réponses peuvent varier en fonction de l'environnement et de l'expérience des stagiaires.

Questions et réponses relatives à l'atelier pratique

Atelier pratique : détection de violation de la sécurité et d'incidents basiques

Questions et réponses

Question : quel paramètre utiliser avec LogonSessions pour voir les processus utilisés dans chaque session ?

Réponse : on utilise le paramètre **-p** pour voir les processus utilisés dans chaque session.

Question : quelle est la principale différence entre Process Explorer et Process Monitor ?

Réponse : Process Explorer est un outil conçu pour voir les activités en temps réel. Process Monitor permet d'enregistrer l'activité pour analyse ultérieure.

Module 2

Protection des informations d'identification et de l'accès privilégié

Sommaire :

Leçon 1

Présentation des droits de l'utilisateur

Sommaire :

Questions et réponses

Question : demandez aux stagiaires de parler de leur façon d'attribuer des privilèges à des comptes Administrateur. Utilisent-ils des comptes qui bénéficient de privilèges sur plusieurs systèmes indépendants, par exemple Exchange et Configuration Manager, ou bien des comptes séparés pour chaque ensemble de tâches d'administration ?

Réponse : les réponses varient en fonction des pratiques de l'entreprise de chaque stagiaire.

Ressources

Principe du privilège minimum

Lectures supplémentaires : pour plus d'informations, consultez « Implémentation de modèles d'administration de privilèges » à l'adresse http://aka.ms/Hw2tr3

Utilisateurs protégés, stratégies d'authentifications et silos de stratégies d'authentification

Lectures supplémentaires : pour plus d'informations, consultez « Authentication Policies and Authentication Policy Silos » à l'adresse http://aka.ms/J0abq2

Démonstration : configuration des droits de l'utilisateur et des options de sécurité de compte

Étapes de la démonstration

1. Connectez-vous à **LON-DC1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Dans la console du **Gestionnaire de serveur**, cliquez sur le menu **Outils**, puis sur **Centre d'administration Active Directory**.
3. Dans la console du **Centre d'administration Active Directory**, double-cliquez sur **Adatum (local)**, puis dans la liste, double-cliquez sur l'unité d'organisation (UO) **IT**.
4. Dans l'unité d'organisation **IT**, double-cliquez sur **Dante Dabney**. La boîte de dialogue **Dante Dabney** s'ouvre.
5. Dans la boîte de dialogue **Dante Dabney**, cliquez sur **Se connecter à**.
6. Dans la boîte de dialogue **Se connecter à**, cliquez sur **Les ordinateurs suivants**, tapez **LON-SVR2**, puis cliquez sur **Ajouter**.
7. Cliquez sur **OK** pour fermer la boîte de dialogue **Se connecter à**.
8. Cliquez sur **OK** pour fermer la boîte de dialogue **Dante Dabney**.
9. Passez à **LON-SVR1**, puis connectez-vous en tant que **Adatum\Dante** avec le mot de passe **Pa55w.rd**.
10. Lisez le message qui vous indique que le compte est configuré de façon à vous empêcher d'utiliser cet ordinateur, puis cliquez sur **OK**.
11. Passez à **LON-SVR2**, puis connectez-vous en tant que **Adatum\Dante** avec le mot de passe **Pa55w.rd**.
12. Une fois connecté, cliquez sur **Démarrer**, sur **Dante Dabney**, puis sur **Se déconnecter**.
13. Connectez-vous à **LON-SVR2** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.

14. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Exécuter**.
15. Dans la boîte de dialogue **Exécuter**, tapez **gpedit.msc**, puis cliquez sur **OK**.
16. Dans l'**Éditeur de stratégie de groupe locale**, sous **Configuration ordinateur**, développez **Paramètres Windows**, **Paramètres de sécurité**, **Stratégies locales**, puis cliquez sur **Attribution des droits utilisateur**.
17. Double-cliquez sur la règle **Interdire l'ouverture d'une session locale**.
18. Dans la boîte de dialogue des propriétés de **Interdire l'ouverture d'une session locale**, cliquez sur **Ajouter un utilisateur ou un groupe**.
19. Dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, tapez **Dante**, cliquez sur **Vérifier les noms**, puis cliquez deux fois sur **OK**.
20. Fermez l'**Éditeur de stratégie de groupe locale**.
21. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Exécuter**.
22. Dans la boîte de dialogue **Exécuter**, tapez **gpupdate /force**, puis cliquez sur OK.
23. Cliquez sur **Démarrer**, sur **Administrator**, puis sur **Se déconnecter**.
24. Essayez de vous connecter à **LON-SVR2** en tant que **Adatum\Dante** avec le mot de passe **Pa55w.rd**. Remarquez que cette méthode de connexion n'est pas autorisée.

Démonstration : délégation des privilèges

Étapes de la démonstration

1. Vérifiez que vous êtes connecté à **LON-DC1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Dans le menu **Outils** de la console du **Gestionnaire de serveur**, cliquez sur **Utilisateurs et ordinateurs Actives Directory**.
3. Cliquez avec le bouton droit sur l'UO **Marketing**, puis cliquez sur **Délégation de contrôle**.
4. Dans l'**Assistant Délégation de contrôle**, sur la page **Bienvenue !**, cliquez sur **Suivant**.
5. Sur la page **Utilisateurs ou groupes**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Sélectionner les utilisateurs, les ordinateurs ou les groupes**, tapez **IT**, cliquez sur **Vérifier les noms**, sur **OK**, puis sur **Suivant**.
7. Sur la page **Tâches à déléguer**, sélectionnez **Réinitialiser les mots de passe utilisateur et forcer le changement de mot de passe à la prochaine ouverture de session**, puis cliquez sur **Suivant**.
8. Cliquez sur **Terminer** pour fermer l'**Assistant Délégation de contrôle**.
9. Connectez-vous à **LON-SVR1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
10. Cliquez sur **Démarrer**, puis sur **Gestionnaire de serveur**. Dans la console du **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sur **Ajouter des rôles et fonctionnalités**.
11. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, à la page **Avant de commencer**, cliquez sur **Suivant**.
12. Sur la page **Sélectionner le type d'installation**, cliquez sur **Installation basée sur un rôle ou une fonctionnalité**, puis sur **Suivant**.
13. Sur la page **Sélectionner le serveur de destination**, cliquez sur **Suivant**.
14. Sur la page **Sélectionner des rôles de serveurs**, cliquez sur **Suivant**.

15. Sur la page **Sélectionner des fonctionnalités**, développez **Outils d'administration de serveur distant**, développez **Outils d'administration de rôles**, sélectionnez **Outils AD DS et AD LDS**, cliquez sur **Suivant**, sur **Installer**, puis sur **Fermer**.
16. Cliquez avec le bouton droit sur **Démarrer**, cliquez sur **Arrêter ou se déconnecter**, puis sur **Se déconnecter**.
17. Connectez-vous à **LON-SVR1** en tant que **Adatum\Beth** avec le mot de passe **Pa55w.rd**.
18. Cliquez sur **Démarrer**, puis sur **Gestionnaire de serveur**.
19. Dans la console du **Gestionnaire de serveur**, dans le menu **Outils**, cliquez sur **Centre d'administration Active Directory**.
20. Sous **Adatum.com**, cliquez sur l'UO **Marketing**. Cliquez avec le bouton droit sur **Ada Russell**, puis cliquez sur Réinitialiser le mot de passe.
21. Dans la boîte de dialogue **Réinitialiser le mot de passe**, tapez le mot de passe **Pa55w.rd2** à deux reprises, puis cliquez deux fois sur **OK**. Cela permet de vérifier que vous pouvez réinitialiser les mots de passe dans l'UO Marketing en utilisant le compte de Beth.
22. Cliquez sur l'**UO Managers**, cliquez avec le bouton droit sur le compte d'utilisateur **Art Odum**, puis sur **Réinitialiser le mot de passe**.
23. Dans la boîte de dialogue **Réinitialiser le mot de passe**, tapez le mot de passe **Pa55w.rd2** à deux reprises, puis cliquez sur **OK**.
24. Remarquez que le système d'exploitation Windows ne peut pas effectuer la modification de mot de passe pour **Art Odum**, car l'accès est refusé.

Leçon 2

Comptes d’ordinateur et de service

Sommaire :

Questions et réponses

Question : demandez aux stagiaires comment ils gèrent les comptes de service dans leur entreprise.

> **Réponse :** les réponses varient en fonction de la façon dont l'entreprise du stagiaire gère les comptes de service.

Démonstration : création et gestion de comptes de service administrés

Étapes de la démonstration

1. Vérifiez que vous êtes connecté à **LON-DC1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (admin)**.
3. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

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

4. Pour créer le nouveau compte de service administré de groupe appelé **LON-SVRS-GMSA**, tapez la commande suivante, puis appuyez sur Entrée :

```
New-ADServiceAccount LON-SVRS-GMSA
-DNSHOSTNAME LON-SVRS-GMSA.adatum.com
```

5. Passez à **LON-SVR1**, déconnectez-vous du compte Beth, puis connectez-vous en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
6. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (admin)**.
7. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
Install-WindowsFeature RSAT-AD-PowerShell
Set-ADServiceAccount -Identity LON-SVRS-GMSA -
PrincipalsAllowedToRetrieveManagedPassword LON-SVR1$
Install-ADServiceAccount LON-SVRS-GMSA
```

8. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Gestion de l'ordinateur**.
9. Développez **Services et applications**, puis cliquez sur **Services**.
10. Cliquez avec le bouton droit sur le service **Base de données interne Windows**, puis cliquez sur **Propriétés.**
11. Dans l'onglet **Se connecter**, cliquez sur **Ce compte**, puis sur **Parcourir**.
12. Dans la boîte de dialogue **Sélectionner un utilisateur**, cliquez sur **Emplacements**.
13. Dans la boîte de dialogue **Emplacements**, cliquez sur **Tout le répertoire**, puis sur **OK**.
14. Dans la boîte de dialogue **Sélectionner un utilisateur ou un compte de service**, tapez **LON-SVRS-GMSA**, puis cliquez sur **OK**.
15. Effacez le contenu des zones de texte **Mot de passe** et **Confirmer le mot de passe**, puis cliquez sur **OK**.
16. Lorsqu'un message vous indique que le compte s'est vu octroyer l'ouverture de session comme privilège de service, cliquez sur **OK**.

Leçon 3

Protection des informations d'identification

Sommaire :

Questions et réponses

Question : que doit faire une entreprise avant de mettre en place le blocage NTLM ?

> **Réponse :** une entreprise doit auditer l'utilisation de NTLM avant de désactiver le protocole d'authentification.

Ressources

Configuration de Credential Guard

 **Lectures supplémentaires :** pour plus d'informations, consultez « Protect derived domain credentials with Credential Guard » à l'adresse : http://aka.ms/Vwpgdp

Blocage de NTLM

 **Lectures supplémentaires :** pour plus d'informations, consultez « Introducing the Restriction of NTLM Authentication » à l'adresse http://aka.ms/Ynbr7l

Démonstration : localisation des comptes problématiques

Étapes de la démonstration

1. Vérifiez que vous êtes connecté à **LON-DC1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Dans la console du **Gestionnaire de serveur**, cliquez sur le menu **Outils**, puis sur **Centre d'administration Active Directory**.
3. Agrandissez la fenêtre **Centre d'administration Active Directory**, puis cliquez sur **Recherche globale**.
4. Cliquez sur la **flèche du bas** dans le cercle, puis sur **Ajouter des critères**.
5. Sélectionnez **Utilisateur dont le mot de passe a une date d'expiration/n'a pas de date d'expiration**, puis cliquez sur **Ajouter**.
6. Cliquez sur **Rechercher**. Remarquez que 255 éléments ont été trouvés.
7. Cliquez sur **Effacer tout**.
8. Cliquez sur **Ajouter des critères**.
9. Sélectionnez **Utilisateurs ayant des comptes activés dont le nombre de jours de connexion n'est pas supérieur à un nombre donné**, puis cliquez sur **Ajouter**.
10. Cliquez sur le paramètre souligné **15 après Nombre de jours**, puis cliquez sur **90**.
11. Cliquez sur **Rechercher**.
12. Remarquez que 250 éléments ont été trouvés.

Leçon 4

Stations de travail à accès privilégié et serveurs de rebond

Sommaire :

Questions et réponses

Question : demandez aux stagiaires s'ils utilisent des stations de travail à accès privilégié ou des serveurs de rebond dans leur environnement, et pourquoi.

> **Réponse :** les réponses varient en fonction de l'environnement dans lequel évoluent les stagiaires.

Ressources

Serveurs de rebond

 **Lectures supplémentaires :** pour plus d'informations, consultez « Stations de travail à accès privilégié » à l'adresse : http://aka.ms/Rd5xkn

Sécurisation des contrôleurs de domaine

 **Lectures supplémentaires :** pour plus d'informations, consultez « Sécurisation des contrôleurs de domaine contre les attaques » à l'adresse : http://aka.ms/H84erd

Leçon 5

LAPS

Sommaire :

Questions et réponses

Question : comment gérez-vous vos mots de passe de compte Administrateur local dans votre entreprise ?

> **Réponse :** les réponses varient. Certains stagiaires indiqueront que leur entreprise n'a pas mis de technologie en place. D'autres stagiaires auront une solution, et certains utiliseront même LAPS.

Démonstration : configuration et déploiement de LAPS

Étapes de la démonstration

1. Vérifiez que vous êtes connecté à **LON-DC1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Dans la console du **Gestionnaire de serveur**, dans le menu **Outils**, cliquez sur **Centre d'administration Active Directory**.
3. Dans l'arborescence de la console **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur le domaine **Adatum.com**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
4. Dans la boîte de dialogue **Nouvel objet - Unité d'organisation**, tapez **Sydney_Computers**, puis cliquez sur **OK**.
5. Sous adatum.com, cliquez sur le conteneur **Computers**, cliquez avec le bouton droit sur **LON-SVR2**, puis cliquez sur **Déplacer**.
6. Dans la boîte de dialogue **Déplacer**, cliquez sur **Sydney_Computers,** puis sur **OK**.
7. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Exécuter**.
8. Dans la boîte de dialogue **Exécuter**, tapez **\\LON-SVR1\d$\Labfiles\Mod02**, puis cliquez sur **OK**.
9. Dans la fenêtre **Mod02**, double-cliquez sur **LAPSx64.msi**.
10. Dans l'assistant **Local Administrator Password Solution Setup**, sur la **Welcome**, cliquez sur **Next**.
11. Sur la page **End-User License Agreement**, cliquez sur **I accept the terms in the License Agreement**, puis sur **Next**.
12. Sur la page **Custom Setup**, supprimez la sélection en regard de **AdmPwd GPO Extension**, sélectionnez les modèles **Management Tools**, **Fat client UI**, **PowerShell module** et **GPO Editor templates**, cliquez sur **Next**, puis sur **Install**.
13. Une fois l'installation terminée, cliquez sur **Finish**.
14. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (admin)**.
15. Dans la fenêtre **Administrator: Windows PowerShell**, tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Import-Module admpwd.ps
Update-AdmPwdADSchema
Set-AdmPwdComputerSelfPermission -Identity "Sydney_Computers"
```

16. Dans le console du **Gestionnaire de serveur**, dans le menu **Outils**, cliquez sur **Gestion des stratégies de groupe**.
17. Dans la Console de **gestion des stratégies de groupe**, développez **Forêt : Adatum.com**, développez **Domaines**, développez **Adatum.com**, cliquez avec le bouton droit sur l'UO **Sydney_Computers**, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici...**
18. Dans la zone de texte **Nom de la boîte** de dialogue **Nouvel objet GPO,** tapez **LAPS_GPO,** puis cliquez sur **OK**.

19. Dans la fenêtre **Gestion des stratégies de groupe**, sous **Sydney_Computers**, cliquez avec le bouton droit sur **LAPS_GPO**, puis cliquez sur **Modifier**.
20. Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, dans **Configuration ordinateur**, développez les nœuds **Stratégies** et **Modèles d'administration**, puis sélectionnez **LAPS**.
21. Double-cliquez sur la stratégie **Enable local admin password management**.
22. Dans la fenêtre **Enable local admin password management**, cliquez sur **Activé**, puis sur **OK**.
23. Double-cliquez sur la stratégie **Password Settings**.
24. Dans la boîte de dialogue de la **stratégie Password Settings**, cliquez sur **Activé** et configurez le paramètre **Password Length** sur **20**.
25. Vérifiez que le paramètre **Password Age** est configuré sur **30**, puis cliquez sur **OK**.
26. Fermez l'**Éditeur de gestion des stratégies de groupe**.
27. Connectez-vous à **LON-SVR2** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
28. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Exécuter**.
29. Dans la boîte de dialogue **Exécuter**, tapez **\\LON-SVR1\d$\Labfiles\Mod02**, puis cliquez sur **OK**.
30. Dans la fenêtre **Mod02**, double-cliquez sur **LAPSx64.msi**.
31. Dans l'assistant **Local Administrator Password Solution Setup**, sur la **Welcome**, cliquez sur **Next**.
32. Sur la page **End-User License Agreement**, cliquez sur **I accept the terms in the License Agreement**, cliquez deux fois sur **Next**, puis sur **Install**.
33. Cliquez sur **Finish** pour fermer le **Local Administrator Password Solution Setup Wizard**.
34. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Exécuter**.
35. Dans la boîte de dialogue **Exécuter**, tapez **gpupdate /force**, puis cliquez sur **OK**.
36. Redémarrez **LON-SVR2**.
37. Passez à **LON-DC1**.
38. Cliquez sur **Démarrer**, sur LAPS, puis sur **LAPS UI**.
39. Dans la boîte de dialogue **LAPS UI**, dans la zone de texte **ComputerName**, tapez **LON-SVR2**, puis cliquez sur **Search**.
40. Vérifiez les valeurs dans les zones **Password** et **Password expires**, puis cliquez sur **Exit**.
41. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :

```
Get-AdmPwdPassword LON-SVR2 | Out-Gridview
```

42. Vérifiez le mot de passe attribué à **LON-SVR2**.

Contrôle des acquis et éléments à retenir

Question de contrôle des acquis

Question : par défaut, les membres de quels groupes de sécurité peuvent utiliser LAPS UI ou Windows PowerShell pour récupérer le mot de passe Administrateur local d'un ordinateur configuré pour utiliser LAPS ?

Réponse : les membres des groupes Admins du domaine et Administrateurs de l'entreprise peuvent récupérer le mot de passe Administrateur local d'un ordinateur configuré pour utiliser LAPS à l'aide de l'application LAPS UI ou de Windows PowerShell.

Questions et réponses relatives à l'atelier pratique

Atelier pratique A : implémentation des droits de l'utilisateur, des options de sécurité et des comptes de service administrés de groupe

Questions et réponses

Question : comment pouvez-vous empêcher certains groupes d'utilisateurs de se connecter à des serveurs contenant des données sensibles ?

> **Réponse :** vous pouvez utiliser la règle Interdire l'ouverture d'une session locale pour empêcher certains groupes d'utilisateurs de se connecter à des serveurs contenant des données sensibles.

Question : quel privilège devriez-vous déléguer si vous souhaitiez allouer l'autorisation de créer, supprimer et gérer des groupes à une équipe spécifique ?

> **Réponse :** vous pourriez déléguer le privilège Créer, supprimer et gérer les groupes au groupe en utilisant l'Assistant Délégation de contrôle.

Atelier pratique B : configuration et déploiement de LAPS

Questions et réponses

Question : quel applet de commande Windows PowerShell utiliser pour configurer une UO spécifique afin que les ordinateurs de cette UO puissent utiliser LAPS ?

> **Réponse :** il faut utiliser l'applet de commande **Set-AdmPwdComputerSelfPermission** pour configurer une UO spécifique afin que les ordinateurs qui ont des comptes dans cette UO puissent utiliser LAPS.

Question : quel applet de commande Windows PowerShell utiliser pour récupérer le mot de passe Administrateur local d'AD DS lorsqu'un ordinateur est configuré pour utiliser LAPS ?

> **Réponse :** il faut utiliser l'applet de commande **Get-AdmPwdPassword** pour récupérer le mot de passe Administrateur local d'AD DS lorsqu'un ordinateur est configuré pour utiliser LAPS.

Module 3

Limitation des droits d'administrateur avec l'administration suffisante (JEA, Just Enough Administration)

Sommaire :

Leçon 1

Présentation de JEA

Sommaire :

Questions et réponses

Question : quelle est l'extension d'un nom de fichier de fonctionnalité de rôle JEA ?

( ) .psrc

( ) .psd1

( ) .pssc

Réponse :

(√) .psrc

( ) .psd1

( ) .pssc

Commentaires :

Les fichiers de fonctionnalité de rôle utilisent l'extension **.psrc**. L'extension **.pssc** est utilisée pour les fichiers de configuration de session. L'extension **.psd1** est utilisée pour les manifestes de module.

Démonstration : création d'un fichier de fonctionnalité de rôle

Étapes de la démonstration

1. Sur **LON-DC1**, cliquez sur **Démarrer**, puis sur **Windows PowerShell ISE**.
2. Agrandissez la fenêtre **Windows PowerShell ISE**.
3. Dans le volet **Windows PowerShell**, tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Cd 'c:\Programmes\WindowsPowerShell\Modules'
Mkdir DNSOps
Cd DNSOps
New-ModuleManifest .\DNSOps.psd1
Mkdir RoleCapabilities
Cd RoleCapabilities
New-PSRoleCapabilityFile -Path .\DNSOps.psrc
Ise DNSOps.psrc
```

4. Dans le volet du script **DNSOps.psrc** de **Windows PowerShell ISE**, placez le curseur sous la ligne commençant par **# VisibleCmdlets =**, puis tapez le texte suivant :

```
VisibleCmdlets = @{ Name = 'Restart-Service'; Parameters = @{ Name='Name';
ValidateSet = 'DNS'}}
```

5. Placez le curseur sous la ligne commençant par **# VisibleFunctions =**, puis tapez le texte suivant :

```
VisibleFunctions = 'Add-DNSServerResourceRecord', 'Clear-DNSServerCache','Get-
DNSServerResourceRecord','Remove-DNSServerResourceRecord'
```

6. Placez le curseur sous la ligne commençant par # **VisibleExternalCommands =**, puis tapez le texte suivant :

```
VisibleExternalCommands = 'C:\Windows\System32\whoami.exe'
```

7. Cliquez sur **Enregistrer**.

Démonstration : création d'un fichier de configuration de session

Étapes de la démonstration

1. Sur **LON-DC1**, dans le volet **Windows PowerShell** de **Windows PowerShell ISE**, tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
New-PSSessionConfigurationFile -Path .\DNSOps.pssc -Full
Ise DNSOps.pssc
```

2. Dans le volet du script **DNSOps.pssc** de **Windows PowerShell ISE**, accédez à la ligne **SessionType = 'Default'** et remplacez-la par **SessionType = 'RestrictedRemoteServer'**.
3. Accédez à la ligne **#RunAsVirtualAccount = $true** et supprimez **#** de façon à ce que la ligne soit : **RunAsVirtualAccount = $true**.
4. Accédez à la ligne commençant par **# RoleDefinitions**, placez le curseur en dessous, puis tapez le texte suivant :

```
RoleDefinitions = @{ 'ADATUM\DNSOps' = @{ RoleCapabilities = 'DNSOps' };}
```

5. Cliquez sur **Enregistrer**.

Démonstration : création d'un point de terminaison JEA

Étapes de la démonstration

1. Dans le volet **Windows PowerShell** de **Windows PowerShell ISE**, tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Register-PSSessionConfiguration -Name DNSOps -Path .\DNSOps.pssc
Restart-Service WinRM
Get-PSSessionConfiguration
```

2. Vérifiez que **DNSOps** est bien répertorié comme point de terminaison Windows PowerShell.

Leçon 2

Vérification et déploiement de JEA

Sommaire :

Questions et réponses

Question : vaut-il mieux créer un point de terminaison JEA avec plusieurs fonctionnalités de rôle ou créer plusieurs points de terminaison JEA, chacun lié à une fonctionnalité de rôle distincte ?

Réponse : les réponses peuvent varier en fonction de l'opinion des stagiaires.

Commentaires : en créant des points de terminaison séparés, il est plus simple de déléguer des tâches individuelles à différentes personnes. Si vous créez un seul point de terminaison JEA lié à plusieurs capacités de rôle, vous pourriez par mégarde assigner des privilèges administratifs inutiles à un ou plusieurs groupes d'utilisateurs.

Démonstration : connexion à un point de terminaison JEA

Étapes de la démonstration

1. Si vous n'êtes pas déjà connecté, connectez-vous à **LON-SVR1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
3. Dans la fenêtre **Windows PowerShell**, tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Enter-PSSession -ComputerName LON-DC1
 (get-command).count
Whoami
Exit-PSSession
```

4. Déconnectez-vous de **LON-SVR1**.
5. Connectez-vous à **LON-SVR1** en tant que **Adatum\Beth** avec le mot de passe **Pa55w.rd**.
6. Cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
7. Dans la fenêtre **Windows PowerShell**, tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Enter-PSSession -ComputerName LON-DC1 -ConfigurationName DNSOps
 (Get-Command).count
WhoAmI
Get-DNSServerResourceRecord -zonename Adatum.com
Add-DNSServerResourceRecord -zonename "Adatum.com" -A -Name "MEL-SVR1" -IPv4Address
"172.16.0.101"
Get-DNSServerResourceRecord -zonename Adatum.com
Restart-Service DNS
Restart-Service WinRM
```

Remarque : vous obtiendrez un message d'erreur en tentant de redémarrer le service Windows Remote Management (WinRM), car le point de terminaison JEA n'est pas configuré pour l'autoriser.

```
Exit-PSsession
```

Démonstration : déploiement d'une configuration JEA sur un autre ordinateur

Étapes de la démonstration

1. Si vous n'êtes pas déjà connecté, connectez-vous à **LON-SVR2** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Exécuter**.
3. Dans la boîte de dialogue **Exécuter**, tapez **\\LON-DC1\c$**, puis cliquez sur **OK**.
4. Dans l'**Explorateur de fichiers**, accédez au dossier **Program Files\WindowsPowerShell\Modules**.
5. Copiez le dossier **DNSOps** dans le dossier local **c:\Programmes\WindowsPowerShell\Modules**.
6. Cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
7. Dans la fenêtre **Windows PowerShell**, tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Cd 'c:\Programmes\WindowsPowerShell\Modules\DNSOps\RoleCapabilities'
Register-PSSessionConfiguration -Name DNSOps -Path .\DNSOps.pssc
Restart-Service WinRM
Get-PSSessionConfiguration
```

8. Vérifiez que **DNSOps** est bien répertorié comme point de terminaison Windows PowerShell.

Contrôle des acquis et éléments à retenir

Question de contrôle des acquis

Question : quel élément de la configuration JEA permet de spécifier les tâches qui peuvent être effectuées lors de la connexion à un point de terminaison JEA ?

Réponse : le fichier de fonctionnalité de rôle permet de spécifier les tâches qui peuvent être effectuées lors de la connexion à un point de terminaison JEA.

Questions et réponses relatives à l'atelier pratique

Atelier pratique : limitation des privilèges d'administrateur avec une administration suffisante (JEA, Just Enough Administration)

Questions et réponses

Question : comment ajouter des fonctions de maintenance de serveur DNS supplémentaires à la configuration JEA ?

Réponse : on modifie le fichier de fonctionnalité de rôle pour ajouter de nouvelles fonctions de maintenance de serveur DNS à la configuration JEA.

Question : quelles commandes vous permettent de vérifier si un compte virtuel est utilisé dans une session JEA ?

Réponse : on peut utiliser la commande **whoami.exe** pour vérifier si un compte virtuel est utilisé dans une session JEA.

Module 4

Gestion des accès privilégiés (PAM, Privileged Access Management) et forêts administratives

Sommaire :

Leçon 1

Forêts ESAE

Sommaire :

Questions et réponses

Question : serait-il intéressant pour vous de déployer une forêt ESAE dans votre environnement pour sécuriser les comptes utilisés pour les tâches d'administration ?

Réponse : les réponses peuvent varier en fonction de votre environnement.

Leçon 2

Vue d’ensemble de Microsoft Identity Manager (MIM)

Sommaire :

Questions et réponses

Question : demandez aux stagiaires s'ils ont déjà déployé MIM ou Forefront Identity Manager (FIM) pour gérer les identités dans leur environnement.

> **Réponse :** les réponses peuvent varier en fonction des spécificités de l'environnement des stagiaires.

Ressources

Configuration requise pour MIM

 **Lectures supplémentaires :** pour plus d'informations sur la configuration requise pour MIM, consultez « Plateformes prises en charge pour MIM 2016 » à l'adresse : http://aka.ms/Armxl4

Leçon 3

Vue d’ensemble de l’administration JIT et de PAM

Sommaire :

Questions et réponses

Question : outre le système d'exploitation du serveur hôte, quels sont les deux produits Microsoft qu'il faut déployer avant de déployer MIM 2016 ?

Réponse : il faut déployer SharePoint et SQL Server avant de déployer MIM 2016.

