Prepare la instalación del servidor SnapCenter

SnapCenter Software 4.9

NetApp
March 20, 2024

Tabla de contenidos

Prepare la instalación del servidor SnapCenter . . . 1
- Requisitos de dominio y grupo de trabajo . . . 1
- Requisitos de espacio y de tamaño . . . 1
- Requisitos del host SAN . . . 2
- Sistemas de almacenamiento y aplicaciones compatibles . . . 3
- Exploradores compatibles . . . 3
- Requisitos de conexión y puerto . . . 4
- Licencias SnapCenter . . . 7
- Métodos de autenticación para las credenciales . . . 10
- Conexiones de almacenamiento y credenciales . . . 11
- Autenticación multifactor (MFA) . . . 12

Prepare la instalación del servidor SnapCenter

Requisitos de dominio y grupo de trabajo

El servidor SnapCenter se puede instalar en sistemas que estén en un dominio o en un grupo de trabajo. El usuario utilizado para la instalación debe tener privilegios de administrador en el equipo en caso de grupo de trabajo y dominio.

Para instalar los plugins de SnapCenter Server y SnapCenter en hosts de Windows, debe usar uno de los siguientes elementos:

- **Dominio de Active Directory**

  Debe usar un usuario de dominio con derechos de administrador local. El usuario de dominio debe ser miembro del grupo de administrador local en el host de Windows.

- **Grupos de trabajo**

  Debe utilizar una cuenta local que tenga derechos de administrador local.

Mientras que las confianzas de dominio, bosques de multidominio y confianzas entre dominios son compatibles, los dominios entre bosques no lo son. La documentación de Microsoft acerca de Dominios y confianzas de Active Directory contiene más información.

Tras instalar el servidor SnapCenter, no debe cambiar el dominio en el que se encuentra el host SnapCenter. Si quita el host de SnapCenter Server del dominio en el que estaba cuando se instaló el servidor SnapCenter y, a continuación, intenta desinstalar SnapCenter Server, la operación de desinstalación fracasará.

Requisitos de espacio y de tamaño

Antes de instalar el servidor SnapCenter, debería estar familiarizado con los requisitos de espacio y tamaño. También debe aplicar las actualizaciones de sistema y seguridad disponibles.

Elemento	Requisitos
Sistemas operativos	Microsoft Windows Solo se admiten las versiones en inglés, alemán, japonés y chino simplificado de los sistemas operativos. Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".
Recuento de CPU mínimo	4 núcleos

Elemento	Requisitos
RAM mínimo	8 GB El grupo de buffers de MySQL Server utiliza el 20 por ciento de la RAM total.
Espacio mínimo en disco duro para el software y los registros del servidor SnapCenter	4 GB Si tiene el repositorio de SnapCenter en la misma unidad donde está instalado el servidor SnapCenter, se recomienda tener 10 GB.
Espacio en disco duro mínimo para el repositorio de SnapCenter	6 GB NOTA: Si tiene el servidor SnapCenter en la misma unidad en la que está instalado el repositorio de SnapCenter, se recomienda tener 10 GB.
Paquetes de software obligatorios	• Microsoft .NET Framework 4.7.2 o posterior • Windows Management Framework (WMF) 4.0 o posterior • PowerShell 4.0 o posterior Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla para sistemas heredados que no tienen conectividad a Internet".

Requisitos del host SAN

Si el host de SnapCenter forma parte de un entorno FC/iSCSI, puede que tenga que instalar software adicionales en el sistema para habilitar el acceso al almacenamiento ONTAP.

SnapCenter no incluye las utilidades de host ni DSM. Si el host de SnapCenter forma parte de un entorno SAN, puede tener que instalar y configurar el siguiente software:

- Utilidades de host

  Las utilidades de host son compatibles con FC e iSCSI, y le permiten usar MPIO en sus servidores Windows. Para obtener más información, consulte "Documentación de utilidades de host".

- Microsoft DSM para Windows MPIO

  Este software funciona con controladores Windows MPIO para gestionar varias rutas entre equipos host de Windows y NetApp.

Se requiere un DSM para configuraciones de alta disponibilidad.

Si estaba utilizando ONTAP DSM, debe migrar a Microsoft DSM. Para obtener más información, consulte "Cómo migrar desde ONTAP DSM a Microsoft DSM".

Sistemas de almacenamiento y aplicaciones compatibles

Debe conocer cuáles son los sistemas de almacenamiento, las aplicaciones y las bases de datos compatibles.

- SnapCenter admite ONTAP 8.3.0 y versiones posteriores para proteger sus datos.
- SnapCenter es compatible con Amazon FSX para ONTAP de NetApp y proteger sus datos de la versión de revisión P1 del software SnapCenter 4.5.

  Si utiliza Amazon FSX para ONTAP de NetApp, asegúrese de que los plugins del host del servidor SnapCenter se actualicen a 4.5 P1 o una versión posterior para realizar operaciones de protección de datos.

  Para obtener más información sobre Amazon FSX para ONTAP de NetApp, consulte "Documentación de Amazon FSX para ONTAP de NetApp".

- SnapCenter admite la protección de distintas aplicaciones y bases de datos.

  Para obtener información detallada sobre las aplicaciones y bases de datos compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

- SnapCenter 4,9 P1 y versiones posteriores admiten la protección de las cargas de trabajo de Oracle y Microsoft SQL en entornos de centro de datos definido por software (SDDC) de VMware Cloud on Amazon Web Services (AWS).

