Microsoft

PRODUCTO OFICIAL DE MICROSOFT LEARNING

26744B

Proteger Windows Server 2016

Contenidos complementarios

Número de producto: 26744B

Publicado: 05/2018

TÉRMINOS DE LICENCIA DE MICROSOFT PARA UN ENTORNO VIRTUAL CON EL SIGUIENTE SOFTWARE DE MICROSOFT:

MICROSOFT ENHANCED MITIGATION EXPERIENCE TOOLKIT (EMET)
SYSINTERNALS
SOLUCIÓN DE CONTRASEÑAS DEL ADMINISTRADOR LOCAL DE MICROSOFT
ANALIZADOR DE MENSAJES DE MICROSOFT
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 PARA WINDOWS SERVER
PAQUETE DE ACTUALIZACIÓN ACUMULATIVA 1 PARA MICROSOFT APPFABRIC 1.1 PARA WINDOWS SERVER
MICROSOFT IDENTITY EXTENSIONS 1.0
MICROSOFT .NET FRAMEWORK VERSION 4.5 PARA SISTEMA OPERATIVO MICROSOFT WINDOWS Y PAQUETES DE IDIOMAS ASOCIADOS
MICROSOFT SHAREPOINT FOUNDATION 2013
MICROSOFT SQL SERVER 2014, EDICIÓN ENTERPRISE DE SERVIDOR/CAL
MICROSOFT SECURITY COMPLIANCE MANAGER VERSIÓN 4.0
MICROSOFT SQL SERVER 2008 R2 EXPRESS
MICROSOFT ADVANCED THREAT ANALYTICS

Los presentes términos de licencia constituyen un contrato entre Microsoft Corporation (o, en función de donde resida, una de sus filiales) y usted. Le rogamos que los lea atentamente. Se aplican al uso de los títulos de software de Microsoft indicados arriba y a cualquier documentación, contenido, guía de preparación del aula, archivos auxiliares y de configuración, servicios en línea y aplicaciones de ejemplo proporcionadas como parte del entorno virtual (denominados en conjunto "**Entorno virtual**") que se incluye en el soporte físico en el que lo recibió, si lo hubiera. Los términos se aplican también a todas las actualizaciones, complementos, servicios basados en Internet y servicios de soporte técnico para los componentes del Entorno virtual.

Las imágenes de disco duro virtual del software de Microsoft para el Entorno virtual se pueden proporcionar en uno o varios discos duros virtuales. Los distintos títulos de software indicados arriba se otorgan normalmente bajo licencia por separado, pero, para su comodidad, se le proporcionan bajo estos términos de licencia consolidados.

COMO SE DESCRIBE A CONTINUACIÓN, EL USO DEL ENTORNO VIRTUAL CONSTITUIRÁ SU CONSENTIMIENTO PARA LA TRANSMISIÓN DE DETERMINADA INFORMACIÓN DEL EQUIPO DURANTE LA ACTIVACIÓN, LA VALIDACIÓN Y PARA LOS SERVICIOS BASADOS EN INTERNET.

AL OBTENER ACCESO A ALGUNA PARTE DEL ENTORNO VIRTUAL, ESTARÁ ACEPTANDO ESTOS TÉRMINOS. SI NO LOS ACEPTA, NO ACCEDA, DESCARGUE NI UTILICE NINGÚN COMPONENTE DEL ENTORNO VIRTUAL.

SU DERECHO A USAR O PROPORCIONAR ACCESO AL ENTORNO VIRTUAL SE LIMITA AL PERÍODO ESPECIFICADO. CONSULTE LA SECCIÓN 8 PARA OBTENER INFORMACIÓN DETALLADA.

Si cumple los presentes términos de licencia, dispondrá de los siguientes derechos, siempre que tenga una licencia válida para el Entorno virtual.

1. DEFINICIONES.

1.1. "**Centro de aprendizaje autorizado**" hace referencia a un miembro de Learning Partner, del Programa Microsoft IT Academy o de otra entidad que Microsoft pueda designar por escrito.

1.2. "**Sesión de aprendizaje autorizada**" es la clase de aprendizaje dirigida por un instructor autorizado por Microsoft en la que se enseña un Curso de Microsoft impartido por un Instructor certificado de Microsoft (MCT, Microsoft Certified Trainer) en un Centro de aprendizaje autorizado como instalación de aprendizaje.

1.3. "**Dispositivo del aula**" es un equipo dedicado y personal, propiedad del Centro de aprendizaje autorizado o controlado por este, que se encuentra en las instalaciones de aprendizaje del Centro de aprendizaje autorizado donde se realiza la Sesión de aprendizaje autorizada que reúne o supera el nivel de hardware especificado para el título del Curso de Microsoft específico.

1.4. "**Usuario final**" es la persona que asiste a una Sesión de aprendizaje autorizada.

1.5. "**Learning Partner**" es un miembro activo del programa Microsoft Partner Network que está al día con la Competencia de aprendizaje y la posee y mantiene actualmente.

1.6. "**MCT**" o "**Instructor certificado de Microsoft**" es una persona que (i) está contratada para impartir una Sesión de aprendizaje autorizada por un Centro de aprendizaje autorizado, (ii) está certificada actualmente como Instructor certificado de Microsoft conforme al Programa de Certificación de Microsoft y (iii) mantiene actualmente una Certificación de Microsoft en la tecnología sobre la que trata la Sesión de aprendizaje autorizada.

1.7. "**Curso de Microsoft**" es la versión del kit del alumno del curso de aprendizaje dirigido por un instructor con la marca y licencia de Microsoft que enseña tecnologías de Microsoft. El título de un Curso de Microsoft puede tener la marca de curso Microsoft Official Course, Microsoft Dynamics o Microsoft Business Group.

1.8. "**Miembro del Programa Microsoft IT Academy**" es una institución académica que es miembro activo del Programa Microsoft IT Academy.

1.9. "**Usted**" hace referencia al Learning Partner o a un MCT que ejerce sus derechos en virtud de esta licencia.

2. DERECHOS DE INSTALACIÓN Y DE USO.

2.1. Sustitución de otros términos de licencia del software de Microsoft. Los términos de este contrato de licencia sustituyen los términos de cualquier contrato de licencia de Microsoft que pueda encontrar en cualquier software del Entorno virtual, incluso si la instalación o uso de ese software requieren la "aceptación" de un contrato de licencia aparte.

2.2. Derechos de uso limitados. El Entorno virtual se otorga bajo licencia, no se vende. El Entorno virtual solo se puede usar junto con el título del Curso de Microsoft asociado al Entorno virtual y, por consiguiente, debe comprar una licencia para el título del Curso de Microsoft asociado al Entorno virtual para cada Usuario final que acceda a dicho entorno y proporcionar a cada Usuario final su propia copia con licencia válida del título del Curso de Microsoft. A continuación se indican los dos conjuntos distintos de derechos de uso. Solo uno de ellos se aplica a su caso.

a. **Si es un Learning Partner,** para cada Sesión de aprendizaje autorizada que imparta, puede:

   i. descargar e instalar solo los componentes del Entorno virtual indicados en la guía de preparación del aula para el título del Curso de Microsoft que se va a impartir en la Sesión de aprendizaje autorizada en un (1) dispositivo host del aula que ejecute una copia con licencia válida de Microsoft Hyper-V para crear el Entorno virtual asociado al Curso de Microsoft;

   ii. o bien

      1. instalar el Entorno virtual en un (1) servidor interno ubicado en las instalaciones del Centro de aprendizaje autorizado donde se va a impartir la Sesión de aprendizaje autorizada **O BIEN**

      2. duplicar el Entorno virtual e instalar una (1) instancia del Entorno virtual en un (1) Dispositivo del aula que ejecute una copia con licencia válida de Microsoft Hyper-V, siempre y cuando no instale el Entorno virtual en más Dispositivos del aula que el número de Usuarios finales inscritos en la Sesión de aprendizaje autorizada en cuestión; y

   iii. permitir el acceso y uso del Entorno virtual únicamente a través de un Dispositivo del aula y solamente a:

1. un (1) Usuario final que haya comprado una licencia válida del título del Curso de Microsoft asociado al Entorno virtual únicamente para realizar las actividades prácticas del Curso de Microsoft y solamente mientras participe en la Sesión de aprendizaje autorizada, y
2. un MCT para que prepare e imparta la Sesión de aprendizaje autorizada.

b. **Si es un MCT,** para cada Sesión de aprendizaje autorizada que imparta, puede:
   i. descargar e instalar solo los componentes del Entorno virtual indicados en la guía de preparación del aula para el título del Curso de Microsoft que se va a impartir en la Sesión de aprendizaje autorizada en un (1) dispositivo host del aula que ejecute una copia con licencia válida de Microsoft Hyper-V para crear el Entorno virtual asociado al Curso de Microsoft;
   ii. o bien
      1. instalar los componentes del Entorno virtual en un (1) servidor interno ubicado en las instalaciones del Centro de aprendizaje autorizado donde se va a impartir la Sesión de aprendizaje autorizada **O BIEN**
      2. duplicar e instalar una (1) instancia de los componentes del Entorno virtual en los Dispositivos del aula que ejecuten una copia con licencia válida de Microsoft Hyper-V, siempre y cuando no instale el Entorno virtual en más Dispositivos del aula que el número de Usuarios finales inscritos en la Sesión de aprendizaje autorizada en cuestión; y
   iii. duplicar e instalar una (1) instancia del Entorno virtual en un (1) equipo personal de su propiedad, que ejecute una copia con licencia válida de Microsoft Hyper-V únicamente para preparar la Sesión de aprendizaje autorizada.

2.3. Ausencia de derechos adicionales. A este Entorno virtual no se puede acceder ni se puede usar de forma individual. Al Entorno virtual solo se puede acceder y usar junto con la Sesión de aprendizaje autorizada en la que se enseña el título del Curso de Microsoft asociado al Entorno virtual. El Entorno virtual proporcionado en virtud de este contrato de licencia no se puede utilizar en un entorno operativo o de producción activo. No se concede derecho a distribuir, mostrar públicamente o ejecutar el Entorno virtual ni ninguno de sus componentes.

2.4. Separación de los componentes. El Entorno virtual de un título de un Curso de Microsoft puede incluir varios títulos de software, contenido y otros componentes que se le pueden proporcionar en distintos soportes físicos o en varias descargas. El Entorno virtual se le proporciona bajo licencia como una sola unidad para su uso según se describe en la Sección 2.2. No podrá separar los componentes del Entorno virtual ni instalarlos en diferentes dispositivos o servidores.

2.5. Sin acceso a red. No podrá instalar el Entorno virtual en Dispositivos del aula o servidores que tengan acceso a otras redes, a menos que Microsoft lo autorice expresamente, tal como se documenta y especifica en la guía de preparación del aula para el Curso de Microsoft asociado.

2.6. Reproducción o redistribución de las imágenes de disco duro virtual de Software de Microsoft en el Entorno virtual. Usted reconoce y acepta que:
   a. el Entorno virtual contiene imágenes de disco duro virtual de software de Microsoft;
   b. el software de Microsoft que se le proporciona en virtud de este contrato constituye un activo valioso para Microsoft, por lo que su duplicación y distribución no autorizada privaría a Microsoft de los ingresos que Microsoft cobra normalmente por licencias como la del software de Microsoft;
   c. Microsoft le proporciona el software de Microsoft sin costo únicamente para ayudar a que los Usuarios finales adquieran competencias para utilizar las tecnologías de Microsoft de acuerdo con la descripción de este contrato de licencia;
   d. no puede vender, alquilar, arrendar, prestar, transferir, asignar ni sublicenciar ninguna parte del software; y
   e. no puede sublicenciar, transferir o asignar esta licencia o contrato de licencia a un tercero.

2.7. Software de terceros. El Entorno virtual puede incluir código de terceros que Microsoft, no el tercero, le proporciona bajo licencia en virtud de este contrato. Las notificaciones, si las hubiera, para el código de terceros se incluyen únicamente para su información.

2.8. Servicios en línea. Si Microsoft pone a su disposición servicios en línea como parte del Curso de Microsoft ("**Servicios en línea**"), el uso de los Servicios en línea se rige por esta sección y por los términos no contradictorios del contrato de Servicios en línea que se le proporciona a usted por separado. Al usar los Servicios en línea durante un Curso de Microsoft, acepta que (a) los Servicios en línea solo se pueden usar para realizar las actividades prácticas del título del Curso de Microsoft asociado al Entorno virtual, (b) las credenciales de autenticación que usa (usted o el Usuario final) para acceder a los Servicios en línea no deben estar asociadas a ninguna cuenta "activa", (c) otorga a Microsoft, sus filiales y todos los sublicenciatarios necesarios todos los derechos necesarios para usar y procesar todo el texto, sonido, imágenes o archivos ("Datos") cargados, procesados o almacenados mediante los Servicios en línea, (d) ni usted ni los Usuarios finales podrán introducir, cargar, procesar o almacenar ningún Dato que contenga información de identificación personal en los Servicios en línea, (e) no se usarán los dispositivos personales de los Usuarios finales ni se inscribirán en los Servicios en línea, (f) Microsoft puede eliminar cualquier Dato en cualquier momento sin previo aviso y sin obligación para con usted, y (g) Microsoft no proporcionará ningún servicio de soporte técnico para los Servicios en línea.

3. REQUISITOS DE LICENCIA Y DERECHOS DE USO ADICIONALES.

3.1 Solo podrá utilizar el Entorno virtual si cumple con los términos y condiciones de este contrato de licencia y con los siguientes requisitos de seguridad:

a. Puede acceder, instalar y usar solo los componentes descritos como componentes del Entorno virtual en la guía de preparación del aula para el título del Curso de Microsoft que se va a enseñar en la Sesión de aprendizaje autorizada programada, y solo puede usar el Entorno Virtual para proporcionar o impartir una Sesión de aprendizaje autorizada en la que se enseñe el título del Curso de Microsoft asociado al Entorno Virtual.

b. Solo puede usar las imágenes de disco duro virtual del software que acompaña a este contrato de licencia para preparar el Entorno virtual.

c. Debe preparar y configurar el Entorno virtual de acuerdo con la guía de preparación del aula del título del Curso de Microsoft que se va a enseñar en la Sesión de aprendizaje autorizada programada. No puede incluir ni usar contenido o software de su propiedad o de un tercero en el Entorno Virtual, a menos que Microsoft lo autorice y documente expresamente en la guía de preparación del aula para el título del Curso de Microsoft pertinente.

d. No puede instalar el Entorno virtual en Dispositivos del aula o servidores que tengan acceso a otras redes, a menos que Microsoft lo autorice y documente expresamente en la guía de preparación del aula para el título del Curso de Microsoft pertinente.

e. Antes del inicio de la Sesión de aprendizaje autorizada, deberá proporcionar a todos los Usuarios finales una copia física de la siguiente declaración:

"Al acceder al software y utilizarlo del modo que sea, usted reconoce y acepta que (a) puede acceder al entorno virtual y usarlo únicamente desde este Dispositivo del aula y solamente para realizar las actividades prácticas de esta sesión de aprendizaje, (b) no puede eludir las limitaciones técnicas del Entorno virtual, (c) no puede descargar, reproducir, transmitir o reenviar ningún software o componente del Entorno virtual de ninguna forma ni por ningún medio sin un permiso previo por escrito de Microsoft, (d) no puede introducir, cargar, procesar o almacenar información de identificación personal en el Entorno virtual, (e) estos términos sustituyen los términos de cualquier contrato de licencia de Microsoft que pueda encontrar en cualquier componente del Entorno virtual, incluso si la instalación o uso de ese componente requiere la "aceptación" de un contrato de licencia aparte. **Al usar el Entorno virtual, usted acepta cumplir los siguientes términos. Si no acepta estos términos, no utilice el Entorno virtual.**

Este Entorno virtual se proporciona "tal cual". Microsoft no otorga ninguna garantía, ni expresa ni implícita.

f. Solo puede permitir el acceso al Entorno virtual y su uso a los Usuarios finales que aceptaron cumplir con la declaración incluida en la sección 3.1.e arriba.

g. Antes del inicio de cada Sesión de aprendizaje autorizada, debe proporcionar a cada Usuario final su propia copia con licencia válida del título de Curso de Microsoft que se va a enseñar en la Sesión de aprendizaje autorizada.

h. No puede permitir que otras personas accedan, reenvíen, copien o descarguen el Entorno virtual.

i. Debe cumplir estrictamente todas las instrucciones de Microsoft relacionadas con la instalación, activación, uso, desactivación y seguridad del Entorno virtual.

j. No puede modificar el Entorno virtual ni ningún componente del mismo, a menos que Microsoft lo autorice expresamente, tal como se documenta en la guía de preparación del aula para el título del Curso de Microsoft.

k. Si es un Learning Partner, debe eliminar todas las copias del Entorno virtual del servidor interno y todos los dispositivos del aula al término de la Sesión de aprendizaje autorizada.

l. Si es un MCT, debe eliminar todas las copias del Entorno virtual (1) del equipo personal e (2) instaladas por usted del servidor interno del Partner Learning y de todos los dispositivos del aula al término de la Sesión de aprendizaje autorizada.

3.2 Si el Entorno virtual incluye software del sistema operativo que está desactivado, deberá obtener una clave de producto de Microsoft para activar el software antes de configurarlo para el Entorno virtual. Las instrucciones específicas sobre cómo obtener y activar el software con la clave del producto de Microsoft se incluyen en la guía de preparación del aula para el título del Curso de Microsoft. Usted es responsable del uso de las claves del producto que se le cedieron. No puede compartir sus claves de producto con terceros y no puede usar las claves de producto asignadas a terceros.

La activación asocia el uso del software a un dispositivo específico. Durante la activación, el software enviará a Microsoft información sobre el propio software y el dispositivo. Esta información incluye la versión, el idioma y la clave de producto del software, la dirección IP del dispositivo y la información derivada de la configuración de hardware del dispositivo. **EL USO DEL SOFTWARE CONSTITUIRÁ SU CONSENTIMIENTO PARA LA TRANSMISIÓN DE ESTA INFORMACIÓN**. Si tiene la licencia apropiada, tiene derecho a utilizar la versión del software que se haya instalado durante el proceso de instalación hasta agotar el plazo permitido para la activación. **A MENOS QUE EL SOFTWARE SE ACTIVE, NO TENDRÁ DERECHO A USAR EL SOFTWARE UNA VEZ TRANSCURRIDO EL PLAZO PERMITIDO PARA LA ACTIVACIÓN.** El motivo de ello es impedir el uso sin licencia. **NO ESTÁ PERMITIDO OMITIR O ELUDIR LA ACTIVACIÓN**. Si el dispositivo está conectado a Internet, el software podrá conectarse automáticamente a Microsoft para llevar a cabo la activación. También puede activar el software manualmente por teléfono o a través de Internet. En tal caso, es posible que deba abonar algún cargo por los servicios de teléfono e Internet. Algunos cambios en los componentes del equipo o en el software podrían requerir la reactivación del software. **EL SOFTWARE LE RECORDARÁ LA NECESIDAD DE ACTIVARLO HASTA QUE LO HAGA.**

3.3 Si el Entorno virtual incluye software de sistema operativo que no requiere el uso de una clave de producto, deberá comprobar el estado del sistema operativo después de la instalación del software en el Entorno virtual. Si el sistema operativo se encuentra en modo "Notificación", deberá volver a activarlo para cambiar el estado del sistema operativo antes de la Sesión de aprendizaje autorizada.

4. SERVICIOS BASADOS EN INTERNET. Es posible que Microsoft proporcione servicios basados en Internet con el software del Entorno virtual. Microsoft podrá modificarlos o cancelarlos en cualquier momento. Si el Entorno virtual contiene versiones preliminares del mismo, es posible que parte de los servicios basados en Internet se activen de forma predeterminada. La configuración predeterminada en estas versiones del software no refleja necesariamente la forma en que se configurarán las características en las versiones comerciales. Sin embargo, en caso de que el software esté configurado para transmitir por Internet, se aplican los siguientes términos:

a. Consentimiento para servicios basados en Internet. Parte del software puede incluir características que se conecten a Microsoft o a los sistemas informáticos del proveedor del servicio a través de Internet. En algunos casos, no recibirá ninguna notificación específica cuando esto ocurra. En algunos casos, puede optar por desactivar estas características o no utilizarlas. **AL USAR ESTAS CARACTERÍSTICAS, USTED ACEPTA LA TRANSMISIÓN DE ESTA INFORMACIÓN Y LA RESPONSABILIDAD DE OBTENER TODOS LOS CONSENTIMIENTOS NECESARIOS DE**

TODOS LOS USUARIOS FINALES PARA TRANSMITIR ESTA INFORMACIÓN A MICROSOFT. Microsoft no utilizará esta información para identificarle ni ponerse en contacto con usted.

b. Información del equipo. Estas características denominadas "servicios basados en Internet" utilizan protocolos de Internet, que envían a los sistemas pertinentes información de su equipo, como la dirección IP, el tipo de sistema operativo y explorador, el nombre y versión del software que esté utilizando y el código de idioma del dispositivo en el que se ejecute el software. Microsoft usa esta información para poner los servicios basados en Internet a su disposición.

c. Uso de la información. Microsoft puede usar la información del equipo y los informes de errores para mejorar su software y servicios. Asimismo, podemos compartir esta información con terceros, como proveedores de software y hardware que podrán utilizar la información para mejorar el funcionamiento de sus productos con el software de Microsoft.

d. Uso indebido de servicios basados en Internet. No puede usar estos servicios de manera que pueda perjudicar u obstaculizar su uso por parte de otros usuarios. Tampoco puede usarlos para intentar obtener acceso no autorizado a cualquier servicio, dato, cuenta o red, sean cuales fueren los métodos.

5. ÁMBITO DE LA LICENCIA. El Entorno virtual se otorga bajo licencia, no se vende. El presente contrato solo le otorga algunos derechos de uso del Entorno virtual. Microsoft se reserva todos los demás derechos. A menos que la legislación aplicable le otorgue más derechos a pesar de esta limitación, solo podrá utilizar el Entorno virtual tal como se permite expresamente en este contrato de licencia. Al hacerlo, deberá ajustarse a las limitaciones técnicas de los componentes del Entorno virtual que solo permiten utilizarlo de determinadas formas. Usted no puede realizar ni permitir que otras personas realicen lo siguiente:

a. crear o instalar una cantidad de copias del Entorno virtual en los Dispositivos del aula mayor que la cantidad de Usuarios finales que participan en la Sesión de aprendizaje autorizada;

b. permitir que la cantidad de Dispositivos de aula que acceden al Entorno virtual sea mayor en el servidor que la cantidad de Usuarios finales que participan en la Sesión de aprendizaje autorizada;

c. permitir el acceso o uso del Entorno virtual a cualquier persona excepto a los usuarios finales que hayan comprado una licencia válida del título del Curso de Microsoft que se vaya a enseñar en la Sesión de aprendizaje autorizada programada, y solo mientras esa persona participe en la Sesión de aprendizaje autorizada en la que se enseña el título del Curso de Microsoft asociado al Entorno Virtual;

d. transmitir, publicar, vincular, mostrar públicamente o reenviar el Entorno virtual o usar el Entorno virtual de forma no autorizada o prohibida;

e. reproducir, usar, descargar, proporcionar acceso o distribuir el Entorno virtual salvo en la forma permitida expresamente en este contrato;

f. alquilar, vender, arrendar o prestar el Entorno virtual, o reproducir el Entorno virtual en algún servidor o ubicación para su posterior reproducción o acceso, salvo en la forma expresamente permitida en este contrato;

g. acceder o utilizar el Entorno virtual para (i) servicios de hosting de software comercial, (ii) fines comerciales generales o (iii) cualquier fin que no haya sido expresamente autorizado por Microsoft en virtud de este contrato de licencia;

h. agregar contenido o software, alterar, modificar, adaptar, editar o crear de otro modo obras derivadas basadas en el Entorno virtual;

i. usar el Entorno virtual en otro sistema operativo o aplicación que se ejecute en otro sistema operativo;

j. eludir las limitaciones técnicas del Entorno virtual o

k. utilizar técnicas de ingeniería inversa, descompilar, personalizar o desensamblar el Entorno virtual en modo alguno.

Los derechos de acceso al Entorno virtual en cualquier dispositivo no le otorgan ningún derecho para implementar patentes u otra propiedad intelectual de Microsoft en el Entorno virtual o en los dispositivos que accedan a dicho Entorno.

6. **DERECHOS RESERVADOS Y PROPIEDAD**. Microsoft y sus proveedores se reservan todos los derechos de titularidad, de autor y de propiedad intelectual del Entorno virtual y sus componentes.

7. **SOFTWARE SUJETO A LIMITACIÓN TEMPORAL**. Tras el lanzamiento inicial, parte del software del Entorno virtual puede dejar de funcionar en la fecha indicada para el software pertinente en la guía de preparación del aula del Curso de Microsoft. No recibirá ninguna otra notificación. Le recomendamos que ejecute el comando de reactivación para restablecer el software del Entorno virtual y así ejecutarlo por un período adicional. El número de días que se puede ejecutar el software para cada lanzamiento y la cantidad de veces que se puede ejecutar el comando de reactivación varían, tal como se indica en la guía de preparación del aula del Curso de Microsoft.

   Debe detener todo el acceso y uso del Entorno virtual si algún programa de software del Entorno virtual deja de funcionar y se han agotado todas las reactivaciones (si las hubiera). No podrá acceder, utilizar ni recuperar los datos del Entorno virtual cuando este deje de funcionar.

8. **PERÍODO DE VIGENCIA Y TERMINACIÓN**. Este contrato de licencia expirará automáticamente (a) en la fecha de expiración de cualquier software indicada en la guía de preparación del aula y cuando se hayan agotado todas las reactivaciones (si las hubiera); (b) cuando Microsoft ponga término a este contrato; (c) (i) en el momento de la expiración o del término de su estado de Competencia de aprendizaje en virtud del programa Microsoft Partner Network o (ii) en el momento de la expiración o término de su estado como MCT, si es un MCT; o (d) al concluir el período de vigencia de la versión beta de cualquier software preliminar incluido en el Entorno virtual (si procede), lo que ocurra primero.

   Microsoft puede rescindir inmediatamente este contrato si existe un motivo para creer que no cumple con los términos y condiciones del mismo.

   En el momento de la terminación de este contrato por cualquier motivo, se pondrá término a todos los derechos concedidos en virtud de este contrato, y deberá dejar de acceder y utilizar inmediatamente el Entorno virtual y eliminará y destruirá permanentemente todas las copias del mismo y sus componentes en su poder o bajo su control.

9. **COMENTARIOS**. Si proporciona comentarios a Microsoft sobre el Entorno virtual, le concede a Microsoft, de forma gratuita, el derecho a utilizar, compartir y comercializar sus comentarios de cualquier forma y para cualquier propósito. También le concede a terceros, de forma gratuita, cualquier derecho de patente que necesiten para sus productos, tecnologías y servicios para utilizar o interactuar con alguna parte específica de un software o servicio de Microsoft que incluya el comentario. No proporcionará comentarios que estén sujetos a una licencia que requiera que Microsoft otorgue su software, productos, tecnologías, servicios o documentación bajo licencia a terceros debido a que incluimos sus comentarios en ellos. Estos derechos seguirán vigentes después de la terminación de este contrato.

10. **RESTRICCIONES EN MATERIA DE EXPORTACIÓN**. El software del Entorno virtual está sujeto a las leyes y a los reglamentos en materia de exportación de Estados Unidos. Debe cumplir todas las leyes y reglamentos, nacionales e internacionales, en materia de exportación que se apliquen al software. Dichas leyes incluyen limitaciones en cuanto al destino, usuarios finales y uso final. Para obtener más información, consulte www.microsoft.com/exporting.

11. **SERVICIOS DE SOPORTE TÉCNICO**. Debido a que este Entorno virtual se proporciona "tal cual", Microsoft no ofrece servicios de soporte técnico para el mismo.

12. **CONTRATO COMPLETO**. Este contrato y los términos aplicables a los complementos, actualizaciones, servicios basados en Internet, Servicios en línea y servicios de soporte técnico que utilice constituyen el contrato completo respecto del Entorno virtual y los servicios de soporte técnico.

13. LEGISLACIÓN APLICABLE.

a. Estados Unidos. Si adquirió los componentes del Entorno virtual en los Estados Unidos de América, la interpretación de este contrato se regirá por la legislación del estado de Washington, que se aplicará a las reclamaciones por incumplimiento del mismo, con independencia de conflictos de principios legales. Para el resto de reclamaciones, será aplicable la legislación de su estado de residencia, incluidas las reclamaciones en virtud de las leyes estatales en materia de protección del consumidor, competencia desleal y responsabilidad extracontractual.

b. Fuera de los Estados Unidos. Si adquirió los componentes del Entorno virtual en otro país, se aplicará la legislación de dicho país.

14. EFECTOS LEGALES. En este contrato se describen determinados derechos legales. Es posible que disponga de otros derechos en virtud de la legislación de su jurisdicción. Este contrato no modifica los derechos de los que dispone en virtud de la legislación de su país si dicha legislación no permite tal cosa.

15. EXCLUSIÓN DE GARANTÍAS. **EL ENTORNO VIRTUAL, CADA UNO DE SUS COMPONENTES Y LOS SERVICIOS EN LÍNEA SE CONCEDEN CON LICENCIA "TAL CUAL". USTED ASUME EL RIESGO DE UTILIZARLOS. MICROSOFT NO OTORGA NINGUNA GARANTÍA NI CONDICIÓN EXPRESAS. ES POSIBLE QUE LA LEGISLACIÓN LOCAL LE OTORGUE DERECHOS COMO CONSUMIDOR ADICIONALES QUE ESTE CONTRATO NO PUEDA MODIFICAR. EN LA MEDIDA EN QUE ASÍ LO PERMITA LA LEGISLACIÓN LOCAL, MICROSOFT EXCLUYE LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD, IDONEIDAD PARA UN FIN PARTICULAR Y AUSENCIA DE INFRACCIÓN DE DERECHOS.**

PARA AUSTRALIA: USTED CUENTA CON GARANTÍAS LEGALES CONFORME A LA LEY DE PROTECCIÓN AL CONSUMIDOR DE AUSTRALIA Y NINGÚN PUNTO DE ESTOS TÉRMINOS PRETENDE MODIFICAR DICHOS DERECHOS.

16. LIMITACIÓN Y EXCLUSIÓN DE RECURSOS E INDEMNIZACIONES. **PUEDE RECUPERAR DE MICROSOFT Y SUS PROVEEDORES SOLO LOS DAÑOS DIRECTOS LIMITADOS AL IMPORTE QUE PAGÓ POR EL ENTORNO VIRTUAL O 5 DÓLARES ESTADOUNIDENSES, LO QUE SEA MAYOR. NO PODRÁ OBTENER INDEMNIZACIÓN ALGUNA POR DAÑOS DE OTRA ÍNDOLE, INCLUIDOS LOS DAÑOS CONSECUENCIALES, POR LUCRO CESANTE, ESPECIALES, INDIRECTOS O INCIDENTALES.**

Esta limitación se aplica a

a. todo lo relacionado con el Entorno virtual, sus componentes, Servicios en línea y contenido (incluido el código) de sitios de Internet de terceros o programas de terceros; y

b. reclamaciones por incumplimiento de contrato, incumplimiento de garantía o condición, responsabilidad objetiva, negligencia u otra responsabilidad extracontractual en la medida que lo permita la legislación aplicable.

Asimismo, también será de aplicación incluso si Microsoft conocía o debería haber conocido la posibilidad de que se produjesen dichos daños. También pueden producirse situaciones en las que la limitación o exclusión precedente no pueda aplicarse a su caso porque su jurisdicción no admite la exclusión o limitación de daños incidentales, consecuenciales o de otra índole.

Módulo 1

Ataques, detección de infracciones y herramientas de Sysinternals

Contenidos:

Lección 1

Descripción de los ataques

Contenidos:

Preguntas y respuestas

Pregunta: Pida a los alumnos que describan los ataques que han experimentado sus empresas.

> **Respuesta:** Las respuestas serán diversas. Esta pregunta pretende suscitar un debate sobre las experiencias de los estudiantes con los ataques.

Recursos

Cronologías de los ataques

 **Lecturas adicionales:** Para obtener más información sobre los ataques pass-the-hash, consulte: "Defending Against Pass-the-Hash Attacks" en http://aka.ms/yxwbip

Lección 2

Detectar infracciones de seguridad

Contenidos:

Preguntas y respuestas

Pregunta: Hable con los estudiantes sobre sus experiencias a la hora de detectar infracciones y pregúnteles qué buscan cuando sospechan que se ha producido una vulneración en su entorno.

Respuesta: Las respuestas serán diversas. Este debate se basa en el que comenzó en la primera lección.

Lección 3

Examinar la actividad con las herramientas de Sysinternals

Contenidos:

Preguntas y respuestas

Pregunta: Pregunte a los alumnos si han utilizado alguna de las herramientas de Sysinternals y cómo las han usado.