Démonstration : configuration de la relation d'approbation PAM

Étapes de la démonstration

1. Sur **SYD-MIM**, assurez-vous d'être connecté en tant que **Adatumadmin\MIMAdmin** avec le mot de passe **Pa$$w0rd**, puis ouvrez la fenêtre **Windows PowerShell**.
2. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :

```
$ca = get-credential  –UserName Adatum\Administrator –Message "Adatum forest domain
admin credentials »
```

3. À l'invite, connectez-vous avec le mot de passe **Pa$$w0rd**, puis cliquez sur **OK**.
4. Dans la fenêtre **Windows PowerShell**, tapez les commandes ci-après, puis appuyez sur Entrée après chaque commande (il faut parfois plusieurs minutes pour que certaines commandes s'exécutent, en fonction de la vitesse de vos ordinateurs virtuels) :

```
New-PAMTrust -SourceForest "adatum.com" -Credentials $ca
New-PAMDomainConfiguration -SourceDomain "adatum" -Credentials $ca
Test-PAMTrust -SourceForest "adatum.com" -CorpCredentials $ca
Test-PAMDomainConfiguration -SourceDomain "adatum" -Credentials $ca
```

5. Passez à **MEL-DC1**. À partir de la console **Gestionnaire de serveur**, cliquez sur Outils, puis sur **Utilisateurs et ordinateurs Active Directory**.
6. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur **Adatum.com**, puis cliquez sur **Délégation de contrôle**.
7. Sur la page **Bienvenue !** de l'Assistant **Délégation de contrôle**, cliquez sur **Suivant**.
8. Sur la page **Utilisateurs ou groupes**, cliquez sur **Ajouter**.
9. Dans la boîte de dialogue **Sélectionner les utilisateurs, les ordinateurs ou les groupes**, cliquez sur **Emplacements**.
10. Dans la boîte de dialogue **Emplacements**, cliquez sur **ADATUMADMIN.COM**, puis sur **OK**.
11. Dans la boîte de dialogue **Sélectionner les utilisateurs, les ordinateurs ou les groupes**, tapez **Admins du domaine**, puis cliquez sur **Vérifier les noms**.
12. Dans la boîte de dialogue **Entrer les informations d'identification réseau**, tapez les informations d'identification suivantes, puis cliquez sur **OK** :
    - Nom d'utilisateur : **adatumadmin\administrator**
    - Mot de passe : **Pa$$w0rd**
13. Dans la boîte de dialogue **Sélectionner les utilisateurs, les ordinateurs ou les groupes**, après Admins du domaine, tapez **Mimmonitor**, cliquez sur **Vérifier les noms**, puis sur **OK**.
14. Sur la page **Utilisateurs ou groupes**, cliquez sur **Suivant**.
15. Sur la page **Tâches à déléguer**, sélectionnez **Lire toutes les informations sur l'utilisateur**, cliquez sur **Suivant**, puis sur **Terminer**.

Démonstration : création de principaux d'utilisateur et de principaux fantômes

Étapes de la démonstration

1. Assurez-vous d'être connecté à **MEL-DC1** en tant que **ADATUM\Administrator** avec le mot de passe **Pa$$w0rd**.
2. Dans la barre des tâches, cliquez sur l'icône **Windows PowerShell**.
3. Dans la fenêtre **Windows PowerShell**, tapez les commandes suivantes et appuyez sur Entrée après chacune d'elles :

```
New-ADGroup –name CorpAdmins –GroupCategory Security –GroupScope Global –
SamAccountName CorpAdmins
New-ADUser –SamAccountName Wayne –name Wayne
$jp = ConvertTo-SecureString 'Pa$$w0rd' –asplaintext –force
Set-ADAccountPassword –identity Wayne –NewPassword $jp
Set-ADUser –identity Wayne –Enabled 1 -DisplayName "Wayne"
```

Remarque : un nouveau groupe nommé CorpAdmins sera créé, ainsi qu'un nouvel utilisateur appelé Wayne, qui sera utilisé plus tard pour faire la démonstration de PAM.

4. Passez à **SYD-MIM**. Vous devez être connecté en tant que **Adatum\Administrateur** avec le mot de passe **Pa$$w0rd**.
5. Dans la fenêtre **Windows PowerShell**, tapez les commandes suivantes et appuyez sur Entrée après chacune d'elles :

```
$sj = New-PAMUser –SourceDomain adatum.com –SourceAccountName Wayne
$jp = ConvertTo-SecureString 'Pa$$w0rd' –asplaintext –force
Set-ADAccountPassword –identity priv.Wayne –NewPassword $jp
Set-ADUser –identity priv.Wayne –Enabled 1
$ca = get-credential –UserName Adatum\Administrator –Message "Informations
d'identification d'administration de domaine de la forêt Adatum"
```

6. Dans la boîte de dialogue, connectez-vous avec le mot de passe **Pa$$w0rd**, puis cliquez sur **OK**.
7. Dans la fenêtre **Windows PowerShell**, tapez les commandes suivantes et appuyez sur Entrée après chacune d'elles :

```
$pg = New-PAMGroup –SourceGroupName "CorpAdmins" –SourceDomain adatum.com –SourceDC
mel-dc1.adatum.com –Credentials $ca
$pr = New-PAMRole –DisplayName "CorpAdmins" –Privileges $pg –Candidates $sj
```

8. Passez à **SYD-DC1**.
9. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
10. Ouvrez le conteneur **PAM Objects** et vérifiez que le groupe **Adatum.CorpAdmins** et l'utilisateur **PRIV.Wayne** y sont bien présents.
11. Si aucune fenêtre **Windows PowerShell** n'est ouverte, ouvrez-en une et tapez les commandes suivantes en appuyant sur Entrée après chacune d'elles :

```
Get-ADGroup -identity Adatum.corpadmins -properties SIDHistory
Get-ADGroup -server mel-dc1.adatum.com -identity corpadmins
```

Remarque : la valeur SID du groupe Adatum et la valeur de l'historique SID du groupe ADATUMADMINS sont identiques.

Démonstration : configuration et demande d'accès privilégié

Étapes de la démonstration

1. Assurez-vous d'être connecté à **MEL-SVR1** en tant que **Adatum\administrator** avec le mot de passe **Pa$$w0rd**.
2. Cliquez sur l'icône de l'Explorateur de fichiers dans la barre des tâches et double-cliquez sur **Lecteur de DVD (D:) MIM2016-EVAL**.
3. Double-cliquez sur le fichier .htm et, dans la boîte de dialogue **Internet Explorer**, cliquez sur **Yes**.
4. Sur la page **Microsoft Identity Manager**, cliquez sur **Install Add-ins and Extensions, 64-bit**.
5. Dans la boîte de dialogue **Voulez-vous exécuter ou enregistrer setup.exe ?**, cliquez sur **Exécuter**.
6. Sur la page **Bienvenue dans l'Assistant Installation des compléments et extensions Microsoft Identity Manager** de **Assistant Microsoft Identity Manager 2016**, cliquez sur **Suivant**.
7. Sur la page **Contrat de licence utilisateur final**, cliquez sur **J'accepte les termes du contrat de licence**, puis sur **Suivant**.
8. Sur la page **Programme d'amélioration de l'expérience utilisateur MIM**, cliquez sur **Je ne souhaite pas participer au programme pour le moment**, puis sur **Suivant**.
9. Sur la page **Installation personnalisée**, cliquez sur **MIM Add-in for Outlook**, puis sur **La característica completa no estará disponible**.
10. Sur la page **Installation personnalisée**, cliquez sur **MIM Password and Authentication**, puis sur **La característica completa no estará disponible**.
11. Sur la page **Installation personnalisée**, cliquez sur **PAM Client**, puis sur **Installation sur le disque dur local**, et enfin sur **Suivant**.
12. Sur la page **Configurez l'adresse de service MIM PAM**, configurez les paramètres suivants, puis cliquez sur **Suivant** :
    - Adresse du serveur PAM : **syd-mim.adatumadmin.com**
    - Port: **5725**
13. Cliquez sur **Installer**, puis, à la fin de l'installation, sur **Terminer**.
14. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Gestion de l'ordinateur**.
15. Dans la console **Gestion de l'ordinateur**, développez **Utilisateurs et groupes locaux**, puis cliquez sur **Groupes**. Double-cliquez sur le groupe **Administrators**.
16. Dans la boîte de dialogue **Propriétés de : Administrators**, cliquez sur **Ajouter**.
17. Dans la boîte de dialogue **Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, tapez **adatumadmin\adatum.corpadmins**, puis cliquez sur Vérifier les noms.
18. Saisissez l'identifiant de connexion **adatumadmin\administrator** et le mot de passe **Pa$$w0rd**, puis cliquez sur **OK** à trois reprises.
19. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Arrêter ou se déconnecter**, et enfin sur **Redémarrer**. Fournissez l'**Atelier pratique**.
20. Connectez-vous à **MEL-SVR1** en tant que **Adatum\Wayne** avec le mot de passe **Pa$$w0rd**.
21. Dans la **barre des tâches**, cliquez sur **Windows PowerShell**, puis, dans la fenêtre **Windows PowerShell**, tapez la commande suivante et appuyez sur Entrée :

```
Whoami /groups
```

22. Vérifiez que le compte **Wayne** n'est pas membre du groupe **CorpAdmins**.
23. Dans la **barre des tâches**, cliquez sur **Gestionnaire de serveur**.
24. Dans le menu **Gérer** de la console **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
25. Sur la page **Avant de commencer**, cliquez sur **Suivant** à quatre reprises.
26. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Serveurs WINS**. Dans la boîte de dialogue **Ajouter des rôles et des fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**.
27. Cliquez sur **Suivant**, puis sur **Installer**.
28. Lisez le message qui vous informe que vous n'avez pas les droits d'utilisateur adéquats pour effectuer des modifications sur l'ordinateur cible, puis cliquez sur **Fermer**.
29. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Arrêter ou fermer la session**, et enfin sur **Fermer la session**.
30. Connectez-vous à **MEL-SVR1** en tant que **ADATUMADMIN\priv.Wayne** avec le mot de passe **Pa$$w0rd**.
31. Dans la **barre des tâches**, cliquez sur **Windows PowerShell**, puis, dans la fenêtre **Windows PowerShell**, tapez la commande suivante et appuyez sur Entrée :

```
Whoami /groups
```

32. Vérifiez que le compte n'est pas membre du groupe **CorpAdmins**.
33. Dans la **barre des tâches**, cliquez sur **Gestionnaire de serveur**.
34. Dans le menu **Gérer** de la console **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
35. Sur la page **Avant de commencer**, cliquez sur **Suivant** à quatre reprises.
36. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Serveurs WINS**.
37. Dans la boîte de dialogue **Ajouter des rôles et des fonctionnalités,** cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**, et enfin sur **Installer**.
38. Lisez le message qui vous informe que vous n'avez pas les droits d'utilisateur adéquats pour effectuer des modifications sur l'ordinateur cible, puis cliquez sur **Fermer**.
39. Dans la fenêtre **Windows PowerShell**, tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Import-Module MIMPAM
Get-PAMRoleForRequest
```

Remarque : une liste de rôles auxquels le compte **priv.Wayne** peut s'appliquer s'affiche. Remarquez la durée de vie (TTL) du rôle affiché.

40. Dans la fenêtre **Windows PowerShell**, tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
New-PamRequest -RoleDisplayName CorpAdmins
```

Remarque : le statut de la demande est défini sur **Traitement en cours**.

41. Cliquez avec le bouton droit sur **Démarrer**, cliquez sur **Arrêter ou se déconnecter**, puis sur **Se déconnecter**.
42. Connectez-vous à **MEL-SVR1** en tant que **ADATUMADMIN\priv.Wayne** avec le mot de passe **Pa$$w0rd**.
43. Dans la **barre des tâches**, cliquez sur **Windows PowerShell**, puis, dans la fenêtre **Windows PowerShell**, tapez la commande suivante et appuyez sur Entrée :

```
Whoami /groups
```

44. Vérifiez que le compte est membre du groupe **CorpAdmins**.
45. Dans la **barre des tâches**, cliquez sur **Gestionnaire de serveur**.
46. Dans le menu **Gérer** de la console **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
47. Sur la page **Avant de commencer**, cliquez sur **Suivant** à quatre reprises.
48. Sur la page **Sélectionner des fonctionnalités**, cliquez sur **Serveurs WINS**.
49. Dans la boîte de dialogue **Ajouter des rôles et des fonctionnalités,** cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant**, et enfin sur **Installer**.
50. Lorsque la fonctionnalité est installée, cliquez sur **Fermer**.

Démonstration : gestion des rôles PAM

Étapes de la démonstration

1. Passez à **MEL-DC1** et vérifiez que vous êtes connecté en tant que **ADATUM\Administrator**.
2. Dans la fenêtre **Windows PowerShell**, tapez les commandes suivantes et appuyez sur Entrée après chacune d'elles :

```
New-ADUser –SamAccountName Gavin –name Gavin
$jp = ConvertTo-SecureString 'Pa$$w0rd' –asplaintext –force
Set-ADAccountPassword –identity Gavin –NewPassword $jp
Set-ADUser –identity Gavin –Enabled 1 -DisplayName "Gavin"
```

Remarque : ce jeu de commandes permet de créer un utilisateur nommé Gavin que vous autoriserez à accéder à PAM.

3. Passez à **SYD-MIM** et assurez-vous que vous êtes connecté en tant que **ADATUMADMIN\MIMAdmin**.
4. Dans la fenêtre **Windows PowerShell**, tapez les commandes suivantes et appuyez sur Entrée après chacune d'elles :

```
$sj = New-PAMUser –SourceDomain adatum.com –SourceAccountName Gavin
$jp = ConvertTo-SecureString 'Pa$$w0rd' –asplaintext –force
Set-ADAccountPassword –identity priv.Gavin –NewPassword $jp
Set-ADUser –identity priv.Gavin –Enabled 1
```

5. Démarrez **Internet Explorer** et accédez à la page **http://syd-mim.adatumadmin.com:82/IdentityManagement/default.aspx**.
6. En cas d'invite, connectez-vous en tant que **ADATUMADMIN\Mimadmin** avec le mot de passe **Pa$$w0rd**.

7. Dans la console **Microsoft Identity Manager**, cliquez sur **PAM Roles** sous **Privileged Access Management**.
8. Dans la liste de rôles **Privileged Access Management**, cliquez sur **CorpAdmins**.
9. Dans l'onglet **General** de la boîte de dialogue **Corpadmins**, changez le paramètre **PAM Role TTL(sec)** de **3600** à **600**, puis cliquez sur **OK**, et enfin sur **Submit**.

Remarque : au cours de la démonstration, vous pouvez également décrire la fonction des autres champs.

10. Dans la liste de rôles **Privileged Access Management**, cliquez sur **Corpadmins**.
11. Dans l'onglet **Candidates** de la boîte de dialogue **Corpadmins**, cliquez sur **Browse**.
12. Dans la boîte de dialogue **Select Users**, cliquez sur la loupe à côté de Search. Wayne et Adatum.Wayne doivent être déjà sélectionnés. Sélectionnez **ADATUM.Gavin** et **Gavin**, puis cliquez sur **OK** à deux reprises et enfin sur **Submit**.
13. Cliquez sur **OK** pour fermer la boîte de dialogue **CorpAdmins**.
14. Sous **Privileged Access Management**, cliquez sur **PAM Requests**.
15. Consultez les requêtes dans **PAM Requests**.
16. Cliquez sur **PRIV.Wayne** et consultez la date de création de la demande, sa date d'expiration et le rôle requis.

Contrôle des acquis et éléments à retenir

Question de contrôle des acquis

Question : quel est le nombre minimum de forêts requises pour déployer PAM ?

Réponse : il faut un minimum de deux forêts pour déployer PAM, la forêt administrative dans laquelle PAM est déployé et la forêt de production.

Questions et réponses relatives à l'atelier pratique

Atelier pratique : limitation des privilèges d'administrateur avec PAM

Questions et réponses

Question : quelle démarche feriez-vous pour vous assurer qu'un utilisateur demandant un rôle PAM a accès à ce rôle pour deux heures au lieu d'une seule ?

Réponse : vous modifieriez la durée de vie (TTL) du rôle sur deux heures.

Question : où peut-on voir les utilisateurs qui se sont vu accorder des rôles PAM ?

Réponse : vous pouvez utiliser la section PAM Requests, sous la zone Privileged Access Management dans la console MIM.

Module 5

Endiguement des programmes malveillants et des menaces

Sommaire :

Leçon 1

Configuration et gestion de Windows Defender

Sommaire :

Questions et réponses

Question : quelles sont les options d'analyse disponibles lorsque vous utilisez Windows Defender ?

Réponse : les options d'analyse sont décrites dans le tableau suivant :

Option d'analyse	Description
Rapide	Vérifie les zones que les programmes malveillants, notamment les virus, les logiciels espions et les logiciels indésirables, sont les plus susceptibles d'infecter.
Complète	Vérifie tous les fichiers sur votre disque dur et tous les programmes en cours d'exécution.
Personnalisée	Permet aux utilisateurs d'analyser des lecteurs et dossiers spécifiques.

Démonstration : utilisation de Windows Defender

Étapes de la démonstration

1. Passez à **LON-CL1**.
2. Cliquez avec le bouton droit sur **Démarrer**, puis sur **Panneau de configuration**.
3. Cliquez sur **Afficher par**, sélectionnez **Grandes icônes**, puis cliquez sur **Windows Defender**.
4. Cliquez sur **Fermer** dans la boîte de dialogue **Nouveautés**.
5. Dans l'onglet **Accueil** de Windows Defender, vérifiez que l'option d'analyse **Rapide** est sélectionnée.
6. Cliquez sur **Analyser maintenant**, puis examinez les résultats.
7. Fermez Windows Defender.
8. Ouvrez l'Explorateur de fichiers, puis accédez à **C:\Files**.
9. Dans le dossier **Files**, ouvrez le fichier **sample.txt** dans le Bloc-notes. Le fichier **sample.txt** contient une chaîne de texte utilisée pour tester la détection des programmes malveillants.
10. Dans le fichier **sample.txt**, supprimez les deux instances **<remove>** y compris les chevrons, les lignes supplémentaires et les espaces vides.
11. Enregistrez et fermez le fichier. Windows Defender détecte immédiatement une menace potentielle.
12. Windows Defender supprime alors **sample.txt** du dossier **Files**.
13. Cliquez avec le bouton droit sur **Démarrer**, puis sur **Panneau de configuration**.
14. Cliquez sur **Windows Defender**.
15. Dans Windows Defender, cliquez sur l'onglet **Historique**.
16. Cliquez sur **Afficher les détails**, puis examinez les résultats.
17. Activez la case à cocher **Virus:DOS/EICAR_Test_File**, puis cliquez sur **Supprimer**.
18. Fermez toutes les fenêtres.

Leçon 2

Restriction logicielle

Sommaire :

Ressources

Qu'est-ce qu'AppLocker ?

Lectures supplémentaires : pour plus d'informations concernant AppLocker, consultez « AppLocker Overview » : http://aka.ms/Amf8jf

Démonstration : création de règles AppLocker

Étapes de la démonstration

Créer un GPO afin d'appliquer les règles AppLocker par défaut pour les fichiers exécutables

1. Sur **LON□DC1**, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans la **Console de gestion des stratégies de groupe (GPMC)**, cherchez **Forêt : Adatum.com\Domains\Adatum.com**.
3. Cliquez sur **Objets de stratégie de groupe**, cliquez avec le bouton droit sur **Objets de stratégie de groupe**, puis cliquez sur **Nouveau**.
4. Dans le menu contextuel **Nouvel objet GPO**, dans la zone de texte **Nom**, saisissez **Stratégie de restriction WordPad,** puis cliquez sur **OK**.
5. Cliquez avec le bouton droit sur **Stratégie de restriction WordPad**, puis cliquez sur **Modifier**.
6. Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de contrôle de l'application\AppLocker**.
7. Cliquez sur **Règles de l'exécutable**, cliquez avec le bouton droit sur **Règles de l'exécutable**, puis sélectionnez **Créer une règle**.
8. Sur la page **Avant de commencer**, cliquez sur **Suivant**.
9. Sur la page des **Autorisations**, cliquez sur **Refuser**, puis sur **Suivant**.
10. Sur la page **Conditions**, cliquez sur **Éditeur**, puis sur **Suivant**.
11. Sur la page **Éditeur**, cliquez sur **Parcourir**, puis sur **Ce PC**.
12. Sur la page **Ouvrir**, double-cliquez sur **Disque local (C:)**.
13. Sur la page **Ouvrir**, double-cliquez sur **Program Files**, sur **Windows NT**, puis sur **Accessories**. Cliquez sur **wordpad.exe**, puis sur **Ouvrir**.
14. Déplacez le curseur vers le haut sur l'emplacement du **nom du fichier**, puis cliquez sur **Suivant**.
15. Cliquez à nouveau sur **Suivant**, puis cliquez sur **Créer**.
16. À l'invite de création des règles par défaut, cliquez sur **Oui**.
17. Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité**.
18. Développez **Stratégies de contrôle de l'application**, cliquez avec le bouton droit sur **AppLocker**, puis sélectionnez **Propriétés**.
19. Dans l'onglet **Contrôle obligatoire**, sous **Règles de l'exécutable**, activez la case à cocher **Configuré**, cliquez sur **Appliquer les règles**, puis sur **OK**.

20. Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, accédez à **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité**.
21. Cliquez sur **Services système**, puis double-cliquez sur **Identité de l'application**.
22. Dans la boîte de dialogue **Propriétés de : Identité de l'application**, au-dessus de **Sélectionnez le mode de démarrage du service**, cliquez sur **Définir ce paramètre de stratégie**, cliquez sur **Automatique**, puis sur **OK**.
23. Fermez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.

Appliquer le GPO au domaine

1. Dans la console **GPMC**, développez **Forêt : Adatum.com**, développez **Domaines**, **Adatum.com**, puis **Objets de stratégie de groupe**.
2. Dans la console **GPMC**, cliquez avec le bouton droit sur **Adatum.com**, puis sur **Lier un objet de stratégie de groupe existant**.
3. Dans la fenêtre **Sélectionner un objet GPO**, dans la fenêtre **Objets de stratégie de groupe**, cliquez sur **Stratégie de restriction WordPad**, puis sur **OK**.
4. Fermez la console **GPMC**.
5. Passez à l'écran **Démarrer** et tapez **cmd**, puis appuyez sur Entrée.
6. Dans la fenêtre **d'invite de commandes**, saisissez **gpupdate /force**, puis appuyez sur Entrée. Attendez que la stratégie soit mise à jour.

Tester la règle AppLocker

1. Connectez-vous à **LON-CL1** en tant que **Adatum\Beth** avec le mot de passe **Pa55w.rd**.
2. Dans la zone de texte **Rechercher**, tapez **cmd**, puis appuyez sur Entrée.
3. Dans la fenêtre **d'invite de commandes**, saisissez **gpupdate /force**, puis appuyez sur Entrée. Attendez que la stratégie soit mise à jour.
4. Dans la zone de texte **Rechercher**, tapez **WordPad**, puis appuyez sur Entrée. Remarquez que WordPad ne démarre pas.

 **Remarque :** il faut quelques minutes pour que gpupdate prenne effet. Si WordPad se lance, attendez une minute, puis réessayez.

Leçon 3

Configuration et utilisation de la fonctionnalité Device Guard

Sommaire :

Ressources

Implémentation de stratégies Device Guard

Lectures supplémentaires : pour plus d'informations, consultez « Configurable Code Integrity Policy for Windows PowerShell » à l'adresse : http://aka.ms/U0nker

Règles du fichier d'intégrité du code

Lectures supplémentaires : pour plus d'informations, consultez « Ajouter des applications non signées à la stratégie d'intégrité du code » à l'adresse : http://aka.ms/Tkie2j

Liens de référence : Pour télécharger un exemplaire de **signtool.exe**, consultez SignTool à l'adresse : http://aka.ms/S4ihkk

Démonstration : création de règles du fichier d'intégrité du code

Étapes de la démonstration

1. Sur **LON-DC1**, ouvrez l'écran **Démarrer** et sélectionnez **Windows PowerShell**.
2. Dans Windows PowerShell, tapez les commandes suivantes et appuyez sur Entrée après chacune d'elles :

```
$CIPolicyPath=$env:userprofile+"\Desktop\"
$InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"
$CIPolicyBin=$CIPolicyPath+"DeviceGuardPolicy.bin"
```

3. Analysez les applications installées sur votre appareil. Créez une stratégie d'intégrité du code en tapant la commande suivante, puis appuyez sur Entrée :

```
New-CIPolicy -Audit -Level Hash -FilePath $InitialCIPolicy -UserPEs -Fallback Hash 3>
Warningslog.txt
```

4. Validez la stratégie d'intégrité du code au format binaire en tapant la commande suivante, puis appuyez sur Entrée :

```
ConvertFrom-CIPolicy $InitialCIPolicy $CIPolicyBin
```

5. Après ces étapes, fermez Windows PowerShell. Le fichier de stratégie Device Guard (**DeviceGuardPolicy.bin**) et le fichier .xml original (**InitialScan.xml**) seront disponibles sur votre bureau.
6. Ouvrez le fichier **InitialScan.xml** situé sur le bureau. Vous pouvez l'ouvrir en cliquant sur l'icône de l'Explorateur de fichiers dans la barre des tâches, puis en saisissant **C:\Utilisateurs\Administrator\Bureau\InitialScan.xml** dans la case **Accès rapide** et en appuyant sur Entrée.

   Vous remarquerez que les rôles actuels pour **SIPolicy** sont définis avec le **mode audit** activé.
7. Sur l'écran d'accueil, sélectionnez **Windows PowerShell**.
8. Dans la fenêtre **Windows PowerShell**, saisissez l'applet de commande et le paramètre suivants pour afficher les options de règle :

```
Set-RuleOption -Help
```

9. Vérifiez la sortie de la commande et remarquez que le **mode audit** est défini dans la règle 3.

10. Dans Windows PowerShell, tapez les commandes suivantes et appuyez sur Entrée après chacune d'elles :

```
# Initialisez les variables qui seront utilisées
$CIPolicyPath=$env:userprofile+"\Desktop\"
$InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"
$CIPolicyBin=$CIPolicyPath+"DeviceGuardPolicy.bin"
$EnforcedCIPolicy=$CIPolicyPath+"EnforcedPolicy.xml”
$CIEnforceBin = $CIPolicyPath + “EnforceDeviceGuardPolicy.bin”
# Copiez le premier fichier pour conserver une copie de l’original
cp $InitialCIPolicy $EnforcedCIPolicy
# Retirez le mode audit
Set-RuleOption -Option 3 -FilePath $EnforcedCIPolicy -Delete
# Convertissez la nouvelle stratégie de code au format binaire
ConvertFrom-CIPolicy $EnforcedCIPolicy $CIEnforceBin
```

11. Ouvrez le fichier **EnforcedPolicy.xml** situé sur le bureau, puis assurez-vous qu'il ne contient plus le **mode audit**.

Leçon 4

Déploiement et utilisation de la trousse à outils EMET

Sommaire :

Démonstration : protection des applications avec la trousse à outils EMET

Étapes de la démonstration

1. Sur **22744B-LON-DC1**, installez le fichier **EMET Setup.msi** situé dans **E:\Labfiles\Mod05**.
2. Une fois l'installation terminée, sélectionnez **Configure Manually Later**, cliquez sur **Finish**, puis sur **Close**.
3. Dans la zone de notification en bas à droite, cliquez avec le bouton droit sur l'icône, puis sélectionnez **Open EMET**.
4. Cliquez sur **Apps** dans la barre de menu supérieure, puis consultez les applications configurées dans la trousse à outils EMET.
5. Fermez la fenêtre **Application Configuration**.
6. Cliquez sur **Import** dans le coin supérieur gauche de la trousse à outils EMET. Étudiez les trois options disponibles. Sélectionnez **Recommended Software.xml**, puis cliquez sur **Ouvrir**.
7. Cliquez sur **Apps** dans la barre de menu supérieure, puis consultez les applications configurées dans la trousse à outils EMET.
8. Vous remarquerez que l'exécutable de Windows PowerShell n'est pas inclus. Cliquez sur **Add Application**. Dans la case **Nom du fichier**, tapez **C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe**.
9. Cliquez sur **Ouvrir**, puis sur **OK**.
10. Cliquez sur **Démarrer**. Cliquez sur l'icône **Windows PowerShell**. Une fois l'application chargée, réduisez-la dans la zone de notification.
11. Sur la page **Enhanced Mitigation Experience Toolkit**, cliquez sur **Refresh**. Vous devriez voir maintenant **PowerShell – Windows PowerShell** sous **Running Processes**.

Contrôle des acquis et éléments à retenir

Meilleure pratique

Lorsque vous utilisez la trousse à outils EMET dans votre entreprise, vous devez utiliser des GPO pour déployer des configurations cohérentes dans tout votre environnement.

Question de contrôle des acquis

Question : quelle est la meilleure façon de déployer la trousse à outils EMET dans une grande entreprise ?

> **Réponse :** il faut utiliser une stratégie de groupe ou Microsoft System Center Configuration Manager. Les versions actuelles disposent d'une prise en charge intégrée pour les stratégies de groupe et Microsoft System Center Configuration Manager.

Problèmes et scénarios réels

Dans le monde entier, on signale de nouveaux programmes malveillants utilisés pour exploiter les vulnérabilités des entreprises. Il est important de consulter la dernière Synthèse des Bulletins de sécurité Microsoft pour en savoir plus sur les vulnérabilités existantes de votre système et être au courant des dernières informations sur les technologies anti-programme malveillant et leurs mises à jour.