  Para obtener más información, consulte "Proteja las cargas de trabajo de Oracle y MS SQL mediante NetApp SnapCenter en entornos SDDC de VMware Cloud on AWS".

Exploradores compatibles

El software SnapCenter se puede usar en diversos exploradores.

- Cromo

  Si utiliza v66, es posible que no se pueda iniciar la interfaz gráfica de usuario de SnapCenter.

- Internet Explorer

  La interfaz de usuario de SnapCenter no se carga correctamente si se utiliza IE 10 o versiones anteriores. Debe actualizar a IE 11.

  - Tan solo se ofrece compatibilidad para las funciones de seguridad de nivel predeterminado.

    Realizar cambios en la configuración de seguridad de Internet Explorer puede dar como resultado problemas significativos de visualización para el explorador.

    - Es necesario deshabilitar la vista de compatibilidad de Internet Explorer.
- Microsoft Edge

Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Requisitos de conexión y puerto

Debe asegurarse de que se cumplan los requisitos de conexiones y puertos antes de instalar SnapCenter Server y los plugins de aplicación o base de datos.

- Las aplicaciones no pueden compartir los puertos.

  Cada puerto debe ser dedicado a la aplicación adecuada.

- En el caso de los puertos personalizables, puede seleccionar un puerto personalizado durante la instalación si no quiere usar el predeterminado.

  Puede cambiar un puerto de plugin después de la instalación usando el asistente Modify host.

- En el caso de los puertos fijos, tiene que aceptar el número de puerto predeterminado.
- Servidores de seguridad
    - Firewalls, proxies u otros dispositivos de red no deben interferir con las conexiones.
    - Si especifica un puerto personalizado al instalar SnapCenter, tendrá que añadir un regla de firewall en el host del plugin para dicho puerto en el cargador del plugin de SnapCenter.

En la tabla siguiente se enumeran los distintos puertos y sus valores predeterminados.

Tipo de puerto	Puerto predeterminado
Puerto SnapCenter	8146 (HTTPS), bidireccional, personalizable, como en la url *https://server:8146* Se usa para la comunicación entre el cliente SnapCenter (el usuario de SnapCenter) y el servidor SnapCenter. También se utiliza para establecer la comunicación de los hosts del plugin con SnapCenter Server. Para personalizar el puerto, consulte "Instale el servidor SnapCenter con el asistente de instalación."
Puerto de comunicación SMCore de SnapCenter	8145 (HTTPS), bidireccional, personalizable El puerto se utiliza para establecer la comunicación entre SnapCenter Server y los hosts en los que se han instalado los plugins de SnapCenter. Para personalizar el puerto, consulte "Instale el servidor SnapCenter con el asistente de instalación."

Tipo de puerto	Puerto predeterminado
Puerto MySQL	3306 (HTTPS), bidireccional El puerto se utiliza para establecer la comunicación entre SnapCenter y la base de datos del repositorio MySQL. Puede crear conexiones seguras desde el servidor SnapCenter al servidor MySQL. "Leer más" Para personalizar el puerto, consulte "Instale el servidor SnapCenter con el asistente de instalación."
Hosts de plugins de Windows	135 DE FEBRERO DE 445 (TCP) Además de los puertos 135 y 445, el intervalo de puertos dinámico especificado por Microsoft también debería estar abierto. Operaciones de instalación remota Utilice el servicio Instrumental de administración de Windows (WMI), que busca dinámicamente este intervalo de puertos. Para obtener información sobre el intervalo de puertos dinámicos admitido, consulte "Descripción general del servicio y requisitos de puertos de red para Windows" Los puertos se utilizan para establecer la comunicación entre SnapCenter Server y el host en el que se está instalando el plugin. Para insertar los archivos binarios de paquetes de plugins en los hosts de plugin de Windows, los puertos deben abrirse con cuidado en el host del plugin y se pueden cerrar después de su instalación.
Hosts de plugins de Linux o AIX	22 (SSH) Los puertos se utilizan para establecer la comunicación entre SnapCenter Server y el host en el que se está instalando el plugin. Los puertos los utiliza SnapCenter para copiar archivos binarios de paquetes de plugin en los hosts de plugin de Linux o AIX y se deben abrir o ejecutar desde el firewall o las iptables.

Tipo de puerto	Puerto predeterminado
Paquete de plugins de SnapCenter para Windows, paquete de plugins de SnapCenter para Linux o paquete de plugins de SnapCenter para AIX	8145 (HTTPS), bidireccional, personalizable El puerto se utiliza para establecer la comunicación entre SMCore y los hosts en los que se ha instalado el paquete de plugins. La ruta de comunicación también debe estar abierta entre el LIF de gestión de SVM y el servidor SnapCenter. Para personalizar el puerto, consulte "Añada hosts e instale el plugin de SnapCenter para Microsoft Windows" o. "Añada hosts e instale el paquete de plugins de SnapCenter para Linux o AIX."
Plugin de SnapCenter para base de datos de Oracle	27216, personalizable El puerto de JDBC predeterminado, lo utiliza el plugin para Oracle para conectarse a la base de datos de Oracle. Para personalizar el puerto, consulte "Añada hosts e instale el paquete de plugins de SnapCenter para Linux o AIX."
Plugins personalizados para SnapCenter	9090 (HTTPS), fija Se trata de un puerto interno que se usa solo en el host del plugin personalizado; no son obligatorias las excepciones de firewall. La comunicación entre SnapCenter Server y los plugins personalizados pasa a través del puerto 8145.
Puerto de comunicación del clúster de ONTAP o de SVM	443 (HTTPS), bidirectional80 (HTTP), bidireccional El puerto se utiliza en SAL (capa de abstracción del almacenamiento) para establecer la comunicación entre el host que ejecuta SnapCenter Server y SVM. Actualmente, el puerto también se utiliza en SAL en SnapCenter para los hosts del plugin de Windows para establecer la comunicación entre el host del plugin de SnapCenter y SVM.