> **Respuesta:** Las respuestas variarán en función de la experiencia del estudiante. Esta pregunta permite al instructor saber más sobre los conocimientos de los estudiantes sobre estas herramientas.

Recursos

Monitor de sistema

Lecturas adicionales: Para obtener más información sobre Sysmon, consulte: "Sysmon v5.02" en: http://aka.ms/Tigm98

Autoruns

Lecturas adicionales: Para obtener más información sobre la herramienta Autoruns, consulte: "Autoruns for Windows v13.7" en: http://aka.ms/Xnt6os

LogonSessions

Lecturas adicionales: Para obtener más información sobre la herramienta LogonSessions, consulte: "LogonSessions v1.4" en: http://aka.ms/Ugnyh8

Process Explorer

Lecturas adicionales: Para obtener más información sobre la herramienta Process Explorer, consulte "Process Explorer v16.20" en: http://aka.ms/usw7c8

Process Monitor

Lecturas adicionales: Para obtener más información sobre el Process Monitor, consulte "Process Monitor v3.32" en: http://aka.ms/Qc19u6

Sigcheck

Lecturas adicionales: Para obtener más información sobre Sigcheck, consulte "Sigcheck v2.54" en: http://aka.ms/Lsef33

Demostración: Herramientas de Sysinternals

Pasos de la demostración

1. Inicie **LON-DC1**. Cuando esta máquina virtual se haya iniciado, inicie **LON-SVR1**.
2. Inicie sesión en **LON-SVR1** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
3. En la barra de tareas, haga clic en **Explorador de archivos**.

4. En el Explorador de archivos, haga doble clic en el volumen **Allfiles (D:)**.
5. Haga doble clic en la carpeta **Labfiles**.
6. Haga doble clic en la carpeta **Mod01**.
7. En la carpeta **Mod01**, haga clic con el botón derecho en **LogonSessions.zip** y, después, haga clic en **Extraer todo**.
8. En el cuadro de diálogo **Extraer carpetas comprimidas (en zip)**, desactive la casilla de verificación **Mostrar los archivos extraídos al completar** y, después, haga clic en **Extraer**.
9. Repita los pasos 7 y 8 para **ProcessExplorer.zip** y **ProcessMonitor.zip**.
10. Cierre el Explorador de archivos.
11. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Administración de equipos**.
12. En la consola de **Administración de equipos**, expanda **Usuarios y grupos locales**, haga clic con el botón derecho en **Usuarios** y, después, haga clic en **Usuario nuevo**.
13. En el cuadro de diálogo **Usuario nuevo**, en el cuadro de texto **Nombre de usuario**, escriba **Atacante**.
14. En los cuadros de texto **Contraseña** y **Confirmar contraseña**, escriba **Pa55w.rd**.
15. Borre la casilla de verificación **El usuario debe cambiar la contraseña al iniciar una sesión de nuevo**, haga clic en **Crear** y, después, haga clic en **Cerrar**.
16. En la lista **Usuarios**, haga clic con el botón derecho en **Attacker** y, después, haga clic en **Propiedades**.
17. En el cuadro de diálogo **Propiedades del atacante**, en la pestaña **Miembro de**, haga clic en **Agregar**.
18. En el cuadro de diálogo **Seleccionar grupos**, escriba **Administradores** y haga clic en **Aceptar**.
19. Para cerrar el cuadro de diálogo **Propiedades del atacante**, haga clic en **Aceptar**.
20. Cierre la consola de **Administración de equipos**.
21. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Ejecutar**.
22. En el cuadro de diálogo **Ejecutar**, escriba **cmd.exe** y haga clic en **Aceptar**.
23. En la ventana **Administrator: C:\Windows\system32\cmd.exe**, escriba el comando siguiente y presione Entrar:

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

24. En el mensaje **Introducir la contraseña para el atacante:**, escriba **Pa55w.rd** y, después, presione Entrar.
25. Ajuste la ventana **cmd.exe (ejecutándose como LON-SVR1\Attacker)** a la derecha de la pantalla.
26. Ajuste la ventana **Administrator:c:\Windows\system32\cmd.exe** al lado izquierdo de la pantalla.
27. En el lado derecho de la pantalla, en la ventana del **símbolo del sistema de LON-SVR1\Attacker** , escriba el comando siguiente y presione Entrar:

```
ftp.exe
```

28. En el lado izquierdo de la pantalla, en la ventana **Administrator**, escriba los comandos siguientes y presione Entrar después de cada uno:

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

29. En el cuadro de diálogo **LogonSessions License Agreement**, haga clic en **Agree**.
30. Revise el resultado de la herramienta LogonSessions.

Nota: Observe los procesos e Id. que se ejecutan en el inicio de sesión para **ADATUM\Administrator** y los procesos e Id. que se ejecutan en el inicio de sesión para **LON-SVR1\Attacker**. Tiene que ver que se está ejecutando ftp.exe.

31. En el símbolo del sistema del **Administrator**, en el lado izquierdo de la pantalla, escriba los siguientes comandos y presione Entrar:

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

32. En el cuadro de diálogo **Process Explorer License Agreement**, haga clic en **Agree**.
33. Ajuste la ventana **Process Explorer** al lado izquierdo de la pantalla.
34. En el Process Explorer, busque el proceso ftp.exe debajo del proceso cmd.exe.
35. Para cerrar la sesión de FTP, en la ventana derecha **cmd.exe**, en el mensaje **ftp>**, escriba **bye** y presione Entrar.

Nota: El elemento ftp.exe se elimina del Process Explorer.

36. En la ventana **cmd.exe**, escriba **notepad newfile1.txt**, presione Entrar y, después, haga clic en **Sí**.

Nota: Aparece un elemento notepad.exe nuevo en el Process Explorer.

37. En la ventana del **Bloc de notas**, escriba algún texto aleatorio y observe los cambios efectuados en la ventana del Process Explorer. Cierre el Bloc de notas sin guardar.
38. En el símbolo del sistema **Administrator**, en el lado izquierdo de la pantalla, escriba los comandos siguientes y presione Entrar después de cada uno:

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

39. En el cuadro de diálogo **Process Monitor License Agreement**, haga clic en **Agree** y, después, ajuste la ventana del **Process Monitor** al lado izquierdo de la pantalla.
40. En la ventana derecha **cmd.exe**, escriba **ftp.exe** y presione Entrar.
41. Desplácese por la ventana del **Process Monitor** hasta que localice el nombre del proceso FTP.exe.
42. Haga clic con el botón derecho en el nombre del proceso **ftp.exe** y, después, haga clic en **Highlight 'ftp.exe'**.
43. Desplácese por la ventana del **Process Monitor** y observe que ahora todas las instancias del nombre del proceso ftp.exe están resaltadas.
44. En la barra de herramientas del **Process Monitor**, haga clic en el icono **Filter**.
45. En el cuadro de diálogo **Process Monitor Filter**, haga clic en el menú desplegable **Architecture** y, después, haga clic en **Process Name**.
46. Escriba **ftp.exe** en el cuadro de texto, haga clic en **Add** y, después, haga clic en **OK**.

47. En la ventana derecha **cmd.exe**, en el mensaje **ftp>**, escriba **bye** y presione Entrar.
48. Revise los cambios en la ventana **Process Monitor**.
49. En la barra de herramientas del **Process Monitor**, haga clic en el icono **Filter**.
50. En la lista de filtros, desactive la casilla situada al lado de **Process Name is ftp.exe**, haga clic en el menú desplegable **Arquitectura** y, después, haga clic en **Process Name**.
51. Escriba **cmd.exe** en el cuadro de texto, haga clic en **Add** y, después, haga clic en **OK**.
52. En la ventana derecha **cmd.exe**, escriba **notepad newfile2.txt**, pulse Entrar, haga clic en **Sí**, introduzca algún texto aleatorio y, después, cierre el archivo sin guardar.
53. Revise la actividad adicional registrada en el Process Monitor a partir del filtro de cmd.exe.
54. Haga clic en el menú **File** y, después, haga clic en **Save**.
55. En el cuadro de diálogo **Save To File**, acepte los valores predeterminados y, después, haga clic en **OK**.

Revisión del módulo y contenidos principales

Pregunta de revisión

Pregunta: ¿Cuál de los tipos de ataques que trata este módulo ha visto en su propio entorno?

Respuesta: Las respuestas variarán en función del entorno y de la experiencia del estudiante.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio: Detección básica de infracciones y estrategias de respuesta a los incidentes

Preguntas y respuestas

Pregunta: ¿Qué conmutador utiliza con LogonSessions para ver los procesos que se están usando en cada sesión?

Respuesta: Puede utilizar el conmutador **-p** para ver los procesos que se están usando en cada sesión.

Pregunta: ¿Cuál es la principal diferencia entre el Process Explorer y el Process Monitor?

Respuesta: El Process Explorer es una herramienta diseñada para que pueda ver la actividad en tiempo real. El Process Monitor le permite registrar la actividad para su análisis posterior.

Módulo 2

Protección de credenciales y del acceso con privilegios

Contenidos:

Lección 1

Descripción de los derechos de usuario

Contenidos:

Preguntas y respuestas

Pregunta: Pregunte a los estudiantes sobre su modelo para asignar privilegios a las cuentas administrativas. ¿Existen cuentas que tienen privilegios para varios sistemas separados, como Exchange y administrador de configuración, o hay cuentas separadas para cada conjunto de tareas administrativas?

Respuesta: Las respuestas variarán en función de las prácticas organizativas de cada estudiante.

Recursos

Principio de los privilegios mínimos

 **Lecturas adicionales:** Para obtener más información, consulte: "Implementing Least-Privilege Administrative Models" en: http://aka.ms/Hw2tr3

Usuarios protegidos, directivas de autenticación y silos de directivas de autenticación

 **Lecturas adicionales:** Para obtener más información, consulte: "Authentication Policies and Authentication Policy Silos" en: http://aka.ms/J0abq2

Demostración: Configuración de los derechos de usuario y opciones de seguridad de la cuenta

Pasos de la demostración

1. Inicie sesión en **LON-DC1** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
2. En la consola del **Administrador del servidor**, en el menú **Herramientas**, haga clic en **Centro de administración de Active Directory**.
3. En la consola del **Centro de administración de Active Directory**, haga doble clic en **Adatum (local)** y, después, haga doble clic en la unidad organizativa (UO) **IT**.
4. En la unidad organizativa **IT**, haga doble clic en **Dante Dabney**. Se abrirá el cuadro de diálogo **Dante Dabney**.
5. En el cuadro de diálogo **Dante Dabney**, haga clic en **Iniciar sesión en**.
6. En el cuadro de diálogo **Iniciar sesión en**, haga clic en **Los siguientes equipos**, escriba **LON-SVR2** y, después, haga clic en **Agregar**.
7. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Iniciar sesión en**.
8. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Dante Dabney**.
9. Vaya a **LON-SVR1** e intente iniciar sesión como **Adatum\Dante** con la contraseña **Pa55w.rd**.
10. Revise el mensaje que le informa de que la cuenta está configurada para evitar que utilice este equipo y, después, haga clic en **Aceptar**.
11. Vaya a **LON-SVR2** e intente iniciar sesión como **Adatum\Dante** con la contraseña **Pa55w.rd**.
12. Después de haber iniciar sesión correctamente, haga clic en **Inicio**, haga clic en **Dante Dabney** y, después, haga clic en **Cerrar sesión**.
13. Inicie sesión en **LON-SVR2** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.

14. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Ejecutar**.
15. En el cuadro de diálogo **Ejecutar**, escriba **gpedit.msc** y, después, haga clic en **Aceptar**.
16. En el editor d **directivas de grupo local**, en **Configuración del equipo**, expanda **Configuración de Windows**, expanda **Configuración de seguridad**, expanda **Directivas locales** y, después, seleccione **Asignación de derechos de usuario**.
17. Haga doble clic en la directiva **Denegar el inicio de sesión localmente**.
18. En el cuadro de diálogo **Propiedades de Denegar el inicio de sesión localmente** haga clic en **Agregar usuario o grupo**.
19. En el cuadro de diálogo **Seleccionar usuarios, equipos, cuentas de servicio o grupos**, escriba **Dante**, haga clic en **Comprobar nombres** y, después, haga clic dos veces en **Aceptar**.
20. Cierre el **Editor de directivas de grupo local**.
21. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Ejecutar**.
22. En el cuadro de diálogo **Ejecutar**, escriba **gpupdate /force** y, después, haga clic en Aceptar.
23. Haga clic en **Inicio**, haga clic en **Administrator** y, después, haga clic en **Cerrar sesión**.
24. Intente iniciar sesión en **LON-SVR2** como **Adatum\Dante** con la contraseña **Pa55w.rd**. Tenga en cuenta que el método de inicio de sesión no está permitido.

Demostración: Delegar privilegios

Pasos de la demostración

1. Asegúrese de haber iniciado sesión en **LON-DC1** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
2. En el menú **Herramientas** de la consola del **Administrador del servidor**, haga clic en **Usuarios y equipos de Active Directory**.
3. Haga clic con el botón derecho en la unidad organizativa **Marketing** y, después, haga clic en **Delegar control**.
4. En el **Asistente para delegación de control**, en la página **Éste es el Asistente para delegación de control**, haga clic en **Siguiente**.
5. En la página **Usuarios o grupos**, haga clic en **Agregar**.
6. En la página **Seleccionar usuarios, equipos o grupos**, escriba **IT**, haga clic en **Comprobar nombres**, haga clic en **Aceptar** y, después, haga clic en **Siguiente**.
7. En la página **Tareas que se delegarán**, seleccione **Restablecer contraseñas de usuario y forzar el cambio de contraseña en el próximo inicio de sesión** y, después, haga clic en **Siguiente**.
8. Haga clic en **Finalizar** para cerrar el **Asistente para delegación de control**.
9. Inicie sesión en **LON-SVR1** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
10. Haga clic en **Inicio** y, después, haga clic en **Administrador del servidor**. En la consola del **Administrador del servidor**, haga clic en **Administrar** y, después, haga clic en **Agregar roles y características**.
11. En el **Asistente para agregar roles y características**, en la página **Antes de comenzar**, haga clic en **Siguiente**.
12. En la página **Seleccionar tipo de instalación**, haga clic en **Instalación basada en características o en roles** y, después, haga clic en **Siguiente**.

13. En la página **Seleccionar servidor de destino**, haga clic en **Siguiente**.
14. En la página **Seleccionar Roles de servidor**, haga clic en **Siguiente**.
15. En la página **Seleccionar características**, expanda **Herramientas de administración remota del servidor**, expanda **Herramientas de administración de roles**, seleccione **Herramientas de AD DS y AD LDS**, haga clic en **Siguiente**, haga clic en **Instalar** y, después, haga clic en **Cerrar**.
16. Haga clic con el botón derecho en **Inicio**, haga clic en **Apagar o cerrar sesión** y, después, haga clic en **Cerrar sesión**.
17. Inicie sesión en **LON-SVR1** como **Adatum\Beth** con la contraseña **Pa55w.rd**.
18. Haga clic en **Inicio** y, después, haga clic en **Administrador del servidor**.
19. En la consola del **Administrador del servidor** en el menú **Herramientas** haga clic en **Usuarios y equipos de Active Directory**.
20. En **Adatum.com**, haga clic en la unidad organizativa **Marketing**. Haga clic con el botón derecho en **Ada Russell** y, después, haga clic en **Restablecer contraseña**.
21. En el cuadro de diálogo **Restablecer contraseña**, escriba dos veces la contraseña **Pa55w.rd2** y haga clic dos veces en **Aceptar**. Así se comprueba que puede restablecer las contraseñas de la unidad organizativa Marketing usando la cuenta de Beth.
22. Haga clic en la unidad organizativa **Administradores**, haga clic con el botón derecho en la cuenta de usuario **Art Odum** y, después, haga clic en **Restablecer contraseña**.
23. En el cuadro de diálogo **Restablecer contraseña**, escriba la contraseña **Pa55w.rd2** dos veces y, después, haga clic en **Aceptar**.
24. Tenga en cuenta que el sistema operativo Windows no puede efectuar el cambio de contraseña de **Art Odum** porque se ha denegado el acceso.

Lección 2

Cuentas de servicio y de equipo

Contenidos:

Preguntas y respuestas

Pregunta: Pregunte a los estudiantes cómo administran las cuentas de servicio en su organización.

> **Respuesta:** Las respuestas variarán en función de cómo administra la organización del estudiante las cuentas de servicio.

Demostración: Crear y administrar cuentas de servicio administradas por un grupo

Pasos de la demostración

1. Asegúrese de haber iniciado sesión en **LON-DC1** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
2. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Windows PowerShell (Administrador)**.
3. En el símbolo del sistema de Windows PowerShell, escriba el comando siguiente y presione Entrar:

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

4. Para crear la nueva cuenta de servicio administrada de grupo denominada **LON-SVRS-GMSA**, escriba el comando siguiente y presione Entrar:

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

5. Vaya a **LON-SVR1**, cierre la sesión con la cuenta de Beth y, después, inicie sesión como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
6. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Windows PowerShell (Administrador)**.
7. En el símbolo del sistema de Windows PowerShell, escriba el comando siguiente y presione Entrar:

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

8. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Administración de equipos**.
9. Expanda **Servicios y Aplicaciones** y, después, haga clic en **Servicios**.
10. Haga clic con el botón derecho en el servicio **Windows Internal Database** y, después, haga clic en **Propiedades**.
11. En la pestaña **Inicio de sesión**, haga clic en **Esta cuenta** y, después, haga clic en **Examinar**.
12. En el cuadro de diálogo **Seleccione usuario**, haga clic en **Ubicaciones**.
13. En el cuadro de diálogo **Ubicaciones**, haga clic en **Todo el directorio** y, después, haga clic en **Aceptar**.
14. En el cuadro de diálogo **Seleccionar usuario o cuenta de servicio**, escriba **LON-SVRS-GMSA** y, después, haga clic en **Aceptar**.
15. Borre los cuadros de texto **Contraseña** y **Confirmar contraseña** y, después, haga clic en **Aceptar**.
16. Cuando se le indique que se ha concedido a la cuenta el derecho Iniciar sesión como servicio, haga clic en **Aceptar**.

Lección 3

Protección de credenciales

Contenidos:

Preguntas y respuestas

Pregunta: ¿Qué debe hacer una organización antes de establecer un bloqueo de NTLM?

> **Respuesta:** Una organización debe auditar el uso de NTLM antes de deshabilitar el protocolo de autenticación.

Recursos

Configuración de Credential Guard

 **Lecturas adicionales:** Para obtener más información, consulte: "Proteger las credenciales de dominio derivadas con Credential Guard" en: http://aka.ms/Vwpgdp

Bloqueo de NTLM

 **Lecturas adicionales:** Para obtener más información, consulte: "Introducing the Restriction of NTLM Authentication" en: http://aka.ms/Ynbr7l

Demostración: Localización de cuentas problemáticas

Pasos de la demostración

1. Asegúrese de haber iniciado sesión en **LON-DC1** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
2. En la consola del **Administrador del servidor** en el menú **Herramientas** haga clic en **Centro de administración de Active Directory**.
3. Maximice la ventana del **Centro de administración de Active Directory** y, después, haga clic en **Búsqueda global**.
4. Haga clic en la **flecha abajo** del círculo y, después, haga clic en **Agregar criterios**.
5. Seleccione **Usuarios cuya contraseña tiene o no tiene fecha de expiración** y, después, haga clic en **Agregar**.
6. Haga clic en **Buscar**. Tenga en cuenta que se han encontrado 255 elementos.
7. Haga clic en **Borrar todo**.
8. Haga clic en **Agregar criterios**.
9. Seleccione **Usuarios con cuentas habilitadas que no iniciaron sesión durante más de un número de días indicado** y, después, haga clic en **Agregar**.
10. Haga clic en el valor subrayado **15 después del número de días** y, después, haga clic en **90**.
11. Haga clic en **Buscar**.
12. Tenga en cuenta que se han encontrado 250 elementos.

Lección 4

Estaciones de trabajo de acceso con privilegios y servidores de salto

Contenidos:

Preguntas y respuestas

Pregunta: Pregunte a los estudiantes si utilizan estaciones de trabajo de acceso con privilegios o servidores de salto en su entorno y por qué lo hacen

Respuesta: Las respuestas variarán en función del entorno del estudiante.

Recursos

Servidores de salto

 **Lecturas adicionales:** Para obtener más información, consulte: "Privileged Access Workstations" en: http://aka.ms/Rd5xkn

Protección de los controladores de dominio

 **Lecturas adicionales:** Para obtener más información, consulte: "Securing Domain Controllers Against Attack" en: http://aka.ms/H84erd

Lección 5

Solución de contraseñas de administrador local

Contenidos:

Preguntas y respuestas

Pregunta: ¿Cómo se gestionan las contraseñas de la cuenta de administrador local en su organización?

> **Respuesta:** Las respuestas serán diversas. Algunos estudiantes indicarán que sus organizaciones no tienen ninguna tecnología implementada. Otros estudiantes tendrán una solución, incluyendo algunos que usan LAPS.

Demostración: Configurar e implementar LAPS

Pasos de la demostración

1. Asegúrese de haber iniciado sesión en **LON-DC1** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
2. En la consola del **Administrador del servidor** en el menú **Herramientas** haga clic en **Usuarios y equipos de Active Directory**.
3. En la consola de **Usuarios y equipos de Active Directory**, haga clic con el botón derecho en el dominio **Adatum.com**, haga clic en **Nuevo** y, después, haga clic en **Unidad organizativa**.
4. En el cuadro de diálogo **Nuevo objeto – Unidad organizativa**, escriba el nombre **Sydney_Computers** y haga clic en **Aceptar**.
5. En adatum.com, haga clic en el contenedor **Equipos**, haga clic con el botón derecho en **LON-SVR2** y, después, haga clic en **Mover**.
6. En el cuadro de diálogo **Mover**, haga clic en **Sydney_Computers** y, después, haga clic en **Aceptar**.
7. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Ejecutar**.
8. En el cuadro de diálogo **Ejecutar**, escriba **\\LON-SVR1\d$\Labfiles\Mod02** y, después, haga clic en **Aceptar**.
9. En la ventana **Mod02**, haga doble clic en **LAPSx64.msi**.
10. En el asistente **Local Administrator Password Solution Setup** en la página **Welcome** haga clic en **Next**.
11. En la página **End-User License Agreement**, haga clic en **I accept the terms in the License Agreement** y, después, haga clic en **Next**.
12. En la página **Custom Setup**, quite la marca de selección junto a la extensión **AdmPwd GPO**, seleccione las plantillas **Management Tools**, **Fat client UI**, **PowerShell module** y **GPO Editor**; haga clic en **Next** y en **Install**.
13. Cuando finalice la instalación, haga clic en **Finish**.
14. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Windows PowerShell (Administrador)**.
15. En la ventana **Administrator: Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada comando:

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

16. En la consola del **Administrador del servidor**, en el menú **Herramientas** haga clic en **Administración de directivas de grupo**.

17. En la consola **Administración de directivas de grupo** expanda **Bosque: Adatum.com**, expanda **Dominios**, expanda **Adatum.com**, haga clic con el botón derecho en la unidad organizativa **Sydney_Computers** y, después, haga clic en **Crear un GPO en este dominio y vincularlo aquí**.
18. En el cuadro de entrada **Nombre** del cuadro de diálogo **Nuevo GPO**, escriba **LAPS_GPO** y haga clic en **Aceptar**.
19. En la ventana **Administración de directivas de grupo**, en **Sydney_Computers**, haga clic con el botón derecho en **LAPS_GPO** y haga clic en **Editar**.
20. En la ventana **Editor de administración de directivas de grupo**, en **Configuración del equipo**, expanda los nodos **Directivas** y **Plantillas administrativas** y, después, seleccione **LAPS**.
21. Haga doble clic en la directiva **Enable local admin password management**.
22. En la ventana **Enable local admin password management**, haga clic en **Habilitado** y, después, haga clic en **Aceptar**.
23. Haga doble clic en la directiva **Configuración de contraseña**.
24. En el cuadro de diálogo **Directiva de configuración de contraseña** haga clic en **Habilitado**, configure **Longitud de la contraseña** en **20**.
25. Verifique que la **vigencia de la contraseña** se configure en **30** y haga clic en **Aceptar**.
26. Cierre el **Editor de administración de directivas de grupo**.
27. Inicie sesión en **LON-SVR2** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
28. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Ejecutar**.
29. En el cuadro de diálogo **Ejecutar**, escriba **\\LON-SVR1\d$\Labfiles\Mod02** y, después, haga clic en **Aceptar**.
30. En la ventana **Mod02**, haga doble clic en **LAPSx64.msi**.
31. En **Local Administrator Password Solution Setup Wizard**, en la página **Welcome** haga clic en **Next**.
32. En la página **End-User License Agreement**, haga clic en **I accept the terms of the License Agreement**, haga clic dos veces en **Next** y, después, haga clic en **Install**.
33. Haga clic en **Finish** para cerrar **Local Administrator Password Solution Setup Wizard**.
34. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Ejecutar**.
35. En el cuadro de diálogo **Ejecutar**, escriba **gpupdate /force** y, después, haga clic en **Aceptar**.
36. Reinicie **LON-SVR2**.
37. Vaya a **LON-DC1**.
38. Haga clic en **Inicio**, haga clic en LAPS y, después, haga clic en **LAPS UI**.
39. En el cuadro de diálogo **LAPS UI**, en el cuadro de texto **ComputerName**, escriba **LON-SVR2** y haga clic en **Search**.
40. Revise los valores **Password** y **Password expires** y, después, haga clic en **Exit**.
41. En la ventana de **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

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

42. Revise la contraseña asignada a **LON-SVR2**.

Revisión del módulo y contenidos principales

Pregunta de revisión

Pregunta: ¿Qué miembros de grupos de seguridad pueden utilizar, de forma predeterminada, la aplicación de interfaz de usuario (IU) de LAPS o de Windows PowerShell para recuperar la contraseña del administrador local de un equipo configurado para usar LAPS?

Respuesta: Los miembros de los grupos Administradores de dominio y Administradores de empresa pueden recuperar la contraseña del administrador local de un equipo configurado para utilizar LAPS con la aplicación LAPS UI o Windows PowerShell.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio A: Implementar derechos de usuario, opciones de seguridad y cuentas de servicio administradas de grupo

Preguntas y respuestas

Pregunta: ¿Cómo se pueden bloquear determinados grupos de usuarios para que no puedan iniciar sesión en servidores confidenciales?

> **Respuesta:** Puede utilizar la directiva Denegar el inicio de sesión localmente para bloquear el inicio de sesión de ciertos grupos de usuarios en servidores confidenciales.

Pregunta: ¿Qué privilegio delegaría si quisiera permitir a un equipo específico de su organización crear, eliminar y administrar grupos?

> **Respuesta:** Delegaría el privilegio Crear, eliminar y administrar grupos al grupo del equipo mediante el Asistente de delegación de control.

Laboratorio B: Configurar e implementar LAPS

Preguntas y respuestas

Pregunta: ¿Qué cmdlet de Windows PowerShell se puede usar para configurar una unidad organizativa específica de manera que los equipos dentro de la unidad organizativa puedan usar LAPS?

> **Respuesta:** El cmdlet **Set-AdmPwdComputerSelfPermission** se utiliza para configurar una unidad organizativa específica para que los equipos que tienen cuentas en esa unidad organizativa puedan usar LAPS.

Pregunta: ¿Qué cmdlet de Windows PowerShell utiliza para recuperar la contraseña del administrador local de AD DS cuando un equipo está configurado para utilizar LAPS?

> **Respuesta:** El cmdlet **Get-AdmPwdPassword** se utiliza para recuperar la contraseña del administrador local de AD DS cuando un equipo está configurado para utilizar LAPS.

Módulo 3

Limitación de los derechos del administrador con Just Enough Administration (JEA)

Contenidos:

Lección 1

Descripción de JEA

Contenidos:

Preguntas y respuestas

Pregunta: ¿Qué extensión de nombre de archivo utiliza un archivo de capacidad de rol de JEA?

( ) .psrc

( ) .psd1

( ) .pssc

Respuesta:

(√) .psrc

( ) .psd1

( ) .pssc

Comentarios:

Los archivos de capacidad de rol de JEA utilizan la extensión **.psrc**. La extensión **.pssc** se utiliza para los archivos de configuración de sesión. La extensión **.psd1** se utiliza para los manifiestos de módulo.

Demostración: Crear un archivo de capacidad de rol

Pasos de la demostración

1. En **LON-DC1**, haga clic en la sugerencia **Inicio** y, después, haga clic en **Windows PowerShell ISE**.
2. Maximice la ventana **Windows PowerShell ISE**.
3. En el panel de **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada uno:

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

4. En el panel de scripts **DNSOps.psrc** de **Windows PowerShell ISE**, desplácese hasta colocar el cursor en la línea que comienza con **# VisibleCmdlets =** y, después, escriba lo siguiente:

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

5. Desplácese y coloque el cursor en la línea que comienza con **# VisibleFunctions =**. Después, escriba lo siguiente:

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

6. Desplácese y coloque el cursor en la línea que comienza con # **VisibleExternalCommands =**. Después, escriba lo siguiente:

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

7. Haga clic en **Guardar**.

Demostración: Crear un archivo de configuración de sesión

Pasos de la demostración

1. En **LON-DC1**, en el panel de **Windows PowerShell** de **Windows PowerShell ISE**, escriba los comandos siguientes y presione Entrar después de cada uno:

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

2. En el panel de scripts **DNSOps.pssc** de **Windows PowerShell ISE**, desplácese hasta la línea **SessionType = 'Default'** y modifíquela por **SessionType = 'RestrictedRemoteServer'**.
3. Vaya a la línea **#RunAsVirtualAccount = $true** y borre el símbolo **#** de modo que la línea quede así: **RunAsVirtualAccount = $true**.
4. Desplácese hasta la línea que empieza con **# RoleDefinitions**, coloque el cursor debajo de esta línea y escriba lo siguiente:

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

5. Haga clic en **Guardar**.

Demostración: Crear un punto de conexión de JEA

Pasos de la demostración

1. En el panel del **Windows PowerShell** de **Windows PowerShell ISE**, escriba los comandos siguientes y presione Entrar después de cada uno:

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

2. Compruebe que **DNSOps** aparece como un punto de conexión de Windows PowerShell.

Lección 2

Verificar e implementar JEA

Contenidos:

Preguntas y respuestas

Pregunta: ¿Es mejor crear un punto de conexión de JEA con varias capacidades de rol o crear varios puntos de conexión de JEA, cada uno vinculado a una capacidad de rol independiente?

> **Respuesta:** Las respuestas variarán en función de las opiniones del estudiante.
>
> **Comentarios:** Al crear puntos de conexión de JEA independientes es más fácil delegar tareas de operaciones distintas a personas diferentes. Si crea un punto de conexión de JEA vinculado a varias capacidades de rol, involuntariamente se podrían asignar privilegios administrativos que no son necesarios para uno o varios grupos de usuarios.

Demostración: Conectarse a un punto de conexión de JEA

Pasos de la demostración

1. Si todavía no ha iniciado sesión, inicie sesión en **LON-SVR1** como **Adatum\Administrator** utilizando **Pa55w.rd** como contraseña.
2. Haga clic en **Inicio** y, después, haga clic en **Windows PowerShell**.
3. En la ventana de **Windows PowerShell** escriba los comandos siguientes y presione Entrar después de cada uno:

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

4. Cierre sesión en **LON-SVR1**.
5. Inicie sesión en **LON-SVR1** como **Adatum\Beth** utilizando **Pa55w.rd** como contraseña.
6. Haga clic en **Inicio** y, después, haga clic en **Windows PowerShell**.
7. En la ventana de **Windows PowerShell** escriba los comandos siguientes y presione Entrar después de cada comando:

```
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
```

Nota: Tenga en cuenta que recibirá un mensaje de error al intentar reiniciar el servicio Administración remota de Windows (WinRM) porque el punto de conexión de JEA no está configurado para permitir esto.

```
Exit-PSsession
```

Demostración: Implementar la configuración de JEA en otro equipo

Pasos de la demostración

1. Si todavía no ha iniciado sesión, inicie sesión en **LON-SVR2** como **Adatum\Administrator** usando **Pa55w.rd** como contraseña.
2. Haga clic con el botón derecho en la sugerencia **Inicio** y, después, haga clic en **Ejecutar**.
3. En el cuadro de diálogo **Ejecutar**, escriba **\\LON-DC1\c$** y, después, haga clic en **Aceptar**.
4. En el **Explorador de archivos**, desplácese hasta la carpeta **Archivos de programa\WindowsPowerShell\Modules**.
5. Copie la carpeta **DNSOps** a la carpeta local **c:\Archivos de programa\WindowsPowerShell\Modules**.
6. Haga clic en **Inicio** y, después, haga clic en **Windows PowerShell**.
7. En la ventana de **Windows PowerShell** escriba los comandos siguientes y presione Entrar después de cada uno:

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

8. Compruebe que **DNSOps** aparece como un punto de conexión de Windows PowerShell.

Revisión del módulo y contenidos principales

Pregunta de revisión

Pregunta: ¿Qué elemento de la configuración de JEA le permite especificar las tareas que se pueden realizar cuando se conecta a un punto de conexión de JEA?