Outils

De nombreux outils peuvent être utilisés pour exploiter les vulnérabilités d'un système Windows. Kali Linux, distribué gratuitement, inclut plusieurs outils que les administrateurs Windows peuvent utiliser pour tester la sécurité de leur système.

Questions et réponses relatives à l'atelier pratique

Atelier pratique : Sécurisation des applications avec AppLocker, Windows Defender, les règles Device Guard et la trousse à outils EMET

Questions et réponses

Question : l'atelier comprend plusieurs options que vous pouvez utiliser pour éviter les programmes malveillants. Quelle solution utilise des technologies de réduction des risques pour la sécurité afin de rendre l'exploitation de failles aussi difficile que possible ?

> **Réponse :** la trousse à outils EMET. Elle complique beaucoup l'exploitation des failles, mais les technologies de réduction des risques pour la sécurité ne garantissent pas que des personnes malveillantes ne puissent pas exploiter des vulnérabilités.

Question : quelles technologies présentées dans ce module se complètent pour lutter contre les programmes malveillants ?

> **Réponse :** Windows Defender, AppLocker, la trousse à outils EMET et Device Guard sont conçus pour se compléter afin de lutter contre les programmes malveillants sur un système Windows.

Module 6

Analyse de l'activité avec audit avancé et Log Analytics

Sommaire :

Leçon 1

Vue d’ensemble de l’audit

Sommaire :

Démonstration : localisation d'événements dans le journal de sécurité

Étapes de la démonstration

1. Sur LON-SVR1, dans la barre des tâches, cliquez sur **Explorateur de fichiers**.
2. Dans le volet de navigation, cliquez sur **Ce PC**.
3. Double-cliquez sur **Allfiles (D:)**.
4. Cliquez avec le bouton droit sur **Labfiles**, puis cliquez sur **Propriétés**.
5. Cliquez sur l'onglet **Partage**, puis sur **Partager**.
6. Dans la zone, tapez **Abbi**, puis cliquez sur **Ajouter**.

Remarque : Abbi Skinner doit avoir des droits d'accès en lecture.

7. Cliquez sur **Partager**.
8. Cliquez sur **Modifier les paramètres**, puis sur **Terminé**, et enfin sur Fermer.
9. Cliquez avec le bouton droit sur **Labfiles**, cliquez sur **Propriétés**, puis sur l'onglet **Sécurité**, et enfin sur **Avancé**.
10. Sélectionnez l'onglet **Audit**, puis cliquez sur **Ajouter**.
11. Cliquez sur **Sélectionnez un principal**. Dans la zone, tapez **Tout le monde**, puis cliquez sur **OK**.
12. Sous **Type**, sélectionnez **Tous**, puis cliquez sur **OK**.
13. Cliquez sur **OK** à deux reprises.
14. Sur LON-DC1, dans le Gestionnaire de serveurs, cliquez sur **Outils**, puis sélectionnez **Gestion des stratégies de groupe**.
15. Développez **Forêt : Adatum.com**, puis **Domaines**, puis **Adatum.com**, sélectionnez et cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
16. Développez Configuration ordinateur, puis Stratégies, puis Paramètres Windows, puis Paramètres de sécurité, et enfin Stratégies locales.
17. Cliquez sur Stratégie d'audit.
18. Double-cliquez sur Auditer l'accès aux objets, puis activez la case à cocher Définir ces paramètres de stratégie.
19. Sélectionnez **Succès** et **Échec**, puis cliquez sur **OK**.
20. Ouvrez une invite de commandes Windows, tapez la commande suivante, puis appuyez sur Entrée.

```
GPUpdate /Force
```

Remarque : vous pouvez également configurer cela dans la configuration de la stratégie d'audit avancé, située dans **Ordinateur** > **Stratégies** > **Paramètres Windows** > **Paramètres de sécurité** > **Configuration avancée de la stratégie Configuration**.

21. Connectez-vous à LON-CL1 en tant que **Abbi** avec le mot de passe **Pa55w.rd.**
22. Dans l'Explorateur de fichiers, ouvrez \\lon-svr1\Labfiles\Mod01\logonSessions.zip.

23. Déconnectez-vous de LON-CL1.
24. Connectez-vous à LON-CL1 en tant que **Beth** avec le mot de passe **Pa55w.rd.**
25. Dans l'Explorateur de fichiers, tentez d'ouvrir **\\lon-svr1\Labfiles\.**
26. Au message d'erreur, cliquez sur Fermer.
27. Sur LON-DC1, dans le **Gestionnaire de serveurs**, cliquez sur **Outils**, puis sélectionnez **Observateur d'événements**.
28. Développez **Journaux Windows**, puis cliquez sur **Sécurité.**
29. Examinez plusieurs événements, dont les événements de succès et d'échec (si disponibles).

Leçon 2

Audit avancé

Sommaire :

Ressources

Services ACS

Lectures supplémentaires : pour plus d'informations sur les services ACS, consultez « How to Install an Audit Collection Services (ACS) Collector and Database » à l'adresse : http://aka.ms/Jwghcp

Démonstration : configuration d'un audit avancé

Étapes de la démonstration

1. Sur LON-DC1, dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
2. Dans Gestion des stratégies de groupe, double-cliquez sur **Forêt : Adatum.com**, puis sur **Domaines**, puis sur **Adatum.com**, puis cliquez avec le bouton droit sur **Objets de stratégie de groupe**, et enfin cliquez sur **Nouveau**.
3. Dans la fenêtre **Nouvel objet GPO**, tapez **Audit de fichier** dans la zone **Nom**, puis appuyez sur Entrée.
4. Double-cliquez sur le conteneur **Objets de stratégie de groupe**, cliquez avec le bouton droit sur **Audit de fichier**, puis cliquez sur **Modifier**.
5. Dans la fenêtre de l'Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, développez **Stratégies**, puis **Paramètres Windows**, puis **Paramètres de sécurité**, puis **Configuration avancée de la stratégie d'audit**, puis **Stratégies d'audit** et cliquez sur **Accès à l'objet**.
6. Double-cliquez sur **Auditer le partage de fichiers détaillé**.
7. Dans la fenêtre **Propriétés**, activez la case à cocher **Configurer les événements d'audit suivants**.
8. Activez les cases à cocher **Succès** et **Échec**, puis cliquez sur **OK**.
9. Double-cliquez sur **Auditer le stockage amovible**.
10. Dans la fenêtre **Propriétés**, activez la case à cocher **Configurer les événements d'audit suivants**.
11. Activez les cases à cocher **Succès** et **Échec**, puis cliquez sur **OK**.
12. Fermez l'Éditeur de gestion des stratégies de groupe.
13. Fermez Gestion des stratégies de groupe.

Démonstration : transfert du journal des événements

Étapes de la démonstration

1. Sur LON-SVR1, cliquez sur Démarrer, puis sur **Windows PowerShell**.
2. Tapez les commandes suivantes, puis appuyez sur Entrée :

```
winrm quickconfig
```

3. Connectez-vous à LON-DC1, puis cliquez sur **Démarrer**.
4. Cliquez sur **Windows PowerShell**, tapez la commande suivante et appuyez sur Entrée :

```
Wecutil qc
```

5. Tapez O à l'invite Le mode de démarrage du service sera changé en Delay-Start. Voulez-vous continuer (O- oui ou N- non) ?
6. Tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Winrm id -remote:lon-svr1
Winrm enumerate winrm/config/listener
```

7. Connectez-vous à LON-SVR1. Sélectionnez la fenêtre **Windows PowerShell**, tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Winrm id -remote:lon-dc1
Winrm enumerate winrm/config/listener
Shutdown -r
```

8. Passez à LON-DC1 et continuez d'utiliser **Windows PowerShell**. Tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
net localgroup "event log readers" LON-DC1$ /add
shutdown -r
```

9. Après le redémarrage de LON-SVR1, reconnectez-vous en tant que **adatum\administrator** avec le mot de passe **Pa55w.rd**.
10. Après le redémarrage de LON-DC1, reconnectez-vous en tant que **adatum\administrator** avec le mot de passe **Pa55w.rd**.
11. Sur LON-DC1, attendez que le **Gestionnaire de serveur** s'ouvre.
12. Cliquez sur **Outils**, puis sélectionnez **Observateur d'événements**.
13. Dans l'arborescence de la console, cliquez sur **Abonnements.** Si vous y êtes invité, cliquez sur **Oui**.
14. Dans le menu **Actions**, cliquez sur **Créer un abonnement**.
15. Dans la zone **Nom d'abonnement**, tapez **LogDemo** comme nom d'abonnement.
16. Dans la zone **Description**, tapez une description (facultatif).
17. Dans la zone **Journal de destination**, assurez-vous que le fichier journal spécifie le journal par défaut **ForwardedEvents**.
18. Cliquez sur **Sélection des ordinateurs**.
19. Cliquez sur **Ajouter des ordinateurs du domaine**, tapez **LON-SVR1**, cliquez sur **Vérifier les noms**, puis cliquez sur **OK** à deux reprises.
20. Cliquez sur **Sélectionner des événements** pour afficher la boîte de dialogue **Filtre de requête**.
21. Utilisez les contrôles de la boîte de dialogue **Filtre de requête** pour spécifier les critères que doivent respecter les événements pour être collectés (**Critique**, **Avertissement**, **Erreur**) pour cette démonstration. En regard de **Journaux d'événements**, sélectionnez **Application** et **Sécurité**. Cliquez sur **OK**.
22. Dans la boîte de dialogue **Propriétés de l'abonnement**, cliquez sur **OK**. L'abonnement est alors ajouté au volet **Abonnements**. Si l'opération a réussi, l'abonnement prend le statut **Actif**.
23. Sur LON-SVR1, cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (admin)**.
24. Tapez la commande suivante, puis appuyez sur Entrée.

```
Eventcreate /id 999 /t error /l application /d "Error test event"
```

25. Au bout de quelques minutes, retournez sur LON-DC1, puis consultez les événements transférés depuis LON-SVR1. Vous les trouverez sous **Événements transférés** dans le nœud **Journaux Windows**.

Remarque : il faut parfois 15 à 20 minutes pour que les événements apparaissent sur LON-DC1.

Leçon 3

Audit et journalisation de Windows PowerShell

Sommaire :

Démonstration : gestion d'un audit avec Windows PowerShell

Étapes de la démonstration

1. Ouvrez le Gestionnaire de serveur et cliquez sur **Outils**, puis sélectionnez **Observateur d'événements**.
2. Consultez les journaux Windows sous **Système**.
3. Cliquez sur **Démarrer**, puis sélectionnez **Windows PowerShell**.
4. Tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Get-EventLog Security -newest 20
Get-EventLog System -newest 20 | Format-List
Get-EventLog "Windows PowerShell" | Group-Object eventid | Sort-Object Name
```

Démonstration : configuration de la journalisation des transcriptions, modules et blocs de script

Étapes de la démonstration

1. Si nécessaire, connectez-vous à LON-DC1 en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Basculez vers la fenêtre **Windows PowerShell**.
3. Entrez la commande suivante, puis appuyez sur Entrée :

```
Get-Module Microsoft.* |
Select Name, LogPipelineExecutionDetails
```

4. Consultez la sortie et remarquez le statut de **LogPipelineExecutionDetails**.
5. Tapez les commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
Get-Module Microsoft.* | ForEach {
  $_.LogPipelineExecutionDetails = $True
}
Get-Module Microsoft.* |
Select Name, LogPipelineExecutionDetails
```

6. Consultez la sortie, puis tapez les commandes suivantes en appuyant sur Entrée après chacune d'elles :

```
Get-EventLog Security -newest 100
Get-ChildItem -Path C:\inetpub\wwwroot
```

7. Consultez le journal des événements.
8. Retournez dans Windows PowerShell, puis tapez la commande suivante et appuyez sur Entrée :