Tipo de puerto	Puerto predeterminado
Plugin de SnapCenter para base de datos SAP HANA vCode Spell Checkports	3instance_number13 o 3instance_number15, HTTP o HTTPS, bidireccional y personalizable Para un tenant único de un contenedor de base de datos multitenant (MDC), el número del puerto termina en 13; para los que no son MDC, el número de puerto termina en 15. Por ejemplo, 32013 es el número de puerto para la instancia 20 y 31015 es el número de puerto para la instancia 10. Para personalizar el puerto, consulte "Añada hosts e instale paquetes de plugins en hosts remotos."
Puerto de comunicación del controlador de dominio	Consulte la documentación de Microsoft para identificar los puertos que se deben abrir en el firewall de un controlador de dominio para que la autenticación funcione correctamente. Es necesario abrir los puertos requeridos por Microsoft en el controlador de dominio para que SnapCenter Server, los hosts del plugin u otro cliente de Windows puedan autenticar los usuarios.

Para modificar los detalles del puerto, consulte "Modifique los hosts de plugins".

Licencias SnapCenter

SnapCenter requiere varias licencias para permitir la protección de datos de aplicaciones, bases de datos, sistemas de archivos y máquinas virtuales. El tipo de licencia de SnapCenter que instale dependerá del entorno de almacenamiento y de las funciones que desee utilizar.

Licencia	Donde se la requiere
Basado en controladora estándar de SnapCenter	Necesaria para cabinas FAS, AFF y All SAN (ASA) La licencia estándar de SnapCenter es una licencia basada en la controladora y se incluye como parte del paquete Premium. Si tiene la licencia de conjunto de SnapManager, también obtendrá el derecho de licencia estándar de SnapCenter. Si desea instalar SnapCenter a modo de prueba con almacenamiento FAS, AFF o ASA, puede obtener una licencia de evaluación Premium Bundle poniéndose en contacto con el representante de ventas. SnapCenter también se ofrece como parte del paquete de protección de datos. Si ha adquirido el A400 o una versión posterior, debe comprar el paquete de protección de datos.
SnapCenter basada en capacidad estándar	Necesario con ONTAP Select y Cloud Volumes ONTAP Si es cliente de Cloud Volumes ONTAP o ONTAP Select, necesita adquirir una licencia basada en capacidad por TB en función de los datos gestionados por SnapCenter. De forma predeterminada, SnapCenter envía una licencia de prueba integrada basada en capacidad estándar de SnapCenter de 90 días y 100 TB. Si desea obtener más detalles, póngase en contacto con el representante de ventas.
SnapMirror o SnapVault	ONTAP Se requieren licencias de SnapMirror o SnapVault si la replicación se habilita en SnapCenter.
SnapRestore	Necesario para restaurar y verificar backups. En sistemas de almacenamiento principales • Requerida en sistemas de destino de SnapVault para realizar la verificación remota y restaurar desde un backup • Requerida en sistemas de destino de SnapMirror para realizar la verificación remota

Licencia	Donde se la requiere
FlexClone	Necesario para clonar bases de datos y operaciones de verificación. En sistemas de almacenamiento principales y secundarios • Requerida en sistemas de destino de SnapVault para crear clones a partir de un backup de almacén secundario • Requerida en sistemas de destino de SnapMirror para crear clones a partir de un backup de SnapMirror secundario
Protocolos	• Licencia de iSCSI o FC para LUN • Licencia de CIFS para recursos compartidos de SMB • Licencia de NFS para VMDK de tipo NFS • Licencia de iSCSI o FC para VMDK de tipo VMFS Requerida en sistemas de destino de SnapMirror para suministrar datos si un volumen de origen no se encuentra disponible
Licencias estándar de SnapCenter (opcional)	Destinos secundarios Se recomienda, pero no es obligatorio, añadir licencias estándar de SnapCenter a destinos secundarios. Si las licencias estándar de SnapCenter están deshabilitadas en destinos secundarios, no puede usar SnapCenter para realizar un backup de los recursos en el destino secundario después de realizar una operación de conmutación al nodo de respaldo. Sin embargo, se requiere una licencia de FlexClone en destinos secundarios para realizar operaciones de clonado y verificación.

Las licencias avanzada y SnapCenter de servicios de archivos NAS de SnapCenter quedaron obsoletas y ya no están disponibles.

Debe instalar una o más licencias de SnapCenter. Para obtener información acerca de cómo agregar licencias, consulte "Añada licencias estándar basadas en controladora de SnapCenter" o. "Añada licencias basadas en capacidad estándar de SnapCenter".