Respuesta: El archivo de capacidad de rol le permite especificar las tareas que se pueden llevar a cabo al conectarse a un punto de conexión de JEA.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio: Limitar los privilegios del administrador con JEA

Preguntas y respuestas

Pregunta: ¿Cómo se agregan funciones adicionales de mantenimiento del servidor DNS a la configuración de JEA?

Respuesta: Se modifica el archivo de capacidad de rol para agregar más funciones de mantenimiento del servidor DNS a la configuración de JEA.

Pregunta: ¿Qué comando le permite comprobar si una cuenta virtual está siendo utilizada en una sesión de JEA?

Respuesta: Puede utilizar el comando **whoami.exe** para comprobar que una cuenta virtual está siendo utilizada en una sesión de JEA.

Módulo 4

Privileged Access Management (PAM) y bosques de administración

Contenidos:

Lección 1

Bosques de ESAE

Contenidos:

Preguntas y respuestas

Pregunta: ¿Debería plantearse la implementación de un bosque de ESAE en su entorno como método para proteger las cuentas utilizadas para llevar a cabo tareas administrativas?

Respuesta: Las respuestas variarán en función de su entorno.

Lección 2

Descripción general de Microsoft Identity Manager

Contenidos:

Preguntas y respuestas

Pregunta: Pregunte a los estudiantes si han implementado MIM o Forefront Identity Manager (FIM) para administrar la identidad en su entorno.

Respuesta: Las respuestas variarán en función de los datos del entorno del estudiante.

Recursos

Requisitos de MIM

Lecturas adicionales: Para obtener más información sobre los requisitos de MIM, consulte Plataformas compatibles con MIM 2016: http://aka.ms/Armxl4

Lección 3

Descripción general de la administración de JIT y de PAM

Contenidos:

Preguntas y respuestas

Pregunta: Aparte del sistema operativo del servidor host, ¿qué dos productos de Microsoft necesita implementar antes de implementar MIM 2016?

Respuesta: Necesita implementar SharePoint y SQL Server antes de implementar MIM 2016.

Demostración: Configurando la relación de confianza con PAM

Pasos de la demostración

1. En **SYD-MIM**, asegúrese de haber iniciado sesión como **Adatumadmin\MIMAdmin** con la contraseña **Pa$$w0rd** y, después, abra la ventana de **Windows PowerShell**.
2. En la ventana de **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

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

3. En el símbolo del sistema, inicie sesión usando **Pa$$w0rd** como contraseña y, después, haga clic en **Aceptar**.
4. En la ventana de **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada comando (algunos comandos pueden tardar varios minutos en efectuar la ejecución según la velocidad de las máquinas virtuales):

```
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. Vaya a **MEL-DC1**. En la consola del **Administrador del servidor**, haga clic en Herramientas y, después, haga clic en **Usuarios y equipos de Active Directory**.
6. En la consola de **Usuarios y equipos de Active Directory**, haga clic con el botón derecho en **Adatum.com** y, después, haga clic en **Delegar control**.
7. En la página **Éste es el Asistente para delegación de control** del **Asistente para delegación de control**, haga clic en **Siguiente**.
8. En la página **Usuarios o grupos**, haga clic en **Agregar**.
9. En la página **Seleccionar usuarios, equipos o grupos,** haga clic en **Ubicaciones**.
10. En el cuadro de diálogo **Ubicaciones**, haga clic en **ADATUMADMIN.COM** y, después, haga clic en **Aceptar**.
11. En el cuadro de diálogo **Seleccionar usuarios, equipos o grupos**, escriba **Administradores de dominio** y haga clic en **Comprobar nombres**.
12. En el cuadro de diálogo **Escribir credenciales de red** proporcione las credenciales siguientes y haga clic en **Aceptar**:
    - Nombre de usuario: **Adatumadmin\administrator**
    - Contraseña: **Pa$$w0rd**
13. En el cuadro de diálogo **Seleccionar usuarios, equipos o grupos**, después de Administradores de dominio, escriba **Mimmonitor**, haga clic en **Comprobar nombres** y, después, haga clic en **Aceptar**.
14. En la página **Usuarios o grupos** haga clic en **Siguiente**.
15. En la página **Tareas que se delegarán**, seleccione **Leer toda la información del usuario**, haga clic en **Siguiente** y, después, haga clic en **Finalizar**.

Demostración: Crear entidades de seguridad de usuario y entidades de seguridad de instantáneas

Pasos de la demostración

1. Asegúrese de haber iniciado sesión en **MEL-DC1** como **ADATUM\Administrator** usando **Pa$$w0rd** como contraseña.
2. Haga clic en el icono de **Windows PowerShell** de la barra de tareas.
3. En la ventana de **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada uno:

```
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"
```

 **Nota:** Se creará un grupo llamado CorpAdmins y un usuario llamado Wayne, que se utilizará más tarde para la demostración de PAM.

4. Vaya a **SYD-MIM**. Debería haber iniciado sesión como **adatumadmin\mimadmin** utilizando **Pa$$w0rd** como contraseña.
5. En la ventana de **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada uno:

```
$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 "Adatum forest domain
admin credentials"
```

6. En el cuadro de diálogo, inicie sesión usando **Pa$$w0rd** como contraseña y, después, haga clic en **Aceptar**.
7. En la ventana de **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada uno:

```
$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. Vaya a **SYD-DC1**.
9. En el **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Usuarios y equipos de Active Directory**.
10. Abra el contenedor **PAM Objects** y verifique que el grupo **Adatum.CorpAdmins** y el usuario **PRIV.Wayne** están presentes.
11. Si uno de ellos no está todavía abierto, abra la ventana de **Windows PowerShell** y escriba los comandos siguientes, presionando Entrar después de cada comando:

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

 **Nota:** El valor de SID del grupo Adatum y el valor del historial de SID del grupo ADATUMADMINS son los mismos.

Demostración: Configurar y solicitar acceso con privilegios

Pasos de la demostración

1. Asegúrese de haber iniciado sesión en **MEL-SVR1** como **Adatum\administrator** usando **Pa$$w0rd** como contraseña.
2. Haga clic en el icono del Explorador de archivos de la barra de tareas y haga doble clic en la **unidad de DVD (D:) MIM2016-EVAL**.
3. Haga doble clic en el archivo .htm y, en el cuadro de diálogo **Internet Explorer**, haga clic en **Sí**.
4. En la página de **Microsoft Identity Manager**, haga clic en **Install Add-ins and Extensions, 64-bit**.
5. En el cuadro de diálogo **¿Quiere guardar o ejecutar el archivo setup.exe?**, haga clic en **Ejecutar**.
6. En la página **Bienvenido al Asistente para instalación de complementos y extensiones de Microsoft Identity Manager** del **Asistente de Microsoft Identity Manager 2016**, haga clic en **Siguiente**.
7. En la página **Contrato de licencia para el usuario final**, haga clic en **Acepto los términos del Contrato de licencia** y, después, haga clic en **Siguiente**.
8. En la página **Programa para la mejora de la experiencia del usuario de MIM**, haga clic en **No deseo participar en el programa en este momento** y haga clic en **Siguiente**.
9. En la página **Configuración personalizada**, haga clic en **MIM Add-in for Outlook** y, después, haga clic en **La característica completa no estará disponible**.
10. En la página **Configuración personalizada**, haga clic en **MIM Password and Authentication** y, después, haga clic en **La característica completa no estará disponible**.
11. En la página **Configuración personalizada**, haga clic en **PAM Client**, haga clic en **La característica entera se instalará en la unidad de disco duro local** y, después, haga clic en **Siguiente**.
12. En la página **Configurar dirección del servicio MIM PAM**, configure las siguientes opciones y haga clic en **Siguiente**:
    - Dirección de servidor PAM: **syd-mim.adatumadmin.com**
    - Puerto: **5725**
13. Haga clic en **Instalar** y, cuando finalice la instalación, haga clic en **Finalizar**.
14. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Administración de equipos**.
15. En la consola de **Administración de equipos**, expanda **Usuarios y grupos locales**. Después, haga clic en **Grupos**. Haga doble clic en el grupo **Administradores**.
16. En el cuadro de diálogo **Propiedades del administrador**, haga clic en **Agregar**.
17. En el cuadro de diálogo **Seleccionar usuarios, equipos, cuentas de servicio o grupos**, escriba **adatumadmin\adatum.corpadmins** y haga clic en Comprobar nombres.
18. Introduzca las credenciales **adatumadmin\administrator** y la contraseña **Pa$$w0rd**. Después, haga clic en **Aceptar** tres veces.
19. Haga clic con el botón derecho en **Inicio**, haga clic en **Apagar o cerrar sesión** y, después, haga clic en **Reiniciar**. Indique el motivo **Laboratorio**.
20. Inicie sesión en **MEL-SVR1** como **Adatum\Wayne** utilizando **Pa$$w0rd** como contraseña.
21. En la **barra de tareas**, haga clic en **Windows PowerShell**. Después, en la ventana de **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

```
Whoami /groups
```

22. Compruebe que la cuenta **Wayne** no sea miembro del grupo **CorpAdmins**.
23. En la **barra de tareas**, haga clic en **Administrador del servidor**.
24. En el menú **Administrar** de la consola del **Administrador del servidor**, haga clic en **Agregar roles y características**.
25. En la página **Antes de comenzar**, haga clic en **Siguiente** cuatro veces.
26. En la página **Seleccionar características** haga clic en **Servidor WINS**. En el cuadro de diálogo **Agregar roles y características**, haga clic en **Agregar características**.
27. Haga clic en **Siguiente** y, después, haga clic en **Instalar**.
28. Revise el mensaje que le informa que no tiene los derechos de usuario adecuados para realizar cambios en el equipo de destino y, después, haga clic en **Cerrar**.
29. Haga clic con el botón derecho en **Inicio**, haga clic en **Apagar o cerrar sesión** y, después, haga clic en **Cerrar sesión**.
30. Inicie sesión en **MEL-SVR1** como **ADATUMADMIN\priv.Wayne** utilizando **Pa$$w0rd** como contraseña.
31. En la **barra de tareas**, haga clic en **Windows PowerShell** y, después, en la ventana de **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

```
Whoami /groups
```

32. Compruebe que la cuenta no sea miembro del grupo **CorpAdmins**.
33. En la **barra de tareas**, haga clic en **Administrador del servidor**.
34. En el menú **Administrar** de la consola del **Administrador del servidor**, haga clic en **Agregar roles y características**.
35. En la página **Antes de comenzar**, haga clic en **Siguiente** cuatro veces.
36. En la página **Seleccionar características** haga clic en **Servidor WINS**.
37. En el cuadro de diálogo **Agregar roles y características**, haga clic en **Agregar características**, haga clic en **Siguiente** y, después, haga clic en **Instalar**.
38. Revise el mensaje que le informa que no tiene los derechos de usuario adecuados para realizar cambios en el equipo de destino y, después, haga clic en **Cerrar**.
39. En la ventana de **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada uno:

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

Nota: Se mostrará una lista de roles que se pueden aplicar a la cuenta **priv.Wayne**. Tenga en cuenta el período de vida del rol enumerado.

40. En la ventana de **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada uno:

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

Nota: El estado de la solicitud cambia a **Procesando**.

41. Haga clic con el botón derecho en **Inicio**, haga clic en **Apagar o cerrar sesión** y, después, haga clic en **Cerrar sesión**.
42. Inicie sesión en **MEL-SVR1** como **ADATUMADMIN\priv.Wayne** utilizando **Pa$$w0rd** como contraseña.
43. En la **barra de tareas**, haga clic en **Windows PowerShell**. En la ventana de **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

```
Whoami /groups
```

44. Compruebe que la cuenta sea miembro del grupo **CorpAdmins**.
45. En la **barra de tareas**, haga clic en **Administrador del servidor**.
46. En el menú **Administrar** de la consola del **Administrador del servidor**, haga clic en **Agregar roles y características.**
47. En la página **Antes de comenzar**, haga clic en **Siguiente** cuatro veces.
48. En la página **Seleccionar características** haga clic en **Servidor WINS**.
49. En el cuadro de diálogo **Agregar roles y características**, haga clic en **Agregar características**, haga clic en **Siguiente** y, después, haga clic en **Instalar**.
50. Cuando se instale la característica, haga clic en **Cerrar**.

Demostración: Administrar roles de PAM

Pasos de la demostración

1. Vaya a **MEL-DC1** y compruebe que ha iniciado sesión como **ADATUM\Administrator**.
2. En la ventana de **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada uno:

```
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"
```

Nota: Este conjunto de comandos le permite crear un usuario nuevo llamado Gavin que habilitará para PAM.

3. Vaya a **SYD-MIM** y asegúrese de haber iniciado sesión como **ADATUMADMIN\MIMAdmin**.
4. En la ventana de **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada uno:

```
$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. Inicie **Internet Explorer** y vaya a **http://syd-mim.adatumadmin.com:82/IdentityManagement/default.aspx**.

6. Si se le solicita, inicie sesión como **ADATUMADMIN\Mimadmin** utilizando **Pa$$w0rd** como contraseña.
7. En la consola de **Microsoft Identity Manager**, haga clic en **PAM Roles** en **Privileged Access Management**.
8. En la lista de roles de **Privileged Access Management**, haga clic en **CorpAdmins**.
9. En la pestaña **General** del cuadro de diálogo **Corpadmins**, cambie el **PAM Role TTL(sec)** de **3600** a **600**, haga clic en **OK** y, después, haga clic en **Submit**.

Nota: Al efectuar esta demostración, también puede describir la función de los otros campos.

10. En la lista de roles de **Privileged Access Management**, haga clic en **Corpadmins**.
11. En la pestaña **Candidates** del cuadro de diálogo **Corpadmins**, haga clic en **Browse**.
12. En el cuadro de diálogo **Select Users**, haga clic en la lupa situada junto a Buscar. Wayne y Adatum.Wayne ya deberían estar seleccionados. Seleccione **ADATUM.Gavin** y **Gavin**. Después, haga clic dos veces en **OK** y haga clic en **Submit**.
13. Haga clic en **OK** para cerrar el cuadro de diálogo **CorpAdmins**.
14. En **Privileged Access Management**, haga clic en **PAM Requests**.
15. Revise las **PAM Requests**.
16. Haga clic en **PRIV.Wayne** y revise la información de cuándo se hizo la solicitud, cuándo caduca la solicitud y el rol solicitado.

Revisión del módulo y contenidos principales

Pregunta de revisión

Pregunta: ¿Cuál es el número mínimo de bosques necesarios para implementar PAM?

Respuesta: Se necesita un mínimo de dos bosques para implementar PAM, incluido el bosque de administración en el que se implementa PAM y el bosque de producción.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio: Limitar los privilegios del administrador con PAM

Preguntas y respuestas

Pregunta: ¿Qué paso seguiría para garantizar que un usuario que solicita un rol de PAM tenga acceso a ese rol durante dos horas en vez de una?

Respuesta: Tendría que cambiar el TTL del rol a dos horas.

Pregunta: ¿Dónde se pueden ver los usuarios a los que se han concedido roles de PAM?

Respuesta: Puede utilizar la sección de solicitudes de PAM, en el área de Privileged Access Management, en la consola de MIM.

Módulo 5

Mitigar malware y amenazas

Contenidos:

Lección 1

Configuración y administración de Windows Defender

Contenidos:

Preguntas y respuestas

Pregunta: ¿Cuáles son algunas de las opciones de examen disponibles cuando se usa Windows Defender?

Respuesta: La siguiente tabla describe las opciones de examen.

Las opciones de examen	Descripción
Examen rápido	Comprueba las áreas que tienen más probabilidades de ser infectadas por malware, incluidos virus, spyware y software no deseado.
Examen completo	Comprueba todos los archivos del disco duro y todos los programas que se estén ejecutando.
Examen personalizado	Permite a los usuarios examinar unidades y carpetas específicas.

Demostración: Uso de Windows Defender

Pasos de la demostración

1. Vaya a **LON-CL1**.
2. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Panel de control**.
3. Haga clic en **Ver por**, seleccione **Iconos grandes** y, después, haga clic en **Windows Defender**.
4. Haga clic en **Cerrar** en el cuadro de diálogo **Novedades**.
5. En la pestaña **Inicio** de Windows Defender, asegúrese de que la opción **Examen rápido** está seleccionada.
6. Haga clic en **Examinar ahora** y revise los resultados.
7. Cierre Windows Defender.
8. Abra el Explorador de archivos y vaya a **C:\Archivos**.
9. En la carpeta **Archivos**, abra **sample.txt** en el Bloc de notas. El archivo **sample.txt** contiene una cadena de texto para probar la detección de malware.
10. En el archivo **sample.txt** elimine ambas instancias de **<remove>**, incluidos los corchetes y las líneas adicionales o espacios en blanco.
11. Guarde el archivo y ciérrelo. Inmediatamente, Windows Defender detecta una amenaza potencial.
12. Windows Defender extrae **sample.txt** de la carpeta **Archivos**.
13. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Panel de control**.
14. Haga clic en **Windows Defender**.
15. En Windows Defender, haga clic en la pestaña **Historial**.
16. Haga clic en **Ver detalles** y revise los resultados.
17. Seleccione la casilla de verificación **Virus:DOS/EICAR_Test_File** y haga clic en **Quitar**.
18. Cierre todas las ventanas abiertas.

Lección 2

Restringir el software

Contenidos:

Recursos

¿Qué es AppLocker?

 **Lecturas adicionales:** Para obtener más información sobre AppLocker, consulte la introducción de AppLocker: http://aka.ms/Amf8jf

Demostración: Crear reglas de AppLocker

Pasos de la demostración

Crear un objeto de directiva de grupo (GPO) para aplicar las reglas ejecutables predeterminadas de AppLocker

1. En **LON-DC1**, en el Administrador del servidor, haga clic en **Herramientas** y, después, haga clic en **Administración de directivas de grupo**.
2. En la **Consola de administración de directivas de grupo (GPMC)**, vaya a **Bosque: Adatum.com\Domains\Adatum.com**.
3. Haga clic en **Objetos de directiva de grupo**, haga clic con el botón derecho en **Objetos de directiva de grupo** y, después, haga clic en **Nuevo**.
4. En la ventana **Nuevo GPO**, en el cuadro de texto **Nombre**, escriba **Directiva de restricción de WordPad** y, después, haga clic en **Aceptar**.
5. Haga clic con el botón derecho en **Directiva de restricción de WordPad** y, después, haga clic en **Editar**.
6. En la ventana **Editor de administración de directivas de grupo** vaya a **Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Directivas de control de aplicaciones\AppLocker**.
7. Haga clic en **Reglas ejecutables**, haga clic con el botón derecho en **Reglas ejecutables** y, después, seleccione **Crear nueva regla**.
8. En la página **Antes de comenzar**, haga clic en **Siguiente**.
9. En la página **Permisos**, haga clic en **Denegar** y en **Siguiente**.
10. En la página **Condiciones**, haga clic en **Editor** y en **Siguiente**.
11. En la página **Editor**, haga clic en **Examinar** y en **Este equipo**.
12. En la página **Abrir**, haga doble clic en **Disco Local (C:)**.
13. En la página **Abrir**, haga doble clic en **Archivos de programa**, haga doble clic en **Windows NT**, haga doble clic en **Accesorios**, haga clic en **wordpad.exe** y, después, haga clic en **Abrir**.
14. Desplace hacia arriba el control deslizante hasta la posición **Nombre de archivo** y haga clic en **Siguiente**.
15. Haga clic de nuevo en **Siguiente** y, después, haga clic en **Crear**.
16. Si se le pregunta si quiere crear reglas predeterminadas, haga clic en **Sí**.
17. En la ventana **Editor de administración de directivas de grupo**, vaya a **Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad**.
18. Expanda **Directivas de control de aplicaciones**, haga clic con el botón derecho en **AppLocker** y, después, seleccione **Propiedades**.

19. En la pestaña **Cumplimiento**, en **Reglas ejecutables**, seleccione la casilla de verificación **Configurado**, haga clic en **Aplicar reglas** y, después, haga clic en **Aceptar**.
20. En la ventana **Editor de administración de directivas de grupo**, vaya a **Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad**.
21. Haga clic en **Servicios del sistema** y haga doble clic en **Identidad de aplicación**.
22. En el cuadro de diálogo **Propiedades de identidad de aplicación**, en **Seleccionar el modo de inicio del servicio**, haga clic en **Definir esta configuración de directiva**, en **Automático** y, después, en **Aceptar**.
23. Cierre la ventana del **Editor de administración de directivas de grupo**.

Aplicar el GPO al dominio

1. En **GPMC**, expanda **Bosque: Adatum.com**, expanda **Dominios**, expanda **Adatum.com** y, después, expanda **Objetos de directiva de grupo**.
2. En **GPMC**, haga clic con el botón derecho en **Adatum.com** y, después, haga clic en **Vincular un GPO existente**.
3. En la ventana **Seleccionar GPO**, en la ventana **Objetos de directiva de grupo**, haga clic en **Directiva de restricción de WordPad** y, después, haga clic en **Aceptar**.
4. Cierre **GPMC**.
5. Vaya a la pantalla **Inicio**, escriba **cmd** y presione Entrar.
6. En la ventana del **símbolo del sistema**, escriba **gpupdate /force** y presione Entrar. Espere a que se actualice la directiva.

Probar la regla de AppLocker

1. Inicie sesión en **LON-CL1** como **Adatum\Beth** con la contraseña **Pa55w.rd**.
2. En el cuadro de texto **Buscar**, escriba **cmd** y presione Entrar.
3. En la ventana del **símbolo del sistema**, escriba **gpupdate /force** y presione Entrar. Espere a que se actualice la directiva.
4. En el cuadro de texto **Buscar**, escriba **WordPad** y presione Entrar. Observe que WordPad no se inicia.

 **Nota:** El comando gpupdate (actualización de directiva de grupo) tardará unos minutos en surtir efecto. Si WordPad se inicia, espere un minuto y vuelva a intentarlo.

Lección 3

Configuración y uso de Device Guard

Contenidos:

Recursos

Implementar directivas de Device Guard

Lecturas adicionales: Para obtener más información, consulte el apartado "Configurable Code Integrity Policy for Windows PowerShell" en http://aka.ms/U0nker

Reglas de archivos de integridad de código

Lecturas adicionales: Para obtener más información, consulte Agregar una aplicación sin firmar a la directiva de integridad de código: http://aka.ms/Tkie2j

Vínculos de referencia: Para descargar una copia de **signtool.exe**, consulte SignTool en: http://aka.ms/S4ihkk

Demostración: Creación de reglas de archivos de integridad de código

Pasos de la demostración

1. En **LON-DC1**, abra la pantalla **Inicio** y seleccione **Windows PowerShell**.
2. En Windows PowerShell, escriba los comandos siguientes y presione Entrar después de cada línea:

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

3. Examine el dispositivo para buscar las aplicaciones instaladas. Cree una nueva directiva de integridad de código escribiendo el comando siguiente y presionando Entrar:

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

4. Convierta la directiva de integridad de código a un formato binario escribiendo el comando siguiente y presionando Entrar:

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

5. Cuando haya acabado estos pasos, cierre Windows PowerShell. El archivo de directiva de Device Guard (**DeviceGuardPolicy.bin**) y el archivo .xml original (**InitialScan.xml**) estarán disponibles en su escritorio.
6. Abra el archivo **Initalscan.xml** ubicado en el escritorio. Para abrir el archivo, haga clic en el icono del Explorador de archivos de la barra de tareas, escriba **C:\Users\Administrator\Desktop\Initialscan.xml** en el cuadro **Acceso rápido** y presione Entrar.

   Verá que las reglas actuales de **SIPolicy** están configuradas con el **modo auditoría** habilitado.
7. En la pantalla Inicio, seleccione **Windows PowerShell**.
8. En la ventana de **Windows PowerShell** escriba el cmdlet y el parámetro siguientes para examinar las opciones de regla:

```
Set-RuleOption -Help
```

9. Revise el resultado del comando. Verá que el **modo auditoría** está definido en la regla 3.

10. En Windows PowerShell, escriba los comandos siguientes y presione Entrar después de cada línea:

```
# Inicialice las variables que serán utilizadas
$CIPolicyPath=$env:userprofile+"\Desktop\"
$InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"
$CIPolicyBin=$CIPolicyPath+"DeviceGuardPolicy.bin"
$EnforcedCIPolicy=$CIPolicyPath+"EnforcedPolicy.xml”
$CIEnforceBin = $CIPolicyPath + “EnforceDeviceGuardPolicy.bin”
# Copie el archivo inicial para conservar la copia original.
cp $InitialCIPolicy $EnforcedCIPolicy
# Quite el modo auditoría
Set-RuleOption -Option 3 -FilePath $EnforcedCIPolicy -Delete
# Pase la nueva directiva de código a un formato binario
ConvertFrom-CIPolicy $EnforcedCIPolicy $CIEnforceBin
```

11. Abra el archivo **EnforcedPolicy.xml** ubicado en el escritorio y, después, asegúrese de que ya no contiene el **modo auditoría**.

Lección 4

Implementar y utilizar EMET

Contenidos:

Demostración: Protección de aplicaciones con EMET

Pasos de la demostración

1. En **26744B-LON-DC1**, instale el archivo **EMET Setup.msi** ubicado en **E:\Labfiles\Mod05**.
2. Una vez finalizada la instalación, seleccione **Configure Manually Later**, haga clic en **Finish** y, después, haga clic en **Close**.
3. En el área de notificación, en la esquina inferior derecha, haga clic con el botón derecho en el icono y, después, seleccione **Open EMET**.
4. Haga clic en **Apps** en la barra de menús superior y, después, revise las aplicaciones que están configuradas en EMET.
5. Cierre la ventana **Application Configuration**.
6. Haga clic en **Import** en la esquina superior izquierda de EMET. Revise las tres opciones disponibles. Seleccione **Recommended Software.xml** y haga clic en **Abrir**.
7. Haga clic en **Apps** en la barra de menús superior y, después, revise las aplicaciones que están configuradas en EMET.
8. Observe que el archivo ejecutable de Windows PowerShell no está incluido. Haga clic en **Add Application**. En el cuadro de texto **Nombre de archivo** escriba **C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe**.
9. Haga clic en **Open** y en **OK**.
10. Haga clic en **Inicio**. Haga clic en el icono de **Windows PowerShell**. Una vez cargada la aplicación, minimícela en el área de notificación.
11. En la página del **Enhanced Mitigation Experience Toolkit**, haga clic en **Refresh**. Ahora debería ver **PowerShell - Windows PowerShell** debajo de **Running Processes**.

Revisión del módulo y contenidos principales

Procedimientos recomendados

Cuando utilice EMET en su organización, debe utilizar objetos de directiva de grupo (GPO) para implementar configuraciones uniformes en todo el entorno.

Pregunta de revisión

Pregunta: ¿Cuál es la mejor forma de implementar EMET en un entorno de empresa grande?

> **Respuesta:** Usar la directiva de grupo o Microsoft System Center Configuration Manager. Las versiones actuales tienen soporte incorporado para la directiva de grupo y System Center Configuration Manager.

Problemas y supuestos reales

Hay informes nuevos de malware que se usa para aprovecharse de organizaciones en todo el mundo. Es importante que revise el último Microsoft Security Bulletin Summary para conocer las vulnerabilidades que puedan existir en su sistema y cómo mantenerse al día en las tecnologías antimalware y actualizaciones.

Herramientas

Hay una serie de herramientas que puede utilizar para aprovechar las vulnerabilidades en un sistema Windows. Kali Linux se distribuye gratuitamente e incluye varias herramientas que los administradores de Windows pueden usar para comprobar la seguridad de su sistema.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio: Proteger las aplicaciones con AppLocker, Windows Defender, las reglas de Device Guard y EMET

Preguntas y respuestas

Pregunta: El laboratorio incluye varias opciones que puede utilizar para ayudar a evitar malware. ¿Qué solución de seguridad utiliza tecnologías de mitigación para hacer lo más difícil posible las vulnerabilidades de seguridad?

Respuesta: EMET. Complica mucho las vulnerabilidades de seguridad, pero estas tecnologías de mitigación de seguridad no garantizan que los hackers no puedan aprovecharse de las vulnerabilidades.

Pregunta: ¿Cuáles de las tecnologías explicadas en este módulo permiten prevenir el malware?

Respuesta: Windows Defender, AppLocker, EMET y Device Guard están diseñados para trabajar juntos para poder combatir el malware en los sistemas Windows.

Módulo 6

Análisis de la actividad con auditoría avanzada y Log Analytics

Contenidos:

Lección 1

Descripción de la auditoría

Contenidos:

Demostración: Ubicar eventos en el registro de seguridad

Pasos de la demostración

1. En la barra de tareas de LON-SVR1, haga clic en el **Explorador de archivos**.
2. En el panel de navegación, haga clic en **Este equipo**.
3. Haga doble clic en **Allfiles (D:)**.
4. Haga clic con el botón derecho en **Labfiles** y, después, haga clic en **Propiedades**.
5. Haga clic en la pestaña **Uso compartido** y, después, haga clic en **Compartir**.
6. En el cuadro, escriba **Abbi** y haga clic en **Agregar**.

Nota: Abbi Skinner debe recibir acceso de lectura.

7. Haga clic en **Compartir**.
8. Haga clic en **Cambiar configuración**, en **Listo** y, después, en **Cerrar**.
9. Haga clic con el botón derecho en **Labfiles**, haga clic en **Propiedades**, haga clic en la pestaña **Seguridad** y, después, haga clic en **Opciones avanzadas**.
10. Seleccione la pestaña **Auditoría** y, después, haga clic en **Agregar**.
11. Haga clic en **Seleccionar una entidad de seguridad**. En el cuadro, escriba **Todos** y haga clic en **Aceptar**.
12. En **Tipo**, seleccione **Todo** y, después, haga clic en **Aceptar**.
13. Haga clic en **Aceptar** dos veces.
14. En el Administrador del servidor de LON-DC1, haga clic en **Herramientas** y, después, seleccione **Administración de directivas de grupo**.
15. Expanda **Bosque:Adatum.com**, expanda **Dominios**, expanda **Adatum.com**, seleccione y haga clic con el botón derecho en **Default Domain Policy** y, después, haga clic en **Editar**.
16. Expanda Configuración del equipo, Directivas, Configuración de Windows, Configuración de seguridad y, después, Directivas locales.
17. Haga clic en Directiva de auditoría.
18. Haga doble clic en Auditar el acceso a objetos y, después, seleccione la casilla de verificación Definir esta configuración de directiva.
19. Seleccione **Correcto** y **Error** y, después, haga clic en **Aceptar**.
20. Abra el símbolo del sistema de Windows, escriba el comando siguiente y presione Entrar.