```
Get-WinEvent -FilterHashtable @{LogName='Windows PowerShell';Id ='800'} -MaxEvents 1 |
Select -Expand Message
```

9. Ouvrez le Gestionnaire de serveur, cliquez sur **Outils**, puis sélectionnez **Gestion des stratégies de groupe**.
10. Cliquez avec le bouton droit sur **Default Domain Policy**, puis cliquez sur **Modifier**.
11. Ouvrez l'**Éditeur de gestion des stratégies de groupe**.

12. Développez **Configuration ordinateur**, puis **Stratégies**, puis **Modèles d'administration**, puis **Composants Windows**, cliquez sur **Windows PowerShell**, et enfin consultez les paramètres GPO sur l'écran principal.
13. Réduisez les nœuds GPO.
14. Développez **Configuration ordinateur**, **Préférences** et **Paramètres Windows**, cliquez avec le bouton droit sur **Environnement**, pointez sur **Nouveau**, puis sélectionnez **EnvironmentVariable**. Entrez les informations suivantes :
    - Nom : **PSLogScriptBlockExecution**
    - Valeur : **0**
15. Cliquez sur **OK**, cliquez avec le bouton droit sur **Environnement**, pointez sur **Nouveau**, puis sélectionnez **EnvironmentVariable**. Saisissez les informations suivantes, puis cliquez sur **OK** :
    - Nom : **PSLogScriptBlockExecutionVerbose**
    - Valeur : **0**
16. Fermez l'Éditeur de gestion des stratégies de groupe.
17. Cliquez sur **Démarrer**, sélectionnez **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Observateur d'événements**.
18. Consultez les journaux Windows sous **Système**.
19. Localisez le suivi d'événements pour Windows (ETW, Event Tracing for Windows) sous le chemin d'accès suivant : **Journaux des applications et des services/Microsoft/Windows/PowerShell/Opérationnel**.
20. Fermez toutes les fenêtres.

Contrôle des acquis et éléments à retenir

Meilleure pratique

Windows Server 2016 dispose de plusieurs améliorations d'audit qui augmentent le niveau de détails des journaux d'audit de sécurité et simplifient le déploiement et la gestion des stratégies d'audit.

L'audit est une activité continue sur votre réseau. C'est l'une des pratiques de sécurité essentielles de votre entreprise. En auditant les événements relatifs à la sécurité, vous pouvez être prévenu tôt des activités malveillantes potentielles et de leurs preuves en cas de violation de la sécurité.

Question de contrôle des acquis

Question : vous avez configuré une stratégie d'audit à l'aide d'une stratégie de groupe afin de l'appliquer à tous les serveurs de fichiers de votre entreprise. Après avoir activé la stratégie et confirmé que les paramètres de la stratégie de groupe sont bien appliqués, vous découvrez que les événements d'audit ne sont pas enregistrés dans les journaux d'événements. Quelle en est la cause la plus probable ?

> **Réponse :** pour auditer l'accès aux fichiers, vous devez configurer les fichiers ou dossiers de façon à auditer des événements spécifiques. Sans cela, les événements d'audit ne sont pas enregistrés.

Problèmes et scénarios réels

Quand vous consultez le journal Événements transférés, si l'autorisation Lecture du journal des événements est omise, le collecteur peut afficher le message suivant : **La description de l'ID d'événement ID 111 de la source Microsoft-Windows-EventForwarder est introuvable. Le composant qui déclenche cet événement n'est pas installé sur l'ordinateur local ou l'installation est endommagée. Vous pouvez installer ou réparer le composant sur l'ordinateur local. Si l'événement provient d'un autre ordinateur, les informations d'affichage doivent être enregistrées avec l'événement.**

Questions et réponses relatives à l'atelier pratique

Atelier pratique : configuration d'un audit avancé

Questions et réponses

Question : pourquoi appliquer des stratégies d'audit dans toute l'entreprise ?

Réponse : que vous tentiez de résoudre un problème général ou de savoir où se produit un événement spécifique, il peut être nécessaire de cibler un grand groupe de serveurs pour capturer un événement. Dans ce cas, vous pouvez utiliser le filtrage des événements pour rechercher un événement d'audit précis. Après avoir mis le doigt sur un problème, il est recommandé de réduire l'étendue de l'audit ou de le désactiver afin de limiter le nombre de journaux générés, de diminuer l'impact sur les performances des ordinateurs et de faciliter la lecture régulière des journaux.

Module 7

Déploiement et configuration de Microsoft Advanced Threat Analytics et Microsoft Operations Management Suite

Sommaire :

Leçon 1

Déploiement et configuration d'ATA

Sommaire :

Questions et réponses

Question : vous devez configurer la mise en miroir de ports quand vous configurez une passerelle légère ATA.

( ) Vrai

( ) Faux

Réponse :

( ) Vrai

(√) Faux

Commentaires :

L'installation d'une passerelle légère ATA sur un contrôleur de domaine évite d'avoir à configurer la mise en miroir de ports.

Question : quelles passerelles ATA devez-vous configurer comme synchronisateurs de domaine possibles ?

( ) Toutes les passerelles ATA

( ) Les passerelles ATA pour un site distant

( ) Les passerelles ATA qui sont installées sur des contrôleurs de domaine en lecture seule

( ) Toute passerelle ATA qui n'est pas un contrôleur de domaine en lecture seule ou qui ne sert pas de passerelle ATA pour un site distant

Réponse :

( ) Toutes les passerelles ATA

( ) Les passerelles ATA pour un site distant

( ) Les passerelles ATA qui sont installées sur des contrôleurs de domaine en lecture seule

(√) Toute passerelle ATA qui n'est pas un contrôleur de domaine en lecture seule ou qui ne sert pas de passerelle ATA pour un site distant

Commentaires :

Par défaut, seules les passerelles ATA sont définies comme synchronisateurs de domaine possibles. Nous recommandons de désactiver les passerelles ATA pour site distant afin qu'elles ne soient pas des synchronisateurs de domaine possibles. Si votre contrôleur de domaine est en lecture seule, ne le configurez pas comme synchronisateur de domaine possible.

Ressources

Présentation d'ATA

 **Lectures supplémentaires :** pour plus d'informations, consultez la feuille de données « Microsoft Advanced Threat Analytics » à l'adresse : https://aka.ms/ul0xra

Conditions requises pour le déploiement d'ATA

 **Lectures supplémentaires :** pour plus d'informations sur les autorisations des objets Active Directory, consultez « View or Set Permissions on a Directory Object » à l'adresse : http://aka.ms/Bgxyha

Démonstration : déploiement et configuration d'ATA

Étapes de la démonstration

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, puis sur **Gestionnaire de serveur**.
2. Dans Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire des services Internet (IIS)**.
3. Dans le Gestionnaire IIS, développez **LON-SVR1**, puis **Sites**, puis cliquez sur **Default Web Site**.
4. Dans le volet **Actions**, cliquez sur **Liaisons.**
5. Sélectionnez **https**, puis cliquez sur **Supprimer**. Cliquez sur **Oui**, puis fermez toutes les fenêtres.
6. Sur **LON-SVR1**, cliquez avec le bouton droit sur l'icône de réseau dans la barre des tâches, puis cliquez sur **Ouvrir le Centre Réseau et partage**.
7. Cliquez sur **Modifier les paramètres de la carte**, cliquez avec le bouton droit sur **Ethernet**, puis cliquez sur **Propriétés**.
8. Sélectionnez **Protocole Internet version 4 (TCP/IPv4)** et cliquez sur **Propriétés**.
9. Dans la boîte de dialogue **Propriétés de : Protocole Internet version 4 (TCP/IPv4)**, cliquez sur **Avancé**.
10. Dans la boîte de dialogue **Paramètres TCP/IP avancés**, dans l'onglet **Paramètres IP**, sous **Adresses IP**, cliquez sur le bouton **Ajouter**.
11. Dans la zone de texte **Adresse IP**, tapez **172.16.0.13**. Vérifiez que le paramètre **Masque de sous-réseau** est défini par défaut sur **255.255.0.0**. Cliquez sur **Ajouter**, cliquez sur **OK** à deux reprises, puis cliquez sur **Fermer**.
12. Sur **LON-SVR1**, dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
13. Accédez à **D:\LabFiles\Mod07**, cliquez avec le bouton droit sur **ATA1.7.iso**, puis sélectionnez **Monter**.
14. Vérifiez que vous pouvez voir un nouveau lecteur de DVD avec **Microsoft ATA Center Setup.exe**.
15. Cliquez avec le bouton droit sur le fichier .exe, puis cliquez sur **Exécuter en tant qu'administrateur**.
16. La première page vous invite à sélectionner la langue. Par défaut, **English** est sélectionné. Choisissez **Français**. Cliquez sur **Suivant** pour accepter les paramètres par défaut.
17. Lisez les Termes du contrat de licence Microsoft, activez la case à cocher **J'accepte les termes du contrat de licence logiciel Microsoft**, puis cliquez sur **Suivant**.
18. Sur la page suivante, où vous pouvez sélectionner l'option de mise à jour Microsoft, laissez les paramètres par défaut, puis cliquez sur **Suivant**.
19. Lisez la page **Configuration du centre ATA** et confirmez que vous avez des adresses IP différentes pour **Adresse IP du service du center** et **Adresse IP de la console**. La première devrait être **172.16.0.11** et **Adresse IP de la console** devrait être **172.16.0.13**.
20. Cliquez sur **Installer**.
21. Ouvrez le Gestionnaire de serveur, puis dans le menu **Outils**, cliquez sur **Gestion de l'ordinateur**.
22. Sous **Outils système**, développez **Utilisateurs et groupes locaux**, puis sélectionnez **Groupes**.
23. Cliquez avec le bouton droit sur **Microsoft Advanced Threat Analytics Administrators**, puis cliquez sur **Ajouter au groupe**.
24. Cliquez sur le bouton **Ajouter**, tapez **Beth** dans la zone de texte, puis cliquez sur **Vérifier les noms** et enfin sur **OK**.

25. Cliquez sur **Ajouter**, dans la zone de texte, tapez **ATARead**, cliquez sur **Vérifier les noms**, puis sur **OK**.
26. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de : Microsoft Advanced Threat Analytics Administrators**.
27. Fermez **Gestion de l'ordinateur**.
28. Une fois l'installation terminée, cliquez sur **Lancer**.
29. Quand l'avertissement relatif à la sécurité s'affiche, cliquez sur **Poursuivre sur ce site Web**.
30. Après quelques instants, lorsque la **page de connexion** s'affiche, tapez **Beth** comme nom d'utilisateur et **Pa55w.rd** comme mot de passe, puis cliquez sur **Se connecter**.
31. Dans le coin supérieur droit du formulaire, cliquez sur les points de suspension (**...**), puis sur **Configuration**.
32. À gauche, sous **Sources de données**, cliquez sur **Services d'annuaire**.
33. Dans la zone de texte **Nom d'utilisateur**, tapez **ATARead**.
34. Pour **Mot de passe**, tapez **Pa55w.rd**.
35. Pour **Domaine**, tapez **adatum.com**, puis cliquez sur **Enregistrer**.
36. Dans l'en-tête bleu, cliquez sur **Télécharger l'installation de la passerelle et installer la première passerelle**
37. Cliquez sur **Télécharger l'installation de la passerelle**.
38. Enregistrez le fichier sous **D:\Labfiles\Mod07**.

 **Remarque :** l'étape du téléchargement ci-dessus ne requiert pas de connexion à Internet. Le téléchargement est créé à partir des éléments déjà présents sur le serveur.

39. Ouvrez l'Explorateur de fichiers, puis accédez à **D:\Labfiles\Mod07**.
40. Copiez le fichier **Microsoft ATA Gateway Setup.zip** et collez-le à l'emplacement suivant : **\\LON-DC1\E$\Labfiles\Mod07**. Remplacez le fichier existant si nécessaire.
41. Fermez l'Explorateur de fichiers.
42. Sur **LON-DC1**, ouvrez l'Explorateur de fichiers, puis accédez à **E:\Labfiles\Mod07**.
43. Cliquez avec le bouton droit sur **Microsoft ATA Gateway Setup.zip**, puis sélectionnez **Extraire tout**.
44. Dans la zone de texte **Les fichiers seront extraits dans ce dossier**, tapez **E:\Labfiles\Mod07\Gateway**, puis cliquez sur **Extraire**.
45. Dans **E:\Labfiles\Mod07\Gateway**, cliquez avec le bouton droit sur **Microsoft ATA Gateway Setup.exe**, puis sélectionnez **Exécuter en tant qu'administrateur**.
46. La première page vous invite à sélectionner la langue. Par défaut, **English** est sélectionné. Choisissez **Français**. Cliquez sur **Suivant** pour accepter les paramètres par défaut.
47. Vérifiez le type de déploiement de la passerelle ATA. Faites remarquer aux stagiaires que la passerelle légère ATA est déjà sélectionnée, car il s'agit d'un contrôleur de domaine. Cliquez sur **Suivant**.
48. Dans la zone de texte **Nom d'utilisateur**, tapez **ATARead**. Dans la zone de texte **Mot de passe**, tapez **Pa55w.rd**, puis cliquez sur **Installer**.
49. Une fois l'installation terminée, cliquez sur **Terminer**.

Leçon 2

Déploiement et configuration de Microsoft Operations Management Suite

Sommaire :

Questions et réponses

Question : quel service de Microsoft Operations Management Suite permet de collecter et d'analyser les données générées par les ressources de vos environnements cloud et local ?

( ) Log Analytics

( ) Data Analytics

( ) Connecteurs de données Microsoft Operations Management Suite

( ) Connecteurs de données réseau

Réponse :

(√) Log Analytics

( ) Data Analytics

( ) Connecteurs de données Microsoft Operations Management Suite

( ) Connecteurs de données réseau

Commentaires :

Log Analytics est un service de Microsoft Operations Management Suite qui vous permet de collecter et d'analyser les données générées par les ressources de vos environnements cloud et local.

Question : Log Analytics requiert des ressources locales qui analysent les données collectées.

( ) Vrai

( ) Faux

Réponse :

( ) Vrai

(√) Faux

Commentaires :

La configuration requise pour le déploiement de Log Analytics est minime, car le cloud Azure héberge les composants principaux. Ceux-ci incluent le référentiel et les services qui vous aident à effectuer la corrélation et l'analyse des données collectées. Vous pouvez accéder au portail de Microsoft Operations Management Suite depuis n'importe quel navigateur. Aucun logiciel client n'est donc requis.

Fonctions de sécurité et d'audit de Microsoft Operations Management Suite

Question : quel produit, qui n'appartient pas à Microsoft, Microsoft Operations Management Suite permet-il de gérer et de protéger ?

( ) AWS

( ) VMware

( ) Linux

( ) OpenStack

Réponse :

(√) AWS

(√) VMware

(√) Linux

(√) OpenStack

Commentaires :

Microsoft Operations Management Suite vous permet de gérer et de protéger Azure ou AWS, Windows Server ou Linux, VMware ou OpenStack.

Ressources

Scénarios d'utilisation et de déploiement de Microsoft Operations Management Suite

Lectures supplémentaires : pour en savoir plus sur Azure Automation et les Runbooks, consultez « Getting Started With Azure Automation – Runbook Management » à l'adresse : http://aka.ms/Cz3zbw

Démonstration : déploiement et configuration de Microsoft Operations Management Suite

Étapes de la démonstration

1. Si nécessaire, créez un compte Microsoft et Azure comme stipulé dans l'exercice de l'atelier « Préparation et déploiement de Microsoft Operations Management Suite », tâches 1 et 2.
2. Connectez-vous à **LON-CL1**, puis cliquez sur **Démarrer**. Dans la barre de recherche, tapez **Internet Explorer**, puis démarrez le programme.
3. Dans Internet Explorer, entrez l'URL suivante, puis appuyez sur Entrée : **https://www.microsoft.com/fr-fr/cloud-platform/operations-management-suite**.
4. Cliquez sur **Créez un compte gratuit**.
5. Cliquez sur **Démarrer gratuitement**.
6. Si vous n'êtes pas connecté, connectez-vous en utilisant votre compte Microsoft.
7. Remplissez le formulaire **Créer un espace de travail** en utilisant l'adresse électronique que vous avez utilisée pour créer votre compte Microsoft, puis cliquez sur **CRÉER**.
8. Sélectionnez l'abonnement Azure de votre choix, puis cliquez sur **LIEN**.
9. Vérifiez que la page **Microsoft Operations Management Suite** s'affiche.
10. Sur la page d'accueil de **Microsoft Operations Management Suite**, cliquez sur **Galerie de solutions**.
11. Passez en revue les solutions disponibles.
12. Cliquez sur l'icône de maison à gauche.
13. Sur la page d'accueil, cliquez sur **Paramètres**.
14. Cliquez sur **Sources connectées** et vérifiez que **Serveurs Windows** est sélectionné.
15. Cliquez sur le bouton **Démarrer** de Windows.
16. Tapez **Notepad**, puis appuyez sur Entrée.
17. Repassez dans **Microsoft Internet Explorer** et cherchez **ID DE L'ESPACE DE TRAVAIL** et **CLÉ PRIMAIRE** dans le volet de droite.
18. Copiez et collez les ID de l'**ESPACE DE TRAVAIL** et **CLÉ PRIMAIRE** dans le Bloc-notes.
19. Enregistrez le fichier Bloc-notes sous **D:\WorkspaceID.txt** pour plus tard.
20. Cliquez sur **Télécharger l'agent Windows (64 bits)** pour télécharger **MMASetup-AMD64.exe**.

21. Cliquez sur **Enregistrer**, puis sur **Exécuter**.
22. Sur la page **Bienvenue dans l'Assistant Installation de l'agent Microsoft Monitoring Agent**, cliquez sur **Suivant**.
23. Si une boîte de dialogue **Contrôle de compte d'utilisateur** s'affiche, cliquez sur **Oui**.
24. Lisez les Termes du contrat de licence Microsoft, puis cliquez sur **J'accepte**.
25. Acceptez le dossier de destination par défaut en cliquant sur **Suivant**.
26. Sélectionnez **Connecter l'agent à Azure Log Analytics (OMS)**, puis cliquez sur **Suivant**.
27. Saisissez l'**ID de l'espace de travail** et la **clé primaire** copiés dans le Bloc-notes, puis cliquez sur **Suivant**.
28. À l'invite des mises à jour Microsoft, cliquez sur **Suivant**.
29. Cliquez sur **Installer**, puis sur **Terminer**.
30. Ouvrez le Panneau de configuration sur LON-CL1.
31. Dans le Panneau de configuration, cliquez sur **Système et sécurité**, puis sur **Microsoft Monitoring Agent**.
32. Si une boîte de dialogue **Contrôle de compte d'utilisateur** s'affiche, cliquez sur **Oui**.
33. Cliquez sur l'onglet **Azure Log Analytics (OMS)**, sélectionnez l'élément de la liste, puis cliquez sur **Modifier**. Cela vous permettra de mettre à jour la **clé de l'espace de travail** si nécessaire. Cliquez sur **Annuler**.
34. Cliquez sur **Annuler**.
35. Retournez sur le site Web de Microsoft Operations Management Suite et actualisez votre navigateur. Montrez aux stagiaires que vous pouvez maintenant voir l'**utilisation** et les données de **LON-CL1**.

 **Remarque :** dans certains cas, les données d'utilisation mettent un peu de temps à s'afficher. Vous pouvez montrer ceci avant l'atelier pratique Microsoft Operations Management Suite.

Contrôle des acquis et éléments à retenir

Meilleure pratique

Dans les environnements plus grands, pensez à mettre en place plusieurs passerelles ATA.

Questions de contrôle des acquis

Question : quels domaines de sécurité pouvez-vous examiner dans Microsoft Operations Management Suite ?

Réponse : vous pouvez examiner les domaines suivants dans Microsoft Operations Management Suite :

- Programmes malveillants
- Évaluation des mises à jour
- Identité et accès

Question : expliquez comment utiliser ATA pour améliorer la sécurité.

Réponse : les avantages d'ATA sont les suivants :

- Il détecte les menaces à l'aide d'analyses du comportement. Inutile de créer des règles, de déployer des agents, d'affiner ou de surveiller de grandes quantités de rapports de sécurité.
- Il s'adapte aussi rapidement que les utilisateurs malveillants. ATA apprend en continu le comportement des entités de l'entreprise (utilisateurs, appareils et ressources) et s'adapte pour refléter les changements au fil de la croissance de votre entreprise.
- Concentrez-vous sur les priorités grâce à une chronologie des attaques simple. Celle-ci est un flux clair, efficace et pratique qui affiche les éléments pertinents chronologiquement. Cela vous permet de connaître les facteurs « qui, quoi, quand et comment » de votre entreprise.
- ATA réduit le temps perdu à cause des faux positifs. Les alertes sont émises uniquement lorsque des activités suspectes sont agrégées par contexte.
- ATA établit des priorités et des plans pour les étapes suivantes. Pour chaque activité suspecte ou attaque connue identifiée, ATA fournit des recommandations afin d'enquêter sur les problèmes et de les corriger.

Fonctionnalités clés d'ATA :

- Prise en charge de la mobilité. Surveille toutes les authentifications et autorisations d'accès aux ressources de l'entreprise dans le périmètre de celle-ci et sur les appareils mobiles.
- Intégration avec SIEM. ATA collabore avec SIEM et offre la possibilité de transmettre les alertes de sécurité à votre SIEM ou d'envoyer des courriers électroniques à des personnes spécifiques.
- Déploiement transparent. ATA fonctionne comme une application et utilise la mise en miroir de ports pour permettre un déploiement transparent.

Question : expliquez comment utiliser Microsoft Operations Management Suite pour améliorer la sécurité.

Réponse : les fonctionnalités de sécurité et de conformité de Microsoft Operations Management Suite vous permettent d'identifier, d'évaluer et de limiter les risques liés à la sécurité au sein de votre infrastructure. Ces fonctionnalités sont implémentées par le biais de plusieurs solutions dans Log Analytics. Celles-ci analysent les données des journaux et la configuration à partir des systèmes d'agent pour vous aider à garantir en permanence la sécurité de votre environnement.

- La solution Security and Audit collecte et analyse les événements de sécurité sur les systèmes gérés afin d'identifier toute activité suspecte.
- La solution Antimalware surveille le statut de la protection contre les programmes malveillants sur les systèmes gérés.
- La solution System Updates analyse les mises à jour de sécurité et autres mises à jour sur vos systèmes gérés afin d'identifier facilement les systèmes requérant des mises à jour.

Problèmes et scénarios réels

Planification des capacités d'ATA Center :

- L'espace disque requis pour une base de données ATA peut varier en fonction du contrôleur de domaine.
- Si vous disposez de plusieurs contrôleurs de domaine, rassemblez l'espace disque requis par contrôleur de domaine afin de calculer l'espace disque total nécessaire pour la base de données ATA.
- Pour calculer avec précision la capacité d'ATA Center en fonction des conditions requises, consultez http://aka.ms/atasizing.

Outils

Wireshark est un analyseur de protocole réseau qui vous permet d'examiner votre réseau précisément. Bien que Wireshark soit très utile, souvenez-vous de ne pas l'installer sur les serveurs que vous utilisez pour les passerelles ATA ou ATA Center.

Problèmes courants et conseils de dépannage

Problème courant	Conseil de dépannage
Certains utilisateurs signalent l'ID d'événement 1013 dans le journal des événements Microsoft ATA dans ATA Center.	Ce problème est souvent lié aux sauvegardes système, lorsque les disques ne peuvent plus fournir assez d'opérations entrantes et sortantes par seconde (IOPS, Input/output Operations Per Second) lors du processus de sauvegarde.

Questions et réponses relatives à l'atelier pratique

Atelier pratique : déploiement de Microsoft Advanced Threat Analytics et Microsoft Operations Management Suite

Questions et réponses

Question : quel avantage y a-t-il à utiliser une passerelle légère ATA ?

Réponse : il est inutile de configurer la mise en miroir de ports pour une passerelle légère ATA.

Question : quelles sont les conditions requises pour installer ATA ?

Réponse : certaines conditions incluent un compte d'utilisateur de domaine, une liste de sous-réseaux avec une courte durée de vie (TTL, Time to Live), un compte honeytoken, Wireshark et Microsoft Message Analyzer.

Module 8

Sécurisation de l'infrastructure de virtualisation

Sommaire :

Leçon 1

Structure Service Guardian

Sommaire :

Questions et réponses

Question : quel service fournit les clés de transport nécessaires pour déverrouiller et faire fonctionner des VM dotées d'une protection maximale sur des hôtes Hyper-V attestés (ou intègres) ?

Réponse : KPS

Ressources

Nano Server en tant qu'hôte Service Guardian avec attestation TPM

 **Lectures supplémentaires :** pour plus d'informations, consultez « Prepare Nano Server Script for Guarded Fabric » à l'adresse : http://aka.ms/V2thr5

Leçon 2

VM dotées d'une protection maximale et acceptant le chiffrement

Sommaire :

Questions et réponses

Question : quelles sont les principales différences entre les VM dotées d'une protection maximale et les VM acceptant le chiffrement ?

Réponse : comme les VM dotées d'une protection maximale, les VM acceptant le chiffrement utilisent les états Démarrage sécurisé, Modules de plateforme sécurisée virtuel (vTPM) et VM chiffrée. Cependant, avec les VM acceptant le chiffrement, ces paramètres peuvent être configurés. Avec les VM dotées d'une protection maximale, ils sont forcément appliqués. De plus, la console **Connexion de l'ordinateur virtuel** est **activée** pour les VM acceptant le chiffrement, alors qu'elle est désactivée pour les VM dotées d'une protection maximale. Enfin, les ports COM/série sont désactivés dans les VM dotées d'une protection maximale, et il n'est pas possible d'attacher un débogueur au processus de VM.

Ressources

Dépannage des VM dotées d'une protection maximale et acceptant le chiffrement

Lectures supplémentaires : pour plus d'informations, consultez « Shielded VMs and Guarded Fabric Troubleshooting Guide for Windows Server 2016 » à l'adresse : https://aka.ms/ehnloq

Contrôle des acquis et éléments à retenir

Meilleure pratique

Bien qu'il soit possible d'utiliser un seul domaine pour configurer une structure Service Guardian, il est conseillé que le SGH n'ait qu'une seule forêt.

Question de contrôle des acquis

Question : quelles approbations sont nécessaires entre les domaines, et de quels domaines l'hôte Service Guardian doit-il être membre ?

> **Réponse :** le serveur SGH doit disposer d'une approbation à sens unique avec le domaine de l'entreprise. L'hôte Service Guardian doit être un membre du domaine de l'entreprise et non un membre de la forêt du SGH.

Problèmes courants et conseils de dépannage

Problème courant	Conseil de dépannage
Une VM dotée d'une protection maximale ne parvient pas à démarrer après l'activation d'un vTPM.	Vérifiez que l'hôte Service Guardian a bien été ajouté au bon groupe de sécurité.

Questions et réponses relatives à l'atelier pratique

Atelier pratique : structure Service Guardian avec attestation Administrateur de confiance et VM dotées d'une protection maximale

Questions et réponses

Question : décrivez les principaux composants de la structure Service Guardian.

Réponse : les VM dotées d'une protection maximale et la structure Service Guardian permettent aux fournisseurs de services cloud ou aux administrateurs de cloud privé d'entreprise de fournir un environnement plus sécurisé pour les ordinateurs virtuels clients. Une structure Service Guardian est constituée d'un SGH, en général composé d'un cluster de trois nœuds, d'un ou plusieurs hôtes Service Guardian et d'un ensemble de VM dotées d'une protection maximale.

Question : dans cet atelier pratique, vous avez créé un environnement composé du SGH et de l'hôte Service Guardian. Vous avez également ajouté un groupe SGH au domaine de l'entreprise. Lequel de ces rôles doit être un serveur physique ?

Réponse : l'hôte Service Guardian, car il ne peut pas s'exécuter dans un environnement virtualisé.

Module 9

Sécurisation du développement des applications et de l'infrastructure de la charge de travail du serveur

Sommaire :

Leçon 1

Utilisation de SCM

Sommaire :

Questions et réponses

Question : quelles lignes de base produit par défaut SCM 4.0 contient-il ?

( ) Internet Explorer 6 et Internet Explorer 7

( ) Microsoft Exchange Server 2007 SP1

( ) Windows 8

( ) Windows Server 2008 SP1

( ) Windows Server 2012

Réponse :

( ) Internet Explorer 6 et Internet Explorer 7

( ) Microsoft Exchange Server 2007 SP1

(√) Windows 8

( ) Windows Server 2008 SP1

(√) Windows Server 2012

Commentaire :

SCM 4.0 ne dispose pas de modèle de ligne de base pour les systèmes et applications créés avant Windows Server 2012, Internet Explorer 8 et Microsoft Exchange Server 2010.

Ressources

Gestion de lignes de base de sécurité

Lectures supplémentaires : pour plus d'informations, consultez « Security baseline for Windows 10 v1607 ("Anniversary edition") and Windows Server 2016 » à l'adresse : https://aka.ms/hhsdmo

Déploiement de configurations de sécurité

Lectures supplémentaires : Vous pouvez télécharger l'outil autonome LGPO.EXE à l'adresse : https://aka.ms/kkvmk5

Démonstration : installation de SCM

Étapes de la démonstration

Installer SCM

1. Sur **LON-SVR1**, cliquez sur l'**Explorateur de fichiers** dans la barre des tâches.
2. Dans **l'Explorateur de fichiers**, accédez à **D:\Labfiles\Mod09**.
3. Double-cliquez sur **Security_Compliance_Manager_Setup.exe**.

   Une fenêtre d'invite de commandes s'ouvre et lance les composants requis pour SCM.
4. Quand la fenêtre **Microsoft Visual C++ 2010 x86 Redistributable Setup** s'affiche, sélectionnez **I have read and accept the license terms**, puis cliquez sur **Install**.
5. Quand la page **Installation is Complete** apparaît, cliquez sur **Finish**.
6. L'assistant **Microsoft Security Compliance Manager Setup Wizard** démarre. Sur la page **Welcome**, décochez la case **Always check for SCM and baseline updates**, puis cliquez sur **Next**.

Remarque : il existe plusieurs nouvelles lignes de base pour Windows 10, Windows Server 2016, Internet Explorer 11, etc. Toutefois, vous devez les télécharger et les importer indépendamment. Puisque vous n'avez pas d'accès à Internet sur les ordinateurs virtuels du cours, vous ne pourrez pas les télécharger ici. C'est pour cette raison que vous avez dû décocher la case **Always check for SCM and baseline updates**.

7. Sur la page **License Agreement**, cliquez sur **I accept the terms of the license agreement**, puis sur **Next**.
8. Sur la page **Installation Folder**, cliquez sur **Next**.
9. Sur la page **SQL Instances found**, sélectionnez **Create a new SQL express instance,** puis cliquez sur **Next.**
10. Sur la page **Microsoft SQL Server 2008 Express**, cliquez sur **Next**.
11. Sur la page **SQL Server 2008 Express License Agreement**, sélectionnez **I accept the terms of the license agreement**, puis cliquez sur **Next**.
12. Sur la page **Ready to Install**, cliquez sur **Install**.
13. Quand la page **Installation Successful** apparaît, cliquez sur **Finish**.
14. La console **SCM** s'ouvre et importe automatiquement plusieurs lignes de base. Laissez la console ouverte pour la démonstration suivante.

Démonstration : configuration et gestion de lignes de base de sécurité

Étapes de la démonstration

Installer les GPO de Windows Server 2016

1. Sur **LON-SVR1**, dans le volet **Actions** de la console **SCM**, cliquez sur **Import – GPO Backup (folder)**.
2. Depuis la fenêtre **Browse for folder**, accédez à **D:\Labfiles\Mod09\Windows 10 RS1 and Server 2016 Security Baseline\GPOs**, sélectionnez le premier identificateur global unique (GUID, Globally Unique Identifier) de GPO, puis cliquez sur **OK**.
3. Dans la fenêtre **GPO Name**, notez le nom du GPO, puis cliquez sur **OK**.
4. Dans la fenêtre **SCM Log**, cliquez sur **OK**.
5. Répétez les étapes 1 à 4 pour les 10 autres GUID de GPO du dossier **GPOs**.

Associer et fusionner le GPO de Windows Server 2016 avec la ligne de base du serveur membre Windows Server 2012

1. Dans la console **SCM**, dans l'arborescence, développez **Custom baselines** (si ce n'est déjà fait), puis **GPO import**.
2. Dans la liste de lignes de base, sélectionnez **SCM Windows Server 2016 - Member Server Baseline – Computer 0.0**.
3. Dans le volet **Actions**, sous **Baseline**, cliquez sur le lien hypertexte **Associate**.
4. Dans la fenêtre **Associate Product with a GPO**, dans la liste **Product name**, sélectionnez **Windows Server 2012**, puis cliquez sur **Associate**.
5. Dans la zone de texte **Baseline name**, tapez **Associated Server 2012-2016**, puis cliquez sur **OK**.
6. Dans l'arborescence de la console **SCM**, si ce n'est pas déjà le cas, sélectionnez **Associated Server 2012-2016** sous **Custom Baselines**, puis, dans le volet **Actions**, sous **Baseline**, cliquez sur le lien hypertexte **Compare/Merge**.

7. Dans la fenêtre **Compare Baselines**, développez **Windows Server 2012**, puis, dans la liste ainsi obtenue, sélectionnez **WS2012 Member Server Security Compliance 1.0**, puis cliquez sur **OK**.
8. Expliquez les informations présentées dans la fenêtre **Compare Baselines**. Expliquez les paramètres des zones **Settings that differ** et **Settings that match**.
9. Dans la fenêtre **Compare Baselines**, cliquez sur **Merge Baselines.**
10. Dans la fenêtre **Merge Baselines**, expliquez les éléments **Merge conflicts to resolve**, puis cliquez sur **OK**.
11. Dans la zone de texte **Specify a name for the merged baseline**, tapez **Fusion serveur membre 2012-2016**, puis cliquez sur **OK**.
12. Expliquez pourquoi les stagiaires devraient choisir un paramètre de ligne de base plutôt qu'un autre. Remarque : les stagiaires peuvent afficher le nom complet d'un paramètre en faisant glisser la barre de séparation de la ligne des en-têtes.
13. Faites défiler le volet d'informations vers le bas pour atteindre la zone **Session Configuration** sous la colonne **Name**.
14. Double-cliquez sur l'élément nommé **Interactive Logon: Message title for users attempting to log on** et désactivez la case à cocher **Not Defined**. Dans la zone de texte **Customize setting value**, tapez **Bienvenue chez A. Datum Corporation !**, puis cliquez sur **Collapse**.
15. Toujours dans la zone **Session Configuration**, sous la colonne **Name**, double-cliquez sur l'élément nommé **Interactive Logon: Message text for users attempting to log on**. Désactivez la case à cocher **Not Defined**, puis, dans la zone de texte **Customize setting value**, tapez **Cet appareil utilise la ligne de base Fusion serveur membre 2012-2016.**, puis cliquez sur **Collapse**.
16. Dans le volet **Actions**, sous **Export**, cliquez sur le lien hypertexte **GPO Backup (folder)**.
17. Dans la fenêtre **Browse For Folder**, développez **Allfiles (D:)**, puis **Labfiles**, et sélectionnez **Mod09**. Enfin, cliquez sur **OK**.
18. Fermez la fenêtre de l'**Explorateur de fichiers**.

Démonstration : déploiement d'une ligne de base de sécurité sur un serveur distant

Étapes de la démonstration

Importer une sauvegarde de GPO SCM dans la Console de gestion des stratégies de groupe

1. Sur **LON-DC1**, dans la barre des tâches, sélectionnez l'**Explorateur de fichiers**.
2. Dans l'**Explorateur de fichiers**, dans la zone de texte **URL**, tapez **\\LON-SVR1\D$\Labfiles\Mod09**, puis appuyez sur Entrée.
3. Cliquez avec le bouton droit sur le dossier GUID, puis copiez-le (exemple : {bed88c04-5ffe-4857-aff6-be595c53ad41}).
4. Dans l'**Explorateur de fichiers**, sur **LON-DC1**, accédez à **Allfiles (E:\)\Labfiles**.

   Cliquez avec le bouton droit dans le volet d'informations, puis cliquez sur **Coller**. Fermez l'**Explorateur de fichiers**.
5. Dans le **Gestionnaire de serveur**, dans le menu **Outils**, cliquez sur **Gestion des stratégies de groupe**.
6. Dans la **Console de gestion des stratégies de groupe**, développez **Forêt : Adatum.com**, puis **Domaines**, puis **Adatum.com** et sélectionnez le nœud **Objets de stratégie de groupe**.

7. Cliquez avec le bouton droit dans l'espace vide du volet d'informations, puis cliquez sur **Nouveau**.
8. Dans la fenêtre **Nouvel objet GPO**, dans le champ **Nom**, tapez **Ligne de base 2012-2016 du serveur membre**, puis cliquez sur **OK**.
9. Dans le volet d'informations, cliquez avec le bouton droit sur l'élément **Ligne de base 2012-2016 du serveur membre**, puis cliquez sur **Importer les paramètres**.
10. Dans l'**Assistant Importation des paramètres,** sur la page **Bienvenue**, cliquez sur **Suivant**.
11. Sur la page **Objet de stratégie de groupe de sauvegarde**, cliquez sur **Suivant**.
12. Sur la page **Emplacement de sauvegarde**, dans le champ **Dossier de sauvegarde**, tapez **E:\Labfiles**, puis cliquez sur **Suivant.**
13. Sur la page **Objet de stratégie de groupe (GPO) source**, assurez-vous que l'élément **Fusion serveur membre 2012-2016** est sélectionné, puis cliquez sur **Suivant**.
14. Sur la page **Analyse de la sauvegarde**, cliquez sur **Suivant**.
15. Sur la page **Migration des références**, expliquez comment utiliser une table de migration pour mapper les paramètres vers un GPO de destination. Toutefois, puisque vous n'avez pas de table de migration, vous devez accepter les paramètres par défaut et cliquer sur **Suivant**.
16. Sur la page **Fin de l'Assistant Importation des paramètres**, cliquez sur **Terminer**, puis, une fois l'importation terminée, cliquez sur **OK**.
17. Cliquez avec le bouton droit sur l'élément **Ligne de base 2012-2016 du serveur membre** dans le volet d'informations, puis cliquez sur **Modifier**.
18. Agrandissez la fenêtre de l'**Éditeur de gestion des stratégies de groupe**.
19. Dans l'**Éditeur de gestion des stratégies de groupe**, dans l'arborescence de la console, sous le nœud **Configuration ordinateur**, développez **Stratégies**, puis **Paramètres Windows**, puis **Paramètres de sécurité** et enfin **Stratégies locales**.
20. Sous **Stratégies locales**, sélectionnez **Options de sécurité**.
21. Faites défiler vers le bas le volet d'informations des **Options de sécurité** jusqu'à l'élément de paramètres appelé **Interactive Logon : Message title for users attempting to log on**, puis double-cliquez dessus.
22. Remarquez que **Bienvenue chez A. Datum Corporation !** est défini pour ce paramètre de stratégie.
23. Faites de même pour l'élément **Interactive Logon : Message text for users attempting to log on**, en veillant à ce qu'il soit défini sur **Cet appareil utilise la ligne de base Fusion serveur membre 2012-2016.**
24. Fermez la fenêtre **Éditeur de gestion des stratégies de groupe**, puis réduisez la **Console de gestion des stratégies de groupe.**

Créer l'UO du serveur membre, déplacez LON-SVR2 à l'intérieur, puis liez le GPO Ligne de base 2012-2016 du serveur membre à l'UO

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, dans le menu **Outils**, sélectionnez **Utilisateurs et ordinateurs Active Directory**.
2. Dans **Utilisateurs et ordinateurs Active Directory**, dans l'arborescence, développez **Adatum.com**.
3. Cliquez avec le bouton droit sur **Adatum.com**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
4. Dans la fenêtre **Nouvel objet - Unité d'organisation**, dans la zone de texte **Nom**, tapez **Serveurs membres**, puis cliquez sur **OK**.
5. Dans l'arborescence de la console, sélectionnez le nœud **Ordinateurs**.

6. Dans le volet d'informations, cliquez avec le bouton droit sur **LON-SVR2**, puis cliquez sur **Déplacer**.
7. Dans la fenêtre **Déplacer**, sélectionnez l'UO **Serveurs membres**, puis cliquez sur **OK**.
8. Dans l'arborescence de la console, sélectionnez **Serveurs membres**, puis vérifiez que **LON-SVR2** se trouve bien dans cette UO.
9. Fermez la console **Utilisateurs et ordinateurs Active Directory**.
10. Agrandissez la **Console de gestion des stratégies de groupe**.
11. Dans l'arborescence de la console, sélectionnez **Adatum.com**, puis cliquez sur l'icône **Actualiser**.
12. L'UO **Serveurs membres** devrait maintenant apparaître sous **Adatum.com**. Sélectionnez-la.
13. Cliquez avec le bouton droit sur **Serveurs membres**, puis cliquez sur **Lier un objet de stratégie de groupe existant**.
14. Dans la fenêtre **Sélectionner un objet de stratégie de groupe**, sélectionnez le GPO **Ligne de base 2012-2016 du serveur membre**, puis cliquez sur **OK**.
15. Fermez la **Console de gestion des stratégies de groupe**.

Démarrez LON-SVR2, puis observez le titre et le texte du message d'Interactive Logon.

1. Dans le **Gestionnaire Hyper-V** sur l'ordinateur hôte, double-cliquez sur **22744B-LON-SVR2**, puis, dans la fenêtre **Connexion à un ordinateur virtuel**, cliquez sur **Démarrer**.
2. Quand l'ordinateur virtuel démarre, vous devriez voir l'écran **Interactive Logon** avant l'écran **Connexion**.
3. Cliquez sur **OK** sur cet écran, puis connectez-vous à **LON-SVR2** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
4. Fermez toutes les fenêtres, puis déconnectez-vous de tous les ordinateurs virtuels.

Leçon 2

Introduction à Nano Server

Sommaire :

Questions et réponses

Activité de séquençage

Question : les étapes suivantes permettent d'appliquer DSC à un Nano Server. Mettez-les dans le bon ordre.

	Étapes
	Créer un script de configuration pour DSC sur le Nano Server.
	Copier le script de configuration sur le Nano Server.
	S'assurer que toutes les ressources DSC nécessaires sont importées et disponibles.
	Exécuter le script de configuration sur le Nano Server pour créer le fichier MOF.
	Utilisez la commande Start-DscConfiguration dans Windows PowerShell pour déployer DSC selon le fichier MOF.
	Vérifier que DSC a été déployé et que la configuration est définie comme il se doit.

Réponse :

	Étapes
1	Créer un script de configuration pour DSC sur le Nano Server.
2	Copier le script de configuration sur le Nano Server.
3	S'assurer que toutes les ressources DSC nécessaires sont importées et disponibles.
4	Exécuter le script de configuration sur le Nano Server pour créer le fichier MOF.
5	Utilisez la commande Start-DscConfiguration dans Windows PowerShell pour déployer DSC selon le fichier MOF.
6	Vérifier que DSC a été déployé et que la configuration est définie comme il se doit.

Ressources

Pourquoi Nano Server est-il plus sécurisé ?

Lectures supplémentaires : pour plus d'informations, consultez « Introducing Server management tools » à l'adresse : https://aka.ms/mwe46x

Préparation, déploiement et gestion de Nano Server

Lectures supplémentaires : vous pouvez télécharger Nano Server Image Builder à l'adresse : http://aka.ms/NanoServerImageBuilder

Démonstration : déploiement et gestion de Nano Server

Étapes de la démonstration

Copier les scripts Windows PowerShell requis

1. Sur **LON-HOST1**, cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (admin)**.
2. Dans la fenêtre **Windows PowerShell**, tapez **cd**, puis appuyez sur Entrée.
3. Dans la fenêtre **Windows PowerShell**, tapez **md Nano**, puis appuyez sur Entrée.
4. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :

```
copy X:\NanoServer\NanoServerImageGenerator\*.ps* c:\nano
```

Remarque : remplacez *X* dans l'étape ci-dessus par la lettre du lecteur affecté au fichier .iso monté.

Importer les modules Windows PowerShell

1. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :

```
Import-Module c:\nano\NanoServerImageGenerator.psm1
```

2. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :

```
New-NanoServerImage -Edition Standard -mediapath X:\ -Basepath c:\nano -targetpath
c:\nano\nano-svr1.vhdx -DeploymentType Guest -computername NANO-SVR1 -storage -
package Microsoft-NanoServer-DSC-Package -Compute
```

Remarque : remplacez *X* dans l'étape ci-dessus par la lettre du lecteur affecté au fichier .iso monté.

3. À l'invite **AdministratorPassword**, connectez-vous avec le mot de passe **Pa55w.rd**, puis appuyez sur Entrée.
4. Lorsque le processus est terminé, dans la barre des tâches, cliquez sur l'**Explorateur de fichiers**, accédez à **C:\Nano**, puis examinez les fichiers répertoriés. Vérifiez que **nano-svr1.vhdx** existe.

Créer un ordinateur virtuel Hyper-V à partir de nano-svr1.vhdx

1. Sur **LON-HOST1**, ouvrez le **Gestionnaire Hyper-V**.
2. Dans la console **Hyper-V**, dans le volet **Actions**, cliquez sur **Nouveau**, puis sur **Ordinateur virtuel**.
3. Dans l'**Assistant Nouvel ordinateur virtuel**, sur la page **Bienvenue**, cliquez sur **Suivant**.
4. Sur la page **Indiquer un nom et un emplacement**, dans la zone de texte **Nom**, tapez **NANO-SVR1**, sélectionnez **Stocker l'ordinateur virtuel à un autre emplacement**, puis cliquez sur **Parcourir**.
5. Dans la fenêtre **Sélectionner un dossier**, dans la zone de texte **URL**, tapez **C:\nano**, appuyez sur Entrée, puis cliquez sur **Sélectionner un dossier**.
6. Sur la page **Indiquer un nom et un emplacement**, cliquez sur **Suivant**.
7. Sur la page **Spécifier la génération**, sélectionnez **Generation 2**, puis cliquez sur **Suivant**.
8. Sur la page **Affecter la mémoire**, cliquez sur **Suivant**.
9. Sur la page **Configurer le réseau**, dans la liste déroulante **Connexion**, sélectionnez **Réseau interne**, puis cliquez sur **Suivant**.

10. Sur la page **Connecter un disque dur virtuel**, cliquez sur **Utiliser un disque dur virtuel existant**, puis sur **Parcourir**.
11. Dans la fenêtre **Ouvrir**, dans la zone de texte **URL**, tapez **C:\nano**, appuyez sur Entrée, sélectionnez l'élément **nano-svr1.vhdx**, puis cliquez sur **Ouvrir**.
12. Sur la page **Connecter un disque dur virtuel**, cliquez sur **Suivant**.
13. Sur la page **Fin de l'Assistant Nouvel ordinateur virtuel**, cliquez sur **Terminer**.
14. Dans le **Gestionnaire Hyper-V**, sur **LON-HOST1**, double-cliquez sur l'élément **NANO-SVR1** du volet **Ordinateurs virtuels**.
15. Dans la fenêtre **NANO-SVR1 sur LON-HOST1 – Connexion à un ordinateur virtuel**, cliquez sur **Démarrer**.

Se connecter à l'ordinateur virtuel NANO-SVR1 et consulter les paramètres de base

1. Sur **NANO-SVR1**, dans la zone de texte **Nom d'utilisateur**, tapez **Administrator**, puis appuyez sur la touche TAB.
2. Dans la zone de texte **Mot de passe**, connectez-vous avec le mot de passe **Pa55w.rd**, puis appuyez sur Entrée.
3. Sur **NANO-SVR1**, dans la **console de récupération de Nano Server**, notez que l'ordinateur se nomme **NANO-SVR1** et qu'il appartient à un groupe de travail. Appuyez sur la touche TAB jusqu'à ce que **Mise en réseau** soit sélectionné, puis appuyez sur Entrée.
4. À l'invite **Ethernet**, appuyez sur Entrée.
5. Dans **Paramètres de carte réseau**, notez que DHCP fournit la configuration IP.
6. Notez l'adresse IP.
7. Appuyez deux fois sur Échap.

Ajouter NANO-SVR1 au domaine

1. Passez à **LON-DC1**.
2. Cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (admin)**.
3. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
djoin.exe /provision /domain adatum /machine nano-svr1 /savefile C:\odjblob
```

 **Remarque :** remplacez l'adresse IP 172.16.0.X dans les commandes suivantes par l'adresse IP que vous avez enregistrée plus tôt lors de l'installation de Nano Server.