Licencias de Single Mailbox Recovery (SMBR)

Si utiliza el plugin de SnapCenter para Exchange para gestionar bases de datos de Microsoft Exchange Server y Single Mailbox Recovery (SMBR), necesita una licencia adicional para SMBR, la cual debe adquirirse por separado en función del buzón de usuario.

NetApp® Single Mailbox Recovery ha llegado al final de la disponibilidad (EOA) el 12 de mayo de 2023. Para obtener más información, consulte "CPC-00507". NetApp continuará prestando soporte a los clientes que hayan adquirido capacidad, mantenimiento y soporte de sus buzones mediante números de referencia de marketing introducidos el 24 de junio de 2020, durante el periodo de concesión de soporte.

Single Mailbox Recovery de NetApp es un producto de partner que proporciona Ontrack. Ontrack PowerControls ofrece capacidades similares a las de Single Mailbox Recovery de NetApp. Los clientes pueden adquirir nuevas licencias de software Ontrack PowerControls y renovaciones de mantenimiento y soporte de Ontrack PowerControls desde Ontrack (hasta licensingteam@ontrack.com) para la recuperación granular de buzones después de la fecha EOA del 12 de mayo de 2023.

Métodos de autenticación para las credenciales

Las credenciales utilizan métodos de autenticación diferentes según la aplicación o el entorno. Las credenciales autentican a los usuarios para que puedan realizar operaciones de SnapCenter. Debe crear un conjunto de credenciales para instalar plugins y otros conjuntos para operaciones de protección de datos.

Autenticación de Windows

El método de autenticación de Windows autentica de acuerdo con Active Directory. Para la autenticación de Windows, se configura Active Directory fuera de SnapCenter. SnapCenter autentica sin configuración adicional. Se necesita una credencial de Windows para realizar ciertas tareas, como añadir hosts, instalar paquetes de plugins y programar trabajos.

Autenticación de dominio que no es de confianza

SnapCenter permite la creación de credenciales de Windows mediante usuarios y grupos que pertenecen a dominios que no son de confianza. Para que la autenticación se complete correctamente, debe registrar los dominios que no son de confianza en SnapCenter.

Autenticación de grupo de trabajo local

SnapCenter permite la creación de credenciales de Windows con grupos y usuarios de grupo de trabajo local. La autenticación de Windows para usuarios y grupos de grupos de trabajo locales no ocurre en el momento de la creación de credenciales de Windows, sino que se aplaza hasta que se realizan el registro de host y otras operaciones de host.

Autenticación de SQL Server

El método de autenticación de SQL se verifica de acuerdo con una instancia de SQL Server. Esto significa que debe detectarse una instancia de SQL Server en SnapCenter. Por lo tanto, antes de añadir una credencial de SQL, debe añadir un host, instalar paquetes de plugins y actualizar los recursos. Necesita la autenticación de SQL Server para realizar operaciones, como programar en SQL Server o detectar recursos.

Autenticación de Linux

El método de autenticación de Linux autentica con un host Linux. Necesita la autenticación de Linux durante el paso inicial de añadir el host Linux e instalar el paquete de plugins de SnapCenter para Linux de forma remota desde la interfaz gráfica de usuario de SnapCenter.

Autenticación AIX

El método de autenticación AIX autentica con un host AIX. Necesita la autenticación de AIX durante el paso inicial de añadir el host AIX e instalar el paquete de plugins de SnapCenter para AIX de forma remota desde la interfaz gráfica de usuario de SnapCenter.

Autenticación de base de datos de Oracle

El método de autenticación de base de datos de Oracle autentica con una base de datos de Oracle. Necesita una autenticación de base de datos de Oracle para realizar operaciones en la base de datos de Oracle si la autenticación de sistema operativo (SO) está deshabilitada en el host de bases de datos. Por lo tanto, antes de agregar una credencial de base de datos Oracle, debe crear un usuario de Oracle en la base de datos Oracle con privilegios sysdba.

Autenticación de Oracle ASM

El método de autenticación de Oracle ASM autentica con una instancia de Oracle Automatic Storage Management (ASM). Si debe acceder a la instancia de Oracle ASM y si la autenticación de sistema operativo (SO) está deshabilitada en el host de bases de datos, se necesita una autenticación de Oracle ASM. Por lo tanto, antes de añadir una credencial de Oracle ASM, debe crear un usuario de Oracle con privilegios sysasm en la instancia de ASM.

Autenticación de catálogo de RMAN

El método de autenticación de catálogo de RMAN autentica con la base de datos de catálogos de Oracle Recovery Manager (RMAN). Si configuró un mecanismo de catálogo externo y registró la base de datos en la base de datos de catálogos, debe añadir una autenticación de catálogo de RMAN.

Conexiones de almacenamiento y credenciales

Antes de ejecutar operaciones de protección de datos, debe configurar las conexiones de almacenamiento y añadir las credenciales que utilizarán SnapCenter Server y los plugins de SnapCenter.

- **Conexiones de almacenamiento**

  Las conexiones de almacenamiento conceden a SnapCenter Server y a los plugins de SnapCenter acceso al almacenamiento de ONTAP. La configuración de estas conexiones también implica la configuración de las funciones AutoSupport y del sistema de gestión de eventos (EMS).

- **Credenciales**

  - Administrador de dominio o cualquier miembro del grupo de administradores

    Especifique el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de

usuario son:

- *NetBIOS\Username*
- *Domain FQDN\Username*
- *Username@upn*

◦ Administrador local (sólo para grupos de trabajo)

Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host.