```
GPUpdate /Force
```

Nota: También puede configurarlo en la configuración avanzada de directivas de auditoría, que se encuentra en **Equipo** > **Directivas** > **Configuración de Windows** >**Configuración de seguridad** > **Configuración de directiva de auditoría avanzada**.

21. Inicie sesión en LON-CL1 como **Abbi** con la contraseña **Pa55w.rd**.
22. Mediante el Explorador de archivos, busque y abra \\lon-svr1\Labfiles\Mod01\logonSessions.zip.
23. Cierre sesión en LON-CL1.
24. Inicie sesión en LON-CL1 como **Beth** con la contraseña **Pa55w.rd**.
25. Mediante el Explorador de archivos, intente buscar y abrir **\\lon-svr1\Labfiles**.
26. Haga clic en Cerrar en el mensaje de error.
27. En LON-DC1, en **Administrador del servidor**, haga clic en **Herramientas** y, después, seleccione **Visor de eventos**.
28. Expanda **Registros de Windows** y haga clic en **Seguridad**.
29. Revise varios eventos, como los eventos correctos y los eventos de error (si están disponibles).

Lección 2

Auditoría avanzada

Contenidos:

Recursos

Servicios de recopilación de auditorías

Lecturas adicionales: Para obtener más información sobre los ACS, consulte "Instalación de un recopilador y base de datos de servicios de recopilación de auditorías (ACS)": http://aka.ms/Jwghcp

Demostración: Configurar las opciones avanzadas de auditoría

Pasos de la demostración

1. En LON-DC1, en el Administrador del servidor, haga clic en **Herramientas** y, después, haga clic en **Administración de directivas de grupo**.
2. En Administración de directivas de grupo, haga doble clic en **Bosque: Adatum.com**, haga doble clic en **Dominios**, haga doble clic en **Adatum.com**, haga clic con el botón derecho en **Objetos de directiva de grupo** y, después, haga clic en **Nuevo**.
3. En la ventana **Nuevo GPO**, escriba **Auditoría de archivo** en el cuadro **Nombre** y, después, presione Entrar.
4. Haga doble clic en el contenedor **Objetos de directiva de grupo**, haga clic con el botón derecho en **Auditoría de archivo** y, después, haga clic en **Editar**.
5. En el Editor de administración de directivas de grupo, en **Configuración del equipo**, expanda **Directivas**, expanda **Configuración de Windows**, expanda **Configuración de seguridad**, expanda **Configuración de directiva de auditoría avanzada**, expanda **Directivas de auditoría** y, después, haga clic en **Acceso a objetos**.
6. Haga doble clic en **Auditar recurso compartido de archivos detallado**.
7. En la ventana **Propiedades**, seleccione la casilla de verificación **Configurar los siguientes eventos de auditoría**.
8. Seleccione las casillas de verificación **Correcto** y **Error**. Después, haga clic en **Aceptar**.
9. Haga doble clic en **Auditar almacenamiento extraíble**.
10. En la ventana **Propiedades**, seleccione la casilla de verificación **Configurar los siguientes eventos de auditoría**.
11. Seleccione las casillas de verificación **Correcto** y **Error**. Después, haga clic en **Aceptar**.
12. Cierre el Editor de administración de directivas de grupo.
13. Cierre la administración de directivas de grupo.

Demostración: Reenvío del registro de eventos

Pasos de la demostración

1. En LON-SVR1, haga clic en Inicio y, después, haga clic en **Windows PowerShell**.
2. Escriba los siguientes comandos y presione Entrar:

```
winrm quickconfig
```

3. Inicie sesión en LON-DC1 y haga clic en **Inicio**.
4. Haga clic en **Windows PowerShell**, escriba el comando siguiente y, después, presione Entrar:

```
Wecutil qc
```

5. Escriba Y cuando se le solicite en el mensaje "El modo de inicio del servicio se cambiará a retrasar el inicio. ¿Desea continuar?"
6. Escriba los comandos siguientes y presione Entrar después de cada uno:

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

7. Inicie sesión en LON-SVR1; seleccione la ventana de **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada uno:

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

8. Vaya a LON-DC1 y continúe utilizando **Windows PowerShell**; escriba los comandos siguientes y presione Entrar después de cada uno:

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

9. Después de que se reinicie LON-SVR1, vuelva a iniciar sesión como **adatum\administrator** con la contraseña **Pa55w.rd**.
10. Después de que se reinicie LON-DC1, vuelva a iniciar sesión como **adatum\administrator** con la contraseña **Pa55w.rd**.
11. En LON-DC1, espere a que se abra el **Administrador del servidor**.
12. Haga clic en **Herramientas** y seleccione **Visor de eventos**.
13. En el árbol de consola, haga clic en **Suscripciones**; si se le pregunta, haga clic en **Sí**.
14. En el menú **Acciones**, haga clic en **Crear suscripción**.
15. En el cuadro **Nombre de suscripción**, escriba **LogDemo** como nombre de la suscripción.
16. En el cuadro **Descripción**, escriba una descripción opcional.
17. En el cuadro **Registro de destino**, asegúrese de que el archivo de registro especifica el registro predeterminado **ForwardedEvents**.
18. Haga clic en **Seleccionar equipos**.
19. Haga clic en **Agregar equipos de dominio**, escriba **LON-SVR1**, haga clic en **Comprobar nombres** y, después, haga clic en **Aceptar** dos veces.
20. Haga clic en **Seleccionar eventos** para que aparezca el cuadro de diálogo **Filtro de consulta**.
21. Utilice los controles del cuadro de diálogo **Filtro de consulta** para especificar los criterios que deben cumplir los eventos para ser recopilados (**Crítico**, **Advertencia** o **Error**). Para esta demostración, al lado de **Registros de eventos**, seleccione **Aplicación** y **Seguridad**. Haga clic en **Aceptar**.
22. En el cuadro de diálogo **Propiedades de suscripción**, haga clic en **Aceptar**. La suscripción se agrega al panel **Suscripciones** y, si la operación se ha efectuado correctamente, el estado de la suscripción será **Activo**.
23. En LON-SVR1, haga clic con el botón derecho en **Inicio** y, después, haga clic en **Windows PowerShell (Administrador)**.

24. Escriba el comando siguiente y presione Entrar.

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

25. Después de unos minutos, vuelva a LON-DC1 y revise los eventos que se reenvían desde LON-SVR1. Encontrará los eventos en **Eventos reenviados**, en el nodo **Registros de Windows**.

Nota: Los eventos pueden tardar en aparecer de 15 a 20 minutos en LON-DC1.

Lección 3

La auditoría y el registro en Windows PowerShell

Contenidos:

Demostración: Administración de la auditoría mediante Windows PowerShell

Pasos de la demostración

1. Abra el Administrador del servidor, haga clic en **Herramientas** y, después, seleccione **Visor de eventos**.
2. Revise los registros de Windows en **Sistema**.
3. Haga clic en **Inicio** y, después, haga clic en **Windows PowerShell**.
4. Escriba lo siguiente y presione Entrar después de cada línea.

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

Demostración: Configuración de transcripción, módulo y registro de bloque de script

Pasos de la demostración

1. Inicie sesión en LON-DC1 como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
2. Vaya a la ventana de **Windows PowerShell**.
3. Escriba lo siguiente y presione Entrar:

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

4. Revise el resultado y observe el estado de **LogPipelineExecutionDetails**.
5. Escriba lo siguiente y presione Entrar después de cada comando:

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

6. Revise el resultado, escriba lo siguiente y, después, presione Entrar después de cada comando:

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

7. Revise el registro de eventos.
8. Vuelva a Windows PowerShell, escriba lo siguiente y presione Entrar:

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

9. Abra el Administrador del servidor, haga clic en **Herramientas** y, después, seleccione **Administración de directivas de grupo**.
10. Haga clic con el botón derecho en **Default Domain Policy** y, después, haga clic en **Editar**.
11. Abra el **Editor de administración de directivas de grupo**.

12. Expanda **Configuración del equipo**, expanda **Directivas**, expanda **Plantillas administrativas**, expanda **Componentes de Windows**, haga clic en **Windows PowerShell** y, después, examine la configuración de GPO que aparece en la pantalla principal.
13. Contraiga los nodos de GPO.
14. Expanda **Configuración del equipo**, expanda **Preferencias**, expanda **Configuración de Windows**, haga clic con el botón derecho en **Entorno**, seleccione **Nuevo** y, después, seleccione **EnvironmentVariable**. Introduzca la siguiente información:
    - Nombre: **PSLogScriptBlockExecution**
    - Valor: **0**
15. Haga clic en **Aceptar**, haga clic con el botón derecho en **Entorno**, seleccione **Nuevo** y, después, seleccione **EnvironmentVariable**. Introduzca la siguiente información y haga clic en **Aceptar**:
    - Nombre: **PSLogScriptBlockExecutionVerbose**
    - Valor: **0**
16. Cierre el Editor de administración de directivas de grupo.
17. Haga clic en **Inicio**, seleccione **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Visor de eventos**.
18. Revise los registros de Windows en **Sistema**.
19. Ubique los registros del Seguimiento de eventos de Windows (ETW) en la siguiente ruta de acceso del archivo: **Aplicaciones y servicios**/**Microsoft**/**Windows PowerShell**/**Funcional**.
20. Cierre todas las ventanas abiertas.

Revisión del módulo y contenidos principales

Procedimientos recomendados

Windows Server 2016 tiene varias mejoras en la auditoría que aumentan el nivel de detalle en los registros de auditoría de seguridad y simplifican la implementación y la administración de las directivas de auditoría.

La auditoría es una actividad permanente en su red y es una de las prácticas de seguridad fundamentales en su organización. Mediante la auditoría de eventos relacionados con la seguridad, puede obtener el aviso anticipado de posibles actividades malintencionadas y pruebas si se produce una infracción de seguridad.

Pregunta de revisión

Pregunta: Ha configurado una directiva de auditoría mediante la directiva de grupo para aplicarla a todos los servidores de archivos de su organización. Después de activar la directiva y confirmar que la configuración de directivas de grupo se ha aplicado, descubre que los eventos de auditoría no se registran en los registros de sucesos. ¿Cuál es el motivo más probable de este problema?

> **Respuesta:** Para auditar el acceso a archivos, debe configurar los archivos o las carpetas para auditar eventos concretos. Si no lo hace, los eventos de auditoría no se grabarán.

Problemas y supuestos reales

Cuando revisa el registro de eventos reenviados, si se omite el permiso del lector de registro de eventos, es posible que el recopilador muestre el siguiente mensaje: **La descripción para el Id. de evento 111 desde el origen Microsoft-Windows-EventForwarder no se ha encontrado. El componente que provoca este evento no está instalado en su equipo local o la instalación está dañada. Puede instalar o reparar el componente en el equipo local. Si el evento se originó en otro equipo, la información de la pantalla tuvo que ser guardada con el evento.**

Preguntas y respuestas de la revisión de laboratorio

Laboratorio: Configurar las opciones avanzadas de auditoría

Preguntas y respuestas

Pregunta: ¿Cuál es la razón para aplicar directivas de auditoría para toda la organización?

Respuesta: Si está tratando de ubicar un problema general o si no está seguro de dónde se está produciendo un evento específico, podría ser necesario focalizarse en un grupo grande de servidores para capturar el evento. En este caso, puede utilizar el filtrado de eventos para buscar un determinado evento de auditoría. Después de identificar un problema, es un buen procedimiento limitar el alcance de la auditoría o inhabilitar la auditoría para reducir el número de registros generados, reducir los impactos en el rendimiento de los equipos y facilitar la lectura de los registros periódicamente.

Módulo 7

Implementación y configuración de Microsoft Advanced Threat Analytics (ATA) y Microsoft Operations Management Suite

Contenidos:

Lección 1

Implementación y configuración de ATA

Contenidos:

Preguntas y respuestas

Pregunta: Es necesario configurar la creación de reflejo del puerto al configurar una puerta de enlace ligera de ATA.

( ) Verdadero

( ) Falso

Respuesta:

( ) Verdadero

(√) Falso

Comentarios:

La instalación de una puerta de enlace ligera de ATA en un controlador de dominio elimina la necesidad de configurar la creación de reflejo del puerto.

Pregunta: ¿Qué puertas de enlace de ATA se deben configurar como candidatos del sincronizador de dominio?

( ) Todas las puertas de enlace de ATA

( ) Puertas de enlace de ATA del sitio remoto

( ) Puertas de enlace de ATA instaladas en los controladores de dominio de solo lectura

( ) Cualquier puerta de enlace de ATA que no sea un controlador de dominio de solo lectura o que actúe como puerta de enlace de ATA del sitio remoto.

Respuesta:

( ) Todas las puertas de enlace de ATA

( ) Puertas de enlace de ATA del sitio remoto

( ) Puertas de enlace de ATA instaladas en los controladores de dominio de solo lectura

(√) Cualquier puerta de enlace de ATA que no sea un controlador de dominio de solo lectura o que actúe como puerta de enlace de ATA del sitio remoto.

Comentarios:

De manera predeterminada, solo las puertas de enlace de ATA se establecen como candidatos del sincronizador de dominio. Le recomendamos deshabilitar cualquier puerta de enlace de ATA del sitio remoto para que no sea candidato del sincronizador de dominio. Si el controlador de dominio es de solo lectura, no lo configure como candidato del sincronizador de dominio.

Recursos

Descripción de ATA

Lecturas adicionales: Para obtener más información, consulte la hoja de datos "Microsoft Advanced Threat Analytics" en: https://aka.ms/ul0xra

Requisitos de implementación de ATA

Lecturas adicionales: Para obtener más información sobre permisos de objeto de directorio, consulte "View or Set Permissions on a Directory Object" (Ver o establecer permisos en un objeto de directorio) en: http://aka.ms/Bgxyha

Demostración: Implementación y configuración de ATA

Pasos de la demostración

1. En **LON-SVR1**, haga clic en **Inicio** y, después, haga clic en **Administrador del servidor**.
2. En el Administrador del servidor, haga clic en **Herramientas** y, después, haga clic en **Administrador de Internet Information Services (IIS)**.
3. En el Administrador de IIS, expanda **LON-SVR1**, expanda **Sites** y, después, haga clic en **Default Web Site**.
4. En el panel **Acciones** haga clic en **Enlaces**.
5. Seleccione **https** y haga clic en **Quitar**. Haga clic en **Sí** y cierre todas las ventanas abiertas.
6. En **LON-SVR1**, haga clic con el botón derecho en el icono de red de la barra de tareas y, después, haga clic en **Abrir el Centro de redes y recursos compartidos**.
7. Haga clic en **Cambiar configuración del adaptador**, haga clic con el botón derecho en **Ethernet** y, después, haga clic en **Propiedades**.
8. Seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** y, después, haga clic en **Propiedades**.
9. En el cuadro de diálogo **Propiedades del protocolo de Internet versión 4** haga clic en **Avanzadas**.
10. En el cuadro de diálogo **Configuración avanzada de TCP/IP** en la pestaña **Configuración de IP** debajo de **Direcciones IP**, haga clic en el botón **Agregar**.
11. En el cuadro de texto **Dirección IP** escriba **172.16.0.13**. Compruebe que la **Máscara de subred** sea de manera predeterminada: **255.255.0.0**. Haga clic en **Agregar**, haga clic en **Aceptar** dos veces y, después, haga clic en **Cerrar**.
12. En **LON-SVR1**, en la barra de tareas haga clic en el icono del **Explorador de archivos**.
13. Vaya a **D:\LabFiles\Mod07**, haga clic con el botón derecho en **ATA1.7.iso** y, después, seleccione **Montar**.
14. Compruebe que puede ver ahora una nueva unidad de DVD con **Microsoft ATA Center Setup.exe**.
15. Haga clic con el botón derecho en el archivo .exe y, después, haga clic en **Ejecutar como administrador**.
16. La primera página le pedirá que elija su idioma. De forma predeterminada está seleccionado en **English**. Elige **Español**. Haga clic en **Siguiente** para aceptar el valor predeterminado.
17. Revise los términos de licencia del software de Microsoft, seleccione el cuadro de diálogo **Acepto los términos de licencia del software de Microsoft** y, después, haga clic en **Siguiente**.
18. En la siguiente página, donde puede seleccionar la opción de Microsoft Update, deje el valor predeterminado y, después, haga clic en **Siguiente**.
19. Revise la página de **Configuración del centro de ATA** y confirme que tienen distintas direcciones IP para el **Servicio de Centro de Dirección IP** y la **consola de dirección IP**. La primera debería ser **172.16.0.11** y la dirección de la **consola de dirección IP** debería ser **172.16.0.13**.
20. Haga clic en **Instalar**.
21. Abra el Administrador del servidor y, después, en el menú **Herramientas**, haga clic en **Administración de equipos**.
22. En **Herramientas del sistema**, expanda **Usuarios y grupos locales** y, después, seleccione **Grupos**.
23. Haga clic con el botón derecho en **Microsoft Advanced Threat Analytics Administrators** y, después, haga clic en **Agregar al grupo**.
24. Haga clic en el botón **Agregar**. En el cuadro de texto, escriba **Beth**, haga clic en **Comprobar nombres** y, después, haga clic en **Aceptar**.

25. Haga clic en **Agregar**. En el cuadro de texto, escriba **ATARead**, haga clic en **Comprobar nombres** y, después, haga clic en **Aceptar**.
26. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Propiedades de Microsoft Advanced Threat Analytics Administrators**.
27. Cierre **Administración de equipos**.
28. Cuando haya terminado la instalación, haga clic en **Iniciar**.
29. En la notificación de seguridad, haga clic en **Pasar a este sitio web**.
30. Después de unos momentos, cuando se muestre la página de **inicio de sesión**, escriba **Beth** como nombre de usuario y **Pa55w.rd** como contraseña. Después, haga clic en **Iniciar sesión**.
31. En la esquina superior derecha del formulario, haga clic en el botón de puntos suspensivos (**...**) y, después, haga clic en **Configuración**.
32. A la izquierda en **Orígenes de datos**, haga clic en **Servicios de directorio**.
33. En **nombre de usuario**, escriba **ATARead**.
34. En **contraseña**, escriba **Pa55w.rd**.
35. En **Dominio**, escriba **adatum.com** y haga clic en **Guardar**.
36. En el encabezado azul, haga clic en **Descargar la configuración de puerta de enlace e instalar la primera puerta de enlace**.
37. Haga clic en **Descargar la configuración de puerta de enlace**.
38. Guarde el archivo en **D:\Labfiles\Mod07**.

Nota: La fase anterior de descarga no requiere una conexión a Internet. La descarga se crea a partir de los bits que ya se encuentran en el servidor.

39. Abra el Explorador de archivos y vaya a **D:\Labfiles\Mod07**.
40. Copie el archivo **Microsoft ATA Gateway Setup.zip** y péguelo a **\\LON-DC1\e$\Labfiles\Mod07**. Reemplace el archivo existente si fuera necesario.
41. Cierre el Explorador de archivos.
42. En **LON-DC1**, abra el Explorador de archivos y vaya a **E:\Labfiles\Mod07**.
43. Haga clic con el botón derecho en **Microsoft ATA Gateway Setup.zip** y, después, seleccione **Extraer todo**.
44. En el cuadro de texto **Los archivos se extraerán a esta carpeta**, escriba **E:\Labfiles\mod07\Gateway** y, después, haga clic en **Extraer**.
45. En **E:\Labfiles\Mod07\Gateway**, haga clic con el botón derecho en **Microsoft ATA Gateway Setup.exe** y, después, seleccione **Ejecutar como administrador**.
46. La primera página le pedirá que elija su idioma. De forma predeterminada está seleccionado en **English**. Elige **Español**. Haga clic en **Siguiente** para aceptar el valor predeterminado.
47. Examine el tipo de implementación de puerta de enlace de ATA. Indique a los estudiantes que, debido a que se trata de un controlador de dominio, la puerta de enlace ligera de ATA ya está seleccionada. Haga clic en **Siguiente**.
48. En el cuadro de texto **Nombre de usuario**, escriba **ATARead**. En el cuadro de texto **Contraseña**, escriba **Pa55w.rd** y, después, haga clic en **Instalar**.
49. Cuando haya terminado la instalación, haga clic en **Finalizar**.

Lección 2

Implementación y configuración de Microsoft Operations Management Suite

Contenidos:

Preguntas y respuestas

Pregunta: ¿Qué servicio de Microsoft Operations Management Suite le ayuda a recopilar y analizar los datos que generan los entornos de recursos en la nube y los entornos locales?

( ) Log Analytics

( ) Análisis de datos

( ) Conector de datos de Microsoft Operations Management Suite

( ) Conectores de datos de red

Respuesta:

(√) Log Analytics

( ) Análisis de datos

( ) Conector de datos de Microsoft Operations Management Suite

( ) Conectores de datos de red

Comentarios:

Log Analytics es un servicio de Microsoft Operations Management Suite que le ayuda a recopilar y analizar los datos que generan los recursos en su nube y en los entornos locales.

Pregunta: Log Analytics requiere recursos locales que analizan los datos recogidos.

( ) Verdadero

( ) Falso

Respuesta:

( ) Verdadero

(√) Falso

Comentarios:

Los requisitos de implementación de Log Analytics son mínimos porque la nube de Azure aloja los componentes centrales. Los componentes incluyen un repositorio y los servicios que le permiten correlacionar y analizar los datos recopilados. Puede acceder al portal de Microsoft Operations Management Suite desde cualquier navegador, así que no hay necesidad de software cliente.

Funciones de seguridad y auditoría de Microsoft Operations Management Suite

Pregunta: ¿Qué producto que no es de Microsoft hace que Microsoft Operations Management Suite le permita administrar y proteger?

( ) AWS

( ) VMware

( ) Linux

( ) OpenStack

Respuesta:

(√) AWS

(√) VMware

(√) Linux

(√) OpenStack

Comentarios:

Microsoft Operations Management Suite le permite administrar y proteger Azure o AWS, Windows Server o Linux, y VMware u OpenStack.

Recursos

Supuestos de implementación y uso de Microsoft Operations Management Suite

 **Lecturas adicionales:** Para obtener más información sobre la automatización de Windows Azure con runbooks, consulte "Getting Started With Azure Automation – Runbook Management", en: http://aka.ms/Cz3zbw

Demostración: Implementación y configuración de Microsoft Operations Management Suite

Pasos de la demostración

1. Si es necesario, cree una cuenta de Microsoft y una cuenta de Azure como se describe en el ejercicio de laboratorio, "Preparación e implementación de Microsoft Operations Management Suite", tareas 1 y 2.
2. Inicie sesión en **LON-CL1** y, después, haga clic en **Inicio**. En la barra de búsqueda, escriba **Internet Explorer** e inicie el programa.
3. En Microsoft Internet Explorer, escriba la siguiente URL y presione Entrar: **https://www.microsoft.com/es-es/cloud-platform/operations-management-suite**.
4. Haga clic en **Crear una cuenta gratuita**.
5. Haga clic en **Introducción**.
6. Si no lo ha hecho, inicie sesión utilizando su cuenta de Microsoft.
7. Rellene el formulario **Crear un área de trabajo nueva** utilizando el correo electrónico que utilizó para crear su cuenta de Microsoft y, después, haga clic en **CREAR**.
8. Seleccione la suscripción a Azure que quiera y, después, haga clic en **ENLACE**.
9. Compruebe que ahora aparece la página de **Microsoft Operations Management Suite**.
10. En la página de inicio de **Microsoft Operations Management Suite**, haga clic en **Galería de soluciones**.
11. Revise las soluciones disponibles.
12. Haga clic en el icono de la casa situado a la izquierda.
13. En la página de inicio, haga clic en **Configuración**.
14. Haga clic en **Orígenes conectados** y asegúrese de que la opción **Servidores de Windows** está seleccionada.
15. Haga clic en el botón **Inicio** de Windows.
16. Escriba **Bloc de notas** y presione Entrar.
17. Vuelva a **Microsoft Internet Explorer** y busque **ID. DEL ÁREA DE TRABAJO** y **CLAVE PRINCIPAL** en el panel de la derecha.
18. Copie y pegue el Id. del **ÁREA DE TRABAJO** y el Id. de la **CLAVE PRINCIPAL** en el Bloc de notas.

19. Guarde el archivo de Bloc de notas como **D:\WorkspaceID.txt**, en caso de que lo necesite más tarde.
20. Haga clic en **Descargar Agente de Windows (64 bits)** para descargar **MMASetup-AMD64.exe**.
21. Haga clic en **Guardar** y, después, haga clic en **Ejecutar**.
22. En el **Asistente para instalación de Microsoft Monitoring Agent**, haga clic en **Siguiente**.
23. Si aparece el cuadro de diálogo **Control de cuentas de usuario**, haga clic en **Sí**.
24. Lea los términos de licencia del software de Microsoft y haga clic en **Acepto**.
25. Acepte la carpeta de destino predeterminada haciendo clic en **Siguiente**.
26. Seleccione **Conectar el agente a Azure Log Analytics (OMS)** y, después, haga clic en **Siguiente**.
27. Indique el **Id. de área de trabajo** y la **clave principal** que ha copiado en el Bloc de notas. Después, haga clic en **Siguiente**.
28. Si se le solicitan actualizaciones de Microsoft, haga clic en **Siguiente**.
29. Haga clic en **Instalar** y, después, haga clic en **Finalizar**.
30. Abra el panel de control en LON-CL1.
31. En el panel de control, haga clic en **Sistema y seguridad** y, después, haga clic en **Microsoft Monitoring Agent**.
32. Si aparece el cuadro de diálogo **Control de cuentas de usuario**, haga clic en **Sí**.
33. Haga clic en la pestaña **Azure Log Analytics (OMS)**, seleccione el elemento de la lista y, después, haga clic en **Editar**. Esto le permitirá actualizar la **clave del área de trabajo** si fuera necesario. Haga clic en **Cancelar**.
34. Haga clic en **Cancelar**.
35. Vuelva a la página web de Microsoft Operations Management Suite y, después, actualice el navegador. Muestre a los estudiantes que ahora puede revisar el **uso** y ver datos de **LON-CL1**.

 **Nota:** En algunos casos, los datos de uso pueden tardar tiempo en aparecer. Esto podría ser algo que puede enseñar antes de realizar el laboratorio de Microsoft Operations Management Suite.

Revisión del módulo y contenidos principales

Procedimientos recomendados

En entornos más grandes, debería considerar la posibilidad de ampliar y utilizar varias puertas de enlace de ATA.

Preguntas de revisión

Pregunta: ¿Qué dominios de seguridad puede examinar en Microsoft Operations Management Suite?

Respuesta: En Microsoft Operations Management Suite se pueden examinar los siguientes dominios:

- Evaluación de malware
- Evaluación de actualización
- Identidad y acceso

Pregunta: Explique cómo utilizar ATA para mejorar la seguridad.

Respuesta: Las ventajas de ATA incluyen:

- Detectar amenazas con análisis de comportamiento. No hay necesidad de crear reglas, implementar agentes o afinar o supervisar un aluvión de informes de seguridad.
- Se adapta tan rápido como los usuarios malintencionados. ATA aprende continuamente del comportamiento de la entidad organizativa (usuarios, dispositivos y recursos) y se ajusta para reflejar los cambios en su empresa de rápida evolución.
- Se centra en lo que es importante utilizando la cronología de ataque simple. La cronología de ataque es una fuente clara, eficiente y cómoda que muestra los elementos correctos en la cronología, otorgándole el poder de la perspectiva sobre el quién, el qué, el cuándo y el cómo de su empresa.
- Reduce el desgaste de los falsos positivos. Las alertas solo ocurren después de que se agreguen actividades sospechosas contextualmente.
- Prioriza y planifica las próximas fases. Para cada actividad sospechosa o ataque conocido identificado, ATA proporciona recomendaciones de investigación y corrección.

Algunas de las características clave de ATA son:

- Apoyo a la movilidad. Es testigo de todos los procesos de autenticación y autorización a los recursos de la organización dentro de la estructura orgánica del perímetro o en dispositivos móviles.
- Se integra con SIEM (Administración de eventos e información de seguridad). ATA funciona con SIEM y proporciona opciones para reenviar las alertas de seguridad para su SIEM o para enviar correos electrónicos a personas específicas.
- Su implementación sin interrupciones. ATA funciona como una aplicación y utiliza la creación de reflejo del puerto para permitir una implementación ininterrumpida.

Pregunta: Explique cómo usar Microsoft Operations Management Suite para mejorar la seguridad.

Respuesta: Las características de cumplimiento y seguridad de Microsoft Operations Management Suite le ayudan a identificar, evaluar y mitigar los riesgos de seguridad en su infraestructura. Estas características se implementan a través de varias soluciones de análisis de registro que analizan los datos de registro y la configuración de los sistemas de agente para ayudarle a garantizar la seguridad continua de su entorno.

- La solución de seguridad y auditoría recopila y analiza los eventos de seguridad en sistemas administrados para identificar actividades sospechosas.
- La solución antimalware informa sobre el estado de la protección antimalware en los sistemas administrados.
- La solución del sistema de actualizaciones analiza las actualizaciones de seguridad y otras actualizaciones en los sistemas administrados para que identifique fácilmente los sistemas que requieren actualizaciones.

Problemas y supuestos reales

Planificación de la capacidad del centro ATA:

- El espacio de disco requerido para una base de datos de ATA puede variar en cada controlador de dominio.
- Si tiene varios controladores de dominio, recapitule el espacio de disco requerido por cada controlador de dominio para calcular la cantidad total de espacio necesario para la base de datos de ATA.
- Para calcular el tamaño del centro ATA de forma precisa en función de sus necesidades, consulte http://aka.ms/atasizing.

Herramientas

Wireshark es un analizador de protocolos de red que le permite examinar su red a un nivel preciso. Aunque Wireshark puede ser de gran valor, recuerde no instalarlo en los servidores que se utilizan para las puertas de enlace de ATA o centros ATA.

Problemas comunes y sugerencias para la resolución de problemas

Problema común	Sugerencia para la resolución de problemas
Algunos usuarios informan que han visto el evento Id. 1013 en el registro de eventos de Microsoft ATA en el centro ATA.	Este problema suele estar relacionado con las copias de seguridad del sistema, cuando los discos no pueden proporcionar suficientes operaciones de entrada/salida (E/S) por segundo (IOPS) durante el proceso de copia de seguridad.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio: Implementar ATA y Microsoft Operations Management Suite

Preguntas y respuestas

Pregunta: ¿Cuál es la ventaja de utilizar una puerta de enlace ligera de ATA?

Respuesta: No necesita configurar la creación de reflejo del puerto para una puerta de enlace ligera de ATA.

Pregunta: ¿Cuáles son algunos de los requisitos para instalar ATA?

Respuesta: Algunos requisitos incluyen una cuenta de usuario de dominio, una lista de subredes que tengan un tiempo corto de vida (TTL), una cuenta de honeytoken, Wireshark y el Analizador de mensajes de Microsoft.

Módulo 8

Proteger la infraestructura de virtualización

Contenidos:

Lección 1

Tejido protegido

Contenidos:

Preguntas y respuestas

Pregunta: ¿Qué servicio proporciona las claves de transporte necesarias para desbloquear y ejecutar máquinas virtuales blindadas en hosts de Hyper-V atestiguados afirmativamente (o en buen estado)?

Respuesta: KPS

Recursos

Nano Server como host protegido atestiguado por Módulo de plataforma segura (TPM)

 **Lecturas adicionales:** Para obtener más información, consulte "Prepare Nano Server Script for Guarded Fabric": http://aka.ms/V2thr5

Lección 2

Máquinas virtuales blindadas y compatibles con cifrado

Contenidos:

Preguntas y respuestas

Pregunta: ¿Cuáles son algunas de las diferencias entre las VM compatibles con cifrado y las VM blindadas?

> **Respuesta:** Como las VM blindadas, las VM compatibles con cifrado utilizan el arranque seguro, el Módulo de plataforma segura virtual (vTPM) y los estados de VM cifrados. Sin embargo, con las VM compatibles con cifrado, estos ajustes se pueden configurar. En las VM blindadas se aplican. Además, la consola de **Conexión a máquina virtual** está configurada en **Encendido** para las VM compatibles con cifrado, pero está deshabilitada en las VM blindadas. Por último, los puertos COM (serie) están deshabilitados en las VM blindadas y no se puede adjuntar un depurador al proceso de la VM.

Recursos

Solución de problemas de las VM blindadas y las VM compatibles con cifrado

 **Lecturas adicionales:** Para obtener más información, consulte "Shielded VMs and Guarded Fabric Troubleshooting Guide for Windows Server 2016": https://aka.ms/ehnloq

Revisión del módulo y contenidos principales

Procedimientos recomendados

Aunque es posible utilizar un dominio para configurar un tejido protegido, recomendamos que el servicio de protección de host (HGS) tenga un bosque único.

Pregunta de revisión

Pregunta: ¿Qué confianzas se necesitan entre dominios y de qué dominio debe ser miembro el host protegido?

> **Respuesta:** El servidor del HGS debe tener una confianza unidireccional con el dominio de la organización. El host protegido debe ser miembro del dominio de la organización, y no un miembro del bosque del HGS.

Problemas comunes y sugerencias para la resolución de problemas

Problema común	Sugerencia para la resolución de problemas
Una VM blindada no se puede arrancar después de encender vTPM.	Compruebe que el host protegido se ha agregado al grupo de seguridad correcto.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio: Tejido protegido con atestación de administrador de confianza y VM blindadas

Preguntas y respuestas

Pregunta: Describa los componentes fundamentales del tejido protegido.

> **Respuesta:** Las máquinas virtuales blindadas y el tejido protegido permiten que los proveedores de servicios en la nube o los administradores de nubes privadas de empresas proporcionen un entorno más seguro para las máquinas virtuales arrendatarias. Un tejido protegido se compone de un HGS, que generalmente consiste en un clúster de tres nodos, uno o más hosts protegidos y un conjunto de VM blindadas.

Pregunta: En el laboratorio ha creado un entorno que estaba compuesto por el HGS y el host protegido, y ha agregado un grupo de HGS al dominio de la empresa. ¿Cuál de estos roles debe ser un servidor físico?

> **Respuesta:** El host protegido, ya que no puede ejecutarse en un entorno virtualizado.

Módulo 9

Proteger el desarrollo de aplicaciones y la infraestructura de la carga de trabajo del servidor

Contenidos:

Lección 1

Uso de SCM

Contenidos:

Preguntas y respuestas

Pregunta: ¿Cuál de las siguientes líneas base de producto predeterminadas tiene SCM 4.0?

( ) Internet Explorer 6 e Internet Explorer 7

( ) Microsoft Exchange Server 2007 SP1

( ) Windows 8

( ) Windows Server 2008 SP1

( ) Windows Server 2012

Respuesta:

( ) Internet Explorer 6 e Internet Explorer 7

( ) Microsoft Exchange Server 2007 SP1

(√) Windows 8

( ) Windows Server 2008 SP1

(√) Windows Server 2012

Comentarios:

SCM 4.0 no tiene una plantilla básica para los sistemas y aplicaciones creados antes de Windows Server 2012, Internet Explorer 8 y Microsoft Exchange Server 2010.

Recursos

Administrar líneas base de seguridad

Lecturas adicionales: Para obtener más información, consulte "Security baseline for Windows 10 v1607 (“Anniversary edition”) and Windows Server 2016": https://aka.ms/hhsdmo

Implementar configuraciones de seguridad

Lecturas adicionales: Puede descargar la herramienta independiente LGPO.EXE en: https://aka.ms/kkvmk5

Demostración: Instalación de SCM

Pasos de la demostración

Instalación de SCM

1. En **LON-SVR1**, haga clic en el **Explorador de archivos** en la barra de tareas.
2. En el **Explorador de archivos**, vaya a **D:\Labfiles\Mod09**.
3. Haga doble clic en **Security_Compliance_Manager_Setup.exe**.

   Se abrirá una ventana del símbolo del sistema y se iniciarán los requisitos previos de SCM.
4. Cuando aparezca la ventana **Microsoft Visual C++ 2010 x86 Redistributable Setup**, seleccione **He leído y acepto los términos de la licencia** y, después, haga clic en **Instalar**.
5. Cuando aparezca la página **Se completó la instalación**, haga clic en **Finalizar**.

6. Se iniciará el **Microsoft Security Compliance Manager Setup Wizard**. En la página de **Welcome**, borre **Always check for SCM and baseline updates** y, después, haga clic en **Next**.

Nota: Hay varias líneas base nuevas para Windows 10, Windows Server 2016, Internet Explorer 11, etc., pero debe descargarlas e importarlas por separado. Como no tiene acceso a Internet en las máquinas virtuales (VM) del curso, no puede descargar estas líneas base. Esta es la razón por la que borró la casilla de verificación **Always check for SCM and baseline updates**.

7. En la página **License Agreement**, haga clic en **I accept the terms of the license agreement** y, después, haga clic en **Next**.
8. En la página **Installation Folder**, haga clic en **Next**.
9. En la página **SQL Instances found**, seleccione **Create a new SQL express instance,** y, después, haga clic en **Next**.
10. En la página **Microsoft SQL Server 2008 Express**, haga clic en **Next**.
11. En la página **SQL Server 2008 Express License Agreement**, seleccione **I accept the terms of the license agreement** y, después, haga clic en **Next**.
12. En la página **Ready to Install**, haga clic en **Install**.
13. Cuando aparezca la página **Installation Successful**, haga clic en **Finish**.
14. Se abre la consola de **SCM** y se importan varias líneas base automáticamente. Deje la consola abierta para la siguiente demostración.

Demostración: Configuración y administración de líneas base de seguridad

Pasos de la demostración

Instalar los GPO de Windows Server 2016

1. En **LON-SVR1**, en la consola de **SCM**, en el panel **Acciones**, haga clic en **Import – GPO Backup (folder)**.
2. En la ventana **Buscar carpeta**, vaya a **D:\Labfiles\Mod09\Windows 10 RS1 and Server 2016 Security Baseline\GPOs**, seleccione el primer identificador único global (GUID) de GPO que aparece y haga clic en **Aceptar**.
3. En la ventana **Nombre del GPO**, escriba el nombre del GPO y haga clic en **Aceptar**.
4. En la ventana **Registro de SCM**, haga clic en **Aceptar**.
5. Repita los pasos del 1 al 4 para los otros 10 GUID de GPO de la carpeta **GPO**.

Asociar y combinar el GPO de Windows Server 2016 con la línea base del servidor miembro de Windows Server 2012

1. En la consola de **SMC**, en el árbol de la consola, expanda **Custom baselines** (si no se ha expandido ya) y, después, expanda **GPO import**.
2. En la lista de líneas base, seleccione **SCM Windows Server 2016 - Member Server Baseline – Computer 0.0**.
3. En el panel **Acciones**, debajo de **Baseline**, haga clic en el hipervínculo **Associate**.
4. En la ventana **Associate Product with a GPO**, en la lista **Product name**, seleccione **Windows Server 2012** y, después, haga clic en **Associate**.
5. En el cuadro de texto **Nombre de línea base**, escriba **Servidor asociado 2012-2016** y haga clic en **Aceptar**.

6. En el árbol de la consola de **SMC** (si todavía no está seleccionado), seleccione **Servidor asociado 2012-2016** debajo de **líneas base personalizadas** y, después, en el panel **Acciones**, debajo de **Baseline**, haga clic en el hipervínculo **Compare/Merge**.
7. En la ventana **Compare Baselines**, expanda **Windows Server 2012** y, de la lista expandida, seleccione **WS2012 Member Server Security Compliance 1.0**. Después, haga clic en **Aceptar**.
8. Explique la información que se presenta en la ventana **Compare Baselines**. Explique la configuración de las áreas **Settings that differ** y **Settings that match**.
9. En la ventana **Compare Baselines**, haga clic en **Merge Baselines**.
10. En la ventana **Merge Baselines**, explique los elementos **Merge conflicts to resolve** y haga clic en **Aceptar**.
11. En el cuadro de texto **Specify a name for the merged baseline**, escriba **Servidor miembro combinado 2012-2016** y, después, haga clic en **Aceptar**.
12. Explique por qué los estudiantes deberían seleccionar una configuración de línea base en comparación con otra. Tenga en cuenta que los estudiantes pueden ver el nombre completo de una configuración deslizando la barra de separación en la fila de encabezados.
13. En el panel de detalles, desplácese hacia abajo hasta llegar al área **Session Configuration** debajo de la columna **Name**.
14. Haga doble clic en el elemento denominado **Interactive Logon: Message title for users attempting to log on** y borre la casilla de verificación **Not Defined**. En el cuadro de texto **Customize setting value**, escriba **¡Bienvenido a A. Datum Corporation!** y, después, haga clic en **Collapse**.
15. Siga en el área **Session Configuration** y, debajo de la columna **Name**, haga doble clic en el elemento llamado **Interactive Logon: Message text for users attempting to log on**. Borre la casilla de verificación **Not Defined** y, en el cuadro de texto **Customize setting value**, escriba **Este dispositivo utiliza la línea base del servidor miembro combinado 2012-2016**. Después, haga clic en **Collapse**.
16. En el panel **Acciones**, debajo de **Export**, haga clic en el hipervínculo **GPO Backup (folder)**.
17. En la ventana **Buscar carpeta**, expanda **Allfiles (D:)**, expanda **Labfiles**, seleccione **Mod09** y, después, haga clic en **Aceptar**.
18. Cierre la ventana del **Explorador de archivos**.

Demostración: Implementar una línea base de seguridad en un servidor remoto

Pasos de la demostración

Importar una copia de seguridad de GPO de SCM en la Consola de administración de directivas de grupo

1. En **LON-DC1**, en la barra de tareas, seleccione **Explorador de archivos**.
2. En el **Explorador de archivos**, en el cuadro de texto **URL**, escriba **\\LON-SVR1\d$\Labfiles\Mod09** y, después, presione Entrar.
3. Haga clic con el botón derecho y copie la carpeta GUID (ejemplo: {bed88c04-5ffe-4857-aff6-be595c53ad41}).
4. En el **Explorador de archivos**, en **LON-DC1**, vaya a **Allfiles (E:\)\Labfiles**.

   En el panel de detalles, haga clic con el botón derecho y, después, haga clic en **Pegar**. Cierre el **Explorador de archivos**.

5. En **Administrador del servidor**, en el menú **Herramientas**, haga clic en **Administración de directivas de grupo**.
6. En el árbol de la **Consola de administración de directivas de grupo**, expanda **Bosque: Adatum.com**, expanda **Dominios**, expanda **Adatum.com** y, después, seleccione el nodo **Objetos de directiva de grupo**.
7. Haga clic con el botón derecho en el espacio en blanco del panel de detalles y, después, haga clic en **Nuevo**.
8. En la ventana **Nuevo GPO**, en el cuadro de texto **Nombre**, escriba **Línea base de servidor miembro 2012-2016** y, después, haga clic en **Aceptar**.
9. En el panel de detalles, haga clic con el botón derecho en el elemento **Línea base de servidor miembro 2012-2016** y, después, haga clic en **Importar configuración**.
10. En el **Asistente para importar configuración**, en la página de **bienvenida**, haga clic en **Siguiente**.
11. En la página **Hacer copia de seguridad de GPO**, haga clic en **Siguiente**.
12. En la página **Ubicación de la copia de seguridad**, en el cuadro de texto **Carpeta de copia de seguridad**, escriba **E:\Labfiles** y, después, haga clic en **Siguiente**.
13. En la página **GPO de origen**, asegúrese de que el elemento **Servidor miembro combinado 2012-2016** está seleccionado y, después, haga clic en **Siguiente**.
14. En la página **Examinar copia de seguridad**, haga clic en **Siguiente**.
15. En la página **Migrar referencias**, explique cómo se puede utilizar una tabla de migración para asignar la configuración a un GPO de destino. Sin embargo, como no tiene ninguna tabla de migración, debe aceptar la configuración predeterminada y hacer clic en **Siguiente**.
16. En la página **Finalización del Asistente para importar configuración**, haga clic en **Finalizar** y, después, cuando la importación se haya realizado correctamente, haga clic en **Aceptar**.
17. Haga clic con el botón derecho en el elemento **Línea base de servidor miembro 2012-2016** del panel de detalles y, después, haga clic en **Editar**.
18. Maximice la ventana del **Editor de administración de directivas de grupo**.
19. En la ventana del **Editor de administración de directivas de grupo**, en el árbol de la consola, debajo del nodo **Configuración del equipo**, expanda **Directivas**, expanda **Configuración de Windows**, expanda **Configuración de seguridad** y, después, expanda **Directivas locales**.
20. En **Directivas locales**, seleccione **Opciones de seguridad**.
21. En el panel de detalles de **Opciones de seguridad**, desplácese hacia abajo hasta el elemento de configuración denominado **Interactive Logon: Message title for users attempting to log on** y, después, haga doble clic en él.
22. Tenga en cuenta que **¡Bienvenido a A. Datum Corporation!** está definido para esta configuración de directiva.
23. Haga lo mismo para el elemento **Interactive Logon: Message text for users attempting to log on**, asegurándose de que esté seleccionado **Este dispositivo utiliza la línea base del servidor miembro combinado 2012-2016**.
24. Cierre la ventana del **Editor de administración de directivas de grupo** y, después, minimice la **Consola de administración de directivas de grupo**.

Crear la unidad organizativa Servidores miembro, mover la VM LON-SVR2 dentro de ella y vincular el GPO Línea base de servidor miembro 2012-2016 con la unidad organizativa

1. En **LON-DC1**, en **Administrador del servidor**, en el menú **Herramientas**, seleccione **Usuarios y equipos de Active Directory**.
2. En **Usuarios y equipos de Active Directory**, en el árbol de la consola, expanda **Adatum.com**.
3. Haga clic con el botón derecho en **Adatum.com**, haga clic en **Nuevo** y, después, haga clic en **Unidad organizativa**.
4. En la ventana **Nuevo objeto – Unidad organizativa**, en el cuadro de texto **Nombre**, escriba **Servidores miembro** y, después, haga clic en **Aceptar**.
5. En el árbol de la consola, seleccione el nodo **Equipos**.
6. En el panel de detalles, haga clic con el botón derecho en **LON-SVR2** y, después, haga clic en **Mover**.
7. En la ventana **Mover**, seleccione la unidad organizativa **Servidores miembro** y, después, haga clic en **Aceptar**.
8. En el árbol de la consola, seleccione **Servidores miembro** y, después, verifique que **LON-SVR2** se encuentra en esta unidad organizativa.
9. Cierre la consola **Usuarios y equipos de Active Directory**.
10. Maximice la **Consola de administración de directivas de grupo**.
11. En el árbol de la consola, seleccione **Adatum.com** y, después, haga clic en el icono **Actualizar**.
12. Ahora debería ver la unidad organizativa **Servidores miembro** en **Adatum.com**. Seleccione la unidad organizativa.
13. Haga clic con el botón derecho en **Servidores miembro** y, después, haga clic en **Vincular un GPO existente**.
14. En la ventana **Seleccionar GPO**, seleccione el GPO **Línea base del servidor miembro 2012-2016** y, después, haga clic en **Aceptar**.
15. Cierre la **Consola de administración de directivas de grupo**.

Iniciar LON-SVR2 y observar el título y el texto del mensaje de Interactive Logon

1. En **Administrador de Hyper-V**, en el equipo host, haga doble clic en **26744B-LON-SVR2** y, después, en la ventana **Conexión a máquina virtual**, haga clic en **Inicio**.
2. Cuando se inicie la VM, debería ver la pantalla **Interactive Logon** antes de la pantalla **Inicio de sesión**.
3. Haga clic en **Aceptar** en esta pantalla y, después, inicie sesión en **LON-SVR2** como **Adatum\Administrator** usando **Pa55w.rd** como contraseña.
4. Cierre todas las ventanas abiertas y, después, cierre sesión en todas las VM.

Lección 2

Introducción a Nano Server

Contenidos:

Preguntas y respuestas

Actividad de secuenciación

Pregunta: A continuación se muestran los pasos necesarios para aplicar DSC a un Nano Server. Coloque los siguientes pasos en el orden correcto.

	Pasos
	Crear un script de configuración para DSC en Nano Server.
	Copiar el script de configuración en Nano Server.
	Asegurarse de que se hayan importado todos los recursos de DSC necesarios y estén disponibles.
	Ejecutar el script de configuración en Nano Server para crear el archivo MOF.
	Utilizar el comando Start-DscConfiguration en Windows PowerShell para implementar DSC en el archivo MOF.
	Comprobar que se ha implementado DSC y que los ajustes estén configurados según lo previsto.

Respuesta:

	Pasos
1	Crear un script de configuración para DSC en Nano Server.
2	Copiar el script de configuración en Nano Server.
3	Asegurarse de que se hayan importado todos los recursos de DSC necesarios y estén disponibles.
4	Ejecutar el script de configuración en Nano Server para crear el archivo MOF.
5	Utilizar el comando Start-DscConfiguration en Windows PowerShell para implementar DSC en el archivo MOF.
6	Comprobar que se ha implementado DSC y que los ajustes estén configurados según lo previsto.

Recursos

¿Por qué es Nano Server más seguro?

Lecturas adicionales: Para obtener más información, consulte "Introducing Server management tools" en: https://aka.ms/mwe46x

La preparación, implementación y administración de Nano Server

Lecturas adicionales: Puede descargar "Nano Server Image Builder": http://aka.ms/NanoServerImageBuilder

Demostración: Implementación y administración de Nano Server

Pasos de la demostración

Copiar los scripts necesarios de Windows PowerShell

1. En **LON-HOST1**, haga clic con el botón derecho en **Inicio** y, después, haga clic en **Windows PowerShell (Administrador)**.
2. En la ventana de **Windows PowerShell**, escriba **cd** y, después, presione Entrar.
3. En la ventana de **Windows PowerShell**, escriba **md Nano** y, después, presione Entrar.
4. En la ventana de **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

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

Nota: Reemplace la *X* del paso anterior por la letra de unidad asignada para el archivo .iso montado.

Importar módulos de Windows PowerShell.

1. En la ventana de **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

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

2. En la ventana de **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