4. À l'invite de commandes, tapez l'applet de commande suivant, puis appuyez sur Entrée. Votre adresse IP sera différente :

```
Set-Item WSMan:\localhost\Client\TrustedHosts "172.16.0.X"
```

5. Tapez **O** et, quand vous y êtes invité, appuyez sur Entrée.
6. À l'invite de commandes, tapez l'applet de commande suivant, puis appuyez sur Entrée. Votre adresse IP sera différente :

```
$ip = "172.16.0.X"
```

7. À l'invite de commandes, tapez l'applet de commande suivant, puis appuyez sur Entrée :

```
Enter-PSSession -ComputerName $ip -Credential $ip\Administrator
```

8. Dans la boîte de dialogue **Demande d'informations d'identification Windows PowerShell**, dans la zone **Mot de passe**, tapez **Pa55w.rd**, puis cliquez sur **OK**.
9. À l'invite de commandes, tapez l'applet de commande suivant, puis appuyez sur Entrée :

```
netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes
```

10. À l'invite de commandes, tapez l'applet de commande suivant, puis appuyez sur Entrée :

```
Exit-PSSession
```

11. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée. Votre adresse IP sera différente :

```
net use z: \\172.16.0.X\c$
```

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

```
copy c:\odjblob
```

14. À l'invite de commandes, tapez l'applet de commande suivant, puis appuyez sur Entrée :

```
Enter-PSSession -ComputerName $ip -Credential $ip\Administrator
```

15. Dans la boîte de dialogue **Demande d'informations d'identification Windows PowerShell**, dans la zone **Mot de passe**, tapez **Pa55w.rd**, puis cliquez sur **OK**.
16. À l'invite de commandes, tapez **cd**, puis appuyez sur Entrée.
17. À l'invite de commandes, tapez l'applet de commande suivant, puis appuyez sur Entrée :

```
djoin /requestodj /loadfile c:\odjblob /windowspath c:\windows /localos
```

18. À l'invite de commandes, forcez Nano Server à redémarrer en tapant l'applet de commande suivant, puis en appuyant sur Entrée :

```
shutdown /r /t 5
```

19. Ne fermez pas Windows PowerShell. Vous l'utiliserez dans la démonstration suivante.
20. Passez à **NANO-SVR1**.
21. Dans la zone de texte **Nom d'utilisateur**, tapez **Administrator**, puis appuyez sur la touche TAB.
22. Dans la zone de texte **Mot de passe**, tapez **Pa55w.rd**, puis appuyez sur la touche TAB.
23. Dans la zone de texte **Domaine**, tapez **Adatum**, puis appuyez sur Entrée.
24. Dans la **console de récupération de Nano Server**, constatez que l'ordinateur est dans le domaine **adatum.com**.

Démonstration : configuration de la sécurité de Nano Server avec DSC

Étapes de la démonstration

Consulter le script DSC

1. Sur **LON-DC1**, dans la barre des tâches, cliquez sur l'**Explorateur de fichiers**.

2. Dans **l'Explorateur de fichiers**, dans l'arborescence de la console, sélectionnez **Ce PC**, puis, sous **Ce PC**, développez **C:\Labfiles\Mod09**.
3. Cliquez avec le bouton droit sur le fichier **Demo2DscNanoConfig.ps1**, puis cliquez sur **Modifier**. Cela ouvrira l'environnement d'écriture de scripts intégré de Windows PowerShell.
4. Expliquez brièvement les principales parties du script. La partie la plus importante est le bloc qui appelle Service. Il vérifie si le **service de gestion d'ordinateurs virtuels (vmms) Hyper-V** est en cours d'exécution.
5. Fermez **Windows PowerShell ISE** sans modifier ni enregistrer le script. Ne fermez pas l'**Explorateur de fichiers**.

Déployer le script DSC vers NANO-SVR1

1. Retournez à la fenêtre **Windows PowerShell**.
2. Le lecteur Z que vous avez mappé dans la dernière démonstration devrait toujours être mappé. Si ce n'est pas le cas, tapez les instructions suivantes en remplaçant *X* par la valeur utilisée dans la démonstration précédente, puis appuyez sur Entrée :

```
net use z: \\172.16.0.X\c$
```

Remarque : vous pouvez ignorer tout message disant « La commande « z » ne s'est pas exécutée car la session dans laquelle elle devait l'être a été fermée ou interrompue ». Le lecteur sera tout de même mappé correctement.

3. Dans **Windows PowerShell**, tapez les commandes suivantes et appuyez sur Entrée après chacune d'elles :

```
z:
md demo
cd demo
copy c:\Labfiles\Mod09\Demo2DscNanoConfig.ps1
```

4. Dans **Windows PowerShell**, tapez la commande suivante et appuyez sur Entrée :

```
Get-Command -Module PSDesiredStateConfiguration
```

La sortie montre que le package DSC s'est installé correctement en tant que module dans la démonstration précédente. Elle montre ensuite toutes les commandes disponibles dans le module.

5. Dans **Windows PowerShell**, tapez la commande suivante et appuyez sur Entrée :

```
Get-DscResource
```

La sortie de cette commande montre les différentes ressources qui peuvent être manipulées par DSC dans Nano Server.

6. À l'invite de commandes, tapez l'applet de commande suivant en remplaçant le *X* par le dernier octet de votre adresse IP, puis appuyez sur Entrée :

```
$ip = "172.16.0.X"
```

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

```
$cred = Get-Credential
```

8. Dans la fenêtre **Demande d'informations d'identification Windows PowerShell**, dans la zone de texte **Nom d'utilisateur**, tapez **Adatum\administrator**, et dans la zone de texte **Mot de passe**, tapez **Pa55w.rd**. Cliquez ensuite sur **OK**.
9. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
Enter-PSSession -ComputerName $ip -Credential $Cred
```

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

```
Cd C:\demo
```

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

```
.\Demo2DscNanoConfig.ps1 -nodes localhost
```

    Le script renverra un fichier .MOF nommé **NANO-SVR1.MOF**.

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

```
Start-DscConfiguration -ComputerName "NANO-SVR1" -Wait -Force -Verbose -Path
.\NanoConfig
```

13. Le paramètre **Wait** fait un arrêt de quelques secondes pour exécuter le nœud. La commande s'exécute avec succès, ce qui confirme que le service vmms s'exécute bien sur NANO-SVR1.
14. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée :

```
Exit-PSSession
```

15. Fermez toutes les fenêtres, puis déconnectez-vous de **LON-DC1**.

Leçon 3

Présentation des conteneurs

Sommaire :

Questions et réponses

Activité de classement

Question : classez chaque élément ci-dessous.

Éléments	
1	Fournit un environnement de système d'exploitation.
2	Ne contient qu'un mode utilisateur.
3	Fournit une limite d'isolation supplémentaire détenant sa propre copie des fichiers binaires du système d'exploitation.
4	La majeure partie de l'interface utilisateur, la pile applicative et .NET Framework sont supprimés.
5	Vous pouvez utiliser cette image plusieurs fois pour déployer des applications sans changer les couches sous-jacentes.
6	Crée automatiquement un ordinateur virtuel Hyper-V à partir d'une image de base.
7	Peut être utilisé comme plateforme pour un conteneur Windows.
8	Utilise un noyau partagé.
9	Fournit l'isolation nécessaire pour permettre aux applications non approuvées de s'exécuter sur le même hôte.

Catégorie 1		Catégorie 2		Catégorie 3
Nano Server		Un conteneur Windows Server		Un conteneur Hyper-V

Réponse :

Catégorie 1		Catégorie 2		Catégorie 3
Nano Server		Un conteneur Windows Server		Un conteneur Hyper-V
Fournit un environnement de système d'exploitation. La majeure partie de l'interface utilisateur, la pile applicative et .NET Framework sont supprimés. Peut être utilisé comme plateforme pour un conteneur Windows.		Ne contient qu'un mode utilisateur. Vous pouvez utiliser cette image plusieurs fois pour déployer des applications sans changer les couches sous-jacentes. Utilise un noyau partagé.		Fournit une limite d'isolation supplémentaire détenant sa propre copie des fichiers binaires du système d'exploitation. Crée automatiquement un ordinateur virtuel Hyper-V à partir d'une image de base. Fournit l'isolation nécessaire pour permettre aux applications non approuvées de s'exécuter sur le même hôte.

Démonstration : déploiement et gestion de conteneurs Windows Server

Étapes de la démonstration

Examiner le référentiel d'images Microsoft Docker

1. Sur **LON-HOST1**, si nécessaire, cliquez avec le bouton droit sur **Démarrer**, puis cliquez sur **Windows PowerShell (admin)**.
2. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante pour afficher les images téléchargées, puis appuyez sur Entrée :

```
Docker search Microsoft
```

Télécharger une image Docker prédéfinie

1. Tapez la commande suivante, puis appuyez sur Entrée pour afficher les images disponibles sur le hub Docker :

```
Docker images
```

2. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante pour télécharger l'exemple d'image IIS, puis appuyez sur Entrée :

```
docker run hello-world:nanoserver
```

3. Patientez quelques instants jusqu'à ce que l'image soit téléchargée. Lisez la description de l'image.

 **Remarque :** l'applet de commande met environ 2 minutes à s'exécuter. Il renvoie les lignes suivantes :

```
Hello from Docker!
Ce message montre que votre installation semble fonctionner correctement.
Pour générer ce message, Docker a suivi les étapes suivantes :
 1. Le client Docker a contacté le démon Docker.
 2. Le démon Docker a extrait l'image « hello-world » du hub Docker.
 3. Le démon Docker a créé un nouveau conteneur à partir de cette image.
    Il lance l'exécutable qui produit la sortie que vous lisez actuellement.
 4. Le démon Docker a transmis cette sortie au client Docker, qui l'a envoyée
    à votre terminal.
```

4. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante pour vérifier l'image téléchargée, puis appuyez sur Entrée :

```
docker images
```

5. Vous devriez voir trois images Docker :
   a. microsoft/iis
   b. microsoft/nanoserver
   c. hello-world

Déployer un nouveau conteneur avec l'image prédéfinie

- Dans la fenêtre **Windows PowerShell**, tapez la commande suivante pour déployer le conteneur **IIS**, puis appuyez sur Entrée :

```
docker run -d -p 80:80 microsoft/iis ping -t localhost
```

Remarque : Cette commande exécute l'image **IIS** en tant que service d'arrière-plan (**-d**). Elle configure également la mise en réseau de telle sorte que le port 80 de l'hôte conteneur mappe vers le port 80 du conteneur.

Gérer le conteneur

1. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante pour afficher les conteneurs en cours d'exécution, puis appuyez sur Entrée :

```
docker ps
```

2. Remarquez les données de la première colonne sous l'en-tête **ID de conteneur** : c'est une longue chaîne de caractères (par exemple, fd85c4dbffba). Vous pouvez l'utiliser pour arrêter le conteneur. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante pour afficher les conteneurs en cours d'exécution, puis appuyez sur Entrée :

```
Docker stop <ID du conteneur>
```

Remarque : remplacez <ID du conteneur> ci-dessus par la chaîne renvoyée par l'applet de commande **Docker ps** exécuté à l'étape 1.

Démonstration : déploiement de conteneurs Hyper-V

Étapes de la démonstration

1. Dans **Windows PowerShell** sur **LON-HOST1**, tapez les commandes suivantes, puis appuyez sur Entrée :

```
Ipconfig
hostname
```

2. Remarquez que l'adresse IP et le nom d'hôte sont pour **LON-HOST1**.
3. Dans **Windows PowerShell**, tapez la commande suivante et appuyez sur Entrée :

```
docker run -it --isolation=hyperv microsoft/nanoserver cmd
```

4. Une fois la commande ci-dessus exécutée, remarquez que dans la console **Windows PowerShell**, une console de commandes avec un arrière-plan noir s'ouvre. À l'invite, tapez les commandes suivantes, puis appuyez sur Entrée :

```
Ipconfig
hostname
```

5. Remarquez que l'**adresse IP** n'est pas la même que celle notée au cours de l'étape 2 et que le nom d'hôte est une longue chaîne de caractères. Il s'agit du Nano Server que vous venez de créer.
6. Sur **LON-HOST1**, cliquez sur Démarrer, puis sur **Windows PowerShell**. Cela ouvrira une autre console **Windows PowerShell**.
7. Dans la nouvelle fenêtre **Windows PowerShell**, tapez la commande suivante pour afficher les conteneurs en cours d'exécution, puis appuyez sur Entrée :

```
docker ps
```

8. Remarquez les données de la première colonne sous l'en-tête **ID de conteneur** : c'est une longue chaîne de caractères (par exemple, fd85c4dbffba). Dans la nouvelle fenêtre **Windows PowerShell**, tapez la commande suivante pour arrêter le conteneur en cours d'exécution, puis appuyez sur Entrée :

```
Docker stop <ID du conteneur>
```

9. Remplacez la variable par l'ID du conteneur de l'applet de commande docker ps de l'étape 7.
10. Fermez toutes les fenêtres.

Contrôle des acquis et éléments à retenir

Meilleures pratiques

- Une fois SCM 3.0 installé sur le principal ordinateur ou serveur client, partagez le dossier **LocalGPO** pour permettre aux périphériques du groupe de travail et autonomes d'y accéder facilement.
- Pour une expérience graphique complète, gérez Docker sur Nano Server à partir d'un système distant doté de capacités d'interface graphique utilisateur.
- Si vous souhaitez partager des données persistantes entre des conteneurs ou utiliser des données provenant de conteneurs non persistants, vous devez créer un conteneur de volume de données nommé, puis monter les données qu'il contient.

Question de contrôle des acquis

Question : quel est l'environnement de traitement le plus sécurisé qu'il est possible d'avoir : Nano Server, des conteneurs Windows ou des conteneurs Hyper-V ?

> **Réponse :** les conteneurs Hyper-V sont plus sécurisés que les conteneurs Windows, qui sont eux-mêmes plus sécurisés qu'un système d'exploitation serveur déployé de façon traditionnelle. Vous pouvez héberger des conteneurs sur Nano Server, ce qui permet de déployer rapidement et facilement des conteneurs. Toutefois, l'utilisation d'un conteneur Hyper-V sur un Nano Server est la plus sécurisée des trois options.

Outils

Outil	Objectif	Emplacement
SCM	Créer, gérer et déployer des lignes de base de sécurité pour divers produits et systèmes d'exploitation Windows.	Téléchargement gratuit sur Microsoft.com
Docker Enterprise Edition for Windows Server 2016	Docker permet aux conteneurs de s'exécuter comme des processus isolés dans l'espace utilisateur du système d'exploitation hôte, quel qu'il soit.	https://aka.ms/y6lgzc
GitHub	Déployer des conteneurs Hyper-V sur Windows Server	https://aka.ms/puavgj

Questions et réponses relatives à l'atelier pratique

Atelier pratique A : utilisation de SCM

Questions et réponses

Question : si **LON-SVR2** est un serveur autonome dans un groupe de travail, que devez-vous faire pour y appliquer les paramètres de sécurité créés dans la ligne de base **Fusion serveur membre 2012-2016** ?

Réponse : vous pouvez utiliser l'outil en ligne de commande LGPO.exe. Sinon, vous devez ajouter les paramètres de sécurité manuellement.

Question : que devez-vous faire pour fusionner deux lignes de base produit différentes dans SCM ?

Réponse : vous devez d'abord associer les produits.

Atelier pratique B : déploiement et configuration de Nano Server

Questions et réponses

Question : que fait la commande Windows PowerShell ci-dessous ?

```
Docker search Microsoft
```

Réponse : Elle établit la liste de tous les rôles et fonctions prédéfinis des conteneurs Windows créés par Microsoft.

Question : que fait la commande Windows PowerShell ci-dessous ?