El formato válido para el campo Username es: *Username*

◦ Credenciales para grupos de recursos individuales

Si se configuran las credenciales para grupos de recursos individuales y el nombre de usuario no tiene privilegios de administrador completos, debe asignar al menos los privilegios de grupo de recursos y backup al nombre de usuario.

Autenticación multifactor (MFA)

Gestionar la autenticación multifactor (MFA)

Puede administrar la funcionalidad de autenticación multifactor (MFA) en el servidor del servicio de federación de Active Directory (AD FS) y el servidor SnapCenter.

Habilitar la autenticación multifactor (MFA)

Puede habilitar la funcionalidad MFA para SnapCenter Server con los comandos de PowerShell.

Acerca de esta tarea

- SnapCenter admite inicios de sesión basados en SSO cuando otras aplicaciones están configuradas en el mismo AD FS. En determinadas configuraciones de AD FS, SnapCenter puede requerir autenticación de usuario por motivos de seguridad, dependiendo de la persistencia de la sesión de AD FS.
- La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help command_name`. Como alternativa, también puede ver "Guía de referencia de cmdlets de SnapCenter Software".

Antes de empezar

- El servicio de Federación de Active Directory de Windows (AD FS) debe estar activo y en ejecución en el dominio correspondiente.
- Debe tener un servicio de autenticación multifactor compatible con AD FS, como Azure MFA, Cisco Duo, etc.
- La Marca de hora del servidor SnapCenter y AD FS debe ser la misma independientemente de la zona horaria.
- Adquirir y configurar el certificado de CA autorizado para SnapCenter Server.

El certificado DE CA es obligatorio por los siguientes motivos:

- Garantiza que las comunicaciones ADFS-F5 no se interrumpan porque los certificados autofirmados son únicos en el nivel de nodo.
- Garantiza que durante la actualización, reparación o recuperación ante desastres en una configuración independiente o de alta disponibilidad, el certificado autofirmado no se vuelva a crear, con lo que se evita la reconfiguración de la MFA.
- Garantiza resoluciones IP-FQDN.

  Para obtener información sobre el certificado de CA, consulte "Genere un archivo CSR de certificado de CA".

Pasos

1. Conéctese al host de Servicios de Federación de Active Directory (AD FS).
2. Descargue el archivo de metadatos de la federación de AD FS desde "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml.
3. Copie el archivo descargado en el servidor SnapCenter para habilitar la función MFA.
4. Inicie sesión en SnapCenter Server como usuario administrador de SnapCenter mediante PowerShell.
5. Con la sesión de PowerShell, genere el archivo de metadatos MFA de SnapCenter mediante el cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

   El parámetro path especifica la ruta al guardar el archivo de metadatos de MFA en el host del servidor de SnapCenter.

6. Copie el archivo generado en el host AD FS para configurar SnapCenter como entidad cliente.
7. Habilite la MFA para el servidor de SnapCenter mediante el `Set-SmMultiFactorAuthentication` cmdlet.
8. (Opcional) Compruebe el estado y la configuración de MFA mediante `Get-SmMultiFactorAuthentication` cmdlet.
9. Vaya a la consola de administración de Microsoft (MMC) y realice los pasos siguientes:
   a. Haga clic en **Archivo** > **Agregar o quitar Snapin**.
   b. En la ventana Agregar o quitar complementos, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
   c. En la ventana del complemento certificados, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
   d. Haga clic en **raíz de consola** > **certificados – Equipo local** > **personal** > **certificados**.
   e. Haga clic con el botón derecho del ratón en el certificado de CA vinculado a SnapCenter y, a continuación, seleccione **todas las tareas** > **Administrar claves privadas**.
   f. En el asistente de permisos, realice los siguientes pasos:
      i. Haga clic en **Agregar**.
      ii. Haga clic en **Ubicaciones** y seleccione el host en cuestión (parte superior de la jerarquía).
      iii. Haga clic en **Aceptar** en la ventana emergente **Ubicaciones**.
      iv. En el campo de nombre de objeto, introduzca 'IIS_IUSRS' y haga clic en **comprobar nombres** y haga clic en **Aceptar**.

      Si la comprobación se realiza correctamente, haga clic en **Aceptar**.

10. En el host AD FS, abra el asistente de administración de AD FS y realice los siguientes pasos:
    a. Haga clic con el botón derecho del ratón en **Fideicomiso del Partido** > **Agregar confianza del Partido** > **Inicio**.
    b. Seleccione la segunda opción y examine el archivo de metadatos de MFA de SnapCenter y haga clic en **Siguiente**.
    c. Especifique un nombre para mostrar y haga clic en **Siguiente**.
    d. Elija una política de control de acceso según sea necesario y haga clic en **Siguiente**.
    e. Seleccione la configuración en la siguiente ficha para Predeterminado.
    f. Haga clic en **Finalizar**.

    SnapCenter se refleja ahora como una parte que confía en el nombre para mostrar proporcionado.

11. Seleccione el nombre y realice los siguientes pasos:
    a. Haga clic en **Editar directiva de emisión de reclamaciones**.
    b. Haga clic en **Agregar regla** y haga clic en **Siguiente**.
    c. Especifique un nombre para la regla de reclamación.
    d. Seleccione **Active Directory** como almacén de atributos.
    e. Seleccione el atributo como **Nombre-principal-usuario** y el tipo de reclamación saliente como **Nombre-ID**.
    f. Haga clic en **Finalizar**.
12. Ejecute los siguientes comandos de PowerShell en el servidor ADFS.