```
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
```

Nota: Reemplace la *X* del paso anterior por la letra de unidad asignada para el archivo .iso montado.

3. En el mensaje **Contraseña del administrador**, inicie sesión utilizando **Pa55w.rd** como contraseña y, después, presione Entrar.
4. Cuando finalice el proceso, en la barra de tareas, haga clic en **Explorador de archivos**, vaya a **C:\Nano** y, después, examine los archivos enumerados. Verifique que aparece **nano-svr1.vhdx**.

Crear una máquina virtual de Hyper-V desde nano-SVR1.vhdx

1. En **LON-HOST1**, abra el **Administrador de Hyper-V**.
2. En la consola de **Hyper-V**, en el panel **Acciones**, haga clic en **Nuevo** y, después, haga clic en **Máquina virtual**.
3. En el **Asistente para nueva máquina virtual**, en la página de **bienvenida**, haga clic en **Siguiente**.
4. En la página **Especificar nombre y ubicación**, en el cuadro de texto **Nombre**, escriba **NANO-SVR1**, seleccione **Almacenar la máquina virtual en otra ubicación** y, después, haga clic en **Examinar**.
5. En la ventana **Seleccionar carpeta**, en el cuadro de texto **URL**, escriba **C:\nano**, presione Entrar y, después, haga clic en **Seleccionar carpeta**.
6. En la página **Especificar nombre y ubicación**, haga clic en **Siguiente**.
7. En la página **Especificar generación**, seleccione **Generación 2** y, después, haga clic en **Siguiente**.
8. En la página **Asignar memoria**, haga clic en **Siguiente**.

9. En la página **Configurar funciones de red**, en la lista desplegable **Conexión**, seleccione **Red interna** y, después, haga clic en **Siguiente**.
10. En la página **Conectar disco duro virtual**, haga clic en **Usar un disco duro virtual existente** y, después, haga clic en **Examinar**.
11. En la ventana **Abrir**, en el cuadro de texto **URL**, escriba **C:\nano**, presione Entrar, seleccione el elemento **nano-svr1.vhdx** y, después, haga clic en **Abrir**.
12. En la página **Conectar disco duro virtual**, haga clic en **Siguiente**.
13. En la página **Finalización del Asistente para crear nueva máquina virtual**, haga clic en **Finalizar**.
14. En el **Administrador de Hyper-V**, en **LON-HOST1**, haga doble clic en el elemento **NANO-SVR1** en el panel **Máquinas virtuales**.
15. En la ventana **NANO-SVR1 en LON-HOST1 – Conexión a máquina virtual**, haga clic en **Inicio**.

Iniciar sesión en la máquina virtual NANO-SVR1 y ver la configuración básica

1. En **NANO-SVR1**, en el cuadro de texto **Nombre de usuario**, escriba **Administrador** y, después, presione la tecla del tabulador.
2. En el cuadro de texto **Contraseña**, inicie sesión usando **Pa55w.rd** como contraseña y, después, presione Entrar.
3. En **NANO-SVR1**, en la **Consola de recuperación de Nano Server**, tenga en cuenta que el nombre del equipo es **NANO-SVR1** y que el equipo está en un grupo de trabajo. Presione la tecla del tabulador hasta seleccionar **Funciones de red** y, después, presione Entrar.
4. En el mensaje **Ethernet**, presione Entrar.
5. En **Configuración de adaptador de red**, observe que el DHCP proporciona la configuración de IP.
6. Anote la dirección IP.
7. Presione la tecla Esc dos veces.

Agregar NANO-SVR1 al dominio

1. Vaya a **LON-DC1**.
2. Haga clic con el botón derecho en **Inicio** y, después, haga clic en **Windows PowerShell (Administrador)**.
3. En el símbolo del sistema, escriba el comando siguiente y presione Entrar:

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

 **Nota:** Reemplace la dirección IP 172.16.0.X de los siguientes comandos por la dirección IP que anotó durante la instalación de Nano Server.

4. En el símbolo del sistema, escriba el cmdlet siguiente y presione Entrar. La dirección IP será diferente:

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

5. Escriba **Y** y, cuando se le solicite, presione Entrar.
6. En el símbolo del sistema, escriba el cmdlet siguiente y presione Entrar. La dirección IP será diferente:

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

7. En el símbolo del sistema, escriba el cmdlet siguiente y presione Entrar:

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

8. En el cuadro de diálogo **Solicitud de credenciales para Windows PowerShell**, en el cuadro de texto **Contraseña**, escriba **Pa55w.rd** y, después, haga clic en **Aceptar**.
9. En el símbolo del sistema, escriba el cmdlet siguiente y presione Entrar:

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

10. En el símbolo del sistema, escriba el cmdlet siguiente y presione Entrar:

```
Exit-PSSession
```

11. En el símbolo del sistema, escriba el comando siguiente y presione Entrar. La dirección IP será diferente:

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

12. En el símbolo del sistema, escriba **Z:** y presione Entrar.
13. En el símbolo del sistema, escriba el comando siguiente y presione Entrar:

```
copy c:\odjblob
```

14. En el símbolo del sistema, escriba el cmdlet siguiente y presione Entrar:

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

15. En el cuadro de diálogo **Solicitud de credenciales para Windows PowerShell**, en el cuadro de texto **Contraseña**, escriba **Pa55w.rd** y, después, haga clic en **Aceptar**.
16. En el símbolo del sistema, escriba **cd** y presione Entrar.
17. En el símbolo del sistema, escriba el cmdlet siguiente y presione Entrar:

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

18. En el símbolo del sistema, fuerce el reinicio de Nano Server escribiendo el siguiente cmdlet y presionando Entrar:

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

19. No cierre Windows PowerShell. Lo utilizará en la siguiente demostración.
20. Vaya a **NANO-SVR1**.
21. En el cuadro de texto **Nombre de usuario**, escriba **Administrador** y, después, presione la tecla del tabulador.
22. En el cuadro de texto **Contraseña**, escriba **Pa55w.rd** y, después, presione la tecla del tabulador.
23. En el cuadro de texto **Dominio**, escriba **Adatum** y, después, presione Entrar.
24. En la **Consola de recuperación de Nano Server**, observe que el equipo se encuentra en el dominio **adatum.com**.

Demostración: Configuración de la seguridad de Nano Server mediante DSC

Pasos de la demostración

Revisar el script de DSC

1. En **LON-DC1**, en la barra de tareas, haga clic en **Explorador de archivos**.
2. En el **Explorador de archivos**, en el árbol de la consola, seleccione **Este equipo** y, después, en **Este equipo**, expanda **C:\Labfiles\Mod09**.
3. Haga clic con el botón derecho en el archivo **Demo2DscNanoConfig.ps1** y, después, haga clic en **Editar**. Se abrirá el script en el Entorno de scripting integrado (ISE) de Windows PowerShell.
4. Explique brevemente las principales partes del script. La parte relevante es el bloque que llama al servicio. Verifica si el **servicio Administración de máquinas virtuales (VMMS) de Hyper-V** se está ejecutando.
5. Cierre **Windows PowerShell ISE** sin alterar ni guardar el script. No cierre el **Explorador de archivos**.

Implementar el script de DSC en NANO-SVR1

1. Vuelva a la ventana de **Windows PowerShell**.
2. La unidad Z que asignó en la última demostración aún debería estar asignada. Si no es así, escriba lo siguiente, sustituyendo la *X* por el mismo valor que utilizó en la demostración anterior y, después, presione Entrar:

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

Nota: Puede ignorar cualquier mensaje que indique: "El comando 'z:' no se ejecutó dado que la sesión en la que se pensaba ejecutar estaba cerrada o interrumpida". La unidad aún estará correctamente asignada.

3. En **Windows PowerShell**, escriba los comandos siguientes y presione Entrar después de cada línea:

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

4. En **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

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

   El resultado muestra que el paquete de DSC se instaló correctamente como módulo en la demostración anterior y después muestra todos los comandos que están disponibles en el módulo.

5. En **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

```
Get-DscResource
```

   El resultado de este comando muestra los distintos recursos que DSC puede operar en Nano Server.

6. En el símbolo del sistema, escriba el siguiente cmdlet, sustituyendo la *X* por el último octeto de la dirección IP y, después, presione Entrar:

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

7. En el símbolo del sistema, escriba el comando siguiente y presione Entrar:

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

8. En la ventana **Solicitud de credenciales para Windows PowerShell**, en el cuadro de texto **Nombre de usuario**, escriba **Adatum\Administrator** y, en el cuadro de texto **Contraseña**, escriba **Pa55w.rd**. Después, haga clic en **Aceptar**.
9. En el símbolo del sistema, escriba el comando siguiente y presione Entrar:

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

10. En el símbolo del sistema, escriba el comando siguiente y presione Entrar:

```
Cd C:\demo
```

11. En el símbolo del sistema, escriba el comando siguiente y presione Entrar:

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

El script devolverá un archivo .MOF llamado **NANO-SVR1.MOF**.

12. En el símbolo del sistema, escriba el comando siguiente y presione Entrar:

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

13. El parámetro **Espere** se detiene unos segundos para ejecutar el nodo. El comando se ejecuta correctamente, lo cual verifica que el servicio de VMMS se está ejecutando en NANO-SVR1.
14. En el símbolo del sistema, escriba el comando siguiente y presione Entrar:

```
Exit-PSSession
```

15. Cierre todas las ventanas abiertas y, después, cierre sesión en **LON-DC1**.

Lección 3

Descripción de los contenedores

Contenidos:

Preguntas y respuestas

Clasificar la actividad

Pregunta: Clasifique los elementos siguientes.

Elementos	
1	Proporciona un entorno de sistema operativo
2	Solo cuenta con un modo usuario.
3	Proporciona un límite de aislamiento adicional que tiene su propia copia de los binarios del sistema operativo
4	Se elimina gran parte de la interfaz de usuario, el conjunto de aplicaciones y el .NET Framework tradicional
5	Puede utilizar esta imagen varias veces para implementar aplicaciones sin cambiar las capas subyacentes
6	Crea automáticamente una máquina virtual de Hyper-V mediante una imagen base
7	Puede usarlo como una plataforma para un contenedor de Windows
8	Utiliza un kernel compartido
9	Proporciona el aislamiento necesario para permitir que las aplicaciones que no son de confianza se ejecuten en el mismo host

Categoría 1		Categoría 2		Categoría 3
Nano Server		Un contenedor de Windows Server		Un contenedor de Hyper-V

Respuesta:

Categoría 1		Categoría 2		Categoría 3
Nano Server		Un contenedor de Windows Server		Un contenedor de Hyper-V

Categoría 1		Categoría 2		Categoría 3
Proporciona un entorno de sistema operativo Se elimina gran parte de la interfaz de usuario, el conjunto de aplicaciones y el .NET Framework tradicional Puede usarlo como una plataforma para un contenedor de Windows		Solo cuenta con un modo usuario. Puede utilizar esta imagen varias veces para implementar aplicaciones sin cambiar las capas subyacentes Utiliza un kernel compartido		Proporciona un límite de aislamiento adicional que tiene su propia copia de los binarios del sistema operativo Crea automáticamente una máquina virtual de Hyper-V mediante una imagen base Proporciona el aislamiento necesario para permitir que las aplicaciones que no son de confianza se ejecuten en el mismo host

Demostración: Implementación y administración de los contenedores de Windows Server

Pasos de la demostración

Examinar el repositorio de imágenes de Microsoft Docker

1. En **LON-HOST1**, si fuera necesario, haga clic con el botón derecho en **Inicio** y, después, haga clic en **Windows PowerShell (Administrador)**.
2. En la ventana de **Windows PowerShell**, escriba el comando siguiente para ver las imágenes descargadas y, después, presione Entrar:

```
Docker search Microsoft
```

Descargar imágenes de Docker predefinidas

1. Escriba el comando siguiente y presione Entrar para ver las imágenes disponibles en Docker Hub:

```
Docker images
```

2. En la ventana de **Windows PowerShell**, escriba el comando siguiente para descargar la imagen de IIS de muestra y, después, presione Entrar:

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

3. Espere unos minutos para que se descargue la imagen. Revise el texto de la pantalla en el que se describe esta imagen.

Nota: El cmdlet tarda aproximadamente 2 minutos en ejecutarse y escribe las siguientes líneas:

```
Hello from Docker!
This message shows that your installation appears to be working correctly.
To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.
```

4. En la ventana de **Windows PowerShell**, escriba lo siguiente para verificar la imagen descargada y, después, presione Entrar:

```
docker images
```

5. Debería ver tres imágenes de Docker:
   a. microsoft/iis
   b. microsoft/nanoserver
   c. hello-world

Implementar un contenedor nuevo con la imagen predeterminada

- En la ventana de **Windows PowerShell**, escriba lo siguiente para implementar el contenedor **IIS** y, después, presione Entrar:

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

Nota: Este comando ejecuta la imagen de **IIS** como un servicio en segundo plano (**-d**). También configura la red de modo que el puerto 80 del host del contenedor se correlacione con el puerto 80 del contenedor.

Administrar el contenedor

1. En la ventana de **Windows PowerShell**, escriba lo siguiente para ver los contenedores que se están ejecutando y, después, presione Entrar:

```
docker ps
```

2. Anote los datos de la primera columna, debajo del encabezado **Id. de contenedor**, que es una cadena larga de caracteres (por ejemplo, fd85c4dbffba). Puede usar esta opción para detener el contenedor. En la ventana de **Windows PowerShell**, escriba lo siguiente para ver los contenedores que se están ejecutando y, después, presione Entrar:

```
Docker stop <Container ID>
```

Nota: Reemplace <Container ID>, que se muestra en la línea anterior, por la cadena devuelta del cmdlet **Docker ps** que ejecutó en el paso 1.

Demostración: Implementar contenedores de Hyper-V

Pasos de la demostración

1. En la ventana de **Windows PowerShell**, en **LON-HOST1**, escriba los comandos siguientes y, después, presione Entrar:

```
Ipconfig
hostname
```

2. Tenga en cuenta que la dirección IP y el nombre de host son de **LON-HOST1**.
3. En **Windows PowerShell**, escriba el comando siguiente y presione Entrar:

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

4. Una vez finalizado el comando anterior, verá que dentro de la consola de **Windows PowerShell** se abrirá una consola de comandos con un fondo negro. En el símbolo del sistema, escriba los comandos siguientes y, después, presione Entrar:

```
Ipconfig
hostname
```

5. Observe que la **dirección IP** no es la misma que la del paso 2 y que el nombre del host es una cadena larga de caracteres. Este es el servidor de Nano Server que acaba de crear.
6. En **LON-HOST1**, haga clic en Inicio y, después, haga clic en **Windows PowerShell**. Se abrirá otra consola de **Windows PowerShell**.
7. En la nueva ventana de **Windows PowerShell**, escriba lo siguiente para ver los contenedores que se están ejecutando y, después, presione Entrar:

```
docker ps
```

8. Anote los datos de la primera columna, debajo del encabezado **Id. de contenedor**, que es una cadena larga de caracteres (por ejemplo, fd85c4dbffba). En la nueva ventana de **Windows PowerShell**, escriba lo siguiente para detener el contenedor que está en ejecución y, después, presione Entrar:

```
Docker stop <Container ID>
```

9. Reemplácelo por el ID del contenedor del cmdlet Docker ps del paso 7.
10. Cierre todas las ventanas abiertas.

Revisión del módulo y contenidos principales

Procedimientos recomendados

- Después de instalar SCM 3.0 en el equipo cliente o servidor principal, comparta la carpeta **LocalGPO** para que los dispositivos independientes y de grupo de trabajo puedan acceder a ella fácilmente.
- Para una experiencia gráfica completa, administre Docker en Nano Server desde un sistema remoto que tenga capacidades de GUI.
- Si quiere compartir datos persistentes entre contenedores o si quiere usar datos de contenedores no persistentes, debe crear un contenedor de volúmenes de datos con nombre y luego montar los datos desde él.

Pregunta de revisión

Pregunta: ¿Cuál es el entorno de procesamiento más seguro que puede tener: Nano Server, contenedores de Windows o contenedores de Hyper-V?

Respuesta: Los contenedores de Hyper-V son más seguros que los contenedores de Windows, que son más seguros que los de un sistema operativo de servidor implementado tradicionalmente. Puede alojar contenedores en Nano Server, lo que proporciona una manera rápida y fácil de implementar un contenedor, pero el uso de un contenedor de Hyper-V en un Nano Server proporciona la mejor seguridad de las tres opciones.

Herramientas

Herramienta	Finalidad	Dónde encontrarla
SCM	Crear, administrar e implementar líneas de base de seguridad para varios productos de Windows y sistemas operativos.	Descarga gratuita de Microsoft.com
Docker Enterprise Edition para Windows Server 2016	Docker permite a los contenedores que se ejecuten como procesos aislados en el espacio de usuario en el sistema operativo host, independientemente del sistema operativo.	https://aka.ms/y6lgzc
GitHub	Implementar contenedores de Hyper-V en Windows Server	https://aka.ms/puavgj

Preguntas y respuestas de la revisión de laboratorio

Laboratorio A: Uso de SCM

Preguntas y respuestas

Pregunta: Si **LON-SVR2** es un servidor independiente de un grupo de trabajo, ¿qué debe hacer para aplicarle la configuración de seguridad que creó en la línea base **Servidor miembro combinado 2012-2016**?

Respuesta: Puede utilizar la herramienta de línea de comandos LGPO.exe. De lo contrario, debe agregar la configuración de seguridad manualmente.

Pregunta: ¿Qué debe hacer para unir dos líneas base de productos diferentes en SCM?

Respuesta: Primero debe asociar los productos.

Laboratorio B: Implementar y configurar Nano Server

Preguntas y respuestas

Pregunta: ¿Qué hace el comando de Windows PowerShell que se muestra a continuación?