```
Get-Command -Module PSDesiredStateConfiguration
```

Réponse : elle montre que le package DSC s'est installé correctement en tant que module, puis elle affiche toutes les commandes disponibles dans le module.

Module 10

Planification et protection des données

Sommaire :

Leçon 1

Planification et implémentation d'un chiffrement

Sommaire :

Questions et réponses

Question : il faut une clé publique pour déchiffrer un fichier chiffré EFS.

( ) Vrai

( ) Faux

Réponse :

( ) Vrai

(√) Faux

Commentaire :

La clé publique permet de chiffrer le fichier. Pour le déchiffrer, il faut une clé privée.

Question : si des utilisateurs disposent de la bonne clé privée, ils peuvent toujours déchiffrer un fichier chiffré EFS.

( ) Vrai

( ) Faux

Réponse :

( ) Vrai

(√) Faux

Commentaire :

Les utilisateurs ne peuvent déchiffrer le fichier que s'ils peuvent y accéder. S'ils n'ont pas l'autorisation de le faire, ils ne pourront pas le déchiffrer.

Question : il faut une AC (autorité de certification) dans le réseau pour chiffrer des fichiers avec EFS.

( ) Vrai

( ) Faux

Réponse :

( ) Vrai

(√) Faux

Commentaires :

Aucune AC n'est requise pour utiliser EFS. Nous vous recommandons d'utiliser des certificats émis par une autorité de certification pour EFS, mais vous pouvez aussi utiliser les certificats auto-signés.

Vue d'ensemble d'EFS

Question : EFS utilise-t-il le chiffrement symétrique ou le chiffrement à clé publique ?

Réponse : EFS utilise une combinaison de ces deux méthodes. Il utilise le chiffrement symétrique pour chiffrer le contenu du fichier et le chiffrement à clé publique pour chiffrer et protéger la clé symétrique utilisée pour le chiffrement du fichier.

Question : qui peut ouvrir un fichier chiffré par EFS ?

Réponse : pour ouvrir un fichier chiffré EFS, l'utilisateur doit avoir l'autorisation d'accéder au fichier. Cependant, il doit aussi avoir la clé privée adéquate, avec laquelle déchiffrer la clé symétrique. L'utilisateur utilise alors la clé symétrique pour déchiffrer et ouvrir le fichier chiffré. Si l'utilisateur dispose de la clé privée adéquate, ce processus est transparent et il peut ouvrir le fichier comme s'il n'était pas chiffré. Si l'utilisateur ne possède pas cette clé, il reçoit un message d'erreur « Accès refusé ».

EFS et certificats

Question : pourquoi les utilisateurs doivent-ils avoir un certificat avant de chiffrer des fichiers avec EFS ?

> **Réponse :** EFS utilise la clé publique de l'utilisateur pour chiffrer la clé symétrique générée aléatoirement pour chiffrer chaque fichier. Si un utilisateur n'a pas de clé publique, EFS ne peut pas chiffrer ni protéger la clé symétrique. Dans ce scénario, EFS obtiendra le certificat utilisateur et effectuera le chiffrement.

Question : est-il possible de partager des fichiers chiffrés EFS avec d'autres utilisateurs ?

> **Réponse :** oui, il est possible de partager des fichiers chiffrés EFS avec d'autres utilisateurs. Cependant, pour ce faire, la clé publique de l'utilisateur doit être disponible. Cela s'explique par le fait qu'EFS en a besoin pour chiffrer la clé symétrique.

Récupération de fichiers chiffrés EFS

Question : comment l'agent de récupération de données peut-il déchiffrer n'importe quel fichier chiffré EFS ?

> **Réponse :** si vous configurez l'agent de récupération de données dans l'environnement, EFS chiffre un exemplaire de la clé symétrique avec la clé publique de l'agent de récupération et l'ajoute au fichier lors du chiffrement. L'agent de récupération de données peut utiliser sa clé privée pour déchiffrer son exemplaire de la clé symétrique et l'utiliser pour déchiffrer le fichier.

Question : si vous ne disposez pas de la bonne clé privée pour déchiffrer le fichier, pouvez-vous copier un fichier chiffré EFS sur la station de travail dédiée de l'agent de récupération depuis l'appareil sur lequel il a été chiffré ?

> **Réponse :** non. Si vous ne disposez pas de la bonne clé privée pour déchiffrer le fichier, vous ne pouvez pas le copier entre des stations de travail. L'opération de copie inclut une opération de lecture du fichier d'origine. Si vous n'avez pas la clé privée appropriée, vous ne pouvez pas ouvrir ni lire le fichier. Vous devez sauvegarder les fichiers chiffrés et les restaurer sur la station de travail dédiée de l'agent de récupération de données.

Résolution des problèmes les plus courants avec EFS

Question : comment un utilisateur qui a perdu sa clé privée peut-il transférer des fichiers chiffrés EFS vers la station de travail dédiée de l'agent de récupération de données ?

> **Réponse :** l'utilisateur n'a pas la clé privée appropriée. Il ne peut donc pas copier les fichiers chiffrés. Cependant, il peut les sauvegarder et transférer la sauvegarde vers la station de travail dédiée de l'agent de récupération de données.

Question : combien de temps faut-il attendre après avoir ajouté le nouvel agent de récupération de données pour pouvoir déchiffrer des fichiers ?

> **Réponse :** le champ de récupération des données (DRF) des fichiers déjà chiffrés ne se met pas à jour automatiquement. Le DRF des fichiers chiffrés est mis à jour quand un utilisateur disposant de la bonne clé privée affiche leurs propriétés ou exécute la commande cipher **/U**.

Ressources

Vue d'ensemble d'EFS

Lectures supplémentaires : pour plus d'informations, consultez « How EFS Works » à l'adresse : http://aka.ms/Uw9drx

Récupération de fichiers chiffrés EFS

Lectures supplémentaires : pour plus d'informations, consultez « Key Recovery vs Data Recovery Differences » à l'adresse : http://aka.ms/Frtdxi

Démonstration : utilisation d'EFS pour sécuriser les données

Étapes de la démonstration

1. Sur **LON-CL1**, dans la barre des tâches, cliquez sur l'icône **Démarrer**, tapez **certmgr.msc**, puis appuyez sur Entrée.
2. Dans la console **Certificats - Utilisateur actuel**, dans le volet de navigation, cliquez sur **Personnel**, puis vérifiez dans le volet d'informations qu'il n'y a pas d'élément à afficher dans cette vue.
3. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
4. Dans l'Explorateur de fichiers, dans le volet de navigation, développez **Ce PC**, puis **Disque local (C:)** et **Labfiles**, et sélectionnez **Mod10**. Dans le volet d'informations, cliquez avec le bouton droit sur **Adam1**, sélectionnez **Propriétés**, puis cliquez sur **Avancé**.
5. Dans la boîte de dialogue **Attributs avancés**, indiquez que le bouton **Détails** est grisé et non disponible, car le fichier n'est pas encore chiffré. Activez la case à cocher **Chiffrer le contenu pour sécuriser les données**, puis cliquez sur **OK**. Cliquez sur **Appliquer**, sélectionnez l'option **Chiffrer le fichier uniquement**, puis cliquez sur **OK**.
6. Attendez quelques secondes, puis expliquez que le chiffrement du premier fichier de l'utilisateur prend quelques secondes, car EFS doit obtenir un certificat utilisateur avant de chiffrer le fichier.
7. Dans la boîte de dialogue **Propriétés de Adam1**, cliquez sur **Avancé**, puis sur **Détails**. Indiquez qu'Adam Hobbs peut accéder au fichier et que l'administrateur a un certificat de récupération pour le fichier.
8. Cliquez sur **Ajouter** et, dans la boîte de dialogue **Système de fichiers EFS (Encrypting File System)**, indiquez que seul Adam Hobbs apparaît dans la liste. Expliquez ensuite qu'Adam est le seul utilisateur à détenir une clé publique. Cliquez quatre fois sur **Annuler**.
9. Dans l'Explorateur de fichiers, indiquez que le fichier **Adam1** est surmonté d'une petite icône de verrou, car il est protégé par EFS. Indiquez que les autres fichiers du dossier n'ont pas cette icône.
10. Dans la console **Certificats - Utilisateur actuel**, actualisez la vue en appuyant sur la touche **F5**. Dans le volet de navigation, développez **Personnel**, puis cliquez sur **Certificats**. Dans le volet d'informations, indiquez qu'un certificat est répertorié et montrez qu'il a été attribué à Adam Hobbs pour chiffrer le système de fichiers.
11. Dans la barre des tâches, cliquez sur l'icône **Démarrer**, puis sur **Adam Hobbs**, et enfin sur **Changer de compte**.
12. Connectez-vous à **LON-CL1** en tant que **ADATUM\Dawn** avec le mot de passe **Pa55w.rd**.

13. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
14. Dans l'Explorateur de fichiers, dans le volet de navigation, développez **Ce PC**, puis **Disque local (C:)** et **Labfiles**, et sélectionnez **Mod10**.
15. Dans le volet d'informations, double-cliquez sur **Adam1** et indiquez que vous obtenez une erreur « Accès refusé », car Dawn ne dispose pas de la clé privée d'Adam pour déchiffrer le fichier. Cliquez sur **OK** et fermez le Bloc-notes.
16. Dans l'Explorateur de fichiers, dans le volet d'informations, cliquez avec le bouton droit sur **Don1**, puis sélectionnez **Propriétés**.
17. Dans la boîte de dialogue **Propriétés**, cliquez sur **Avancé**. Activez la case à cocher **Chiffrer le contenu pour sécuriser les données**, cliquez sur **OK**, puis cliquez à nouveau sur **OK**. Sélectionnez **Chiffrer le fichier uniquement**, activez la case à cocher **Toujours chiffrer le fichier uniquement**, puis cliquez sur **OK**.
18. Attendez quelques secondes et indiquez que c'est le premier fichier chiffré par Dawn. Expliquez que, de ce fait, EFS doit obtenir un certificat utilisateur. Le chiffrement est donc un peu plus lent que lorsqu'un utilisateur détient déjà un certificat EFS.
19. Dans la boîte de dialogue **Propriétés de Don1**, cliquez sur **Avancé**, puis sur **Détails**. Indiquez que Dawn Williamson peut accéder au fichier et que l'administrateur a un certificat de récupération pour ce dernier.
20. Cliquez sur **Ajouter**, sélectionnez **Adam Hobbs**, puis cliquez sur **OK**. Indiquez qu'à présent Adam Hobbs et Dawn Williamson peuvent accéder au fichier, puis cliquez trois fois sur **OK**.
21. Dans la barre des tâches, cliquez sur l'icône **Démarrer**, puis sur **Dawn Williamson**, et sélectionnez **ADATUM\Adam**.
22. Connectez-vous à **LON-CL1** en tant que **ADATUM\Adam** avec le mot de passe **Pa55w.rd**.
23. Dans l'Explorateur de fichiers, double-cliquez sur **Don1**. Vérifiez que le fichier s'ouvre et que vous pouvez en lire le contenu. Expliquez que Dawn a fourni à Adam un accès au fichier chiffré.
24. Fermez le Bloc-notes.

Leçon 2

Planification et implémentation de BitLocker

Sommaire :

Questions et réponses

Question : pour utiliser BitLocker, votre appareil doit avoir un TPM.

( ) Vrai

( ) Faux

Réponse :

( ) Vrai

(√) Faux

Commentaires :

Windows Server 10 vous permet d'utiliser BitLocker sans TPM.

Question : les lecteurs protégés avec BitLocker à partir de Windows 8.1 peuvent être déverrouillés sous Windows 10.

( ) Vrai

( ) Faux

Réponse :

( ) Vrai

(√) Faux

Commentaires :

La version de BitLocker contenu dans les versions antérieures de Windows 10 est compatible avec Windows 10. Dans Windows 10 version 1511 et ultérieure, vous pouvez utiliser le nouveau mode de chiffrement BitLocker, qui n'est pas rétrocompatible.

Question : quand vous activez BitLocker pour le lecteur C, vous pouvez aussi préciser de stocker la clé de récupération dans AD DS.

( ) Vrai

( ) Faux

Réponse :

( ) Vrai

(√) Faux

Commentaire :

Quand vous activez BitLocker pour un lecteur, vous pouvez spécifier où l'emplacement de stockage du lecteur de récupération, mais vous pouvez seulement choisir une clé USB, un fichier, un compte Microsoft ou de l'imprimer. Vous ne pouvez pas stocker la clé de récupération BitLocker sur AD DS dans un assistant. Vous ne pouvez le faire qu'en utilisant une stratégie de groupe.

Vue d'ensemble de BitLocker

Question : peut-on utiliser BitLocker pour chiffrer uniquement les données confidentielles du volume, en omettant les autres données ?

Réponse : non. Quand vous activez BitLocker sur un volume, toutes ses données sont chiffrées.

Question : peut-on utiliser BitLocker pour chiffrer tous les volumes d'un appareil Windows ?

Réponse : non. BitLocker ne peut pas chiffrer les volumes système, mais il peut chiffrer tous les autres volumes, quel que soit leur système d'exploitation.

BitLocker et TPM

Question : comment configurer BitLocker afin qu'il fonctionne sur un appareil sans TPM ?

> **Réponse :** par défaut, BitLocker nécessite un TPM. Pour les appareils qui n'en ont pas, vous pouvez utiliser une stratégie de groupe pour lui permettre de fonctionner sans TPM. Dans ce cas, BitLocker a besoin d'une clé de démarrage USB pour chiffrer un volume.

Question : quel est l'inconvénient d'exécuter BitLocker sur un appareil Windows sans TPM ?

> **Réponse :** il est toujours possible de chiffrer des volumes sur un appareil Windows, même s'il n'a pas de TPM. Toutefois, l'appareil ne sera pas en mesure d'utiliser la vérification de l'intégrité du système lors du démarrage.

Configuration et gestion de BitLocker

Question : quels outils peut-on utiliser pour la configuration et la gestion de BitLocker ?

> **Réponse :** on peut configurer et gérer BitLocker avec l'outil de chiffrement de lecteur BitLocker du panneau de configuration, des applets de commande Windows PowerShell, l'outil de configuration du chiffrement de lecteur BitLocker (Manage-bde.exe), ainsi que l'outil MBAM, si votre entreprise dispose de la licence pour utiliser le Microsoft Desktop Optimization Pack (MDOP).

Question : vous avez activé le paramètre de stratégie de groupe **Enregistrer les informations de récupération BitLocker dans les services de domaine Active Directory (Windows Server 2008 et Windows Vista)** sur un appareil Windows 10. Les informations de récupération de BitLocker sont-elles enregistrées dans AD DS quand vous activez BitLocker ?

> **Réponse :** non. Ce paramètre de stratégie de groupe s'applique uniquement à Windows Server 2008 et Windows Vista. Il ne s'applique pas à Windows 10. Si vous voulez enregistrer une clé de récupération BitLocker sur un appareil Windows 10, vous devez activer l'option **Sélectionner la méthode de récupération des lecteurs du système d'exploitation protégés par BitLocker**, **Sélectionner la méthode de récupération des lecteurs fixes protégés par BitLocker** ou **Sélectionner la méthode de récupération des lecteurs amovibles protégés par BitLocker**.

Récupération d'un lecteur chiffré avec BitLocker

Question : lors de l'activation de BitLocker sur un appareil avec TPM, quel est l'intérêt d'enregistrer le mot de passe de récupération ?

> **Réponse :** si le TPM change ou est inaccessible, si des modifications sont apportées à des fichiers système clés ou si quelqu'un essaie de démarrer l'appareil à partir d'un support de démarrage pour contourner le système d'exploitation, l'appareil bascule en mode de récupération et y reste jusqu'à ce que l'utilisateur fournisse le mot de passe de récupération. Le fait d'enregistrer le mot de passe de récupération afin qu'il soit accessible à l'utilisateur permet à ce dernier d'effectuer le processus de démarrage.

Question : quelle est la différence entre le mot de passe de récupération et l'ID de mot de passe ?

> **Réponse :** le mot de passe de récupération est un mot de passe à 48 chiffres qui déverrouille un appareil protégé avec BitLocker. Il est propre à un chiffrement BitLocker particulier. Vous pouvez l'enregistrer dans AD DS, sur une clé USB ou dans un fichier. L'ID de mot de passe est un identifiant à 32 caractères propre à un lecteur chiffré. On le trouve dans l'onglet **Récupération BitLocker** sur la page de propriétés de l'objet Ordinateur dans Utilisateurs et ordinateurs Active Directory.

Gestion de BitLocker avec Microsoft BitLocker Administration and Monitoring (MBAM)

Question : comment pouvez-vous utiliser MBAM pour réduire le temps que le support technique passe à récupérer une clé de déverrouillage BitLocker pour un utilisateur à distance ?

> **Réponse :** les administrateurs peuvent activer le portail libre-service de MBAM afin de permettre aux utilisateurs de récupérer un mot de passe de récupération BitLocker sans avoir à téléphoner à leur support technique.

Question : votre entreprise n'utilise que des appareils Windows 10 protégés avec BitLocker et gérés avec Microsoft Intune. Pouvez-vous déployer MBAM dans votre entreprise ?

> **Réponse :** MBAM nécessite AD DS et SQL Server. Votre entreprise n'utilisant que des appareils Windows 10, elle ne dispose pas de la configuration requise pour déployer MBAM.

Ressources

Vue d'ensemble de BitLocker

Lectures supplémentaires : pour plus d'informations, consultez « BitLocker Overview » à l'adresse : http://aka.ms/eiaxj5

Configuration et gestion de BitLocker

Lectures supplémentaires : pour plus d'informations, consultez « BitLocker: Use BitLocker Drive Encryption Tools to manage BitLocker » à l'adresse : http://aka.ms/kyndxu

Lectures supplémentaires : pour plus d'informations, consultez « BitLocker Group Policy Settings » à l'adresse : http://aka.ms/Bvxso5

Gestion de BitLocker avec Microsoft BitLocker Administration and Monitoring (MBAM)

Lectures supplémentaires : pour plus d'informations, consultez « Microsoft BitLocker Administration and Monitoring » à l'adresse : https://technet.microsoft.com/fr-fr/windows/hh826072.aspx

Démonstration : Utilisation de Bitlocker

Étapes de la démonstration

1. Sur **LON-CL1**, dans la barre des tâches, cliquez sur l'icône **Démarrer**, tapez **gpedit.msc**, puis appuyez sur Entrée.
2. Dans l'Éditeur de stratégie de groupe locale, dans le volet de navigation, développez **Configuration ordinateur**, puis **Modèles d'administration**, puis **Composants Windows** et enfin **Chiffrement de lecteur BitLocker**.
3. Dans le volet de navigation, cliquez sur **Lecteurs du système d'exploitation**, puis, dans le volet d'informations, double-cliquez sur **Exiger une authentification supplémentaire au démarrage**.

4. Dans la boîte de dialogue **Exiger une authentification supplémentaire au démarrage**, cliquez sur **Activé**. Vérifiez que la case à cocher **Autoriser BitLocker sans un module de plateforme sécurisée compatible** est activée, puis cliquez sur **OK**.

Remarque : expliquez que cette configuration n'est nécessaire que si l'appareil n'a pas de TPM.

5. Dans le volet de navigation, cliquez sur le nœud **Lecteurs de données fixes** et, dans le volet d'informations, double-cliquez sur **Sélectionner la méthode de récupération des lecteurs fixes protégés par BitLocker**.
6. Dans la boîte de dialogue **Sélectionner la méthode de récupération des lecteurs fixes protégés par BitLocker**, cliquez sur **Activé**, puis sur **OK**.
7. Sur **LON-CL1**, dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**.
8. Dans l'Explorateur de fichiers, dans le volet de navigation, développez **Ce PC**, cliquez sur **Data (E:)**, cliquez avec le bouton droit dans l'espace vide du volet d'informations, sélectionnez **Nouveau**, cliquez sur **Document texte**, tapez votre nom et appuyez sur Entrée.
9. Dans l'Explorateur de fichiers, dans le volet de navigation, cliquez avec le bouton droit sur **Data (E:)**, puis cliquez sur **Activer BitLocker**.
10. Dans la boîte de dialogue **Chiffrement de lecteur BitLocker (E:)**, activez la case à cocher **Utiliser un mot de passe pour déverrouiller le lecteur**. Dans les zones de texte **Entrer votre mot de passe** et **Entrer à nouveau votre mot de passe**, tapez **Pa55w.rd**, puis cliquez sur **Suivant**.
11. Sur la page **Comment voulez-vous sauvegarder votre clé de récupération ?**, cliquez sur **Enregistrer dans un fichier**.
12. Dans la boîte de dialogue **Enregistrer la clé de récupération BitLocker sous**, dans le volet de navigation, cliquez sur **Ce PC**, faites défiler le volet d'informations et double-cliquez sur **Lecteur de disquettes (A:)**, puis cliquez sur **Enregistrer** et sur **Suivant**.
13. Sur la page **Choisir le mode de chiffrement à utiliser**, cliquez sur **Suivant**, puis sur **Démarrer le chiffrement**.
14. Dans l'Explorateur de fichiers, dans le volet de navigation, indiquez que Disque local (E:) est surmonté d'une petite icône de verrou.
15. Dans la fenêtre de **connexion de l'ordinateur virtuel 22744B-LON-CL1**, cliquez sur le menu **Fichier**, puis sur **Paramètres**.
16. Dans la fenêtre **Paramètres pour 22744B-LON-CL1**, dans le volet de navigation, sous Contrôleur SCSI, cliquez sur **Disque dur Disk1.vhd**. Dans le volet d'informations, cliquez sur **Supprimer**, puis sur **OK**.
17. Dans la fenêtre de **connexion de l'ordinateur virtuel 22744B-LON-CL2**, cliquez sur le menu **Fichier**, puis sur **Paramètres**.
18. Dans la boîte de dialogue **Paramètres pour 22744B-LON-CL2**, dans le volet de navigation, cliquez sur **Contrôleur SCSI**. Dans le volet d'informations, cliquez sur **Disque dur**, sur **Ajouter**, puis sur **Parcourir**, accédez à **D:\Program Files\Microsoft Learning\22744\Drives**, cliquez sur **Disk1.vhd**, sur **Ouvrir**, puis sur **OK**.
19. Dans la barre des tâches, cliquez sur l'icône **Explorateur de fichiers**. Dans le volet de navigation, indiquez que le lecteur E est répertorié sous le nom **Disque local (E:)** et qu'il est surmonté d'une petite icône de verrou.

20. Dans l'Explorateur de fichiers, dans le volet de navigation, cliquez sur **Disque local (E:)**. La boîte de dialogue **BitLocker (E:)** s'affiche.
21. Dans la boîte de dialogue **BitLocker (E:)**, dans la zone de texte, saisissez **Pa55w.rd**, puis cliquez sur **Déverrouiller**.
22. Dans l'Explorateur de fichiers, dans le volet de navigation, indiquez que le lecteur E apparaît sous le nom Data (E:) et plus comme Disque local (E:).

Remarque : dans le volet d'informations, indiquez que vous voyez le fichier portant votre nom.

23. Sur **LON-DC1**, dans la barre des tâches, cliquez sur l'icône **Gestionnaire de serveur**.
24. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
25. Dans la fenêtre Utilisateurs et ordinateurs Active Directory, dans le volet de navigation, développez **Adatum.com**, puis cliquez sur **Ordinateurs**.
26. Dans le volet d'informations, cliquez avec le bouton droit sur **LON-CL1**, puis cliquez sur **Propriétés**.
27. Dans la boîte de dialogue **Propriétés de : LON-CL1**, cliquez sur l'onglet **Récupération BitLocker**.

Remarque : indiquez que le mot de passe de récupération BitLocker pour le disque chiffré sur **LON-CL1** s'affiche.

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : peut-on chiffrer un volume entier avec le chiffrement de fichier EFS ?

Réponse : on peut activer EFS au niveau des fichiers ou des dossiers, mais pas au niveau du volume. Toutefois, il est possible d'appliquer EFS à tous les dossiers et fichiers du dossier racine du volume, ce qui chiffre toutes les données de ce dernier.

Question : peut-on chiffrer des fichiers système Windows avec EFS ?

Réponse : non. On ne peut pas chiffrer des fichiers ayant l'attribut Système avec le chiffrement de fichiers EFS.

Question : peut-on effectuer le nettoyage complet d'un appareil Windows perdu ?

Réponse : non. Les appareils Windows ne prennent en charge que le nettoyage sélectif. Il est possible d'effectuer un nettoyage sélectif sur un appareil Windows si ce dernier est géré par Microsoft Intune, Microsoft System Center Configuration Manager ou une autre solution de gestion d'appareil mobile.

Questions et réponses relatives à l'atelier pratique

Atelier pratique : protection des données avec le chiffrement et BitLocker

Questions et réponses

Question : pourquoi l'administrateur de **LON-CL2** n'a-t-il pas pu ouvrir le fichier **Adam1.txt** bien que le compte soit un agent de récupération de données ?

Réponse : par défaut, le certificat de récupération de données de l'administrateur n'est enregistré que sur le premier contrôleur de domaine. L'administrateur n'ayant pas son certificat de récupération de données sur **LON-CL2**, il n'a pas pu ouvrir le fichier. Il a pu le faire après avoir importé le certificat.

Question : pourquoi avez-vous dû configurer **LON-CL1** de façon à autoriser l'utilisation de BitLocker sans TPM compatible ?

Réponse : les ordinateurs virtuels n'ont pas de TPM. BitLocker nécessite un TPM par défaut. Si cette condition n'est pas modifiée, vous ne pouviez pas utiliser BitLocker sur **LON-CL1**.

Module 11

Optimisation et sécurisation des services de fichiers

Sommaire :

Leçon 1

Gestionnaire de ressources du serveur de fichiers

Sommaire :

Questions et réponses

Question : les quotas doivent-ils être implémentés dans toutes les données ou uniquement à des emplacements sélectionnés ?

> **Réponse :** les réponses peuvent varier. Cependant, les quotas appliqués à toutes les données peuvent entraîner des conséquences inattendues. Vous devez planifier soigneusement les paramètres de quota avant d'implémenter ceux-ci.

Question : dans votre environnement, implémenteriez-vous le filtrage de fichiers ?

> **Réponse :** les réponses varient. Cependant, vous devez prendre en compte les implications du filtrage de fichiers avant de le mettre en place.

Démonstration : installation et configuration de FSRM

Étapes de la démonstration

Installer le service de rôle FSRM

1. Si vous n'êtes pas connecté, connectez-vous à **LON-SVR1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, sur **Gestionnaire de serveur**, sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**.
3. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Suivant**.
4. Vérifiez que l'option **Installation basée sur un rôle ou une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.
5. Vérifiez que **LON-SVR1.Adatum.com** est sélectionné, puis cliquez sur **Suivant**.
6. Sur la page **Sélectionner des rôles de serveurs**, développez **Services de fichiers et de stockage (2 sur 12 installés)**, développez **Services de fichiers et iSCSI (1 sur 11 installés)**, puis activez la case à cocher **Gestionnaire de ressources du serveur de fichiers**.
7. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**.
8. Cliquez deux fois sur **Suivant** pour confirmer la sélection de service de rôle et des fonctionnalités.
9. Sur la page **Confirmer les sélections d'installation**, cliquez sur **Installer**.
10. Une fois l'installation terminée, cliquez sur **Fermer**.

Spécifier les options de configuration FSRM

1. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire de ressources du serveur de fichiers**.
2. Dans la console **Gestionnaire de ressources du serveur de fichiers**, dans le panneau de navigation, cliquez avec le bouton droit sur **Gestionnaire de ressources du serveur de fichiers (local)**, puis cliquez sur **Configurer les options**.
3. Dans la boîte de dialogue **Options du gestionnaire de ressources du serveur de fichiers**, cliquez sur l'onglet **Vérification du filtrage de fichiers**, puis activez la case à cocher **Enregistrer l'activité de filtrage de fichiers dans la base de données de vérification**.
4. Cliquez sur **OK** pour fermer la boîte de dialogue **Options du gestionnaire de ressources du serveur de fichiers**. Fermez la console **Gestionnaire de ressources du serveur de fichiers**.

Utiliser Windows PowerShell pour gérer FSRM

1. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Windows PowerShell**.
2. Dans l'invite de commandes **Windows PowerShell**, tapez la commande suivante et appuyez sur Entrée :

```
set-FSRMSetting -SMTPServer "SMTPServer" –AdminEmailAddress "fileadmin@adatum.com" –
FromEmailAddress Lon-SVR1@adatum.com
```

3. Fermez la fenêtre **Windows PowerShell**.
4. Ouvrez la console **Gestionnaire de ressources du serveur de fichiers**.
5. Dans la fenêtre **Gestionnaire de ressources du serveur de fichiers**, dans le volet de navigation, cliquez avec le bouton droit sur **Gestionnaire de ressources du serveur de fichiers (local)**, puis cliquez sur **Configurer les options**.
6. Dans l'onglet **Notifications par courrier électronique**, vérifiez les options configurées pour confirmer qu'il s'agit des options spécifiées dans la commande **Set-FSRMSetting**.
7. Fermez toutes les fenêtres.

Démonstration : surveillance du rapport d'utilisation des quotas

Étapes de la démonstration

Créer un quota

1. Si vous n'êtes pas connecté, connectez-vous à **LON-SVR1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Cliquez sur **Démarrer**, puis sur **Gestionnaire de serveur**.
3. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire de ressources du serveur de fichiers**.
4. Dans le **Gestionnaire de ressources du serveur de fichiers**, développez le nœud **Gestion de quota**, puis cliquez sur **Modèles de quotas**.
5. Cliquez avec le bouton droit sur le modèle **Limite de 100 Mo**, puis cliquez sur **Créer un quota à partir d'un modèle**.
6. Dans la fenêtre **Créer un quota**, cliquez sur **Parcourir**.
7. Dans la fenêtre **Rechercher un dossier**, développez **Allfiles (D:)**, puis **Labfiles** et **Mod11**. Cliquez ensuite sur **Données**, puis sur **OK**.
8. Dans la fenêtre **Créer un quota**, cliquez sur **Créer**.
9. Dans la fenêtre **Gestionnaire de ressources du serveur de fichiers**, cliquez sur **Quotas** pour afficher le quota récemment créé.

Tester un quota

1. Cliquez sur **Démarrer**, puis sur l'icône **Windows PowerShell**.
2. Dans la fenêtre **Windows PowerShell**, tapez les deux commandes suivantes, puis appuyez sur Entrée après chacune d'elles :

```
cd D:\labfiles\Mod11\data
Fsutil file createnew largefile.txt 130000000
```

3. Notez que le message suivant s'affiche : **Erreur : Espace insuffisant sur le disque.**
4. Fermez la fenêtre **Windows PowerShell**.

Démonstration : implémentation d'un filtre de fichiers

Étapes de la démonstration

Créer un filtre de fichiers

1. Dans la fenêtre **Gestionnaire de ressources du serveur de fichiers**, développez le nœud **Gestion du filtrage de fichiers**, puis cliquez sur **Modèles de filtres de fichiers**.
2. Cliquez avec le bouton droit sur le modèle **Bloquer les fichiers image**, puis cliquez sur **Créer un filtre de fichiers à partir d'un modèle**.
3. Dans la fenêtre **Créer un filtre de fichiers**, cliquez sur **Parcourir**.
4. Dans la fenêtre **Rechercher un dossier**, développez **Allfiles (D:)**, puis **Labfiles** et **Mod11**. Cliquez ensuite sur **Données**, puis sur **OK**.
5. Dans la fenêtre **Créer un filtre de fichiers**, cliquez sur **Créer**.

Tester un filtre de fichiers

1. Ouvrez l'**Explorateur de fichiers**.
2. Dans la fenêtre de l'**Explorateur de fichiers**, développez **Ce PC**, puis **Allfiles (D:)** et **Labfiles**, puis cliquez sur **Mod11**.
3. Dans l'**Explorateur de fichiers**, cliquez sur l'onglet **Accueil**, puis sur **Nouvel élément** et **Image bitmap**.
4. Tapez **testimage** et appuyez sur Entrée.
5. Confirmez que le fichier a été créé avec succès.
6. Cliquez avec le bouton droit sur **testimage**, puis cliquez sur **Copier**.
7. Cliquez avec le bouton droit sur **Données**, puis cliquez sur **Coller**.
8. Vous recevrez un message indiquant que vous avez besoin d'une autorisation pour effectuer cette action. Cliquez sur **Annuler** pour fermer la boîte de dialogue.
9. Fermez l'**Explorateur de fichiers**.

Démonstration : génération de rapports de stockage à la demande

Étapes de la démonstration

Générer un rapport de stockage

1. Dans le **Gestionnaire de ressources du serveur de fichiers**, dans le volet de navigation, cliquez et cliquez avec le bouton droit sur **Gestion des rapports de stockage**, puis cliquez sur **Générer les rapports maintenant**.
2. Dans la fenêtre **Propriétés des tâches de rapports de stockage**, activez la case à cocher **Fichiers volumineux**
3. Cliquez sur l'onglet **Étendue**, puis sur **Ajouter**.
4. Dans la boîte de dialogue **Rechercher un dossier**, cliquez sur **Allfiles (D:)**, puis sur **OK**.
5. Dans la boîte de dialogue **Propriétés des tâches de rapports de stockage**, cliquez sur **OK**.

6. Dans la boîte de dialogue **Générer des rapports de stockage**, vérifiez qu'**Attendre que les rapports soient générés avant de les afficher** est sélectionné, puis cliquez sur **OK** pour générer le rapport.
7. Dans **l'Explorateur de fichiers**, dans le dossier **Interactive**, cliquez avec le bouton droit sur le fichier html, cliquez sur **Ouvrir avec**, puis sur **Internet Explorer**, sur **OK** et examinez le rapport.
8. Fermez la fenêtre du rapport.
9. Fermez la fenêtre de l'**Explorateur de fichiers**.
10. Fermez la fenêtre **Gestionnaire de ressources du serveur de fichiers**.
11. Fermez la fenêtre **Gestionnaire de serveur**.

Leçon 2

Implémentation de tâches de classification et de gestion de fichiers

Sommaire :

Questions et réponses

Question : comment pourriez-vous utiliser la classification automatique dans votre environnement ?

> **Réponse :** les réponses varient. Certains stagiaires peuvent évoquer la classification avec AD RMS afin de mettre en place une solution basique de prévention des pertes de données.

Démonstration : Configuration de la classification des fichiers

Étapes de la démonstration

Créer une propriété de classification

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, puis sur l'icône **Gestionnaire de serveur**.
2. Dans la console **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire de ressources du serveur de fichiers**.
3. Dans le **Gestionnaire de ressources du serveur de fichiers**, développez **Gestion de la classification**, puis cliquez et cliquez avec le bouton droit sur **Propriétés de classification** et cliquez sur **Créer une propriété locale**.
4. Dans la fenêtre **Créer la propriété de classification locale**, dans la zone de texte **Nom**, tapez **Documents**. Dans la liste déroulante **Type de propriété**, vérifiez que **Oui/Non** est sélectionné, puis cliquez sur **OK**.

Créer une règle de classification

1. Dans le **Gestionnaire de ressources du serveur de fichiers**, développez **Gestion de la classification**, cliquez sur **Règles de classification**, puis, dans le volet **Action**, cliquez sur **Créer une règle de classification**.
2. Dans la fenêtre **Créer une règle de classification**, dans l'onglet **Général**, dans la zone de texte **Nom de la règle**, tapez **Règle des documents d'entreprise** et vérifiez que la case **Activé** est sélectionnée.
3. Dans la fenêtre **Créer une règle de classification**, dans l'onglet **Étendue**, cliquez sur **Ajouter**.
4. Dans la fenêtre **Rechercher un dossier**, développez **Allfiles (D:)**, **Labfiles**, **Mod11**, puis cliquez sur le dossier **Documents** et sur **OK**.
5. Dans la fenêtre **Créer une règle de classification**, dans l'onglet **Classification**, dans la liste déroulante **Méthode de classification**, cliquez sur **Classificateur de dossiers**. Dans la liste déroulante **Propriété - Choisissez une propriété à attribuer aux fichiers**, cliquez sur **Documents**, puis, dans la liste déroulante **Propriété - Spécifier une valeur**, cliquez sur **Oui**.
6. Dans la fenêtre **Créer une règle de classification**, dans l'onglet **Type d'évaluation**, cliquez sur **Réévaluer les valeurs de propriété existantes** et vérifiez que l'option **Agréger les valeurs** est sélectionnée, puis cliquez sur **OK**.
7. Dans le **Gestionnaire de ressources du serveur de fichiers**, dans le volet **Action**, cliquez sur **Exécuter la classification avec toutes les règles maintenant.**
8. Dans la fenêtre **Exécuter la classification**, sélectionnez la case d'option **Attendre la fin de la classification**, puis cliquez sur **OK**.
9. Examinez le **Rapport de classification automatique** qui s'affiche dans Windows Internet Explorer, puis vérifiez que le rapport répertorie le même nombre de fichiers que ceux classifiés dans le dossier **Documents**. Il devrait y avoir trois fichiers.
10. Fermez Internet Explorer.

Démonstration : configuration des tâches de gestion de fichiers

Étapes de la démonstration

Créer un fichier

1. Sur **LON-SVR1**, dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
2. Dans **D:\Labfiles\Mod11\Documents**, cliquez avec le bouton droit sur **Strategy1.txt**, puis cliquez sur **Copier**. Cliquez avec le bouton droit dans le volet droit, puis cliquez sur **Coller**.

Créer une tâche de gestion de fichiers

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, puis sur le raccourci **Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire de ressources du serveur de fichiers**.
3. Dans le **Gestionnaire de ressources du serveur de fichiers**, sélectionnez le nœud **Tâches de gestion de fichiers** et cliquez dessus avec le bouton droit, puis cliquez sur **Créer une tâche de gestion de fichiers**.
4. Dans la zone de texte **Nom de la tâche**, tapez **Documents expirés**.
5. Dans la zone de texte **Description**, tapez **Déplacer les anciens documents dans un autre dossier**.
6. Cliquez sur l'onglet **Étendue**.
7. Dans la section **Étendue**, cliquez sur **Ajouter**.
8. Développez **Allfiles (D:)**, **Labfiles** et **Mod11**, puis cliquez sur **Documents** et sur **OK**.

Configurer une tâche de gestion de fichiers pour les documents expirés

1. Dans la fenêtre **Créer une tâche de gestion de fichiers**, cliquez sur l'onglet **Action**.
2. Dans l'onglet **Action**, sous Type, sélectionnez **Expiration de fichier**.
3. Dans **Répertoire d'expiration**, tapez **D:\Labfiles\Mod11\Data**.
4. Dans la fenêtre **Créer une tâche de gestion de fichiers**, cliquez sur l'onglet **Condition**.
5. Sous l'onglet **Condition**, activez la case à cocher **Modèles de noms de fichiers**, puis tapez ***Copier*** dans la zone de texte.
6. Dans la fenêtre **Créer une tâche de gestion de fichiers**, cliquez sur l'onglet **Planification**.
7. Sélectionnez **Tous les mois**, puis activez la case à cocher **Dernier**.
8. Dans la fenêtre **Créer une tâche de gestion de fichiers**, cliquez sur **OK**.
9. Cliquez avec le bouton droit sur la tâche **Documents expirés**, puis cliquez sur **Exécuter maintenant une tâche de gestion de fichiers...**
10. Dans la fenêtre **Exécuter une tâche de gestion de fichiers**, choisissez **Attendre la fin de l'exécution de la tâche**, puis cliquez sur **OK**.
11. Affichez le rapport généré et confirmez qu'un fichier a été déplacé.
12. Cliquez sur le lien **Répertoire d'expiration** dans l'en-tête du rapport, puis développez les répertoires pour voir le fichier expiré.
13. Ouvrez le dossier **D:\Labfiles\Mod11\Documents** pour voir le contenu. Le fichier **Strategy1 - Copy.txt** ne s'y trouve pas.
14. Fermez toutes les fenêtres.

Leçon 3

Contrôle d’accès dynamique

Sommaire :

Questions et réponses

Question : quelles technologies sont requises pour utiliser le contrôle d'accès dynamique ?

( ) Services de domaine Active Directory

( ) Kerberos

( ) AD CS

( ) AD RMS

( ) AD FS

Réponse :

(√) Services de domaine Active Directory

(√) Kerberos

( ) AD CS

( ) AD RMS

( ) AD FS

Commentaire :

Seuls AD DS et Kerberos sont requis pour le contrôle d'accès dynamique, même si la classification des fichiers peut utiliser AD RMS.

Question : le contrôle d'accès dynamique dans Windows Server 2016 prend en charge les revendications des utilisateurs et des ordinateurs.

( ) Vrai

( ) Faux

Réponse :

(√) Vrai

( ) Faux

Commentaire :

Le contrôle d'accès dynamique prend en charge les revendications des utilisateurs et des ordinateurs. Ces dernières sont basées sur des attributs dans AD DS et sur les valeurs de ceux-ci.

Ressources

Technologies de base pour le contrôle d'accès dynamique

Lectures supplémentaires : pour plus d'informations sur les modifications dans Kerberos v5 relatives au blindage Kerberos, consultez : http://aka.ms/v54k6z

Implémentation et configuration de stratégies d'accès centralisées

Lectures supplémentaires : téléchargez Microsoft Data Classification Toolkit à l'adresse : http://aka.ms/alw15o

Lectures supplémentaires : pour dépanner le contrôle d'accès dynamique si vos utilisateurs n'obtiennent pas un accès correct, téléchargez le guide « Understand and Troubleshoot Dynamic Access Control in Windows Server 2012 » à l'adresse : http://aka.ms/w2d2fo

Démonstration : configuration du contrôle d'accès dynamique

Étapes de la démonstration

Préparer AD DS pour le contrôle d'accès dynamique

1. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans la fenêtre **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur **Adatum.com**, cliquez sur **Nouveau**, puis sur **Unité d'organisation**.
3. Dans la boîte de dialogue **Nouvel objet - Unité d'organisation**, dans la zone de texte **Nom**, tapez **DAC-Ordinateurs protégés**, puis cliquez sur **OK**.
4. Cliquez sur le conteneur **Ordinateurs**, cliquez avec le bouton droit sur **LON-SVR1**, puis cliquez sur **Déplacer**.
5. Dans la fenêtre **Déplacer**, cliquez sur **DAC-Ordinateurs protégés**, puis sur **OK**.
6. Passez à la fenêtre du **Gestionnaire de serveur**. Cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
7. Développez **Forêt : Adatum.com**, **Domaines**, **Adatum.com**, puis cliquez sur le conteneur **Objets de stratégie de groupe**.
8. Dans le volet des résultats, cliquez avec le bouton droit sur **Stratégie des contrôleurs de domaine par défaut**, puis cliquez sur **Modifier**.
9. Dans l'**Éditeur de gestion des stratégies de groupe**, sous **Configuration ordinateur**, développez **Stratégies**, **Modèles d'administration**, **Système**, puis cliquez sur **KDC**.
10. Dans le volet d'informations, double-cliquez sur **Prise en charge du contrôleur de domaine Kerberos pour les revendications, l'authentification composée et le blindage Kerberos**.
11. Dans la fenêtre **Prise en charge du contrôleur de domaine Kerberos pour les revendications, l'authentification composée et le blindage Kerberos**, sélectionnez **Activée**. Dans la section **Options**, dans la liste déroulante, sélectionnez **Toujours fournir des revendications**, puis cliquez sur **OK**.
12. Fermez l'**Éditeur de gestion des stratégies de groupe** et la **console de gestion des stratégies de groupe**.
13. Cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
14. Dans la fenêtre **Windows PowerShell**, tapez **gpupdate /force**, puis appuyez sur Entrée. Après la mise à jour de la stratégie de groupe, fermez **Windows PowerShell**.
15. Passez à la fenêtre **Utilisateurs et ordinateurs Active Directory**.
16. Dans le volet de navigation, cliquez sur l'UO **Recherche**, dans le volet du contenu, cliquez avec le bouton droit sur **Connie Vaughn**, puis cliquez sur **Propriétés**.
17. Dans la fenêtre **Propriétés de Connie Vaughn**, cliquez sur l'onglet **Organisation**. Vérifiez que la zone de texte **Service** contient la valeur **Recherche**, puis cliquez sur **Annuler**.
18. Fermez **Utilisateurs et ordinateurs Active Directory**.

Configurer les revendications, les propriétés de ressources et les règles d'accès centralisées

1. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Centre d'administration Active Directory.**

2. Dans le **Centre d'administration Active Directory**, dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur **Types de revendications**.
3. Dans le volet **Tâches**, cliquez sur **Nouveau**, puis sur **Type de revendication**.
4. Dans la fenêtre **Créer Type de revendication**, dans la section **Attribut source**, sélectionnez **Service**.
5. Dans la zone de texte **Nom d'affichage**, tapez **Service entreprise**.
6. Sélectionnez **Utilisateur** et **Ordinateur**, puis cliquez sur **OK**.
7. Dans le **Centre d'administration Active Directory**, cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur **Propriétés de ressources**.
8. Dans la liste **Propriétés de ressources**, cliquez avec le bouton droit sur **Service**, puis sur **Activer**.
9. Double-cliquez sur **Service**.
10. Faites défiler vers le bas jusqu'à la section **Valeurs suggérées**, puis cliquez sur **Ajouter**.
11. Dans la fenêtre **Ajouter une valeur suggérée**, dans les zones de texte **Valeur** et **Nom d'affichage**, tapez **Recherche**, puis cliquez deux fois sur **OK**.
12. Cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur les **listes de propriétés de ressources**.
13. Dans le volet central, double-cliquez sur la **liste des propriétés de ressources globales**, vérifiez que **Service** s'affiche, puis cliquez sur **Annuler**. S'il ne s'affiche pas, cliquez sur **Ajouter**, ajoutez la propriété, puis cliquez sur **OK**.
14. Dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur les **règles d'accès central**.
15. Dans le volet **Tâches**, cliquez sur **Nouveau**, puis sur la **règle d'accès central**.
16. Dans la boîte de dialogue de **création d'une règle d'accès centralisée**, dans la zone de texte **Nom**, tapez **Correspondance service**.
17. Dans la section **Ressources cibles**, cliquez sur **Modifier**.
18. Dans la boîte de dialogue des **règles d'accès central**, cliquez sur **Ajouter une condition**.
19. Dans la dernière liste déroulante, sélectionnez **Recherche**. Vérifiez que la condition est **Resource-Department-Equals-Value-Research**, puis cliquez sur **OK**.
20. Dans la section **Autorisations**, sélectionnez **Utiliser les autorisations suivantes en tant qu'autorisations actuelles**, puis cliquez sur **Modifier**.
21. Sélectionnez l'entrée d'autorisation pour **DROITS DU PROPRIÉTAIRE**, puis cliquez sur **Supprimer**. Répétez l'étape pour les **Administrateurs (ADATUM\Administrateurs)** et les groupes **SYSTÈME**.
22. Dans la boîte de dialogue des **Paramètres de sécurité avancés pour Autorisations**, cliquez sur **Ajouter**.
23. Dans la boîte de dialogue **Entrée d'autorisation pour Autorisations**, cliquez sur **Sélectionner un principal**.
24. Dans la fenêtre **Sélectionner un utilisateur, un ordinateur, un compte de service ou un groupe**, tapez **Utilisateurs authentifiés**, cliquez sur **Vérifier les noms**, puis sur **OK**.
25. Dans la section **Autorisations de base**, sélectionnez **Modification**, **Lecture et exécution**, **Lecture** et **Écriture**.
26. Cliquez sur **Ajouter une condition**.

27. Dans la zone de liste déroulante **Groupe**, sélectionnez **Service entreprise**. Dans la zone de liste déroulante **Valeur**, sélectionnez **Ressource**. Dans la zone de liste déroulante, sélectionnez **Service**, puis cliquez trois fois sur **OK**.

Classifier les fichiers manuellement

1. Passez à **LON-SVR1**.
2. Cliquez sur **Démarrer**, puis sur **Gestionnaire de serveur**.
3. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestionnaire de ressources du serveur de fichiers**.
4. Dans le **Gestionnaire de ressources du serveur de fichiers**, développez **Gestion de la classification**, cliquez sur **Propriétés de classification**, cliquez avec le bouton droit sur **Propriétés de classification**, puis cliquez sur **Actualiser**.
5. Vérifiez que la propriété **Service** est répertoriée.
6. Dans la barre des tâches, cliquez sur l'icône de l'**Explorateur de fichiers**.
7. Dans la fenêtre de l'**Explorateur de fichiers**, dans la barre d'adresse, tapez **D:\Labfiles\Mod11** et appuyez sur Entrée. Dans le volet de contenu, cliquez avec le bouton droit sur le dossier **Recherche**, puis cliquez sur **Propriétés**.
8. Cliquez sur l'onglet **Classification**, sur **Service** et, dans la section **Valeur**, cliquez sur **Recherche**, puis sur **OK**.

Configurer et déployer une stratégie d'accès centralisée

1. Passez à **LON-DC1**.
2. Dans le **Centre d'administration Active Directory**, dans le volet de navigation, cliquez sur **Contrôle d'accès dynamique**, puis double-cliquez sur **Stratégies d'accès centralisées**.
3. Dans le volet **Tâches**, cliquez sur **Nouveau**, puis sur **Stratégie d'accès centralisée**.
4. Dans la zone de texte **Nom**, tapez **Correspondance service** et cliquez sur **Ajouter**.
5. Cliquez sur la règle **Correspondance service**, cliquez sur **>>**, puis deux fois sur **OK**.
6. Fermez le **Centre d'administration Active Directory**.
7. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
8. Dans la **Console de gestion des stratégies de groupe**, cliquez avec le bouton droit sur **DAC-Ordinateurs protégés**, puis cliquez sur **Créer un GPO dans ce domaine et le lier ici**.
9. Dans la boîte de dialogue **Nouvel objet GPO**, dans la zone de texte **Nom**, tapez **Stratégie DAC**, puis cliquez sur **OK**.
10. Cliquez avec le bouton droit sur **Stratégie DAC**, puis cliquez sur **Modifier**.
11. Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, sous Configuration ordinateur, développez **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, **Système de fichiers**, puis cliquez avec le bouton droit sur **Stratégie d'accès centralisée** et **Gérer les stratégies d'accès centralisées.**
12. Cliquez sur **Correspondance service**, sur **Ajouter**, puis sur **OK**.
13. Fermez l'**Éditeur de gestion des stratégies de groupe** et la **console de gestion des stratégies de groupe**.
14. Passez à **LON-SVR1**.

15. Sur **LON-SVR1**, cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
16. Dans l'invite de commandes **Windows PowerShell**, tapez la commande suivante et appuyez sur Entrée :