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None

Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. Realice los siguientes pasos para confirmar que los metadatos se han importado correctamente.
    a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía y seleccione **Propiedades**.
    b. Asegúrese de que se rellenan los campos puntos finales, identificadores y firma.
14. Cierre todas las pestañas del navegador y vuelva a abrir un navegador para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

La funcionalidad MFA de SnapCenter también se puede habilitar usando las API de REST.

Para obtener información sobre la solución de problemas, consulte "Los intentos de inicio de sesión simultáneos en varias pestañas muestran un error MFA".

Actualizar metadatos de MFA de AD FS

Debe actualizar los metadatos de la MFA de AD FS en SnapCenter cada vez que haya alguna modificación en el servidor de AD FS, como la actualización, la renovación de certificados de CA, la recuperación ante desastres, etc.

Pasos

1. Descargue el archivo de metadatos de la federación de AD FS desde "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copie el archivo descargado en el servidor SnapCenter para actualizar la configuración de MFA.
3. Actualice los metadatos de AD FS en SnapCenter ejecutando el siguiente cmdlet:

   ```
   Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
   ```

4. Cierre todas las pestañas del navegador y vuelva a abrir un navegador para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

Actualice los metadatos de MFA de SnapCenter

Debe actualizar los metadatos del MFA de SnapCenter en AD FS cada vez que haya alguna modificación en el servidor ADFS como, por ejemplo, la reparación, la renovación de certificados de CA, la recuperación ante desastres, etc.

Pasos

1. En el host AD FS, abra el asistente de administración de AD FS y realice los siguientes pasos:
   a. Haga clic en **fideicomisos de parte**.
   b. Haga clic con el botón derecho del ratón en la confianza de la parte que confía que se creó para SnapCenter y haga clic en **Eliminar**.

      Se mostrará el nombre definido por el usuario de la confianza de la parte que confía.

   c. Habilite la autenticación multifactor (MFA).

      Consulte "Active la autenticación multifactor".
2. Cierre todas las pestañas del navegador y vuelva a abrir un navegador para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

Deshabilitar la autenticación multifactor (MFA)

Pasos

1. Deshabilite la MFA y borre los archivos de configuración que se crearon cuando se habilitó MFA con el `Set-SmMultiFactorAuthentication` cmdlet.
2. Cierre todas las pestañas del navegador y vuelva a abrir un navegador para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

Gestione la autenticación multifactor (MFA) con la API de REST, PowerShell y SCCLI

El inicio de sesión de MFA es compatible con el explorador, la API de REST, PowerShell y SCCLI. MFA es compatible a través de un gestor de identidades de AD FS. Puede habilitar MFA, deshabilitar MFA y configurar MFA desde la GUI, la API de REST, PowerShell y SCCLI.

Configure AD FS como OAuth/OIDC

- Configurar AD FS usando el asistente de la GUI de Windows*

1. Vaya a **Server Manager Dashboard** > **Tools** > **ADFS Management**.
2. Vaya a **ADFS** > **Grupos de aplicaciones**.
   a. Haga clic con el botón derecho en **Grupos de aplicaciones**.
   b. Seleccione **Agregar grupo de aplicaciones** e introduzca **Nombre de la aplicación**.
   c. Seleccione **Aplicación de servidor**.
   d. Haga clic en **Siguiente**.
3. Copiar **Identificador de Cliente**.

   Este es el ID de cliente. .. Agregar URL de devolución de llamada (URL del servidor de SnapCenter) en URL de redireccionamiento. .. Haga clic en **Siguiente**.

4. Selecciona **Generar secreto compartido**.

   Copie el valor secreto. Este es el secreto del cliente. .. Haga clic en **Siguiente**.

5. En la página **Resumen**, haz clic en **Siguiente**.
   a. En la página **Completo**, haz clic en **Cerrar**.
6. Haga clic con el botón derecho en el recién agregado **Grupo de aplicaciones** y seleccione **Propiedades**.
7. Seleccione **Añadir aplicación** en Propiedades de la aplicación.
8. Haga clic en **Añadir aplicación**.

   Seleccione Web API y haga clic en **Siguiente**.

9. En la página Configurar API Web, introduzca la URL del servidor SnapCenter y el identificador de cliente creados en el paso anterior en la sección Identificador.
   a. Haga clic en **Agregar**.
   b. Haga clic en **Siguiente**.
10. En la página **Elegir Política de Control de Acceso**, selecciona la política de control en función de tus requisitos (por ejemplo, Permitir a todos y requerir MFA) y haz clic en **Siguiente**.
11. En la página **Configurar permiso de aplicación**, por defecto se selecciona openid como un ámbito, haga clic en **Siguiente**.
12. En la página **Resumen**, haz clic en **Siguiente**.

    En la página **Completo**, haz clic en **Cerrar**.

13. En la página **Sample Application Properties**, haz clic en **OK**.
14. Token JWT emitido por un servidor de autorización (AD FS) y destinado a ser consumido por el recurso.

    La reclamación 'aud' o de público de este token debe coincidir con el identificador del recurso o la API web.

15. Edite la WebAPI seleccionada y compruebe que la URL de devolución de llamada (URL del servidor de SnapCenter) y el identificador de cliente se han agregado correctamente.