```
Docker search Microsoft
```

Respuesta: Enumera las diferentes funciones y roles predeterminados para contenedores de Windows que ha creado Microsoft.

Pregunta: ¿Qué hace el comando de Windows PowerShell que se muestra a continuación?

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

Respuesta: Muestra que el paquete DSC se instaló correctamente como módulo y luego muestra todos los comandos disponibles en el módulo.

Módulo 10

Planificación y protección de datos

Contenidos:

Lección 1

Planificación e implementación de cifrado

Contenidos:

Preguntas y respuestas

Pregunta: Se necesita una clave pública para descifrar un archivo cifrado con EFS.

( ) Verdadero

( ) Falso

Respuesta:

( ) Verdadero

(√) Falso

Comentarios:

La clave pública se usa para cifrar el archivo. Para descifrar el archivo, necesita una clave privada.

Pregunta: Si los usuarios tienen una clave privada adecuada, ¿pueden descifrar siempre un archivo cifrado con EFS?

( ) Verdadero

( ) Falso

Respuesta:

( ) Verdadero

(√) Falso

Comentarios:

Los usuarios pueden descifrar el archivo solo si pueden acceder a él. Si no tienen los permisos de archivo para acceder al archivo, no pueden descifrarlo.

Pregunta: Se necesita una entidad emisora de certificados (CA) en la red para cifrar archivos mediante EFS.

( ) Verdadero

( ) Falso

Respuesta:

( ) Verdadero

(√) Falso

Comentarios:

No se necesita ninguna CA para usar EFS. Le recomendamos que utilice certificados emitidos por una CA para EFS, aunque también puede utilizar certificados autofirmados.

Descripción general de EFS

Pregunta: ¿Utiliza EFS el cifrado simétrico o el cifrado de clave pública?

Respuesta: EFS utiliza una combinación de ambos métodos de cifrado. Utiliza el cifrado simétrico para cifrar el contenido del archivo y utiliza el cifrado de clave pública para cifrar y proteger la clave simétrica que se utiliza para el cifrado de archivos.

Pregunta: ¿Quién puede abrir un archivo que está cifrado mediante EFS?

Respuesta: Para abrir un archivo cifrado con EFS, el usuario debe tener permisos de archivo para acceder a este. Sin embargo, el usuario también debe tener la clave privada adecuada, con la que descifrar la clave simétrica. El usuario utiliza después la clave simétrica para descifrar y abrir el archivo cifrado. Si el usuario tiene una clave privada adecuada, este proceso es transparente y se puede abrir el archivo como si no estuviera cifrado. Si el usuario no dispone de la clave privada adecuada, el usuario verá un mensaje de error de acceso denegado.

EFS y los certificados

Pregunta: ¿Por qué los usuarios deben tener certificados para poder cifrar archivos mediante EFS?

> **Respuesta:** EFS utiliza la clave pública del usuario para cifrar la clave simétrica que se genera de forma aleatoria para cifrar cada archivo. Si un usuario no dispone de una clave pública, EFS no puede cifrar y proteger la clave simétrica. En este supuesto, EFS obtendrá el certificado de usuario y después realizará el cifrado.

Pregunta: ¿Se pueden compartir archivos cifrados con EFS con otros usuarios?

> **Respuesta:** Sí, se pueden compartir archivos cifrados con EFS con otros usuarios. Para ello, sin embargo, la clave pública del usuario debe estar disponible. Esto se debe a que EFS utiliza su clave pública para cifrar la clave simétrica.

Recuperar archivos cifrados con EFS

Pregunta: ¿Cómo puede descifrar el agente de recuperación de datos cualquier archivo cifrado con EFS?

> **Respuesta:** Si configura el agente de recuperación de datos en el entorno, EFS cifra una copia de la clave simétrica con la clave pública del agente de recuperación y la agrega al archivo durante el cifrado. El agente de recuperación de datos puede usar su clave privada para descifrar su copia de la clave simétrica y utilizarla para descifrar el archivo.

Pregunta: Si no tiene la clave privada adecuada para descifrar el archivo, ¿puede copiar un archivo cifrado con EFS del dispositivo en el que se cifró a la estación de trabajo dedicada del agente de recuperación de datos?

> **Respuesta:** No. Si no tiene la clave privada adecuada para descifrar el archivo, no puede copiar el archivo cifrado con EFS entre las estaciones de trabajo. La operación de copia incluye una operación de lectura del archivo original. Si no tiene la clave privada adecuada, no podrá abrir y leer el archivo. Debe realizar una copia de seguridad de los archivos cifrados y restaurarlos en la estación de trabajo dedicada del agente de recuperación de datos.

Resolver problemas comunes de EFS

Pregunta: ¿Cómo puede transferir archivos cifrados con EFS a la estación de trabajo dedicada del agente de recuperación de datos un usuario que ha perdido su clave privada?

> **Respuesta:** El usuario no tiene la clave privada adecuada, por lo que no puede copiar archivos cifrados. Sin embargo, el usuario puede realizar copias de seguridad de archivos cifrados y después, transferir la copia de seguridad a la estación de trabajo dedicada del agente de recuperación de datos.

Pregunta: ¿Cuánto tiempo después de agregar el agente de recuperación de datos nuevo se tiene que esperar para poder descifrar los archivos?

> **Respuesta:** El campo de recuperación de datos (DRF) de los archivos ya cifrados no se actualiza automáticamente. El DRF de los archivos cifrados se actualiza cuando un usuario con la clave privada adecuada ve sus propiedades o ejecuta el comando cipher **/U**.

Recursos

Descripción general de EFS

Lecturas adicionales: Para obtener más información, consulte: Cómo funciona EFS en: http://aka.ms/Uw9drx

Recuperar archivos cifrados con EFS

Lecturas adicionales: Para obtener más información, consulte "Key Recovery vs Data Recovery Differences" en: http://aka.ms/Frtdxi

Demostración: Utilizar EFS para proteger datos

Pasos de la demostración

1. En **LON-CL1**, en la barra de tareas, haga clic en el icono de **Inicio**, escriba **certmgr.msc** y, después, presione Entrar.
2. En la consola **Certificados: usuario actual**, en el panel de navegación, haga clic en **Personal** y, después, en el panel de detalles, compruebe que no hay elementos que mostrar en esta vista.
3. En la barra de tareas haga clic en el icono del **Explorador de archivos**.
4. En el Explorador de archivos, en el panel de navegación, expanda **Este equipo**, expanda **Disco Local (C:)**, expanda **Labfiles** y, después, seleccione **Mod10**. En el panel de detalles, haga clic con el botón derecho en **Adam1**, seleccione **Propiedades** y, después, haga clic en **Avanzadas**.
5. En el cuadro de diálogo **Atributos avanzados**, destaque que el botón **Detalles** aparece atenuado y no está disponible, ya que el archivo aún no está cifrado. Seleccione la casilla de verificación **Cifrar contenido para proteger datos** y, después, haga clic en **Aceptar**. Haga clic en **Aplicar**, seleccione la opción **Cifrar solo el archivo** y, después, haga clic en **Aceptar**.
6. Espere unos segundos y luego explique que el cifrado del primer archivo del usuario tarda unos segundos, porque EFS debe obtener un certificado de usuario antes de cifrar el archivo.
7. En el cuadro de diálogo **Propiedades de Adam1**, haga clic en **Avanzadas** y, después, haga clic en **Detalles**. Indique que Adam Hobbs puede acceder al archivo y que el administrador tiene un certificado de recuperación para el archivo.
8. Haga clic en **Agregar** y, en el cuadro de diálogo **Sistema de cifrado de archivos (EFS)**, remarque que solo Adam Hobbs aparece en la lista. Luego, explique que Adam es el único usuario que tiene una clave pública en este momento. Haga clic en **Cancelar** cuatro veces.
9. En el Explorador de archivos, señale que el archivo **Adam1** tiene un pequeño icono de bloqueo de clave porque está protegido por EFS. Remarque que los demás archivos de la carpeta no tienen ningún icono de bloqueo de clave.
10. En la consola **Certificados - Usuario actual**, actualice la vista presionando la tecla **F5**. En el panel de navegación, expanda **Personal** y, después, haga clic en **Certificados**. En el panel de detalles, indique que hay un certificado en la lista y muestre que se emite a Adam Hobbs para cifrar el sistema de archivos.
11. En la barra de tareas, haga clic en el icono de **Inicio**, haga clic en **Adam Hobbs** y, después, haga clic en **Cambiar cuenta**.

12. Inicie sesión en **LON-CL1** como usuario **ADATUM\Dawn** con la contraseña **Pa55w.rd**.
13. En la barra de tareas, haga clic en el icono del **Explorador de archivos**.
14. En el Explorador de archivos, en el panel de navegación, expanda **Este equipo**, expanda **Disco Local (C:)**, expanda **Labfiles** y, después, seleccione **Mod10**.
15. En el panel de detalles, haga doble clic en **Adam1** y señale que aparece el error "Acceso denegado", porque Dawn no tiene la clave privada de Adam para descifrar el archivo. Haga clic en **Aceptar** y, después, cierre el Bloc de notas.
16. En el Explorador de archivos, haga clic con el botón derecho en **Don1** y, después, seleccione **Propiedades**.
17. En el cuadro de diálogo **Propiedades**, haga clic en **Avanzadas**. Seleccione la casilla de verificación **Cifrar contenido para proteger datos**, haga clic en **Aceptar** y, después, haga clic en **Aceptar**. Seleccione **Cifrar solo el archivo**, seleccione la casilla de verificación **Siempre cifrar solo el archivo** y, después, haga clic en **Aceptar**.
18. Espere unos segundos y señale que este es el primer archivo que está cifrando Dawn. Explique que por ese motivo EFS debe obtener un certificado de usuario y el cifrado tarda un poco más que si el usuario ya tiene un certificado de EFS.
19. En el cuadro de diálogo **Propiedades de Don1**, haga clic en **Avanzadas** y, después, haga clic en **Detalles**. Indique que Dawn Williamson puede acceder al archivo y que el Administrador tiene un certificado de recuperación para el archivo.
20. Haga clic en **Agregar**, seleccione **Adam Hobbs** y, después, haga clic en **Aceptar**. Señale que ahora Adam Hobbs y Dawn Williamson pueden acceder al archivo y, después, haga clic en **Aceptar** tres veces.
21. En la barra de tareas, haga clic en el icono de **Inicio**, haga clic en **Dawn Williamson** y, después, seleccione **ADATUM\Adam**.
22. Inicie sesión en **LON-CL1** como usuario **ADATUM\Adam** con la contraseña **Pa55w.rd**.
23. En el Explorador de archivos, haga doble clic en **Don1**. Compruebe que el archivo se abre y que puede leer el contenido. Explique que Dawn le proporcionó a Adam acceso al archivo cifrado.
24. Cierre el Bloc de notas.

Lección 2

Planificación e implementación de BitLocker

Contenidos:

Preguntas y respuestas

Pregunta: Para usar BitLocker, el dispositivo debe tener un Módulo de plataforma segura (TPM).

( ) Verdadero

( ) Falso

Respuesta:

( ) Verdadero

(√) Falso

Comentarios:

Windows 10 permite el uso de BitLocker sin un TPM.

Pregunta: Las unidades protegidas con BitLocker de Windows 8.1 se pueden desbloquear en Windows 10.

( ) Verdadero

( ) Falso

Respuesta:

( ) Verdadero

(√) Falso

Comentarios:

El programa BitLocker de versiones anteriores de Windows es compatible con Windows 10. En Windows 10, versión 1511 y versiones posteriores, puede utilizar el nuevo modo de cifrado BitLocker, que no es compatible con versiones anteriores.

Pregunta: Cuando se activa BitLocker para la unidad C, también se puede especificar el almacenamiento de la clave de recuperación en AD DS.

( ) Verdadero

( ) Falso

Respuesta:

( ) Verdadero

(√) Falso

Comentarios:

Al activar BitLocker en una unidad, puede especificar dónde almacenar la unidad de recuperación, pero solo puede seleccionar una unidad flash USB, un archivo, una cuenta de Microsoft o imprimirlo. No se puede almacenar la clave de recuperación de BitLocker en AD DS mediante un asistente. Se puede hacer solamente a través de la directiva de grupo.

Descripción general de BitLocker

Pregunta: ¿Se puede usar BitLocker para cifrar solo datos confidenciales en el volumen, dejando sin cifrar otros datos en el volumen?

Respuesta: No. Al activar BitLocker en cada volumen, se cifran todos los datos del volumen.

Pregunta: ¿Se puede usar BitLocker para cifrar todos los volúmenes en un dispositivo de Windows?

Respuesta: No. BitLocker no puede cifrar los volúmenes del sistema, pero puede cifrar todos los demás volúmenes, independientemente del sistema de archivos.

BitLocker y los Módulos de plataforma segura (TPM)

Pregunta: ¿Cómo se puede configurar BitLocker para que funcione en un dispositivo sin un TPM?

> **Respuesta:** De forma predeterminada, BitLocker requiere un TPM. Si un dispositivo no tiene un TPM, puede usar la directiva de grupo para dar permiso a BitLocker sin un TPM. En tal caso, para cifrar un volumen debe proporcionar una clave de inicio USB para BitLocker.

Pregunta: ¿Cuál es el inconveniente de ejecutar BitLocker en un dispositivo Windows que no tenga un TPM?

> **Respuesta:** Se pueden cifrar volúmenes en dispositivos con Windows, incluso si no se tiene un TPM. Sin embargo, los dispositivos Windows sin TPM no podrán usar la verificación de integridad del sistema durante el inicio.

Configurar y administrar BitLocker

Pregunta: ¿Cuáles herramientas se pueden usar para configurar y administrar BitLocker?

> **Respuesta:** Puede configurar y administrar BitLocker mediante la herramienta de Cifrado de unidad BitLocker en el panel de control, los cmdlets de Windows PowerShell, la herramienta de configuración del Cifrado de unidad BitLocker (Manage-bde.exe) y también la herramienta Microsoft BitLocker Administration and Monitoring (MBAM), si su empresa tiene licencia para utilizar el MDOP.

Pregunta: Se permitió a la configuración de directiva de grupo **Almacenar información de recuperación de BitLocker en los Servicios de dominio de Active Directory (Windows Server 2008 y Windows Vista)** en un dispositivo de Windows 10. ¿Se almacena la información de recuperación de BitLocker en AD DS cuando habilitas BitLocker?

> **Respuesta:** No. Esta opción de configuración de directiva de grupo se aplica únicamente a Windows Server 2008 y Windows Vista; no se aplica a Windows 10. Si desea almacenar una clave de recuperación de BitLocker en un dispositivo de Windows 10, debe habilitar las opciones de directivas de grupo: **Elegir cómo se pueden recuperar unidades del sistema operativo protegidas por BitLocker**, **Elegir cómo se pueden recuperar unidades fijas protegidas por BitLocker** o **Elegir cómo se pueden recuperar unidades extraíbles protegidas por BitLocker**.

Recuperación de una unidad cifrada con BitLocker

Pregunta: Cuando se activa BitLocker en un dispositivo con un TPM, ¿cuál es el propósito de guardar la contraseña de recuperación?

> **Respuesta:** Si el TPM nunca cambia o no se puede acceder a él, si hay cambios en los archivos clave del sistema, o si alguien intenta iniciar el dispositivo desde un medio de inicio para evitar el sistema operativo, el dispositivo cambiará al modo de recuperación y permanecerá allí hasta que el usuario proporcione la contraseña de recuperación. Si almacena la contraseña de recuperación para que el usuario pueda acceder a ella, este podrá llevar a cabo el proceso de inicio.

Pregunta: ¿Cuál es la diferencia entre la recuperación de la contraseña y el Id. de contraseña?

> **Respuesta:** La recuperación de la contraseña es una contraseña de 48 dígitos que desbloquea una unidad protegida con BitLocker. La recuperación de la contraseña es exclusiva para un cifrado de BitLocker en concreto y se puede almacenar en AD DS, en una unidad flash USB o en un archivo. Un Id. de contraseña es un Id. de 32 caracteres que es único para una unidad cifrada. Encontrará el Id. de contraseña en la pestaña **Recuperación de BitLocker**, en la página de propiedades del objeto de equipo en Usuarios y equipos de Active Directory.

Administrar BitLocker utilizando Microsoft BitLocker Administration and Monitoring (MBAM)

Pregunta: ¿Cómo se puede utilizar MBAM para reducir el tiempo que el servicio de asistencia pasa recuperando una clave de desbloqueo de BitLocker para un usuario remoto?

> **Respuesta:** Los administradores pueden habilitar el Portal de autoservicio de MBAM que permite a los usuarios recuperar una contraseña de recuperación de BitLocker sin tener que llamar a su servicio de asistencia.

Pregunta: Su empresa solo utiliza dispositivos de Windows 10 que están protegidas por BitLocker y administrados por Microsoft Intune. ¿Puede implementar MBAM en su empresa?

> **Respuesta:** MBAM requiere AD DS y SQL Server. Como su empresa solo usa dispositivos con Windows 10, no cumple con los requisitos previos y no puede implementar MBAM en la empresa.

Recursos

Descripción general de BitLocker

Lecturas adicionales: Para obtener más información, consulte la descripción de BitLocker en: http://aka.ms/eiaxj5

Configurar y administrar BitLocker

Lecturas adicionales: Para obtener más información sobre BitLocker, consulte: "Use BitLocker Drive Encryption Tools to manage BitLocker" en: http://aka.ms/kyndxu

Lecturas adicionales: Para obtener más información, consulte la configuración de directiva de grupo de BitLocker en: http://aka.ms/Bvxso5

Administrar BitLocker utilizando Microsoft BitLocker Administration and Monitoring (MBAM)

Lecturas adicionales: Para obtener más información, consulte Microsoft BitLocker Administration and Monitoring (MBAM) en: http://aka.ms/L3su1s

Demostración: Uso de BitLocker

Pasos de la demostración

1. En **LON-CL1**, en la barra de tareas, haga clic en el icono de **Inicio**, escriba **gpedit.msc** y, después, presione Entrar.
2. En el Editor de directivas de grupo local, en el panel de navegación, expanda **Configuración del equipo**, expanda **Plantillas administrativas**, expanda **Componentes de Windows** y, después, expanda **Cifrado de unidad BitLocker**.
3. En el panel de navegación, haga clic en **Unidades del sistema operativo** y, después, en el panel de detalles, haga doble clic en **Requerir autenticación adicional al iniciar**.

4. En el cuadro de diálogo **Requerir autenticación adicional al iniciar**, haga clic en **Habilitado**. Compruebe que la casilla de verificación **Permitir BitLocker sin un TPM compatible** esté seleccionada y, después, haga clic en **Aceptar**.

Nota: Explique que esta configuración solo es necesaria si el dispositivo no tiene un TPM.

5. En el panel de navegación, haga clic en el nodo **Unidades de datos fijas** y, después, en el panel de detalles, haga doble clic en **Elegir cómo se pueden recuperar unidades fijas protegidas por BitLocker**.
6. En el cuadro de diálogo **Elegir cómo se pueden recuperar unidades fijas protegidas por BitLocker**, haga clic en **Habilitado** y, después, haga clic en **Aceptar**.
7. En **LON-CL1**, en la barra de tareas, haga clic en el icono del **Explorador de archivos**.
8. En el Explorador de archivos, en el panel de navegación, expanda **Este equipo**, haga clic en **Data (E:)**, haga clic con el botón derecho en el espacio vacío en el panel de detalles, seleccione **Nuevo**, haga clic en **Documento de texto**, escriba su nombre y, después, presione Entrar.
9. En el Explorador de archivos, en el panel de navegación, haga clic con el botón derecho en **Datos (E:)** y, después, haga clic en **Activar BitLocker**.
10. En el cuadro de diálogo **Cifrado de unidad BitLocker (E:)**, seleccione la casilla de verificación **Usar una contraseña para desbloquear la unidad**. En los cuadros de texto **Escribir una contraseña** y **Vuelva a escribir la contraseña**, escriba **Pa55w.rd** y, después, haga clic en **Siguiente**.
11. En la página **¿Cómo desea realizar la copia de seguridad de la clave de recuperación?**, haga clic en **Guardar en un archivo**.
12. En el cuadro de diálogo **Guardar clave de recuperación de BitLocker como**, en el panel de navegación, haga clic en **Este equipo**. En el panel de detalles, desplácese hacia abajo, haga doble clic en **Unidad de disquete (A:)**, haga clic en **Guardar** y, después, haga clic en **Siguiente**.
13. En la página **Elección del modo de cifrado que se usará**, haga clic en **Siguiente** y, después, haga clic en **Iniciar cifrado**.
14. En el Explorador de archivos, en el panel de navegación, indique que el disco local (E:) tiene un icono pequeño de bloqueo de clave.
15. En la ventana **Conexión a máquina virtual 26744B-LON-CL1**, haga clic en el menú **Archivo** y, después, haga clic en **Configuración**.
16. En la ventana **Configuración de 26744B-LON-CL1**, en el panel de navegación, debajo de Controlador SCSI, haga clic en **Disco duro1.vhd**. Luego, en el panel de detalles, haga clic en **Quitar** y haga clic en **Aceptar**.
17. En la ventana **Conexión a máquina virtual 26744B-LON-CL2**, haga clic en el menú **Archivo** y, después, haga clic en **Configuración**.
18. En el cuadro de diálogo **Configuración de 26744B-LON-CL2**, en el panel de navegación, haga clic en **Controlador SCSI**. En el panel de detalles, haga clic en **Disco duro**, haga clic en **Agregar**, haga clic en **Examinar**, vaya a **D:\Archivos de programa\Microsoft Learning\26744\Drives**, haga clic en **Disk1.vhd**, haga clic en **Abrir** y, después, haga clic en **Aceptar**.
19. En la barra de tareas, haga clic en el icono del **Explorador de archivos**. En el panel de navegación, indique que la unidad E aparece como **Disco local (E:)** y que tiene un pequeño icono de bloqueo de clave.

20. En el Explorador de archivos, en el panel de navegación, haga clic en **Disco local (E:)**. Se abrirá el cuadro de diálogo **BitLocker (E:)**.
21. En el cuadro de diálogo **BitLocker (E:)**, en el cuadro de texto, escriba **Pa55w.rd** y, después, haga clic en **Desbloquear**.
22. En el Explorador de archivos, en el panel de navegación, señale que la unidad E aparece como Datos (E:), y no como Disco local (E:).

Nota: En el panel de detalles, señale que se puede ver el archivo con su nombre.

23. En **LON-DC1**, en la barra de tareas, haga clic en el icono del **Administrador del servidor**.
24. En el Administrador del servidor, haga clic en **Herramientas** y, después, haga clic en **Usuarios y equipos de Active Directory**.
25. En Usuarios y equipos de Active Directory, en el panel de navegación, expanda **Adatum.com** y, después, haga clic en **Equipos**.
26. En el panel de detalles, haga clic con el botón derecho en **LON-CL1** y, después, haga clic en **Propiedades**.
27. En el cuadro de diálogo **Propiedades de LON-CL1** haga clic en la pestaña **Recuperación de BitLocker**.

Nota: Comente que aparece la contraseña de recuperación de BitLocker del disco cifrado en **LON-CL1**.

Revisión del módulo y contenidos principales

Preguntas de revisión

Pregunta: ¿Se puede cifrar todo un volumen mediante el cifrado de archivos de EFS?

Respuesta: Puede habilitar EFS en el nivel de archivo o de carpeta, pero no en el nivel de volumen. Sin embargo, puede habilitar EFS en todas las carpetas y archivos de la carpeta raíz del volumen, con lo que se cifraría todo el contenido de ese volumen.

Pregunta: ¿Se pueden cifrar archivos de sistema de Windows utilizando EFS?

Respuesta: No. No puede cifrar archivos que tienen configurado el atributo Sistema mediante el cifrado de archivos de EFS.

Pregunta: ¿Se puede realizar un borrado completo de un dispositivo perdido de Windows?

Respuesta: No. Los dispositivos de Windows solo admiten borrado selectivo. Puede realizar un borrado selectivo de un dispositivo de Windows si el dispositivo está administrado por Microsoft Intune, Microsoft System Center Configuration Manager o alguna otra solución de administración de dispositivos móviles.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio: Protección de datos mediante el cifrado y BitLocker

Preguntas y respuestas

Pregunta: ¿Por qué no ha podido abrir el administrador en **LON-CL2** el archivo **Adam1.txt** aunque la cuenta es un agente de recuperación de datos?

Respuesta: El certificado de recuperación de datos del administrador solo se almacena en el primer controlador de dominio de forma predeterminada. Debido a que no cuenta con su certificado de recuperación de datos en **LON-CL2**, no ha podido abrir el archivo. Después de importar el certificado de recuperación de datos, ha podido abrir el archivo.

Pregunta: ¿Por qué tienes que configurar **LON-CL1** para dar permiso a BitLocker sin un TPM compatible?

Respuesta: Las máquinas virtuales no tienen un TPM. BitLocker requiere un TPM predeterminado y sin modificar este requisito, no puede usar BitLocker en **LON-CL1**.

Módulo 11

Optimizar y proteger los servicios de archivo

Contenidos:

Lección 1

Administrador de recursos del servidor de archivos (FSRM)

Contenidos:

Preguntas y respuestas

Pregunta: ¿Las cuotas son algo que se podría implementar en todos los datos o solo en ubicaciones seleccionadas?

> **Respuesta:** Las respuestas pueden variar. Sin embargo, las cuotas implementadas en todos los datos pueden tener consecuencias no deseadas. Debe realizar una planificación cuidadosa de la configuración de las cuotas antes de implementarlas.

Pregunta: En su entorno, ¿implementaría el filtrado de archivos?

> **Respuesta:** Las respuestas serán diversas. Sin embargo, debe considerar cuidadosamente las implicaciones del filtrado de archivos antes de implementarlo.

Demostración: Instalación y configuración de FSRM

Pasos de la demostración

Instalar el servicio de rol de FSRM

1. Si todavía no ha iniciado sesión, inicie sesión en **LON-SVR1** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
2. Haga clic en **Inicio**, en **Administrador del servidor**, en **Administrar** y en **Agregar roles y características**.
3. En el **Asistente para agregar roles y características**, haga clic en **Siguiente**.
4. Confirme que la opción **Instalación basada en características o en roles** está seleccionada y, después, haga clic en **Siguiente**.
5. Confirme que esté seleccionada **LON-SVR1.Adatum.com** y, después, haga clic en **Siguiente**.
6. En la página **Seleccionar roles de servidor**, expanda **Servicios de archivos y almacenamiento (2 de 12 instalados)**, expanda **Servicios de iSCSI y archivo (1 de 11 instalado)** y, después, seleccione la casilla de verificación **Administrador de recursos del servidor de archivos**.
7. En el **Asistente para agregar roles y características**, haga clic en **Agregar características**.
8. Haga clic en **Siguiente** dos veces para confirmar el servicio de rol y la selección de características.
9. En la página **Confirmar selecciones de instalación** haga clic en **Instalar**.
10. Cuando termine la instalación, haga clic en **Cerrar**.

Especificar opciones de configuración de FSRM

1. En el **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Administrador de recursos del servidor de archivos**.
2. En la consola del **Administrador de recursos del servidor de archivos**, en el panel de navegación, haga clic con el botón derecho en **Administrador de recursos del servidor de archivos (local)** y, después, haga clic en **Configurar opciones**.
3. En el cuadro de diálogo **Opciones del Administrador de recursos del servidor de archivos**, haga clic en la pestaña **Auditoría de filtro de archivos** y, después, seleccione la casilla de verificación **Registrar la actividad de filtrado de archivos en la base de datos de auditoría**.
4. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Opciones del Administrador de recursos del servidor de archivos**. Cierre la consola **Administración del Administrador de recursos del sistema de archivos**.

Usar Windows PowerShell para administrar FSRM

1. En el **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Windows PowerShell**.
2. En el símbolo del sistema de **Windows PowerShell**, escriba el comando siguiente y presione Entrar.

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

3. Cierre la ventana de **Windows PowerShell**.
4. Abra la consola de administración del **Administrador de recursos del servidor de archivos**.
5. En la ventana del **Administrador de recursos del servidor de archivos**, en el panel de navegación, haga clic con el botón derecho en **Administrador de recursos del servidor de archivos (local)** y, después, haga clic en **Configurar opciones**.
6. En la pestaña **Notificaciones de correo electrónico**, revise las opciones configuradas para confirmar que son las mismas que las opciones especificadas en el comando **Set-FSRMSetting**.
7. Cierre todas las ventanas abiertas.

Demostración: Supervisión del uso cuotas

Pasos de la demostración

Crear una cuota

1. Si todavía no ha iniciado sesión, inicie sesión en **LON-SVR1** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
2. Haga clic en **Inicio** y, después, haga clic en **Administrador del servidor**.
3. En el **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Administrador de recursos del servidor de archivos**.
4. En el **Administrador de recursos del servidor de archivos**, expanda el nodo **Administración de cuotas** y, después, haga clic en **Plantillas de cuota**.
5. Haga clic con el botón derecho en la plantilla **Límite de 100 MB** y, después, haga clic en **Crear cuota a partir de una plantilla**.
6. En la ventana **Crear cuota**, haga clic en **Examinar**.
7. En la ventana **Buscar carpeta**, expanda **Allfiles (D:)**, expanda **Labfiles**, expanda **Mod11**, haga clic en **Datos** y, después, haga clic en **Aceptar**.
8. En la ventana **Crear cuota**, haga clic en **Crear**.
9. En la ventana del **Administrador de recursos del servidor de archivos**, haga clic en **Cuotas** para ver la cuota recién creada.

Probar una cuota

1. Haga clic en **Inicio** y, después, haga clic en el icono de **Windows PowerShell**.
2. En la ventana de **Windows PowerShell** escriba los comandos siguientes y presione Entrar después de cada uno.