```
gpupdate /force
```

17. Fermez **Windows PowerShell**.
18. Passez à la fenêtre de l'**Explorateur de fichiers**.
19. Dans la fenêtre de l'**Explorateur de fichiers**, cliquez avec le bouton droit sur le dossier **Recherche**, puis cliquez sur **Propriétés**.
20. Dans la boîte de dialogue **Propriétés de Recherche**, cliquez sur l'onglet **Sécurité**, puis sur **Avancé**.
21. Dans la fenêtre **Paramètres de sécurité avancés pour Recherche**, cliquez sur l'onglet **Stratégie centralisée**, puis sur **Modifier**.
22. Dans la zone de liste déroulante, sélectionnez **Correspondance service**, puis cliquez deux fois sur **OK**.

Démonstration : configuration de l'assistance en cas d'accès refusé

Étapes de la démonstration

1. Passez à **LON-DC1**.
2. Sur **LON-DC1**, dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
3. Dans la **Console de gestion des stratégies de groupe**, cliquez avec le bouton droit sur **Stratégie DAC**, puis cliquez sur **Modifier**.
4. Dans la fenêtre de l'**Éditeur de gestion des stratégies de groupe**, sous **Configuration ordinateur**, développez **Stratégies**, **Modèles d'administration**, **Système**, puis cliquez sur **Assistance en cas d'accès refusé**.
5. Dans le volet d'informations, double-cliquez sur **Personnaliser le message des erreurs d'accès refusé**.
6. Dans la fenêtre **Personnaliser le message des erreurs d'accès refusé**, cliquez sur **Activé**.
7. Dans la zone de texte **Afficher le message suivant aux utilisateurs auxquels l'accès est refusé**, tapez **L'accès vous est refusé à cause d'une stratégie d'autorisation. Veuillez demander un accès**.
8. Sélectionnez **Autoriser les utilisateurs à demander de l'assistance**, examinez les autres options, ne changez rien, puis cliquez sur **OK**.
9. Dans le volet d'informations de l'**Éditeur de gestion des stratégies de groupe**, double-cliquez sur **Activer l'assistance en cas d'accès refusé pour tous les types de fichiers**, cliquez sur **Activé**, puis sur **OK**.
10. Fermez l'**Éditeur de gestion des stratégies de groupe** et la **console de gestion des stratégies de groupe**.

Contrôle des acquis et éléments à retenir

Meilleures pratiques

- Utilisez des modèles de quota pour contrôler et surveiller la quantité de données que les groupes stockent.
- Utilisez la classification des fichiers pour identifier et contrôler de façon plus granulaire certains types de données.

Questions de contrôle des acquis

Question : comment les modèles FSRM pour les quotas et les filtres de fichiers fournissent-ils une expérience de gestion FSRM plus efficace ?

Réponse : les modèles permettent aux administrateurs de créer rapidement des quotas et des filtres de fichiers basés sur des modèles prédéfinis. Vous pouvez aussi utiliser des modèles pour gérer les quotas enfants de manière globale. Pour changer la taille de fichier pour plusieurs quotas créés à partir d'un modèle, il vous suffit de modifier le modèle.

Question : comment l'assistance en cas d'accès refusé améliore-t-elle l'expérience de l'utilisateur ?

Réponse : quand la fonctionnalité d'assistance en cas d'accès refusé est configurée avec des explications simples et des informations de contact à jour, cela permet aux utilisateurs de comprendre pourquoi ils ne peuvent pas accéder à une ressource particulière. Cela leur permet aussi d'être dirigés vers le contact adapté qui peut leur fournir un accès.

Outils

Outil	Utilisation	Emplacement
Gestionnaire de ressources du serveur de fichiers	Gestion de quotas, filtres de fichiers, gestion de la classification et rapports de stockage	• Ajoutez un service de rôle FSRM depuis l'**Assistant Ajout de rôles et de fonctionnalités** ou en utilisant **Windows PowerShell**. • Gestionnaire de serveur - Outils
Windows PowerShell	Gestion de FSRM	Windows PowerShell : `import-module FileServerResourceManager`

Problèmes courants et conseils de dépannage

Problème courant	Conseil de dépannage
Quand vous tentez d'exécuter une tâche de gestion de fichier à une invite de commandes, vous pouvez recevoir une erreur indiquant que la tâche n'a pas pu être trouvée.	Cela se produit lorsque le nom de la tâche dans l'interface du serveur de fichiers ne correspond pas au nom de la tâche requis par l'invite de commandes. Par exemple, vous pouvez créer une tâche appelée Task1, mais le nom requis par l'invite de commandes est *FileManagement-Task1*.

Questions et réponses relatives à l'atelier pratique

Atelier pratique A : quotas et filtrage des fichiers

Questions et réponses

Question : quel critère devez-vous respecter pour utiliser FSRM afin de gérer une structure de fichiers sur un serveur ?

Réponse : les serveurs doivent exécuter Windows Server 2003 SP1 ou une version ultérieure pour utiliser FSRM. Si vous voulez utiliser ICF, vous devez exécuter Windows Web Server 2008 R2 ou une version ultérieure. De plus, vous devez formater les volumes sur lesquels vous souhaitez faire des opérations FSRM avec NTFS.

Question : de quelles façons les tâches de gestion de la classification et de gestion de fichiers réduisent-elles le traitement administratif dans le cas d'une structure de fichiers et de dossiers complexe ?

Réponse : les tâches de gestion de la classification et des fichiers peuvent permettre aux administrateurs d'automatiser la classification et la modification manuelles des fichiers sur un serveur de fichiers. Plutôt que d'inspecter les fichiers manuellement et d'exécuter des opérations manuelles sur eux, les administrateurs peuvent configurer ICF pour classer les fichiers, puis exécuter les opérations nécessaires sur ces fichiers en utilisant les tâches de gestion de fichiers.

Atelier pratique B : implémentation du contrôle d'accès dynamique

Questions et réponses

Question : comment les classifications de fichiers améliorent-elles l'utilisation du contrôle d'accès dynamique ?

Réponse : lorsque vous utilisez les classifications de fichiers, vous pouvez définir automatiquement des attributs sur des fichiers, puis utiliser ces attributs dans des expressions conditionnelles lorsque vous implémentez le contrôle d'accès dynamique.

Question : pouvez-vous implémenter le contrôle d'accès dynamique sans stratégie d'accès centralisée ?

Réponse : oui, vous pouvez configurer des expressions conditionnelles directement sur les ressources.

Module 12

Sécurisation du trafic réseau avec des pare-feu et le chiffrement

Sommaire :

Leçon 1

Présentation des menaces courantes pour la sécurité du réseau

Sommaire :

Questions et réponses

Discussion : menaces courantes pour la sécurité du réseau

Question : quelles menaces pour la sécurité connaissez-vous ?

> **Réponse :** les réponses peuvent varier, mais elles incluront sûrement les courriers d'hameçonnage, les logiciels espions et les rançongiciels.

Ressources

Ports connus

 **Lectures supplémentaires :** Pour une liste complète des ports connus et des ports enregistrés, consultez « Service Name and Transport Protocol Port Number Registry » à l'adresse : https://aka.ms/ivsdso

Leçon 2

Présentation du Pare-feu Windows avec fonctions avancées de sécurité

Sommaire :

Questions et réponses

Question : quels sont les avantages de l'utilisation d'un pare-feu basé sur l'hôte tel que le Pare-feu Windows avec fonctions avancées de sécurité ?

Réponse : le Pare-feu Windows avec fonctions avancées de sécurité apporte les avantages suivants :

- Les ordinateurs bénéficient d'une protection améliorée contre les attaques du réseau interne. Cela peut empêcher les programmes malveillants de se déplacer dans ce dernier en bloquant le trafic entrant non sollicité.
- Les règles entrantes permettent d'empêcher l'analyse de réseau dans le but d'identifier les hôtes du réseau. Les scanneurs réseau les plus simples effectuent un test ping sur les hôtes d'un réseau afin de les identifier. Le Pare-feu Windows avec fonctions avancées de sécurité permet d'empêcher les serveurs membres de répondre aux requêtes de test ping. Les contrôleurs de domaine répondent quant à eux aux requêtes de test ping.
- Lorsque vous activez les règles sortantes, elles peuvent empêcher les programmes malveillants de s'étendre en évitant que ceux-ci communiquent sur le réseau. Dans le cas d'un virus, vous pouvez configurer les ordinateurs avec une règle sortante spécifique qui empêche le virus de communiquer sur le réseau.
- Les règles de sécurité de connexion vous permettent de créer des règles de pare-feu sophistiquées qui utilisent des informations d'authentification d'utilisateur et d'ordinateur pour limiter la communication avec des ordinateurs hautement sécurisés.

Démonstration : utilisation du Pare-feu Windows pour gérer le trafic réseau

Étapes de la démonstration

Créer une règle de pare-feu de trafic entrant

1. Sur **LON-DC1**, ouvrez une fenêtre d'**invite de commandes**, tapez le texte suivant, puis appuyez sur Entrée.

```
Ping LON-SVR2
```

Remarque : le résultat devrait être « Délai d'attente de la demande dépassé ».

2. Sur **LON-SVR2**, ouvrez une fenêtre **Windows PowerShell**, tapez le texte suivant, puis appuyez sur Entrée.

```
Test-Connection LON-DC1
```

Remarque : le test ping vers **LON-DC1** devrait réussir.

3. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.
4. Cliquez sur **Système et sécurité**, puis sur **Pare-feu Windows**.
5. Dans la fenêtre **Pare-feu Windows**, cliquez sur le lien **Paramètres avancés** à gauche pour ouvrir la console de gestion du **Pare-feu Windows avec fonctions avancées de sécurité**.

6. Sous **Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local**, dans le volet de navigation, cliquez sur **Règles de trafic entrant**.
7. Cliquez avec le bouton droit sur **Règles de trafic entrant**, puis cliquez sur **Nouvelle règle**.
8. Dans l'**Assistant Nouvelle règle de trafic entrant**, sur la page **Type de règle**, cliquez sur **Personnalisée**, puis sur **Suivant**.
9. Sur la page **Programme**, cliquez sur **Tous les programmes**, puis sur **Suivant**.
10. Sur la page **Protocole et ports**, dans la liste **Type de protocole**, cliquez sur **ICMPv4**, puis sur **Suivant**.
11. Sur la page **Étendue**, cliquez sur **Suivant**.
12. Sur la page **Action**, cliquez sur **Autoriser la connexion**, puis sur **Suivant**.
13. Sur la page **Profil**, cliquez sur **Suivant**.
14. Sur la page **Nom**, dans la zone de texte **Nom**, tapez **Règle Autoriser le ping**, puis cliquez sur **Terminer**.
15. Dans le volet de navigation, développez **Analyse**, puis cliquez sur **Pare-Feu**.
16. Vérifiez que la **Règle Autoriser le ping** a été créée.

Tester la règle de pare-feu de trafic entrant

- Sur **LON-DC1**, tapez la ligne suivante dans la fenêtre d'**invite de commandes**, puis appuyez sur Entrée.

```
Ping LON-SVR2
```

Remarque : le test ping vers **LON-SVR2** devrait réussir.

Créer une règle de pare-feu de trafic sortant

1. Passez à **LON-SVR2**, puis cliquez sur **Règles de trafic sortant**.
2. Cliquez avec le bouton droit sur **Règles de trafic sortant**, puis cliquez sur **Nouvelle règle**.
3. Dans l'**Assistant Nouvelle règle de trafic sortant**, sur la page **Type de règle**, cliquez sur **Personnalisée**, puis sur **Suivant**.
4. Sur la page **Programme**, cliquez sur **Tous les programmes**, puis sur **Suivant**.
5. Sur la page **Protocole et ports**, dans la liste **Type de protocole**, cliquez sur **ICMPv4**, puis sur **Suivant**.
6. Sur la page **Étendue**, cliquez sur **Suivant**.
7. Sur la page **Action**, cliquez sur **Bloquer la connexion**, puis sur **Suivant**.
8. Sur la page **Profil**, cliquez sur **Suivant**.
9. Sur la page **Nom**, dans la zone de texte Nom, tapez **Règle Éviter le ping**, puis cliquez sur **Terminer**.
10. Dans le volet de navigation, développez **Analyse**, puis cliquez sur **Pare-Feu**.
11. Vérifiez que la **Règle Éviter le ping** a été créée.

Tester la règle de pare-feu de trafic sortant

- Dans la fenêtre **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée.

```
Test-Connection LON-DC1
```

Remarque : le résultat devrait être « Test-Connection : Le test de la connexion à l'ordinateur « LON-DC1 » a échoué : Erreur inconnue (0x2b2a). »

Réinitialiser les règles de pare-feu sur LON-SVR2

1. Dans la console **Pare-feu Windows avec fonctions avancées de sécurité**, dans le volet de navigation, cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local**.
2. Dans le volet **Actions**, cliquez sur **Restaurer la stratégie par défaut**.
3. Dans la boîte de dialogue **Pare-feu Windows avec fonctions avancées de sécurité**, cliquez sur **Oui**, puis sur **OK**.
4. Dans la fenêtre **Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée.