    Configure OpenID Connect para proporcionar un nombre de usuario como reclamaciones.

16. Abra la herramienta **AD FS Management** ubicada en el menú **Tools** en la parte superior derecha del Administrador del servidor.
    a. Seleccione la carpeta **Grupos de aplicaciones** en la barra lateral izquierda.
    b. Seleccione la API web y haga clic en **EDITAR**.
    c. Vaya a la pestaña Reglas de transformación de emisión
17. Haga clic en **Agregar regla**.
    a. Seleccione el **Enviar atributos LDAP como reclamaciones** en el menú desplegable de la plantilla de regla de reclamación.
    b. Haga clic en **Siguiente**.
18. Introduzca el nombre de la regla de reclamación *.
    a. Seleccione **Active Directory** en el menú desplegable del almacén de atributos.
    b. Seleccione **User-Principal-Name** en el menú desplegable **LDAP Attribute** y **UPN** en el menú desplegable O*utgoing Claim Type*.
    c. Haga clic en **Finalizar**.

Crear grupo de aplicaciones con comandos de PowerShell

Puede crear el grupo de aplicaciones, la API web y agregar el alcance y las reclamaciones mediante comandos de PowerShell. Estos comandos están disponibles en formato de script automatizado. Para obtener más información, consulte <link to KB article>.

1. Cree el nuevo grupo de aplicaciones en AD FS mediante el siguiente comamnd.

   ```
   New-AdfsApplicationGroup -Name $ClientRoleIdentifier
   -ApplicationGroupIdentifier $ClientRoleIdentifier
   ```

   `ClientRoleIdentifier` nombre del grupo de aplicaciones

   `redirectURL` URL válida para redirección después de la autorización

2. Cree la aplicación de servidor de AD FS y genere el secreto de cliente.

   ```
   Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
   -ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
   -Identifier $identifier -GenerateClientSecret
   ```

3. Cree la aplicación API Web de ADFS y configure el nombre de política que debe utilizar.

   ```
   $identifier = (New-Guid).Guid

   Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
   -Name "App Web API"

   -Identifier $identifier -AccessControlPolicyName "Permit everyone"
   ```

4. Obtenga el ID de cliente y el secreto de cliente del resultado de los siguientes comandos, porque solo se muestra una vez.

   ```
   "client_id = $identifier"
   ```

```
"client_secret: "$($ADFSApp.ClientSecret)
```

5. Otorgue a la aplicación AD FS los permisos allatclaims y openid.

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
-ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. Escriba el archivo de reglas de transformación.

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. Asigne un nombre a la aplicación Web API y defina sus reglas de transformación de emisión mediante un archivo externo.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Actualizar tiempo de caducidad del token de acceso

Puede actualizar el tiempo de caducidad del token de acceso mediante el comando PowerShell.

Acerca de esta tarea

- Un token de acceso solo se puede utilizar para una combinación específica de usuario, cliente y recurso. Los tokens de acceso no se pueden revocar y son válidos hasta su vencimiento.
- De forma predeterminada, el tiempo de caducidad de un token de acceso es de 60 minutos. Este tiempo de caducidad mínimo es suficiente y se escala. Debe proporcionar el valor suficiente para evitar trabajos críticos para el negocio en curso.

Paso

Para actualizar el tiempo de caducidad del token de acceso para un grupo de aplicaciones WEBAPI, utilice el siguiente comando en el servidor AD FS.

+ `Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"`

Obtenga el token portador de AD FS

Debe rellenar los parámetros mencionados a continuación en cualquier cliente REST (como Postman) y le pedirá que rellene las credenciales de usuario. Además, debe introducir la autenticación de segundo factor (algo que tiene y algo que es) para obtener el token de portador.

+ La validez del token portador se puede configurar desde el servidor de AD FS por aplicación y el período de validez predeterminado es de 60 minutos.

Campo	Valor
Tipo de concesión	Código de autorización
URL de devolución de llamada	Introduzca la URL base de la aplicación si no tiene una URL de devolución de llamada.
URL de autenticación	[adfs-domain-name]/adfs/oauth2/authorized
URL de token de acceso	[adfs-domain-name]/adfs/oauth2/token
ID del cliente	Introduzca el ID de cliente de AD FS
Secreto de cliente	Introduzca el secreto de cliente de AD FS
Ámbito	ID de código abierto
Autenticación de cliente	Enviar como cabecera de AUTENTICACIÓN básica
Recurso	En la pestaña **Opciones avanzadas**, agregue el campo Recurso con el mismo valor que la URL de devolución de llamada, que viene como un valor “aud” en el token JWT.

Configure MFA en SnapCenter Server mediante PowerShell, SCCLI y la API de REST

Es posible configurar la MFA en SnapCenter Server mediante PowerShell, SCCLI y la API DE REST.

Autenticación CLI MFA de SnapCenter

En PowerShell y SCCLI, el cmdlet existente (Open-SmConnection) se amplía con un campo más llamado “AccessToken” para utilizar el token portador para autenticar al usuario.

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

Una vez ejecutado el cmdlet anterior, se crea una sesión para que el usuario respectivo ejecute más cmdlets de SnapCenter.

Autenticación de la API de REST MFA de SnapCenter

Use el token portador en el formato *Authorization=Bearer <access token>* en el cliente de la API REST (como Postman o Swagger) y mencione el nombre de rol del usuario en el encabezado para obtener una respuesta exitosa de SnapCenter.