```
Cd D:\Labfiles\Mod11\Datos
Fsutil file createnew largefile.txt 130000000
```

3. Observe que aparece el siguiente mensaje: **Error: No hay suficiente espacio en el disco**.
4. Cierre la ventana de **Windows PowerShell**.

Demostración: Implementación de un filtro de archivos

Pasos de la demostración

Crear un filtro de archivos

1. En la ventana **Administrador de recursos del servidor de archivos**, expanda el nodo **Administración del filtrado de archivos** y, después, haga clic en **Plantillas de filtro de archivos**.
2. Haga clic con el botón derecho en la plantilla **Bloquear archivos de imagen** y, después, haga clic en **Crear filtro de archivos a partir de una plantilla**.
3. En la ventana **Crear filtro de archivos** haga clic en **Examinar**.
4. En la ventana **Buscar carpeta**, expanda **Allfiles (D:)**, expanda **Labfiles**, expanda **Mod11**, haga clic en **Datos** y, después, haga clic en **Aceptar**.
5. En la ventana **Crear filtro de archivos** haga clic en **Crear**.

Probar un filtro de archivos

1. Abra el **Explorador de archivos**.
2. En la ventana del **Explorador de archivos**, expanda **Este equipo**, expanda **Allfiles (D:)**, expanda **Labfiles** y, después, haga clic en **Mod11**.
3. En el **Explorador de archivos**, haga clic en la pestaña **Inicio**, haga clic en **Nuevo elemento** y, después, haga clic en **Imagen de mapa de bits**.
4. Escriba **testimage** y presione Entrar.
5. Confirme que el archivo se ha creado correctamente.
6. Haga clic con el botón derecho en **testimage** y, después, haga clic en **Copiar**.
7. Haga clic con el botón derecho en **Datos** y, después, haga clic en **Pegar**.
8. Recibirá un mensaje diciendo que necesita permiso para realizar esta acción. Haga clic en **Cancelar** para cerrar el cuadro de diálogo.
9. Cierre el **Explorador de archivos**.

Demostración: Generar informes de almacenamiento a petición

Pasos de la demostración

Generar un informe de almacenamiento

1. En el **Administrador de recursos del servidor de archivos**, en el panel de navegación, haga clic con el botón derecho en **Administración de informes de almacenamiento** y, después, haga clic en **Generar informes ahora**.
2. En el cuadro de diálogo **Propiedades de la tarea de informes de almacenamiento** seleccione la casilla de verificación **Archivos grandes**.
3. Haga clic en la pestaña **Ámbito** y, después, haga clic en **Agregar**.
4. En la ventana **Buscar carpeta**, haga clic en **Allfiles (D:)** y, después, haga clic en **Aceptar**.

5. En el cuadro de diálogo **Propiedades de la tarea de informes de almacenamiento** haga clic en **Aceptar**.
6. En el cuadro de diálogo **Generar informes de almacenamiento**, compruebe que esté seleccionado **Esperar a que se generen los informes y mostrarlos a continuación** y, después, haga clic en **Aceptar** para generar el informe.
7. En el **Explorador de archivos**, en la carpeta **Interactivo** haga clic con el botón derecho en el archivo HTML, haga clic en **Abrir con**, haga clic en **Internet Explorer**, haga clic en **Aceptar** y examine el informe.
8. Cierre la ventana del informe.
9. Cierre la ventana del **Explorador de archivos**.
10. Cierre la ventana **Administrador de recursos del servidor de archivos**.
11. Cierre la ventana **Administrador del servidor**.

Lección 2

Implementando tareas de clasificación y administración de archivos

Contenidos:

Preguntas y respuestas

Pregunta: ¿Cómo podría utilizar la clasificación automática en su entorno?

> **Respuesta:** Las respuestas serán diversas; algunos estudiantes puede que quieran vincular la clasificación automática con AD RMS, para proporcionar una solución básica de prevención de la pérdida de datos.

Demostración: Configurar la clasificación de archivos

Pasos de la demostración

Crear una propiedad de clasificación

1. En **LON-SVR1**, haga clic en **Inicio** y, después, haga clic en el icono del **Administrador del servidor**.
2. En la consola del **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Administrador de recursos del servidor de archivos**.
3. En el **Administrador de recursos del servidor de archivos**, expanda **Administración de clasificaciones**, haga clic y, después, haga clic con el botón derecho en **Propiedades de la clasificación**. Después, haga clic en **Crear propiedad local**.
4. En la ventana **Crear propiedad de clasificación local**, en el cuadro de texto **Nombre**, escriba **Documents**. En la lista desplegable **Tipo de propiedad**, asegúrese de que está seleccionado **Sí/No** y, después, haga clic en **Aceptar**.

Crear una regla de clasificación

1. En el **Administrador de recursos del servidor de archivos**, expanda **Administración de clasificaciones**, haga clic en **Reglas de clasificación** y, después, en el panel **Acción**, haga clic en **Crear regla de clasificación**.
2. En la ventana **Crear regla de clasificación**, en la pestaña **General**, en el cuadro de texto **Nombre de la regla**, escriba **Regla de documentos corporativos** y asegúrese de que esté seleccionada la casilla de verificación **Habilitar**.
3. En la ventana **Crear regla de clasificación**, en la pestaña **Ámbito** haga clic en **Agregar**.
4. En la ventana **Buscar carpeta**, expanda **Allfiles (D:\)**, expanda **Labfiles**, expanda **Mod11**, haga clic en la carpeta **Documents** y, después, haga clic en **Aceptar**.
5. En la ventana **Crear regla de clasificación** en la pestaña **Clasificación** en la lista desplegable **Método de clasificación** haga clic en **Clasificador de carpetas**. En la lista desplegable **Propiedades - Elija una propiedad para asignar a los archivos**, haga clic en **Documents** y, después, en la lista desplegable **Propiedades - Especifique un valor**, haga clic en **Sí**.
6. En la ventana **Crear regla de clasificación**, en la pestaña **Tipo de evaluación**, haga clic en **Volver a evaluar los valores de propiedad existentes**, asegúrese de que esté seleccionado el botón de la opción **Agregar los valores** y, después, haga clic en **Aceptar**.
7. En el **Administrador de recursos del servidor de archivos**, en el panel **Acción** haga clic en **Ejecutar clasificación con todas las reglas ahora**.
8. En la ventana **Ejecutar clasificación**, seleccione el botón de radio **Esperar a que termine la clasificación** y, después, haga clic en **Aceptar**.
9. Revise el **Informe de clasificación automática** que aparece en Windows Internet Explorer y asegúrese de que en el informe se indica el mismo número de archivos que se clasificaron en la carpeta **Documents**. Habrá tres archivos.
10. Cierre el Explorador de archivos.

Demostración: Configurar las tareas de administración de archivos

Pasos de la demostración

Crear un archivo

1. En **LON-SVR1**, en la barra de tareas haga clic en el icono del **Explorador de archivos**.
2. Busque **D:\LabFiles\Mod11\Documents**, haga clic con el botón derecho en **Strategy1.txt** y, después, seleccione **Copiar**. Haga clic con el botón derecho y haga clic en **Pegar**.

Crear una tarea de administración de archivos

1. En **LON-SVR1**, haga clic en **Inicio** y, después, haga clic en el acceso directo del **Administrador del servidor**.
2. En el **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Administrador de recursos del servidor de archivos**.
3. En el **Administrador de recursos del servidor de archivos**, seleccione y haga clic con el botón derecho en el nodo **Tareas de administración de archivos** y, después, haga clic en **Crear tarea de administración de archivos**.
4. En el cuadro de texto **Nombre de la tarea** escriba **Caducar documentos**.
5. En el cuadro de texto **Descripción** escriba **Mover documentos antiguos a otra carpeta**.
6. Haga clic en la pestaña **Ámbito**.
7. En la sección **Ámbito** haga clic en **Agregar**.
8. Expanda **Allfiles (D:)**, expanda **Labfiles**, expanda **Mod11**, haga clic en **Documents** y, después, haga clic en **Aceptar**.

Configurar una tarea de administración de archivos para hacer caducar documentos

1. En la ventana **Crear tarea de administración de archivos**, haga clic en la pestaña **Acción**.
2. En la pestaña **Acción** debajo de Tipo, seleccione **Expiración de archivo**.
3. En el **Directorio de expiración**, escriba **D:\Labfiles\Mod11\Datos**.
4. En la ventana **Crear tarea de administración de archivos**, haga clic en la pestaña **Condiciones**.
5. En la pestaña **Condiciones**, seleccione la casilla de verificación **Modelos de nombre de archivo** y, después, escriba ***Copie*** en el cuadro de texto.
6. En la ventana **Crear tarea de administración de archivos**, haga clic en la pestaña **Programación**.
7. Seleccione **Mensual** y, después, seleccione la casilla de verificación **Último**.
8. En la ventana **Crear tarea de administración de archivos**, haga clic en **Aceptar**.
9. Haga clic con el botón derecho en la tarea **Caducar documentos** y, después, haga clic en **Ejecutar tarea de administración de archivos ahora**.
10. En la ventana **Ejecutar tarea de administración de archivos**, elija **Esperar a que la tarea termine** y, después, haga clic en **Aceptar**.
11. Vea el informe generado y confirme que se movió un archivo.
12. En el encabezado del informe, haga clic en el vínculo **Directorio de expiración** y, después, expanda los directorios para ver el archivo caducado.
13. Abra la carpeta **D:\Labfiles\Mod11\Documents** y vea el contenido. El archivo **Strategy1 - Copy.txt** no estará allí.
14. Cierre todas las ventanas abiertas.

Lección 3

Control de acceso dinámico

Contenidos:

Preguntas y respuestas

Pregunta: ¿Qué tecnologías se requieren si quiere utilizar Control de acceso dinámico?

( ) Servicios de dominio de Active Directory (AD DS)

( ) Kerberos

( ) AD CS

( ) AD RMS

( ) AD FS

Respuesta:

(√) Servicios de dominio de Active Directory

(√) Kerberos

( ) AD CS

( ) AD RMS

( ) AD FS

Comentarios:

Control de acceso dinámico solo requiere AD DS y Kerberos, aunque la clasificación de archivos puede utilizar AD RMS.

Pregunta: Control de acceso dinámico en Windows Server 2016 es compatible tanto con las notificaciones de usuario como con las de equipo.

( ) Verdadero

( ) Falso

Respuesta:

(√) Verdadero

( ) Falso

Comentarios:

Control de acceso dinámico es compatible con las notificaciones de usuario y de equipo. Las notificaciones se basan en los atributos de AD DS y los valores de esos atributos.

Recursos

Las tecnologías de base para Control de acceso dinámico.

Lecturas adicionales: Para obtener más información sobre los cambios en el protocolo Kerberos v5 sobre protección de Kerberos, consulte: http://aka.ms/v54k6z

Implementación y configuración de directivas de acceso central

Lecturas adicionales: Descargue "Microsoft Data Classification Toolkit" en: http://aka.ms/alw15o

Lecturas adicionales: Para solucionar problemas de Control de acceso dinámico si los usuarios no están recibiendo el acceso correcto, descargue la guía "Understand and Troubleshoot Dynamic Access Control in Windows Server 2012" en: http://aka.ms/w2d2fo

Demostración: Configuración del Control de acceso dinámico

Pasos de la demostración

Preparar AD DS para Control de acceso dinámico

1. En **LON-DC1**, en el **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Usuarios y equipos de Active Directory**.
2. En la ventana **Usuarios y equipos de Active Directory**, haga clic con el botón derecho en **Adatum.com**, haga clic en **Nuevo** y, después, haga clic en **Unidad organizativa**.
3. En el cuadro de diálogo **Nuevo objeto – Unidad organizativa**, en el cuadro de texto **Nombre**, escriba **DAC-Protected computers** y, después, haga clic en **Aceptar**.
4. Haga clic en el contenedor **Equipos**, haga clic con el botón derecho en **LON-SVR1** y, después, haga clic en **Mover**.
5. En la ventana **Mover**, haga clic en **DAC-Protected computers** y, después, haga clic en **Aceptar**.
6. Vaya a la ventana **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Administración de directivas de grupo**.
7. Expanda **Bosque: Adatum.com**, expanda **Dominios**, expanda **Adatum.com** y, después, haga clic en el contenedor **Objetos de directiva de grupo**.
8. En el panel de resultados, haga clic con el botón derecho en **Directiva predeterminada de controladores de dominio** y, después, haga clic en **Editar**.
9. En el **Editor de administración de directivas de grupo**, debajo de **Configuración del equipo**, expanda **Directivas**, expanda **Plantillas administrativas**, expanda **Sistema** y, después, haga clic en **KDC**.
10. En el panel de detalles, haga doble clic en **KDC admite notificaciones, autenticación compuesta y protección de Kerberos**.
11. En la ventana **KDC admite notificaciones, autenticación compuesta y protección de Kerberos**, seleccione **Habilitado** y, en la sección **Opciones**, en la lista desplegable, seleccione **Siempre proporcionar notificaciones**. Después, haga clic en **Aceptar**.
12. Cierre el **Editor de administración de directivas de grupo** y la **Consola de administración de directivas de grupo**.
13. Haga clic en **Inicio** y, después, haga clic en **Windows PowerShell**.
14. En la ventana de **Windows PowerShell**, escriba **gpupdate /force** y presione Entrar. Cuando se haya actualizado la directiva de grupo, cierre **Windows PowerShell**.
15. Vaya a la ventana **Usuarios y equipos de Active Directory**.
16. En el panel de navegación, haga clic en la unidad organizativa **Research** y, en el panel de contenido, haga clic con el botón derecho en **Connie Vaughn**. Después, haga clic en **Propiedades**.
17. En la ventana **Propiedades de Connie Vaughn** haga clic en la pestaña **Organización**. Asegúrese de que el cuadro de texto **Departamento** contenga el valor **Research** y, después, haga clic en **Cancelar**.
18. Cierre **Usuarios y equipos de Active Directory**.

Configurar las notificaciones, las propiedades de los recursos y las reglas de acceso central

1. En **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Centro de administración de Active Directory**.
2. En **Centro de administración de Active Directory**, en el panel de navegación, haga clic en **Control de acceso dinámico** y, después, haga doble clic en **Tipos de notificación**.
3. En el panel **Tareas**, haga clic en **Nuevo** y, después, haga clic en **Tipo de notificación**.
4. En la ventana **Crear tipo de notificación** en la sección **Atributos de origen** busque y seleccione **Departamento**.
5. En el cuadro de texto **Nombre para mostrar** escriba **Departamento de la empresa**.
6. Seleccione tanto **Usuario** como **Equipo** y, después, haga clic en **Aceptar**.
7. En el **Centro de administración de Active Directory**, haga clic en **Control de acceso dinámico** y, después, haga doble clic en **Propiedades del recurso**.
8. En la lista **Propiedades del recurso**, haga clic con el botón derecho en **Departamento** y, después, haga clic en **Habilitar**.
9. Haga doble clic en **Departamento**.
10. Desplácese hacia abajo hasta la sección **Valores sugeridos** y, después, haga clic en **Agregar**.
11. En la ventana **Agregar un valor sugerido**, en los cuadros de texto **Valor** y **Nombre para mostrar**, escriba **Research** y, después, haga clic en **Aceptar** dos veces.
12. Haga clic en **Control de acceso dinámico** y, después, haga doble clic en **Listas de propiedades de recursos**.
13. En el panel central, haga doble clic en **Lista de propiedades de recursos globales**, asegúrese de que aparece **Departamento** y, después, haga clic en **Cancelar**. Si no aparece, haga clic en **Agregar**, agregue la propiedad y haga clic en **Aceptar**.
14. En el panel de navegación, haga clic en **Control de acceso dinámico** y, después, haga doble clic en **Reglas de acceso central**.
15. En el panel **Tareas**, haga clic en **Nuevo** y, después, haga clic en **Regla de acceso central**.
16. En el cuadro de diálogo **Crear regla de acceso central** en el cuadro de texto **Nombre** escriba **Coincidencia de departamento**.
17. En la sección **Recursos de destino** haga clic en **Editar**.
18. En el cuadro de diálogo **Regla de acceso central** haga clic en **Agregar una condición**.
19. En la última lista desplegable, seleccione **Research**. Verifique que la condición es **Recurso-Departamento-Igual-Valor-Investigación** y, después, haga clic en **Aceptar**.
20. En la sección **Permisos**, seleccione **Usar los siguientes permisos como permisos actuales** y, después, haga clic en **Editar**.
21. Seleccione la entrada de permiso para **DERECHOS DE PROPIETARIO** y, después, haga clic en **Quitar**. Repita este paso para los grupos de **Administradores (ADATUM\Administradores)** y **SISTEMA**.
22. En el cuadro de diálogo **Configuración de seguridad avanzada para permisos** haga clic en **Agregar**.
23. En el cuadro de diálogo **Entrada de permiso para permisos** haga clic en **Seleccionar una entidad de seguridad**.

24. En la ventana **Seleccionar usuario, equipo, cuenta de servicio o grupo**, escriba **Usuarios autenticados**, haga clic en **Comprobar nombres** y, después, haga clic en **Aceptar**.
25. En la sección **Permisos Básicos**, seleccione **Modificar**, **Leer y ejecutar**, **Leer** y **Escribir**.
26. Haga clic en **Agregar una condición**.
27. En el cuadro de la lista desplegable **Grupo**, seleccione **Departamento de la empresa** y, en el cuadro de la lista desplegable **Valor**, seleccione **Recurso**. En el último cuadro de la lista desplegable, seleccione **Departamento** y, después, haga clic en **Aceptar** tres veces.

Clasificar archivos manualmente

1. Vaya a **LON-SVR1**.
2. Haga clic en **Inicio** y, después, haga clic en **Administrador del servidor**.
3. En el **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Administrador de recursos del servidor de archivos**.
4. En el **Administrador de recursos del servidor de archivos**, expanda **Administración de clasificaciones**, haga clic en **Propiedades de la clasificación**, haga clic con el botón derecho en **Propiedades de la clasificación** y, después, haga clic en **Actualizar**.
5. Verifique que la propiedad del **Departamento** está en la lista.
6. En la barra de tareas, haga clic en el icono del **Explorador de archivos**.
7. En la ventana del **Explorador de archivos**, en la barra de direcciones, escriba **D:\Labfiles\Mod11**, presione Entrar y, en el panel de contenido, haga clic con el botón derecho en la carpeta **Research**. Después, haga clic en **Propiedades**.
8. Haga clic en la pestaña **Clasificación**, haga clic en **Departamento** y, en la sección **Valor**, haga clic en **Research**. Después, haga clic en **Aceptar**.

Configurar e implementar una directiva de acceso central

1. Vaya a **LON.DC1**.
2. En el **Centro de administración de Active Directory**, en el panel de navegación, haga clic en **Control de acceso dinámico** y, después, haga doble clic en **Directivas de acceso central**.
3. En el panel **Tareas**, haga clic en **Nuevo** y, después, haga clic en **Directiva de acceso central**.
4. En el cuadro de texto **Nombre**, escriba **Coincidencia de departamento** y, después, haga clic en **Agregar**.
5. Haga clic en la regla **Coincidencia de departamento**, haga clic en **>>** y, después, haga clic en **Aceptar** dos veces.
6. Cierre el **Centro de administración de Active Directory**.
7. En el **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Administración de directivas de grupo**.
8. En la **Consola de administración de directivas de grupo**, haga clic con el botón derecho en **DAC-Protected computers** y, después, haga clic en **Crear un GPO en este dominio y vincularlo aquí**.
9. En el cuadro de diálogo **Nuevo GPO**, en el cuadro de texto **Nombre**, escriba **Directiva de DAC** y, después, haga clic en **Aceptar**.
10. Haga clic con el botón derecho en **Directiva de DAC** y, después, haga clic en **Editar**.

11. En la ventana del **Editor de administración de directivas de grupo**, debajo de Configuración del equipo, expanda **Directivas**, expanda **Configuración de Windows**, expanda **Configuración de seguridad**, expanda **Sistema de archivos**, haga clic con el botón derecho en **Directiva de acceso central** y, después, haga clic en **Administrar directivas de acceso central**.
12. Haga clic en **Coincidencia de departamento**, haga clic en **Agregar** y, después, haga clic en **Aceptar**.
13. Cierre el **Editor de administración de directivas de grupo** y la **Consola de administración de directivas de grupo**.
14. Vaya a **LON-SVR1**.
15. En **LON-SVR1**, haga clic en **Inicio** y, después, haga clic en **Windows PowerShell**.
16. En el símbolo del sistema de **Windows PowerShell**, escriba el comando siguiente y presione Entrar.

```
gpupdate /force
```

17. Cierre **Windows PowerShell**.
18. Vaya a la ventana del **Explorador de archivos**.
19. En la ventana del **Explorador de archivos**, haga clic con el botón derecho en la carpeta **Research** y, después, haga clic en **Propiedades**.
20. En el cuadro de diálogo **Propiedades de Research**, haga clic en la pestaña **Seguridad** y, después, haga clic en **Avanzada**.
21. En la ventana **Configuración de seguridad avanzada para investigación**, haga clic en la pestaña **Directiva central** y, después, haga clic en **Cambiar**.
22. En el cuadro de la lista desplegable, seleccione **Coincidencia de departamento** y, después, haga clic en **Aceptar** dos veces.

Demostración: Configuración de la asistencia para acceso denegado

Pasos de la demostración

1. Vaya a **LON-DC1**.
2. En **LON-DC1**, en el **Administrador del servidor**, haga clic en **Herramientas** y, después, haga clic en **Administración de directivas de grupo**.
3. En la **Consola de administración de directivas de grupo**, haga clic en **Directiva de DAC** y, después, haga clic en **Editar**.
4. En el **Editor de administración de directivas de grupo**, debajo de **Configuración del equipo**, expanda **Directivas**, expanda **Plantillas administrativas**, expanda **Sistema** y, después, haga clic en **Asistencia de acceso denegado**.
5. En el panel de detalles, haga doble clic en **Personalizar mensaje para errores de acceso denegado**.
6. En la ventana **Personalizar mensaje para errores de acceso denegado** haga clic en **Habilitado**.
7. En el cuadro de texto **Mostrar el mensaje siguiente a usuarios a los que se deniegue el acceso**, escriba **Se le ha denegado el acceso debido a la directiva de permisos. Solicite acceso**.
8. Seleccione **Permitir que los usuarios soliciten asistencia**, revise otras opciones, pero no realice cambios y, después, haga clic en **Aceptar**.

9. En el panel de detalles del **Editor de administración de directivas de grupo**, haga doble clic en **Permitir la asistencia de acceso denegado en el cliente para todos los tipos de archivos**, haga clic en **Habilitado** y, después, haga clic en **Aceptar**.
10. Cierre el **Editor de administración de directivas de grupo** y la **Consola de administración de directivas de grupo**.

Revisión del módulo y contenidos principales

Procedimientos recomendados

- Utilice plantillas de cuota para controlar y supervisar la cantidad de datos que almacenan los grupos.
- Utilice la clasificación de archivos para identificar y proporcionar un control con más nivel de detalle sobre ciertos tipos de datos.

Preguntas de revisión

Pregunta: ¿De qué manera las plantillas de FSRM para cuotas y filtros de archivos hacen la administración de FSRM más eficiente?

Respuesta: Las plantillas permiten a los administradores crear cuotas y filtros de archivos rápidamente, sobre la base de plantillas predefinidas. También puede utilizar plantillas para administrar cuotas de elementos secundarios en una relación de uno a varios. Para cambiar el tamaño de archivo para varias cuotas creadas a partir de la plantilla, solo tiene que cambiar la plantilla.

Pregunta: ¿Cómo mejora la experiencia del usuario gracias a la asistencia para acceso denegado?

Respuesta: Cuando la función de asistencia de acceso denegado está configurada con explicaciones fáciles de comprender e información de contacto actualizada, ayuda a los usuarios a comprender por qué no pueden acceder a un recurso en particular y le permite indicarles el contacto correcto que puede proporcionarle acceso.

Herramientas

Herramienta	Para qué se utiliza	Dónde encontrarla
Administrador de recursos del servidor de archivos (FSRM)	Administración de cuotas, filtros de archivos, administración de clasificaciones e informes de almacenamiento	• Agregue el servicio del rol de FSRM desde el **Asistente para agregar roles y características** o mediante **Windows PowerShell**. • Administrador del servidor - Herramientas
Windows PowerShell	Administrar FSRM	Windows PowerShell: `import-module FileServerResourceManager`

Problemas comunes y sugerencias para la resolución de problemas

Problema común	Sugerencia para la resolución de problemas
Cuando intente ejecutar una tarea de administración de archivos en el símbolo del sistema, puede aparecer un mensaje de error indicando que la tarea no se pudo encontrar.	Esto ocurre porque el nombre de la tarea en la interfaz del servidor de archivo no coincide con el nombre de la tarea requerida por el símbolo del sistema. Por ejemplo, puede crear una tarea denominada Tarea1, pero el nombre requerido por la línea de comandos es *AdministraciónDeArchivos-Tarea1*.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio A: Las cuotas y el filtrado de archivos

Preguntas y respuestas

Pregunta: ¿Qué criterios debe cumplir para utilizar FSRM en la administración de la estructura de archivos de un servidor?

> **Respuesta:** Los servidores deben ejecutar Windows Server 2003 SP1 o posterior para utilizar el FSRM. Si desea utilizar FCI, debe ejecutar Windows Server 2008 R2 o posterior. Además, debe formatear con NTFS los volúmenes en los que se realicen operaciones de FSRM.

Pregunta: ¿De qué manera las tareas de administración de clasificaciones y de administración de archivos pueden disminuir la carga administrativa, cuando se trata de una estructura compleja de archivos y carpetas?

> **Respuesta:** Las tareas de administración de clasificaciones y administración de archivos permiten a los administradores automatizar la clasificación manual y la modificación de archivos en un servidor de archivos. En lugar de inspeccionar los archivos manualmente y realizar operaciones de archivo manual, los administradores pueden configurar FCI para clasificar los archivos y después, realizar las operaciones necesarias en esos archivos mediante las tareas de administración de archivos.

Laboratorio B: Implementar Control de acceso dinámico.

Preguntas y respuestas

Pregunta: ¿Cómo mejoran las clasificaciones de archivos el uso de Control de acceso dinámico?

> **Respuesta:** Cuando utilice clasificaciones de archivos, puede definir los atributos en los archivos automáticamente y luego usar esos atributos en expresiones condicionales cuando implemente Control de acceso dinámico.

Pregunta: ¿Se puede implementar Control de acceso dinámico sin una directiva de acceso central?

> **Respuesta:** Sí, puede definir expresiones condicionales directamente en los recursos.

Módulo 12

Proteger el tráfico de red con firewalls y cifrado

Contenidos:

Lección 1

Descripción de las amenazas de seguridad relacionadas con la red

Contenidos:

Preguntas y respuestas

Discusión: Amenazas de seguridad relacionadas con la red frecuentes

Pregunta: ¿Cuáles son algunas de las amenazas de seguridad con las que está familiarizado?

> **Respuesta:** Las respuestas pueden variar, pero podrían incluir los correos electrónicos de suplantación de identidad (phishing), spyware y ransomware.

Recursos

Puertos conocidos

 **Lecturas adicionales:** Para obtener una lista completa de puertos conocidos y puertos registrados, consulte "Service Name and Transport Protocol Port Number Registry" en: https://aka.ms/ivsdso

Lección 2

Introducción a Firewall de Windows con Seguridad avanzada

Contenidos:

Preguntas y respuestas

Pregunta: ¿Cuáles son las ventajas de utilizar un firewall basado en host, como el Firewall de Windows con seguridad avanzada?

Respuesta: Firewall de Windows con seguridad avanzada ofrece las siguientes ventajas:

- Los equipos han mejorado la protección contra los ataques en la red interna. Esto puede ayudar a evitar que el malware se desplace a través de la red interna mediante el bloqueo de tráfico entrante no solicitado.
- Las reglas de entrada ayudan a evitar la exploración de redes para identificar los hosts en la red. Los escáneres de red más simples hacen ping a los hosts en una red, intentando identificarlos. Firewall de Windows con seguridad avanzada ayuda a evitar que los servidores miembro respondan a las solicitudes de ping. Los controladores de dominio responden a las solicitudes de ping.
- Cuando habilita reglas de salida, estas pueden evitar que el malware se propague al impedir que se comunique en la red. En el caso de un brote de virus, puede configurar los equipos con una regla de salida específica que ayude a evitar que el virus se comunique a través de la red.
- Las reglas de seguridad de conexión le permiten crear reglas de firewall sofisticadas, que utilizan la información de autenticación del usuario y del equipo para limitar la comunicación con equipos de alta seguridad.

Demostración: Cómo usar Firewall de Windows para administrar el tráfico de red

Pasos de la demostración

Crear una regla de firewall de entrada

1. En **LON-DC1**, abra la ventana **Símbolo del sistema**, escriba lo siguiente y, después, presione Entrar.

```
Ping LON-SVR2
```

Nota: El resultado debería ser "Tiempo de espera agotado para esta solicitud".

2. Vaya a **LON-SVR2**, abra la ventana de **Windows PowerShell**, escriba lo siguiente y presione Entrar.

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

Nota: El ping a **LON-DC1** debería ser correcto.

3. Haga clic en el botón de **Inicio** y, después, haga clic en **Panel de control**.
4. Haga clic en **Sistema y seguridad** y, después, haga clic en **Firewall de Windows**.
5. En la ventana **Firewall de Windows** haga clic en el enlace del lado izquierdo **Configuración avanzada** para abrir la consola de administración **Firewall de Windows con seguridad avanzada**.
6. En **Firewall de Windows con seguridad avanzada en el equipo local**, en el panel de navegación, haga clic en **Reglas de entrada**.
7. Haga clic con el botón derecho en **Reglas de entrada** y, después, haga clic en **Nueva regla**.

8. En el **Asistente para nueva regla de entrada**, en la página **Tipo de regla**, haga clic en **Personalizada** y, después, haga clic en **Siguiente**.
9. En la página **Programa**, haga clic en **Todos los programas** y, después, haga clic en **Siguiente**.
10. En la página **Protocolo y puertos**, en la lista **Tipo de protocolo**, haga clic en **ICMPv4** y, después, haga clic en **Siguiente**.
11. En la página **Ámbito** haga clic en **Siguiente**.
12. En la página **Acción**, haga clic en **Permitir la conexión** y, después, haga clic en **Siguiente**.
13. En la página **Perfil** haga clic en **Siguiente**.
14. En la página **Nombre**, en el cuadro de texto **Nombre**, escriba **Permitir regla de ping** y, después, haga clic en **Finalizar**.
15. En el panel de navegación, expanda **Supervisión** y, después, haga clic en **Firewall**.
16. Compruebe que se creó la regla **Permitir regla de ping**.

Probar la regla de firewall de entrada

- Vaya a **LON-DC1**, escriba lo siguiente en la ventana del **Símbolo del sistema** y, después, presione Entrar.