```
Test-Connection LON-DC1
```

Remarque : le test ping vers **LON-DC1** devrait réussir.

Leçon 3

Configuration d'IPsec

Sommaire :

Questions et réponses

Question : dans votre environnement, utilisez-vous IPsec ou l'utiliseriez-vous ?

> **Réponse :** les réponses varient. Pour entamer la discussion, suggérez d'utiliser IPsec pour les systèmes de la zone de périmètre ou pour les tunnels VPN qui passent par le réseau Internet public.

Ressources

Qu'est-ce qu'IPsec ?

 **Lectures supplémentaires :** Pour plus d'informations, consultez « What Is IPSec? » à l'adresse : http://aka.ms/G0crt8

Démonstration : création et configuration de règles de sécurité de connexion

Étapes de la démonstration

Autoriser le trafic ICMP sur LON-SVR1 s'il est sécurisé

1. Passez à **LON-SVR1**.
2. Ouvrez le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Pare-feu Windows avec fonctions avancées de sécurité**.
3. Dans **Pare-feu Windows avec fonctions avancées de sécurité**, cliquez, puis cliquez avec le bouton droit sur **Règles de trafic entrant** et cliquez sur **Nouvelle règle**.
4. Dans la boîte de dialogue **Assistant Nouvelle règle de trafic entrant**, cliquez sur **Personnalisée**, puis sur **Suivant**.
5. Sur la page **Programme**, cliquez sur **Suivant**.
6. Sur la page **Protocole et ports**, dans la liste **Type de protocole**, cliquez sur **ICMPv4**, puis sur **Suivant**.
7. Sur la page **Étendue**, cliquez sur **Suivant**.
8. Sur la page **Action**, cliquez sur **Autoriser la connexion si elle est sécurisée**, puis cliquez sur **Suivant**.
9. Sur la page **Utilisateurs**, cliquez sur **Suivant**.
10. Sur la page **Ordinateurs**, cliquez sur **Suivant**.
11. Sur la page **Profil**, cliquez sur **Suivant**.
12. Sur la page **Nom**, dans la zone **Nom**, tapez **ICMPv4 autorisé**, puis cliquez sur **Terminer**.

Créer une règle serveur à serveur sur des serveurs connectés

1. Sur **LON-SVR1**, dans **Pare-feu Windows avec fonctions avancées de sécurité**, cliquez, puis cliquez avec le bouton droit sur **Règles de sécurité de connexion** et cliquez sur **Nouvelle règle**.
2. Dans l'**Assistant Nouvelle règle de sécurité de connexion**, cliquez sur **Serveur à serveur**, puis sur **Suivant**.
3. Sur la page **Points de terminaison**, cliquez sur **Suivant**.
4. Sur la page **Configuration requise**, cliquez sur **Imposer l'authentification des connexions entrantes et sortantes**, puis sur **Suivant**.
5. Sur la page **Méthode d'authentification**, cliquez sur **Avancée**, puis sur **Personnaliser**.

6. Dans la boîte de dialogue **Personnaliser les méthodes d'authentification avancées**, sous **Premières méthodes d'authentification**, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Ajouter la première méthode d'authentification**, cliquez sur **Clé pré-partagée**, tapez **secret**, puis cliquez sur **OK**.
8. Dans la boîte de dialogue **Personnaliser les méthodes d'authentification avancées**, cliquez sur **OK**.
9. Sur la page **Méthode d'authentification**, cliquez sur **Suivant**.
10. Sur la page **Profil**, cliquez sur **Suivant**.
11. Sur la page **Nom**, dans la zone **Nom**, tapez **Adatum-Serveur-à-serveur**, puis cliquez sur **Terminer**.

Créer une règle serveur à serveur sur LON-CL1

1. Passez à **LON-CL1**.
2. Si nécessaire, connectez-vous en tant que **Adatum\administrator** avec le mot de passe **Pa55w.rd**.
3. Dans Cortana, tapez **Pare-feu Windows**, puis cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité**.
4. Cliquez et cliquez avec le bouton droit sur **Règles de sécurité de connexion**, puis cliquez sur **Nouvelle règle**.
5. Dans l'**Assistant Nouvelle règle de sécurité de connexion**, cliquez sur **Serveur à serveur**, puis sur **Suivant**.
6. Sur la page **Points de terminaison**, cliquez sur **Suivant**.
7. Sur la page **Configuration requise**, cliquez sur **Imposer l'authentification des connexions entrantes et sortantes**, puis sur **Suivant**.
8. Sur la page **Méthode d'authentification**, cliquez sur **Avancée**, puis sur **Personnaliser**.
9. Dans la boîte de dialogue **Personnaliser les méthodes d'authentification avancées**, sous **Premières méthodes d'authentification**, cliquez sur **Ajouter**.
10. Dans la boîte de dialogue **Ajouter la première méthode d'authentification**, cliquez sur **Clé pré-partagée**, tapez **secret**, puis cliquez sur **OK**.
11. Dans la boîte de dialogue **Personnaliser les méthodes d'authentification avancées**, cliquez sur **OK**.
12. Sur la page **Méthode d'authentification**, cliquez sur **Suivant**.
13. Sur la page **Profil**, cliquez sur **Suivant**.
14. Sur la page **Nom**, dans la zone **Nom**, tapez **Adatum-Serveur-à-serveur**, puis cliquez sur **Terminer**.

Tester la règle.

1. Dans Cortana, tapez **cmd.exe**, puis appuyez sur Entrée.
2. À l'invite de commandes, tapez **ping 172.16.0.11**, puis appuyez sur Entrée.
3. Passez au Pare-feu Windows avec fonctions avancées de sécurité.
4. Développez **Analyse**, puis **Associations de sécurité** et cliquez sur **Mode principal**.
5. Dans le volet **Mode principal**, double-cliquez sur l'élément dans la liste.
6. Examinez les informations dans **Mode principal**, puis cliquez sur **OK**.
7. Cliquez sur **Mode rapide**.
8. Dans le volet **Mode rapide**, double-cliquez sur l'élément dans la liste.
9. Examinez les informations dans **Mode rapide**, puis cliquez sur **OK**.

Leçon 4

Pare-feu du centre de données

Sommaire :

Questions et réponses

Question : dans votre environnement, prévoyez-vous d'utiliser le pare-feu du centre de données ou des NSG ?

Réponse : les réponses varient en fonction de la complexité des réseaux sur lesquels travaillent les stagiaires.

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : quand vous configurez une règle de pare-feu pour autoriser l'accès à une application sur un port spécifique, à quel(s) profil(s) réseau devez-vous appliquer cette règle ?

Réponse : la règle doit s'appliquer à un profil réseau à partir duquel le trafic est attendu.

Question : quels sont les avantages de l'utilisation du pare-feu du centre de données dans un environnement de réseau privé ?

Réponse : plusieurs avantages sont à mentionner :

- Le pare-feu du centre de données est une solution de pare-feu logicielle intégrée à Microsoft System Center Virtual Machine Manager. Il peut être géré par des clients ou des administrateurs et est assez évolutif pour permettre le déploiement d'ordinateurs virtuels à petite ou grande échelle.
- Les stratégies de pare-feu attribuées aux ordinateurs virtuels suivent ceux-ci lorsqu'ils sont déplacés sur un nouvel hôte. Ceci est possible car :
    - Le pare-feu du centre de données est déployé en tant que pare-feu de l'agent hôte du port du vSwitch
    - Les stratégies du pare-feu du centre de données attribuées par les clients du fournisseur de service sont indépendantes des paramètres de pare-feu des autres clients
    - Chaque port du vSwitch est configuré indépendamment de l'hôte sur lequel l'ordinateur virtuel est exécuté
- Il fournit des fonctionnalités de protection pour les ordinateurs virtuels clients qui sont indépendants du système d'exploitation invité client.

Question : dans quels scénarios utilise-t-on IPsec ?

Réponse : les réponses varient, mais on peut utiliser IPsec pour :

- Sécuriser le trafic hôte à hôte
- Sécuriser le trafic vers les serveurs
- Utiliser L2TP
- Le tunneling site à site (passerelle à passerelle)
- La mise en place de réseaux logiques

Question : vous devez vous assurer que le trafic est chiffré et authentifié lorsqu'il passe entre un ordinateur du réseau de périmètre et un ordinateur de votre réseau interne. L'ordinateur du réseau de périmètre n'est pas membre de votre forêt AD DS. Quelles méthodes d'authentification pourriez-vous utiliser si vous tentiez d'établir une règle IPsec entre ces deux ordinateurs ?

Réponse : vous ne pourriez pas utiliser l'authentification Kerberos parce que l'ordinateur de périmètre n'est pas dans la forêt. Par conséquent, vous pourriez utiliser des certificats ou une clé pré-partagée.

Questions et réponses relatives à l'atelier pratique

Atelier pratique : configuration du Pare-feu Windows avec fonctions avancées de sécurité

Questions et réponses

Question : vous voulez mettre en place une nouvelle application qui nécessite l'utilisation de ports spécifiques. De quelles informations avez-vous besoin pour configurer le Pare-feu Windows avec fonctions avancées de sécurité ? Depuis quelle source obtenir ces informations ?

> **Réponse :** vous devez savoir quels ports et adresses IP l'application utilisera afin qu'elle puisse fonctionner tout en étant protégée des menaces relatives à la sécurité. Vous pouvez obtenir ces informations auprès du fournisseur de l'application.

Question : expliquez pourquoi **LON-CL1** peut se connecter à **LON-SVR1** et **LON-SVR2** dans l'atelier pratique, alors que **LON-SVR2** ne peut pas se connecter à **LON-SVR1**.

> **Réponse : LON-SVR1** est configuré pour l'isolation de serveur. De ce fait, seuls les ordinateurs qui utilisent IPsec pour sécuriser le trafic réseau peuvent s'y connecter. **LON-CL1** étant dans l'UO des clients sécurisés, la stratégie de requête de sécurité s'y applique. De ce fait, elle requerra IPsec lors de la connexion à un autre serveur. **LON-SVR2** n'a pas de sécurité configurée. **LON-CL1** peut donc s'y connecter sans utiliser IPsec. **LON-SVR2** ne peut pas se connecter à **LON-SVR1**, car **LON-SVR2** n'est pas configuré pour requérir une sécurité et **LON-SVR1** refuse toutes les connexions non sécurisées.

Module 13

Sécurisation du trafic réseau

Sommaire :

Leçon 1

Configuration des paramètres DNS avancés

Sommaire :

Questions et réponses

Question : les stratégies DNS et RRL sont des nouveautés dans Windows Server 2016. Comment utiliseriez-vous ces nouvelles fonctionnalités dans votre environnement ?

> **Réponse :** les réponses peuvent varier en fonction de la façon dont les stagiaires abordent la sécurité réseau. Les stagiaires avec des serveurs DNS Windows publics implémentent généralement RRL.

Ressources

Stratégies DNS

 **Lectures supplémentaires :** Pour plus d'informations, consultez « Set-DnsServerQueryResolutionPolicy » à l'adresse : http://aka.ms/D9e1pv

Démonstration : configuration de DNSSEC

Étapes de la démonstration

Configurer DNSSEC

1. Si ce n'est pas déjà le cas, connectez-vous à **LON-DC1** en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **DNS** dans la liste déroulante.
3. Dans **DNS**, développez **LON-DC1**, puis **Zones de recherche directes**, et cliquez avec le bouton droit sur **Adatum.com**.
4. Dans le menu, cliquez sur **DNSSEC>Signer la zone**.
5. Dans l'**Assistant de connexion à la zone**, cliquez sur **Suivant**.
6. Cliquez sur **Personnalisez les paramètres de signature de zone**, puis sur **Suivant**.
7. Sur la page **Maître des clés**, cliquez sur **Le serveur DNS LON-DC1 est le maître des clés**, puis sur **Suivant**.
8. Sur la page **Clé KSK**, cliquez sur **Suivant**.
9. Sur la page **Clé KSK**, cliquez sur **Ajouter**.
10. Sur la page **Nouvelle clé KSK**, cliquez sur **OK**.
11. Sur la page **Clé KSK**, cliquez sur **Suivant**.
12. Sur la page **Clé ZSK**, cliquez sur **Suivant**.
13. Sur la page **Clé ZSK**, cliquez sur **Ajouter**.
14. Sur la page **Nouvelle clé ZSK**, cliquez sur **OK**.
15. Sur la page **Clé ZSK**, cliquez sur **Suivant**.
16. Sur la page **Next Secure (NSEC)**, cliquez sur **Suivant**.
17. Sur la page **Ancres d'approbation (TA)**, activez la case à cocher **Activer la distribution d'ancres d'approbation pour cette zone**, puis cliquez sur **Suivant**.
18. Sur la page **Paramètres de signature et d'interrogation**, cliquez sur **Suivant**.
19. Sur la page **Extensions de sécurité DNS**, cliquez sur **Suivant**, puis sur **Terminer**.

20. Dans le **Gestionnaire DNS**, développez **Points d'approbation**, développez **com**, puis cliquez sur **Adatum**. Assurez-vous que les enregistrements de ressources DNSKEY existent et que leur statut est valide.
21. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe** dans la liste déroulante.
22. Dans la **Console de gestion des stratégies de groupe**, développez **Forêt : Adatum.com**, développez **Domaines**, **Adatum.com**, cliquez avec le bouton droit sur **Stratégie de domaine par défaut**, puis cliquez sur **Modifier**.
23. Dans l'**Éditeur de gestion des stratégies de groupe**, sous **Configuration ordinateur**, développez **Stratégies**, développez **Paramètres Windows**, puis cliquez sur le dossier **Stratégie de résolution de noms**.
24. Dans la section **Créer des règles**, dans le champ **Suffixe**, tapez **Adatum.com** pour appliquer la règle au suffixe de l'espace de noms.
25. Sélectionnez **Activer DNSSEC dans cette règle** et **Demander aux clients DNS de vérifier que les données de nom et d'adresse ont été validées par le serveur DNS**, puis cliquez sur **Créer**.
26. Faites défiler vers le bas et cliquez sur **Appliquer**.
27. Fermez toutes les fenêtres.

Démonstration : configuration des stratégies DNS et de RRL

Étapes de la démonstration

Configurer des stratégies DNS

1. Sur **LON-DC1**, cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
2. Pour créer un sous-réseau client pour les clients de Londres, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Add-DnsServerClientSubnet -Name "LondonSubnet" -IPv4Subnet "172.16.0.0/16" -PassThru
```

3. Pour créer un sous-réseau client pour les clients de Paris, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Add-DnsServerClientSubnet -Name "ParisSubnet" -IPv4Subnet "172.17.0.0/16" -PassThru
```

4. Pour créer une étendue de zone pour l'Angleterre, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Add-DnsServerZoneScope -ZoneName "adatum.com" -Name "adatum_england" -PassThru
```

5. Pour créer une étendue de zone pour la France, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Add-DnsServerZoneScope -ZoneName "adatum.com" -Name "adatum_france" -PassThru
```

6. Pour créer un enregistrement de ressource permettant de trouver le serveur web dans l'étendue England, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Add-DnsServerResourceRecord -ZoneName "adatum.com" -A -Name "www" -IPv4Address
172.16.0.11 -ZoneScope "adatum_england" -PassThru
```

7. Pour créer un enregistrement de ressource pour trouver le serveur web en France, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Add-DnsServerResourceRecord -ZoneName "adatum.com" -A -Name "www" -IPv4Address
172.17.0.11 -ZoneScope "adatum_france" -PassThru
```

8. Pour créer la stratégie DNS pour l'Angleterre, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Add-DnsServerQueryResolutionPolicy -Name "EnglandPolicy" -Action ALLOW -ClientSubnet
'eq,LondonSubnet' -ZoneScope 'adatum_england,1' -ZoneName "adatum.com" -PassThru
```

9. Pour créer la stratégie DNS pour la France, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Add-DnsServerQueryResolutionPolicy -Name "FrancePolicy" -Action ALLOW -ClientSubnet
'eq,ParisSubnet' -ZoneScope 'adatum_france,2' -ZoneName "adatum.com" -PassThru
```

10. Pour afficher les stratégies DNS définies, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Get-DnsServerQueryResolutionPolicy -ZoneName adatum.com
```

11. Pour vérifier que la résolution de noms fonctionne, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Ping www.adatum.com
```

Remarque : l'adresse www.adatum.com doit être résolue en 172.16.0.11.

12. Pour configurer une stratégie basée sur l'heure, tapez la commande suivante à l'invite de commandes Windows PowerShell, modifiez l'intervalle de temps de façon à ce que Paris soit utilisé 90 % du temps de 9 h à 17 h, puis appuyez sur Entrée.

```
Add-DnsServerQueryResolutionPolicy -Name AdatumPeakPolicy -Action ALLOW -ZoneScope
'adatum_england,1;adatum_france,9' –TimeOfDay 'EQ,09:00-17:00' -ZoneName adatum.com -
ProcessingOrder 1 -PassThru
```

Remarque : veillez à inclure l'heure actuelle dans la valeur **-TimeofDay**.

13. Pour tester la résolution de noms, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Ping www.adatum.com
```

Remarque : l'adresse www.adatum.com sera résolue en 172.17.0.11 90 % du temps. Si ce n'est pas le cas la première fois, videz le cache DNS en tapant **ipconfig /flushdns** à l'invite de commandes, puis réessayez.

Configurer RRL

1. Pour activer RRL avec les paramètres par défaut, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Set-DNSServerRRL
```

2. Lorsque vous êtes invité à **confirmer** la commande, tapez **O**, puis appuyez sur Entrée.
3. Lisez bien l'avertissement qui s'affiche.
4. Pour afficher les paramètres RRL, tapez la commande suivante à l'invite de commandes Windows PowerShell, puis appuyez sur Entrée :

```
Get-DNSServerRRL | FL
```

5. Vérifiez que les paramètres RRL s'affichent.

Leçon 2

Analyse du trafic réseau avec Message Analyzer

Sommaire :

Questions et réponses

Question : pour quels types de problèmes de dépannage Message Analyzer serait-il le plus utile ?

( ) Accès refusé à un fichier

( ) Accès refusé à un partage

( ) Accès refusé à un site web

( ) Lenteurs de connexion

( ) Toutes ces réponses

Réponse :

( ) Accès refusé à un fichier

( ) Accès refusé à un partage

( ) Accès refusé à un site web

( ) Lenteurs de connexion

(√) Toutes ces réponses

Commentaire :

Message Analyzer ne se contente pas d'évaluer le trafic réseau. Il évalue aussi les journaux des événements Windows et les fichiers journaux texte.

Démonstration : installation de Message Analyzer

Étapes de la démonstration

1. Passez à **LON-SVR1**.
2. Cliquez sur **Démarrer**, puis sur **Explorateur de fichiers**. Dans l'**Explorateur de fichiers**, développez **Ce PC**, **Allfiles (D:)**, puis **Labfiles** et cliquez sur le dossier **Mod13**.
3. Dans le dossier **Mod13**, double-cliquez sur **MessageAnalyzer64.msi**.
4. Dans l'**Assistant d'installation de Microsoft Message Analyzer**, sur la page **Welcome to the Microsoft Message Analyzer Setup Wizard**, cliquez sur **Next**.
5. Sur la page **End-User License Agreement**, activez la case à cocher **I accept the terms in the License Agreement**, puis cliquez sur **Next**.
6. Sur la page **Microsoft Message Analyzer Optimization**, cliquez sur **Next**.
7. Sur la page **Ready to install Microsoft Message Analyzer**, cliquez sur **Install**.
8. Sur la page **Completed the Microsoft Message Analyzer Setup Wizard**, cliquez sur **Finish**.
9. Une fois l'installation terminée, fermez toutes les fenêtres et redémarrez **LON-SVR1**.
10. Lorsque le serveur redémarre, connectez-vous en tant que **Adatum\Administrator** avec le mot de passe **Pa55w.rd**.

Démonstration : capture et analyse du trafic réseau à l'aide de Message Analyzer

Étapes de la démonstration

Capturer un trafic réseau non chiffré

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, développez le dossier **Microsoft Message Analyzer**, puis cliquez sur **Microsoft Message Analyzer**.
2. Dans la boîte de dialogue **Welcome to Microsoft Message Analyzer**, cliquez sur **Do not update items** et sur **No, I do not want to participate**, puis cliquez sur **OK**.
3. Parcourez la page de démarrage, puis cliquez sur **Start Local Trace**.
4. Quand la capture commence, passez à **LON-CL1**.
5. Sur **LON-CL1**, cliquez sur **Démarrer**, tapez **\\lon-svr1\d$\Labfiles\Mod13**, puis appuyez sur Entrée.
6. Copiez le fichier **MessageAnalyzer64.msi** vers le bureau local.
7. Passez à **LON-SVR1**.
8. Dans **Microsoft Message Analyzer**, cliquez sur **Session**, puis sur **Stop**.

Examiner les outils d'analyse

1. Dans le champ **Filter**, tapez le filtre suivant, puis cliquez sur **Apply** :

```
*address==172.16.0.40
```

2. Cliquez sur l'en-tête **Module** pour faire un tri par module.
3. Faites défiler le trafic et montrez les divers types de trafic capturés.

Remarque : Conseil : si vous placez le curseur sur un nom de module, une info-bulle affiche le nom complet.

4. Si des **types de diagnostic** s'affichent, cliquez sur l'un d'eux, puis montrez l'erreur.
5. Défilez vers le bas pour trouver **SMB2** dans la colonne **Module**.
6. Ajoutez un filtre en cliquant avec le bouton droit sur **SMB2** dans la colonne **Module**, puis en cliquant sur **Add 'Module' to Filter**.
7. Dans le filtre, remplacez **OR** par **AND**, puis cliquez sur **Apply**.
8. Examinez le trafic de SMB2.

Activer IPSec dans un GPO

1. Passez à **LON-DC1**, puis ouvrez le **Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.
3. Dans la **Console de gestion des stratégies de groupe**, développez **Forêt : Adatum.com**, développez **Domaines**, **Adatum.com**, cliquez avec le bouton droit sur **Stratégie de domaine par défaut**, puis cliquez sur **Modifier**.
4. Dans l'**Éditeur de gestion des stratégies de groupe**, sous **Configuration ordinateur**, développez **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, puis cliquez sur **Stratégies de sécurité IP sur Active Directory (ADATUM.COM)**.

5. Cliquez avec le bouton droit sur **Serveur (demandez la sécurité)**, puis cliquez sur **Attribuer**.
6. Fermez toutes les fenêtres.
7. Passez à **LON-SVR1**.
8. Cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
9. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
GPUDPATE /Force
```

10. Une fois la mise à jour terminée, fermez l'invite de commandes Windows PowerShell.
11. Passez à **LON-CL1**.
12. Cliquez sur **Démarrer**, tapez **Windows PowerShell**, puis cliquez sur **Windows PowerShell**.
13. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
GPUDPATE /Force
```

14. Une fois la mise à jour terminée, fermez toutes les fenêtres.

Capturer un trafic réseau chiffré

1. Sur **LON-SVR1**, dans la **barre d'outils globale**, cliquez sur **New session**.
2. Dans la boîte de dialogue **New Session**, cliquez sur **Live trace**, sur **Select Scenario**, puis sur **Local Network Interfaces (Win 8.1 and later)**.
3. Cliquez sur **Démarrer**.
4. Quand la capture commence, passez à **LON-CL1**.
5. Sur **LON-CL1**, cliquez sur **Démarrer**, tapez **\\lon-svr1\d$\Labfiles\Mod13**, puis appuyez sur Entrée.
6. Copiez le fichier **MessageAnalyzer64.msi** vers le bureau local. À l'invite, choisissez de remplacer le fichier sur le bureau.
7. Passez à **LON-SVR1**.
8. Dans **Microsoft Message Analyzer**, cliquez sur **Session**, puis sur **Stop**.

Examiner les outils d'analyse

1. Dans le champ **Filter**, tapez le filtre suivant, puis cliquez sur **Apply** :

```
*address==172.16.0.40
```

2. Cliquez sur l'en-tête **Module** pour faire un tri par module.
3. Remarquez que la majeure partie du trafic capturé provient du module ESP (IP Encapsulating Security Payload).
4. Si des **types de diagnostic** s'affichent, cliquez sur l'un d'eux, puis montrez l'erreur.
5. Fermez toutes les fenêtres.

Désactiver IPsec dans le GPO

1. Passez à **LON-DC1**, puis ouvrez le Gestionnaire de serveur.
2. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion des stratégies de groupe**.

3. Dans la **Console de gestion des stratégies de groupe**, développez **Forêt : Adatum.com**, développez **Domaines**, **Adatum.com**, cliquez avec le bouton droit sur **Stratégie de domaine par défaut**, puis cliquez sur **Modifier**.
4. Dans l'Éditeur de gestion des stratégies de groupe, sous **Configuration ordinateur**, développez **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, puis cliquez sur **Stratégies de sécurité IP sur Active Directory (ADATUM.COM)**.
5. Cliquez avec le bouton droit sur **Serveur (demandez la sécurité)**, puis cliquez sur **Supprimer l'attribution**.
6. Fermez toutes les fenêtres.
7. Passez à **LON-SVR1**.
8. Cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
9. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
GPUDPATE /Force
```

10. Une fois la mise à jour terminée, fermez toutes les fenêtres.
11. Passez à **LON-CL1**.
12. Dans Cortana, tapez **Windows PowerShell**, puis cliquez sur **Windows PowerShell**.
13. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
GPUDPATE /Force
```

14. Une fois la mise à jour terminée, fermez toutes les fenêtres.

Leçon 3

Sécurisation et analyse du trafic SMB

Sommaire :

Questions et réponses

Question : Quel est le risque encouru si vous laissez SMB 1.x activé dans votre environnement ?

> **Réponse :** SMB 1.x n'est pas un protocole sécurisé. S'il est activé dans votre environnement, vous pourriez être vulnérable aux attaques qui profitent des failles de SMB 1.x.

Ressources

Présentation du protocole de sécurité SMB 3.1.1

 **Lectures supplémentaires :** Pour plus d'informations, consultez Microsoft Open Specifications Support Team Blog : http://aka.ms/Aldg7y

Démonstration : désactivation de SMB 1.0 et configuration du chiffrement SMB sur les partages

Étapes de la démonstration

Désactiver SMB 1.x sur Windows 10

1. Passez à **LON-CL1**.
2. Cliquez sur **Démarrer**, tapez **Windows PowerShell**, puis cliquez sur **Windows PowerShell**.
3. À l'**invite de commandes Windows PowerShell**, tapez la commande suivante, puis appuyez sur Entrée :

```
Set-SmbServerConfiguration –EnableSMB1Protocol $false
```

4. Quand vous y êtes invité, tapez **O**, puis appuyez sur Entrée.
5. Fermez toutes les fenêtres.

Désactiver SMB 1.x sur Windows Server 2016

1. Passez à **LON-SVR1**.
2. Cliquez sur **Démarrer**, puis sur **Windows PowerShell**.
3. À l'invite de commandes Windows PowerShell, tapez la commande suivante, puis appuyez sur Entrée :

```
Set-SmbServerConfiguration –EnableSMB1Protocol $false
```

4. Quand vous y êtes invité, tapez **O**, puis appuyez sur Entrée.

Configurer un partage pour le chiffrement SMB

1. À l'invite de commandes Windows PowerShell, pour créer le partage chiffré, tapez la commande suivante, puis appuyez sur Entrée :

```
New-SmbShare –Name "Mod13" -Path "D:\Labfiles\Mod13" –EncryptData $true
```

2. À l'invite de commandes Windows PowerShell, pour accorder le niveau d'autorisation Contrôle total du partage à tout le monde, tapez la commande suivante, puis appuyez sur Entrée :

```
Grant-FileShareAccess –Name Mod13 -AccountName "Everyone" -AccessRight Full
```

Capturer le trafic SMB chiffré

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, développez le dossier **Microsoft Message Analyzer**, puis cliquez sur **Microsoft Message Analyzer**.
2. Sur la page de **démarrage**, cliquez sur **Start Local Trace**.
3. Quand la capture commence, passez à **LON-CL1**.
4. Sur **LON-CL1**, cliquez sur **Démarrer**, tapez **\\lon-svr1\Mod13**, puis appuyez sur Entrée.
5. Copiez le fichier **MessageAnalyzer64.msi** vers le bureau local. À l'invite, choisissez de remplacer le fichier sur le bureau.
6. Passez à **LON-SVR1**.
7. Dans **Microsoft Message Analyzer**, cliquez sur **Session**, puis sur **Stop**.

Examiner les outils d'analyse

1. Dans le champ **Filter**, tapez le filtre suivant, puis cliquez sur **Apply** :

```
(*address==172.16.0.40) and (SMB2)
```

2. Cliquez sur l'en-tête **Summary** pour faire un tri par module.
3. Remarquez que la majeure partie du trafic SMB2 est de type **TransformMessage, Encrypted**.

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : dans quels scénarios envisageriez-vous d'utiliser Message Analyzer comme outil de dépannage ?

> **Réponse :** les réponses peuvent varier, mais on peut utiliser Message Analyzer pour identifier le trafic réseau illégitime et résoudre les problèmes de réseau ou d'applications.

Question : quels sont les risques encourus si on désactive les communications SMB 1.0 ? Quels sont les risques encourus si on ne désactive pas ce protocole ?

> **Réponse :** SMB 1.0 est un ancien protocole qui a été développé dans la même optique de sécurité que SMB 3 ou ultérieur. SMB 1.0, qui ne force pas le chiffrement, est moins sécurisé. Cependant, certaines applications anciennes peuvent encore nécessiter ce protocole. De ce fait, elles peuvent ne pas fonctionner si vous désactivez SMB 1.0. Si vous ne le désactivez pas, vous ne bénéficierez pas des fonctionnalités de sécurité offertes par SMB 3 ou ultérieur.

Questions et réponses relatives à l'atelier pratique

Atelier pratique A : sécurisation des DNS

Questions et réponses

Question : pourquoi seule l'analyse en mode principal montre-t-elle que le chiffrement était utilisé ?

Réponse : le chiffrement n'était configuré que pour le protocole ICMPv4, qui n'est pas utilisé par la session en mode rapide.

Question : pourquoi créer une zone séparée pour DNSSEC ?

Réponse : les réponses varient. Cela peut être pour utiliser différents paramètres pour différentes zones. Ainsi, si une zone est compromise, les autres zones ne le seront pas forcément.

Atelier pratique B : Microsoft Message Analyzer et chiffrement SMB

Questions et réponses

Question : IPsec étant appliqué à tout le trafic, une capture de réseau fournit-elle des indications sur l'utilisation du trafic ?

Réponse : non. Tout le trafic protégé par IPsec s'affiche comme du trafic ESP. Il n'y a donc aucune indication sur ce que contiennent ses paquets.

Question : pour votre environnement, quelle méthode de chiffrement fonctionnerait le mieux ? IPsec ou SMB 3.1.1 ?

Réponse : les réponses varient. Vous pouvez configurer IPsec de façon à chiffrer tout le trafic réseau, tandis que SMB 3.1.1 ne chiffre que le trafic SMB des partages Windows 10 ou Windows Server 2016.

Module 14

Mise à jour de Windows Server

Sommaire :

Leçon 1

Vue d’ensemble de WSUS

Sommaire :

Questions et réponses

Question : parmi ces produits, lesquels WSUS peut-il mettre à jour ?

( ) Microsoft Visual Studio 2010

( ) Microsoft Security Essentials

( ) Microsoft Office 2010

( ) Microsoft Silverlight

( ) Windows RT

Réponse :

(√) Microsoft Visual Studio 2010

(√) Microsoft Security Essentials

(√) Microsoft Office 2010

(√) Microsoft Silverlight

(√) Windows RT

Commentaire :

WSUS prend en charge de nombreux produits Microsoft.

Ressources

Options de déploiement du serveur WSUS

Lectures supplémentaires : pour plus d'informations, consultez « Determine Capacity Requirements » à l'adresse : http://aka.ms/Scktfu

Leçon 2

Déploiement des mises à jour avec WSUS

Sommaire :

Questions et réponses

Question : utilisez-vous plusieurs groupes d'ordinateurs dans votre environnement WSUS ?

> **Réponse :** les réponses varient. Certains stagiaires peuvent tester manuellement les mises à jour et les déployer automatiquement après approbation. D'autres peuvent utiliser un déploiement automatique pour faire un test avant un déploiement automatique plus important.

Ressources

Résolution des problèmes de WSUS

 **Lectures supplémentaires :** pour plus d'informations, consultez « Windows Server Update Services Tools and Utilities » à l'adresse : http://aka.ms/Erqdqk

Démonstration : approbation des mises à jour avec WSUS

Étapes de la démonstration

1. Sur **LON-SVR1**, cliquez sur **Démarrer**, sur **Outils d'administration Windows**, puis sur la console **Windows Server Update Services**.
2. Dans **Windows Server Update Services (WSUS)**, développez **LON-SVR1**, **Mises à jour** et cliquez sur **Mises à jour critiques**. Dans la liste déroulante **État**, sélectionnez **Toutes**, puis cliquez sur **Actualiser**.
3. Cliquez avec le bouton droit sur **Mise à jour pour Windows 10 Version 1607 pour ordinateurs à processeur x64 (KB3199209)**, puis cliquez sur **Approuver**.
4. Dans la fenêtre **Approuver les mises à jour**, dans la liste déroulante **Tous les ordinateurs**, sélectionnez **Approuvée pour l'installation**.
5. Cliquez sur **OK**, puis sur **Fermer**.
6. Vérifiez que la colonne **Approbation** affiche **Installer**.
7. Fermez la console **Update Services**.

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

Question : votre responsable a demandé si toutes les mises à jour du système d'exploitation Windows devaient être appliquées automatiquement dès leur publication. Recommandez-vous un autre processus ?

> **Réponse :** toutes les mises à jour doivent être testées avant d'être appliquées dans un environnement de production. Autrement dit, vous devez d'abord déployer les mises à jour sur un ensemble d'ordinateurs test à l'aide de WSUS.

Question : votre entreprise implémente plusieurs applications qui ne sont pas des applications Microsoft. Un collègue a proposé d'utiliser WSUS pour déployer des mises à jour pour les applications et le système d'exploitation. L'utilisation de WSUS peut-elle poser des problèmes ?

> **Réponse :** oui. WSUS est un excellent outil pour le déploiement de mises à jour pour des applications Microsoft comme Microsoft Office System et les mises à jour des systèmes d'exploitation Windows. Cependant, WSUS ne déploie pas de mises à jour pour toutes les applications Microsoft et n'en déploie aucune pour les applications non Microsoft. Microsoft System Center 2012 Configuration Manager est un choix plus avisé lorsque vous souhaitez déployer des mises à jour pour des applications non Microsoft.

Question : pourquoi WSUS est plus facile à gérer dans un domaine Active Directory Domain Services (AD DS) ?

> **Réponse :** WSUS tire parti de la structure d'unité d'organisation (UO) AD DS pour le déploiement des paramètres du client à l'aide d'une stratégie de groupe. Vous pouvez également utiliser les paramètres de stratégie de groupe pour configurer le ciblage côté client afin de déterminer l'appartenance au groupe WSUS d'un ordinateur client.

Outils

Le tableau suivant comprend les outils requis pour ce module.

Outil	Utilisation	Emplacement
Console d'administration WSUS	Gestion de WSUS	**Gestionnaire de serveur** - Outils
Applets de commande WSUS Windows PowerShell	Gestion de WSUS à partir de l'interface de ligne de commande	Windows PowerShell

Questions et réponses relatives à l'atelier pratique

Atelier pratique : implémentation de la gestion des mises à jour

Questions et réponses

Question : vous avez créé un groupe distinct pour le service Recherche. Pourquoi configurer un groupe distinct pour certains ordinateurs de votre entreprise ?

Réponse : le service Recherche peut avoir des exigences ou des règles de sécurité qui nécessitent un processus de test et d'approbation des mises à jour différent de celui suivi dans le reste de l'entreprise. De plus, les autres services peuvent avoir des administrateurs dont le rôle est de s'occuper de la gestion du processus d'approbation des mises à jour.

Question : quel avantage apporte la configuration d'un serveur WSUS en aval ?

Réponse : si la connexion de réseau étendu (WAN, Wide Area Network) qui lie le serveur WSUS principal et le serveur en aval est lente, le serveur WSUS en aval télécharge une seule fois les mises à jour pour tous les ordinateurs clients qu'il gère, au lieu que chaque ordinateur client les télécharge de manière individuelle à partir du serveur WSUS principal via la connexion WAN.