Flujo de trabajo de la API de REST de MFA

Cuando MFA se configura con AD FS, debe autenticarse mediante un token de acceso (portador) para acceder a la aplicación SnapCenter mediante cualquier API REST.

Acerca de esta tarea

- Puede utilizar cualquier cliente de REST, como Postman, Swagger UI o FireCamp.
- Obtenga un token de acceso y utilícelo para autenticar las solicitudes posteriores (API de REST de SnapCenter) para realizar cualquier operación.
- Pasos*

Para autenticarse a través de AD FS MFA

1. Configure el cliente REST para que llame al punto final de AD FS para obtener el token de acceso.

   Cuando pulse el botón para obtener un token de acceso para una aplicación, se le redirigirá a la página SSO de AD FS, donde debe proporcionar sus credenciales de AD y autenticarse con MFA. 1. En la página SSO de AD FS, escriba su nombre de usuario o correo electrónico en el cuadro de texto Nombre de usuario.

   + Los nombres de usuario deben formatearse como usuario@dominio o dominio\usuario.

2. En el cuadro de texto Contraseña, escriba la contraseña.
3. Haga clic en **Iniciar sesión**.
4. En la sección **Opciones de inicio de sesión**, selecciona una opción de autenticación y autentica (dependiendo de tu configuración).
   - Push: Aprueba la notificación push que se envía al teléfono.
   - Código QR: Utilice la aplicación móvil AUTH Point para escanear el código QR y, a continuación, escriba el código de verificación que se muestra en la aplicación
   - Contraseña de un solo uso: Escriba la contraseña de un solo uso para el token.
5. Después de la autenticación correcta, se abrirá una ventana emergente que contiene el acceso, el ID y el token de refrescamiento.

   Copie el token de acceso y utilícelo en la API de REST de SnapCenter para realizar la operación.

6. En la API de REST, debe pasar el token de acceso y el nombre de rol en la sección de encabezado.
7. SnapCenter valida este token de acceso desde AD FS.

Si es un token válido, SnapCenter lo decodifica y obtiene el nombre de usuario.

8. Con el nombre de usuario y el nombre de rol, SnapCenter autentica al usuario para ejecutar la API.

   Si la autenticación se realiza correctamente, SnapCenter devuelve el resultado si se muestra un mensaje de error.

Habilite o deshabilite la funcionalidad MFA de SnapCenter para la API de REST, la interfaz de línea de comandos y la interfaz gráfica de usuario

GUI

- Pasos*
  1. Inicie sesión en el servidor de SnapCenter como administrador de SnapCenter.
  2. Haga clic en **Ajustes** > **Ajustes globales** > **Ajustes de autenticación multifactorAuthentication(MFA)**
  3. Seleccione la interfaz (GUI/RST API/CLI) para habilitar o deshabilitar el inicio de sesión MFA.

Interfaz PowerShell

- Pasos*

  1. Ejecute los comandos de PowerShell o la CLI para habilitar la MFA en la interfaz gráfica de usuario, la API de REST, PowerShell y SCCLI.

     ```
     Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
     -IsCliMFAEnabled -Path
     ```

     El parámetro PATH especifica la ubicación del archivo xml de metadatos de MFA de AD FS.

  Habilita la MFA para la interfaz gráfica de usuario de SnapCenter, la API de REST, PowerShell y SCCLI configuradas con la ruta de archivo de metadatos de AD FS especificada.

  1. Compruebe el estado y la configuración de MFA mediante `Get-SmMultiFactorAuthentication` cmdlet.

Interfaz SCCLI

- Pasos*

  1. `# sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
  2. `# sccli Get-SmMultiFactorAuthentication`

API REST

1. Ejecute la siguiente API posterior para habilitar la MFA en la interfaz gráfica de usuario, la API de REST, PowerShell y SCCLI.

Parámetro	Valor

Dirección URL solicitada	/api/4,9/settings/multifactorauthentication
Método HTTP	Publicación
Cuerpo de la solicitud	{ «IsGuiMFAEnabled»: Falso, «IsRestApiMFAEnabled»: Verdadero, «IsCliMFAEnabled»: Falso, ADFSConfigFilePath: C:\\ADFS_metadata\\abc.xml }
Cuerpo de respuesta	{ «MFAConfiguration»: { «IsGuiMFAEnabled»: Falso, «ADFSConfigFilePath»: «C:\\ADFS_metadata\\abc.xml», «SCConfigFilePath»: Null, «IsRestApiMFAEnabled»: Verdadero, «IsCliMFAEnabled»: Falso, «ADFSHostName»: «win-adfs-sc49.winscedom2.com» } }

2. Compruebe el estado y la configuración de MFA mediante la siguiente API.

Parámetro	Valor
Dirección URL solicitada	/api/4,9/settings/multifactorauthentication
Método HTTP	Obtenga
Cuerpo de respuesta	{ «MFAConfiguration»: { «IsGuiMFAEnabled»: Falso, «ADFSConfigFilePath»: «C:\\ADFS_metadata\\abc.xml», «SCConfigFilePath»: Null, «IsRestApiMFAEnabled»: Verdadero, «IsCliMFAEnabled»: Falso, «ADFSHostName»: «win-adfs-sc49.winscedom2.com» } }