```
Ping LON-SVR2
```

Nota: El ping a **LON-SVR2** debería ser correcto.

Crear una regla de firewall de salida

1. Vaya a **LON-SVR2** y, después, haga clic en **Reglas de salida**.
2. Haga clic con el botón derecho en **Reglas de salida** y, después, haga clic en **Nueva regla**.
3. En el **Asistente para nueva regla de salida**, en la página **Tipo de regla**, haga clic en **Personalizada** y, después, haga clic en **Siguiente**.
4. En la página **Programa**, haga clic en **Todos los programas** y, después, haga clic en **Siguiente**.
5. En la página **Protocolo y puertos**, en la lista **Tipo de protocolo**, haga clic en **ICMPv4** y, después, haga clic en **Siguiente**.
6. En la página **Ámbito** haga clic en **Siguiente**.
7. En la página **Acción**, haga clic en **Bloquear la conexión** y, después, haga clic en **Siguiente**.
8. En la página **Perfil** haga clic en **Siguiente**.
9. En la página **Nombre**, en el cuadro de texto **Nombre**, escriba **Impedir la regla de ping** y, después, haga clic en **Finalizar**.
10. En el panel de navegación, expanda **Supervisión** y, después, haga clic en **Firewall**.
11. Compruebe que se creó la regla **Impedir la regla de ping**.

Probar la regla de firewall de salida

- En la ventana de **Windows PowerShell**, escriba lo siguiente y presione Entrar.

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

Nota: El resultado debería ser "Prueba de conexión: Error en la conexión de prueba al equipo 'LON-DC1': Error desconocido (0x2b2a)".

Restablecer las reglas de firewall en LON-SVR2

1. Vaya a la consola de **Firewall de Windows con seguridad avanzada** y, en el panel de navegación, haga clic en **Firewall de Windows con seguridad avanzada en el equipo local**.
2. En el panel **Acciones** haga clic en **Restaurar directiva predeterminada**.
3. En el cuadro de diálogo **Firewall de Windows con seguridad avanzada**, haga clic en **Sí** y, después, haga clic en **Aceptar**.
4. Vaya a la ventana de **Windows PowerShell**, escriba lo siguiente y presione Entrar.

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

Nota: El ping a **LON-DC1** debería ser correcto.

Lección 3

Configuración de IPsec

Contenidos:

Preguntas y respuestas

Pregunta: En su entorno, ¿está utilizando o utilizaría IPsec?

> **Respuesta:** Las respuestas serán diversas. Para comenzar el debate, puede sugerir el uso de IPsec en los sistemas de zona perimetral o para túneles VPN que pasan por el Internet público.

Recursos

¿Qué es IPsec?

 **Lecturas adicionales:** Para obtener más información, consulte "What Is IPSec?" en: http://aka.ms/G0crt8

Demostración: Creación y configuración de las reglas de seguridad de conexión

Pasos de la demostración

Permitir el tráfico ICMP en LON-SVR1 si es seguro

1. Vaya a **LON-SVR1**.
2. Abra el Administrador del servidor, haga clic en **Herramientas** y, después, haga clic en **Firewall de Windows con seguridad avanzada**.
3. En **Firewall de Windows con seguridad avanzada**, haga clic y, después, haga clic con el botón derecho en **Reglas de entrada**. Después, haga clic en **Nueva regla**.
4. En el cuadro de diálogo **Asistente para nueva regla de entrada**, haga clic en **Personalizada** y, después, haga clic en **Siguiente**.
5. En la página **Programa** haga clic en **Siguiente**.
6. En la página **Protocolos y puertos**, en la lista **Tipo de protocolo**, haga clic en **ICMPv4** y, después, haga clic en **Siguiente**.
7. En la página **Ámbito** haga clic en **Siguiente**.
8. En la página **Acción**, haga clic en **Permitir la conexión si es segura** y, después, haga clic en **Siguiente**.
9. En la página **Usuarios** haga clic en **Siguiente**.
10. En la página **Equipos** haga clic en **Siguiente**.
11. En la página **Perfil** haga clic en **Siguiente**.
12. En la página **Nombre**, en el cuadro **Nombre**, escriba **ICMPv4 permitido** y, después, haga clic en **Finalizar**.

Crear una regla de servidor a servidor en los servidores conectados

1. En **LON-SVR1**, en **Firewall de Windows con seguridad avanzada**, haga clic y, después, haga clic con el botón derecho en **Reglas de seguridad de conexión**. Después, haga clic en **Nueva regla**.
2. En el **Asistente para nueva regla de seguridad de conexión**, haga clic en **De servidor a servidor** y, después, haga clic en **Siguiente**.
3. En la página **Extremos** haga clic en **Siguiente**.
4. En la página **Requisitos**, haga clic en **Requerir autenticación para conexiones entrantes y salientes** y, después, haga clic en **Siguiente**.

5. En la página **Método de autenticación**, haga clic en **Avanzado** y, después, haga clic en **Personalizar**.
6. En el cuadro de diálogo **Personalizar métodos de autenticación avanzada** debajo de **Métodos de primera autenticación**, haga clic en **Agregar**.
7. En el cuadro de diálogo **Agregar método de primera autenticación**, haga clic en **Clave previamente compartida**, escriba **Secreta** y, después, haga clic en **Aceptar**.
8. En el cuadro de diálogo **Personalizar métodos de autenticación avanzada** haga clic en **Aceptar**.
9. En la página **Método de autenticación** haga clic en **Siguiente**.
10. En la página **Perfil** haga clic en **Siguiente**.
11. En la página **Nombre**, en el cuadro **Nombre**, escriba **Adatum de servidor a servidor** y, después, haga clic en **Finalizar**.

Crear una regla de servidor a servidor en LON-CL1

1. Vaya a **LON-CL1**.
2. Si fuera necesario inicie sesión como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
3. En Cortana, escriba **Firewall de Windows** y, después, haga clic en **Firewall de Windows con seguridad avanzada**.
4. Haga clic y, después, haga clic con el botón derecho en **Reglas de seguridad de conexión**. Después, haga clic en **Nueva regla**.
5. En el **Asistente para nueva regla de seguridad de conexión**, haga clic en **De servidor a servidor** y, después, haga clic en **Siguiente**.
6. En la página **Extremos** haga clic en **Siguiente**.
7. En la página **Requisitos**, haga clic en **Requerir autenticación para conexiones entrantes y salientes** y, después, haga clic en **Siguiente**.
8. En la página **Método de autenticación**, haga clic en **Avanzado** y, después, haga clic en **Personalizar**.
9. En el cuadro de diálogo **Personalizar métodos de autenticación avanzada** debajo de **Métodos de primera autenticación**, haga clic en **Agregar**.
10. En el cuadro de diálogo **Agregar método de primera autenticación**, haga clic en **Clave previamente compartida**, escriba **Secreta** y, después, haga clic en **Aceptar**.
11. En el cuadro de diálogo **Personalizar métodos de autenticación avanzada** haga clic en **Aceptar**.
12. En la página **Método de autenticación** haga clic en **Siguiente**.
13. En la página **Perfil** haga clic en **Siguiente**.
14. En la página **Nombre**, en el cuadro **Nombre**, escriba **Adatum de servidor a servidor** y, después, haga clic en **Finalizar**.

Probar la regla

1. En Cortana, escriba **cmd.exe** y presione Entrar.
2. En el símbolo del sistema, escriba **ping 172.16.0.11** y presione Entrar.
3. Vaya a Firewall de Windows con seguridad avanzada.
4. Expanda **Supervisión**, expanda **Asociaciones de seguridad** y, después, haga clic en **Modo principal**.
5. En el panel **Modo principal** haga doble clic en el elemento de la lista.

6. Consulte la información de **Modo principal** y, después, haga clic en **Aceptar**.
7. Haga clic en **Modo rápido**.
8. En el panel **Modo rápido** haga doble clic en el elemento de la lista.
9. Consulte la información de **Modo rápido** y, después, haga clic en **Aceptar**.

Lección 4

Datacenter Firewall

Contenidos:

Preguntas y respuestas

Pregunta: En su entorno, ¿prevé utilizar Datacenter Firewall o NSG?

Respuesta: Las respuestas variarán dependiendo de la complejidad de las redes de trabajo de los estudiantes.

Revisión del módulo y contenidos principales

Preguntas de revisión

Pregunta: Cuando se configura una regla de firewall para permitir el acceso a una aplicación en un puerto específico, ¿a qué perfil o perfiles de red debe aplicarse la regla?

Respuesta: La regla debe aplicarse al perfil de red desde el cual se espera el tráfico.

Pregunta: ¿Cuáles son las ventajas de utilizar Datacenter Firewall en un entorno de red privada?

Respuesta: Se pueden mencionar varias ventajas:

- Proporciona una solución de firewall basada en software que se integra con Microsoft System Center Virtual Machine Manager; puede ser administrada por los inquilinos o por los administradores y puede ampliarse para ayudar a las implementaciones de máquinas virtuales pequeñas y grandes.
- Las directivas de firewall que están asignadas a las máquinas virtuales se mueven con las máquinas virtuales cuando estas se desplazan a un host nuevo. Esto es posible porque:
  - Datacenter Firewall está implementado como un conmutador virtual de firewall de agente de host de puerto.
  - Las directivas de Datacenter Firewall asignadas por los inquilinos del proveedor de servicios, son independientes de la configuración del firewall de otros inquilinos.
  - Cada puerto de conmutador virtual se configura independientemente del host en el que se ejecuta la máquina virtual.
- Proporciona funciones de protección para las máquinas virtuales del inquilino que son independientes del sistema operativo invitado del inquilino.

Pregunta: ¿Para qué supuestos utiliza IPsec?

Respuesta: Las respuestas pueden variar, pero puede utilizar IPsec para:

- Proteger el tráfico de host a host
- Proteger el tráfico a servidores
- Usar L2TP
- Túneles de sitio a sitio (de puerta de enlace a puerta de enlace)
- Aplicar redes lógicas

Pregunta: Necesita garantizar que el tráfico esté cifrado y autenticado cuando pasa de un equipo de la red perimetral a un equipo de la red interna. El equipo de la red perimetral no es miembro de su bosque de AD DS. ¿Qué métodos de autenticación puede utilizar si intenta establecer una regla de IPsec entre estos dos equipos?

Respuesta: No puede utilizar la autenticación Kerberos porque el equipo perimetral no está en el bosque. Por lo tanto, puede utilizar certificados o una clave previamente compartida.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio: Configurar Firewall de Windows con Seguridad avanzada

Preguntas y respuestas

Pregunta: Quiere introducir una nueva aplicación que necesita para utilizar puertos específicos. ¿Qué información necesita para configurar Firewall de Windows con seguridad avanzada y de qué fuente se puede obtener esta información?

> **Respuesta:** Necesita saber qué puertos y direcciones IP usará la aplicación para que se pueda ejecutar sin dejar de estar protegida ante las amenazas de seguridad. Puede obtener esta información del proveedor de la aplicación.

Pregunta: Explique por qué **LON-CL1** puede conectarse tanto a **LON-SVR1** como a **LON-SVR2** en el laboratorio, pero **LON-SVR2** no se puede conectar a **LON-SVR1**.

> **Respuesta: LON-SVR1** está configurada para el aislamiento de servidor y, por lo tanto, solo los equipos que utilicen IPsec para proteger el tráfico de red se pueden conectar a ella. Debido a que **LON-CL1** está en la unidad organizativa Clientes seguros, se le aplica la directiva de solicitud de seguridad y, por lo tanto, solicitará IPsec cuando se conecte a otro servidor. **LON-SVR2** no tiene ningún tipo de seguridad configurada, así que **LON-CL1** puede conectarse a ella sin utilizar IPsec. **LON-SVR2** no se puede conectar a **LON-SVR1** porque **LON-SVR2** no está configurada para hacer solicitudes de seguridad y **LON-SVR1** rechaza todas las conexiones no seguras.

Módulo 13

Proteger el tráfico de red

Contenidos:

Lección 1

Configuración avanzada de DNS

Contenidos:

Preguntas y respuestas

Pregunta: Las directivas de DNS y RRL son nuevos en Windows Server 2016. ¿Cómo podría utilizar estas características nuevas en su entorno?

> **Respuesta:** Las respuestas variarán dependiendo del enfoque del alumno sobre la seguridad de la red. Los estudiantes con servidores DNS de Windows que se conectan al público generalmente implementarán RRL.

Recursos

Directivas de DNS

 **Lecturas adicionales:** Para obtener más información consulte «Set-DnsServerQueryResolutionPolicy» en: http://aka.ms/D9e1pv

Demostración: Configuración de DNSSEC

Pasos de la demostración

Configurar DNSSEC

1. Si todavía no lo ha hecho, inicie sesión en **LON-DC1** como **Adatum\Administrator** con la contraseña **Pa55w.rd**.
2. En el **Administrador del servidor**, haga clic en **Herramientas** y después en el cuadro de la lista desplegable haga clic en **DNS**.
3. En **DNS**, expanda **LON-DC1**, expanda **Zonas de búsqueda directa** y después seleccione y haga clic con el botón derecho en **Adatum.com**.
4. En el menú, haga clic en **DNSSEC>Firmar la zona**.
5. En el **Asistente para firmar zona**, haga clic en **Siguiente**.
6. Haga clic en **Personalizar los parámetros de firma de zona** y después haga clic en **Siguiente**.
7. En la página del **Maestro de claves** haga clic en **El servidor DNS LON-DC1 es el Maestro de claves** y, después, haga clic en **Siguiente**.
8. En la página **Clave de firma de clave (KSK)** haga clic en **Siguiente**.
9. En la página **Clave de firma de clave (KSK)** haga clic en **Agregar**.
10. En la página **Nueva clave de firma de clave (KSK)** haga clic en **Aceptar**.
11. En la página **Clave de firma de clave (KSK)** haga clic en **Siguiente**.
12. En la página **Clave de firmas de zona (ZSK)** haga clic en **Siguiente**.
13. En la página **Clave de firmas de zona (ZSK)** haga clic en **Agregar**.
14. En la página **Nueva clave de firma de zona (ZSK)** haga clic en **Aceptar**.
15. En la página **Clave de firmas de zona (ZSK)** haga clic en **Siguiente**.
16. En la página **Next Secure (NSEC)** haga clic en **Siguiente**.
17. En la página **Anclajes de veracidad (TA)** seleccione la casilla de verificación **Habilitar la distribución de anclajes de veracidad para esta zona** y después haga clic en **Siguiente**.
18. En la página **Parámetros de firma y sondeo** haga clic en **Siguiente**.

19. En la página **Extensiones de seguridad de DNS** haga clic en **Siguiente** y, después, haga clic en **Finalizar**.
20. En **Administrador de DNS**, expanda **Puntos de confianza**, expanda **com** y después haga clic en **Adatum**. Asegúrese de que existen los registros de recursos DNSKEY y que su estado es válido.
21. En el **Administrador del servidor**, haga clic en **Herramientas** y, después, en el cuadro de la lista desplegable haga clic en **Administración de directivas de grupo**.
22. En la **Consola de administración de directivas de grupo**, expanda **Bosque: Adatum.com**, expanda **Dominios**, expanda **Adatum.com**, haga clic con el botón derecho en **Directiva de dominio predeterminado** y después haga clic en **Editar**.
23. En el **Editor de administración de directivas de grupo**, debajo de **Configuración del equipo**, expanda **Directivas**, expanda **Configuración de Windows** y, después, haga clic en la carpeta **Directiva de resolución de nombres**.
24. En la sección **Crear reglas** en el campo **Sufijo** escriba **Adatum.com** para aplicar la regla al sufijo del espacio de nombres.
25. Seleccione ambas casillas de verificación **Habilitar DNSSEC en esta regla** y **Requerir que los clientes de DNS verifiquen que los datos de nombre y dirección han sido validados por el servidor DNS** y después haga clic en **Crear**.
26. Desplácese hacia abajo y después haga clic en **Aplicar**.
27. Cierre todas las ventanas abiertas.

Demostración: Configuración de directivas de DNS y RRL

Pasos de la demostración

Configurar directivas de DNS

1. En **LON-DC1**, haga clic en **Inicio** y, después, haga clic en **Windows PowerShell**.
2. Para crear una subred de cliente nueva para los clientes de Londres, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

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

3. Para crear una subred de cliente nueva para los clientes de París, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

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

4. Para crear un ámbito de zona nuevo para el Reino Unido, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

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

5. Para crear un ámbito de zona nuevo para Francia, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

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

6. Para crear un registro de recursos para encontrar el servidor web en el Reino Unido, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

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

7. Para crear un registro de recursos para encontrar el servidor web en Francia, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

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

8. Para crear la directiva DNS para el Reino Unido, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

```
Add-DnsServerQueryResolutionPolicy -Name “EnglandPolicy” -Action ALLOW -ClientSubnet
‘eq,LondonSubnet’ -ZoneScope ‘adatum_england,1’ -ZoneName “adatum.com” -PassThru
```

9. Para crear la directiva DNS para Francia, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

```
Add-DnsServerQueryResolutionPolicy -Name “FrancePolicy” -Action ALLOW -ClientSubnet
‘eq,ParisSubnet’ -ZoneScope ‘adatum_france,2’ -ZoneName “adatum.com” -PassThru
```

10. Para ver las directivas DNS definidas, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

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

11. Para comprobar que funciona la resolución de nombres, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

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

Nota: La dirección www.adatum.com debería convertirse en 172.16.0.11.

12. Para configurar una directiva basada en tiempo, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell, cambie el intervalo de tiempo de modo que París sea utilizado un 90 por ciento de las veces, a partir de las 9 de la mañana hasta las 5 de la tarde y después presione Entrar:

```
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
```

Nota: Asegúrese de que incluye la hora actual en el valor **-TimeofDay**.

13. Para probar la resolución de nombres, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

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

Nota: El 90 por ciento de las veces la dirección www.adatum.com se convertirá en 172.17.0.11. Si no lo hace la primera vez, vacíe la memoria caché DNS escribiendo **ipconfig/flushdns** en un símbolo del sistema y después inténtelo de nuevo.

Configurar RRL

1. Para habilitar RRL con la configuración predeterminada, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

```
Set-DNSServerRRL
```

2. Cuando se lo solicite el comando **Confirmar** escriba **S** y, después, presione Entrar.
3. Lea la advertencia que aparece.
4. Para ver la configuración de RRL, escriba el comando siguiente en el símbolo del sistema de Windows PowerShell y después presione Entrar:

```
Get-DNSServerRRL | FL
```

5. Compruebe que aparece la pantalla de configuración de RRL.

Lección 2

Examinar el tráfico de red con el Analizador de mensajes

Contenidos:

Preguntas y respuestas

Pregunta: ¿Para qué tipos de cuestiones de resolución de problemas sería más útil el uso del Analizador de mensajes?

( ) Acceso denegado a un archivo

( ) Acceso denegado a un recurso compartido

( ) Acceso denegado a un sitio web

( ) Conexiones lentas

( ) Todas las anteriores

Respuesta:

( ) Acceso denegado a un archivo

( ) Acceso denegado a un recurso compartido

( ) Acceso denegado a un sitio web

( ) Conexiones lentas

(√) Todas las anteriores

Comentarios:

El Analizador de mensajes evalúa más que el tráfico de red, incluidos los registros de eventos de Windows y los archivos de registro basados en texto.

Demostración: Instalación del Analizador de mensajes

Pasos de la demostración

1. Cambie a **LON-SVR1**.
2. Haga clic en **Inicio** y después haga clic en el **Explorador de archivos**. En el **Explorador de archivos**, expanda **Este PC**, expanda **Allfiles (D:)**, expanda **Labfiles** y después haga clic en la carpeta **Mod13**.
3. En la carpeta **Mod13** haga doble clic en **MessageAnalyzer64.msi**.
4. En el **Microsoft Message Analyzer Setup Wizard**, en la página **Welcome to the Microsoft Message Analyzer Setup Wizard** haga clic en **Next**.
5. En la página **End-User License Agreement** seleccione la casilla de verificación **I accept the terms in the License Agreement** y después haga clic en **Next**.
6. En la página **Microsoft Message Analyzer Optimization** haga clic en **Next**.
7. En la página **Ready to install Microsoft Message Analyzer** haga clic en **Install**.
8. En la página **Completed the Microsoft Message Analyzer Setup Wizard** haga clic en **Finish**.
9. Cuando termine la instalación, cierre todas las ventanas abiertas y después reinicie **LON-SVR1**.
10. Una vez que se reinicie el servidor, inicie sesión como **Adatum\Administrator** con la contraseña **Pa55w.rd**.

Demostración: Captura y análisis del tráfico con el Analizador de mensajes

Pasos de la demostración

Capturar tráfico de red no cifrado

1. En **LON-SVR1**, haga clic en **Inicio**, expanda la carpeta **Microsoft Message Analyzer** y después haga clic en **Microsoft Message Analyzer**.
2. En el cuadro de diálogo **Welcome to Microsoft Message Analyzer** haga clic en ambos **Do not update items** y **No, I do not want to participate** y después haga clic en **OK**.
3. Revise la página de inicio y después haga clic en **Start Local Trace**.
4. Cuando comience la captura, cambie a **LON-CL1**.
5. En **LON-CL1**, haga clic en **Inicio**, escriba **\\lon-svr1\d$\Labfiles\Mod13** y después presione Entrar:
6. Copie el archivo **MessageAnalyzer64.msi** en el escritorio local.
7. Cambie a **LON-SVR1**.
8. En el **Microsoft Message Analyzer**, haga clic en **Session** y después haga clic en **Stop**.

Examinar las herramientas de análisis

1. En el campo **Filter** escriba el filtro siguiente y después haga clic en **Apply**:

```
*address==172.16.0.40
```

2. Haga clic en el encabezado **Module** para ordenar por módulo.
3. Desplácese por el tráfico y luego muestre los distintos tipos de tráfico capturados.

 **Nota: Sugerencia:** Si pasa el cursor sobre el nombre de un módulo, la información sobre herramientas le mostrará el nombre completo.

4. Si aparece cualquier **DiagnosisTypes** haga clic en uno y después muestre el error.
5. Desplácese hacia abajo hasta que vea **SMB2** en la columna **Module**.
6. Agregue un filtro haciendo clic con el botón derecho en **SMB2** en la columna del **Module** y después haga clic en **Add 'Module' to Filter**.
7. En el filtro, cambie **OR** por **AND** y, después, haga clic en **Apply**.
8. Examine el tráfico SMB2.

Habilitar IPSEC en un Objeto de directiva de grupo (GPO)

1. Cambie a **LON-DC1** y después abra el **Administrador del servidor**.
2. En el **Administrador del servidor**, haga clic en **Herramientas** y después haga clic en **Administración de directivas de grupo**.
3. En la **Consola de administración de directivas de grupo**, expanda **Bosque: Adatum.com**, expanda **Dominios**, expanda **Adatum.com**, haga clic con el botón derecho en **Directiva de dominio predeterminado** y después haga clic en **Editar**.
4. En el **Editor de administración de directivas de grupo**, debajo de **Configuración del equipo**, expanda **Directivas**, expanda **Configuración de Windows**, expanda **Configuración de seguridad** y después haga clic en **Directivas de seguridad IP en Active Directory (ADATUM.COM)**.

5. Haga clic con el botón derecho en **Servidor (solicitar seguridad)** y, después, haga clic en **Asignar**.
6. Cierre todas las ventanas abiertas.
7. Cambie a **LON-SVR1**
8. Haga clic en **Inicio** y después haga clic en **Windows PowerShell**.
9. En el símbolo del sistema de Windows PowerShell escriba el comando siguiente y después presione Entrar:

```
GPUDPATE /Force
```

10. Cuando termine la actualización, cierre el símbolo del sistema de Windows PowerShell.
11. Cambie a **LON-CL1**.
12. Haga clic en **Inicio**, escriba **Windows PowerShell** y después haga clic en **Windows PowerShell**.
13. En el símbolo del sistema de Windows PowerShell escriba el comando siguiente y después presione Entrar:

```
GPUDPATE /Force
```

14. Cuando termine la actualización, cierre todas las ventanas abiertas.

Capturar tráfico de red cifrado

1. En **LON-SVR1**, en la **Barra de herramientas global**, haga clic en **Nueva sesión**.
2. En el cuadro de diálogo **Nueva sesión** haga clic en **Seguimiento en vivo**, haga clic en **Seleccionar escenario** y, después, haga clic en **Interfaces de red local (Win 8.1 y posterior)**.
3. Haga clic en **Inicio**.
4. Cuando comience la captura, cambie a **LON-CL1**.
5. En **LON-CL1**, haga clic en **Inicio**, escriba **\\lon-svr1\d$\Labfiles\Mod13** y después presione Entrar.
6. Copie el archivo **MessageAnalyzer64.msi** en el escritorio local. Cuando se le solicite, elija reemplazar el archivo en el escritorio.
7. Cambie a **LON-SVR1**.
8. En el **Microsoft Message Analyzer**, haga clic en **Session** y después haga clic en **Stop**.

Examinar las herramientas de análisis

1. En el campo **Filter** escriba el filtro siguiente y después haga clic en **Apply**:

```
*address==172.16.0.40
```

2. Haga clic en el encabezado **Module** para ordenar por módulo.
3. Tenga en cuenta que la mayor parte del tráfico capturado es del módulo ESP (Carga de seguridad encapsuladora IP).
4. Si aparece cualquier **DiagnosisTypes** haga clic en uno y después muestre el error.
5. Cierre todas las ventanas abiertas.

Deshabilitar IPSEC en el GPO

1. Cambie a **LON-DC1** y después abra el Administrador del servidor.
2. En el Administrador del servidor, haga clic en **Herramientas** y después haga clic en **Administración de directivas de grupo**.
3. En la **Consola de administración de directivas de grupo**, expanda **Bosque: Adatum.com**, expanda **Dominios**, expanda **Adatum.com**, haga clic con el botón derecho en **Directiva de dominio predeterminado** y después haga clic en **Editar**.
4. En el Editor de administración de directivas de grupo, debajo de **Configuración del equipo**, expanda **Directivas**, expanda **Configuración de Windows**, expanda **Configuración de seguridad** y después haga clic en **Directivas de seguridad IP en Active Directory (ADATUM.COM)**.
5. Haga clic con el botón derecho en **Servidor (solicitar seguridad)** y después haga clic en **Cancelar asignación**.
6. Cierre todas las ventanas abiertas.
7. Cambie a **LON-SVR1**.
8. Haga clic en **Inicio** y después haga clic en **Windows PowerShell**.
9. En el símbolo del sistema de Windows PowerShell escriba el comando siguiente y después presione Entrar:

```
GPUDPATE /Force
```

10. Cuando termine la actualización, cierre todas las ventanas abiertas.
11. Cambie a **LON-CL1**.
12. En Cortana, escriba **Windows PowerShell** y, después, haga clic en **Windows PowerShell**.
13. En el símbolo del sistema de Windows PowerShell escriba el comando siguiente y después presione Entrar:

```
GPUDPATE /Force
```

14. Cuando termine la actualización, cierre todas las ventanas abiertas.

Lección 3

Protección y análisis del tráfico SMB

Contenidos:

Preguntas y respuestas

Pregunta: ¿Qué riesgo conlleva dejar SMB 1.x habilitado en su entorno?

> **Respuesta:** SMB 1.x no es un protocolo seguro. Si está habilitado en su entorno, podría ser vulnerable a los ataques que se aprovechan de SMB 1.x.

Recursos

Introducción al protocolo de seguridad de SMB 3.1.1

 **Lecturas adicionales:** Para obtener más información, consulte «Microsoft Open Specifications Support Team Blog» en: http://aka.ms/Aldg7y

Demostración: Deshabilitación de SMB 1.0 y configuración del cifrado de SMB en recursos compartidos

Pasos de la demostración

Deshabilitar SMB 1.x en Windows 10

1. Cambie a **LON-CL1**.
2. Haga clic en **Inicio**, escriba **Windows PowerShell** y después haga clic en **Windows PowerShell**.
3. En el **Símbolo del sistema de Windows PowerShell** escriba el comando siguiente y después presione Entrar:

```
-EnableSMB Set-SmbServerConfiguration1protocolo $false.
```

4. Cuando se le solicite, presione **S** y, después, presione Entrar.
5. Cierre todas las ventanas abiertas.

Deshabilitar SMB 1.x en Windows Server 2016

1. Cambie a **LON-SVR1**.
2. Haga clic en **Inicio** y después haga clic en **Windows PowerShell**.
3. En el símbolo del sistema de Windows PowerShell escriba el comando siguiente y después presione Entrar:

```
-EnableSMB Set-SmbServerConfiguration1protocolo $false.
```

4. Cuando se le solicite, presione **S** y, después, presione Entrar.

Configurar un recurso compartido para cifrado de SMB

1. En el símbolo del sistema de Windows PowerShell, para crear el recurso compartido cifrado, escriba el comando siguiente y después presione Entrar:

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

2. En el símbolo del sistema de Windows PowerShell, para proporcionar permiso de control total sobre el recurso compartido a Todos, escriba el comando siguiente y después presione Entrar:

```
Grant-FileShareAccess –Name Mod13 -AccountName “Everyone” -AccessRight Full
```

Capturar tráfico SMB cifrado

1. En **LON-SVR1**, haga clic en **Inicio**, expanda la carpeta **Microsoft Message Analyzer** y después haga clic en **Microsoft Message Analyzer**.
2. En la página **Inicio** haga clic en **Start Local Trace**.
3. Cuando comience la captura, cambie a **LON-CL1**.
4. En **LON-CL1**, haga clic en **Inicio**, escriba **\\lon-svr1\Mod13** y después presione Entrar.
5. Copie el archivo **MessageAnalyzer64.msi** en el escritorio local. Cuando se le solicite, elija reemplazar el archivo en el escritorio.
6. Cambie a **LON-SVR1**.
7. En el **Microsoft Message Analyzer**, haga clic en **Session** y después haga clic en **Stop**.

Examinar las herramientas de análisis

1. En el filtro **Filter** escriba el siguiente filtro y después haga clic en **Apply**:

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

2. Haga clic en el encabezado **Summary** para ordenar por módulo.
3. Tenga en cuenta que la mayoría del tráfico SMB2 capturado es **TransformMessage, Encrypted**.

Revisión del módulo y contenidos principales

Preguntas de revisión

Pregunta: ¿En qué supuestos consideraría utilizar el Analizador de mensajes como una herramienta de solución de problemas?

Respuesta: Las respuestas pueden variar, pero puede utilizar el Analizador de mensajes para identificar el tráfico de red ilícito y solucionar problemas de red o de aplicaciones.

Pregunta: ¿Cuáles son los riesgos si deshabilita las comunicaciones SMB 1.0? ¿Cuáles son los riesgos si no deshabilita este protocolo antiguo?

Respuesta: SMB 1.0 es un protocolo antiguo que fue desarrollado sin la misma preocupación por la seguridad que SMB 3 o posterior. SMB 1.0 no impone el cifrado y es menos seguro. Sin embargo, algunas aplicaciones antiguas aún podrían requerir este protocolo, por lo que estas aplicaciones podrían fallar si desactiva SMB 1.0. Si no desactiva SMB 1.0, no obtendrá las características de seguridad disponibles con SMB 3 o posterior.

Preguntas y respuestas de la revisión de laboratorio

Laboratorio A: Protección de DNS

Preguntas y respuestas

Pregunta: ¿Por qué solo la supervisión del Modo principal mostró que se estaba utilizando cifrado?

Respuesta: El cifrado fue configurado solo para el protocolo ICMPv4 y la sesión de Modo rápido no utiliza ICMPv4.

Pregunta: ¿Por qué crearía una zona independiente para utilizar DNSSEC?

Respuesta: Las respuestas serán diversas. Una razón sería permitir ajustes diferentes para distintas zonas, de forma que si una zona está en peligro, las otras zonas no lo estarán necesariamente.

Laboratorio B: Microsoft Message Analyzer y cifrado SMB

Preguntas y respuestas

Pregunta: Con IPSEC aplicado a todo el tráfico, ¿ofrece una captura de red algún indicio de la finalidad del tráfico?

Respuesta: No. Todo el tráfico protegido por IPSEC aparece como tráfico ESP y no hay indicadores de lo que hay en los paquetes.

Pregunta: Para su entorno, ¿funcionaría mejor el método de cifrado IPSEC o SMB 3.1.1?

Respuesta: Las respuestas serán diversas. Puede configurar IPSEC para cifrar todo el tráfico de red, mientras que SMB 3.1.1 solo cifra el tráfico SMB de los recursos compartidos de Windows 10 o Windows Server 2016.

Módulo 14

Actualizar Windows Server

Contenidos:

Lección 1

Descripción general de WSUS

Contenidos:

Preguntas y respuestas

Pregunta: ¿Cuál de los productos siguientes puede actualizar WSUS?

( ) Microsoft Visual Studio 2010

( ) Microsoft Security Essentials

( ) Microsoft Office 2010

( ) Microsoft Silverlight

( ) Windows RT

Respuesta:

(√) Microsoft Visual Studio 2010

(√) Microsoft Security Essentials

(√) Microsoft Office 2010

(√) Microsoft Silverlight

(√) Windows RT

Comentarios:

WSUS es compatible con una amplia variedad de productos de Microsoft.

Recursos

Opciones de implementación del servidor de WSUS

 **Lecturas adicionales:** Para obtener más información, consulte: "Determine Capacity Requirements" en: http://aka.ms/Scktfu

Lección 2

Implementación de las actualizaciones con WSUS

Contenidos:

Preguntas y respuestas

Pregunta: ¿Utiliza varios grupos de equipos en su entorno de WSUS?

> **Respuesta:** Las respuestas serán diversas. Algunos estudiantes pueden probar manualmente las actualizaciones e implementarlas automáticamente después de su aprobación. Otros podrían utilizar una implementación automatizada de prueba antes de una implementación automatizada más amplia.

Recursos

Resolución de problemas de WSUS

 **Lecturas adicionales:** Para obtener más información, consulte: "Windows Server Update Services Tools and Utilities" en: http://aka.ms/Erqdqk

Demostración: Aprobar actualizaciones con WSUS

Pasos de la demostración

1. En **LON-SVR1**, haga clic en **Inicio**, haga clic en **Herramientas administrativas de Windows** y, después, haga clic en la consola **Windows Server Update Services**.
2. En **Windows Server Update Services**, expanda **LON-SVR1**, expanda **Actualizaciones**, haga clic en **Actualizaciones críticas**, en la lista desplegable **Estado** seleccione **Todo** y, después, haga clic en **Actualizar**.
3. Haga clic con el botón derecho en **Update for Windows 10 Version 1607 for x64-based Systems (KB3199209)** (Actualización para Windows 10, versión 1607, para sistemas basados en x64 [KB3199209]) y, después, haga clic en **Aprobar**.
4. En la ventana **Aprobar actualizaciones** en la lista desplegable **Todos los equipos** seleccione **Aprobada para su instalación**.
5. Haga clic en **Aceptar** y, después, haga clic en **Cerrar**.
6. Compruebe que en la columna **Aprobación** aparece **Instalar**.
7. Cierre la consola **Update Services**.

Revisión del módulo y contenidos principales

Preguntas de revisión

Pregunta: Su superior ha preguntado si todas las actualizaciones del sistema operativo Windows deberían aplicarse automáticamente cuando aparecen. ¿Recomienda un proceso alternativo?

> **Respuesta:** Todas las actualizaciones deben ser probadas antes de aplicarse en un entorno de producción. Es decir, primero debe implementar actualizaciones para un conjunto de equipos de prueba mediante el uso de WSUS.

Pregunta: Su organización implementa varias aplicaciones que no son aplicaciones de Microsoft. Un colega ha propuesto utilizar WSUS para implementar aplicaciones y actualizaciones del sistema operativo. ¿Hay algún problema potencial con el uso de WSUS?

> **Respuesta:** Sí. WSUS es una herramienta excelente para implementar actualizaciones para aplicaciones de Microsoft como Microsoft Office System y actualizaciones del sistema operativo Windows. Sin embargo, WSUS no implementa actualizaciones para todas las aplicaciones de Microsoft y no implementa actualizaciones para las aplicaciones que no son de Microsoft. Microsoft System Center Configuration Manager 2012 es la mejor elección cuando necesite implementar actualizaciones para las aplicaciones que no son de Microsoft.

Pregunta: ¿Por qué WSUS es más fácil de administrar en un dominio de Servicios de dominio de Active Directory (AD DS)?

> **Respuesta:** WSUS saca partido de la estructura de la unidad organizativa (UO) de AD DS para implementar la configuración del cliente mediante Directiva de grupo. También puede utilizar la configuración de Directiva de grupo para configurar los destinatarios del lado del cliente y determinar la pertenencia a un grupo de WSUS de un equipo cliente.

Herramientas

La siguiente tabla incluye las herramientas que se necesitan para este módulo.

Herramienta	Uso	Dónde encontrarla
Consola de administración de WSUS	Administrar WSUS	**Administrador del servidor** - Herramientas
Cmdlets WSUS de Windows PowerShell	Administrar WSUS desde la interfaz de línea de comandos	Windows PowerShell

Preguntas y respuestas de la revisión de laboratorio

Laboratorio: Implementar la Administración de actualizaciones

Preguntas y respuestas

Pregunta: Creó un grupo independiente para el departamento de investigación. ¿Por qué configuraría un grupo separado para una parte de los equipos de su organización?

Respuesta: El departamento de investigación podría tener consideraciones especiales o prácticas de seguridad que requieren un proceso diferente para probar y aprobar las actualizaciones que el resto de la organización. Además, otros departamentos pueden tener administradores a los que se les haya delegado la responsabilidad de administrar el proceso de aprobación de actualizaciones.

Pregunta: ¿Cuál es la ventaja de la configuración de un servidor de WSUS que sigue en la cadena?

Respuesta: Si una conexión lenta de red de área extensa (WAN) vincula el servidor de WSUS principal y el servidor que sigue en la cadena, el servidor de WSUS que sigue en la cadena solo descarga las actualizaciones una vez para los equipos cliente a los que presta servicios, en lugar de que cada equipo cliente descargue la actualización individualmente a través de la conexión WAN del servidor de WSUS principal.