



# **Prepárese para instalar el servidor SnapCenter**

SnapCenter software

NetApp  
November 06, 2025

# Tabla de contenidos

- Prepárese para instalar el servidor SnapCenter ..... 1
  - Requisitos para instalar SnapCenter Server ..... 1
    - Requisitos de dominio y grupo de trabajo para el host de Windows ..... 1
    - Requisitos de espacio y tamaño ..... 1
    - Requisitos del host SAN ..... 3
    - Requisitos del navegador..... 3
    - Requisitos del puerto ..... 3
  - Regístrese para acceder al SnapCenter software ..... 8
- Autenticación multifactor (MFA) ..... 9
  - Administrar la autenticación multifactor (MFA) ..... 9
  - Administrar la autenticación multifactor (MFA) mediante Rest API, PowerShell y SCCLI..... 12
  - Configurar MFA en SnapCenter Server mediante PowerShell, SCCLI y API REST ..... 16

# Prepárese para instalar el servidor SnapCenter

## Requisitos para instalar SnapCenter Server

Antes de instalar SnapCenter Server en un host Windows o Linux, debe revisar y asegurarse de que se cumplan todos los requisitos para su entorno.

### Requisitos de dominio y grupo de trabajo para el host de Windows

El servidor SnapCenter se puede instalar en un host Windows que esté en un dominio o en un grupo de trabajo.

El usuario con privilegios de administrador puede instalar el servidor SnapCenter .

- Dominio de Active Directory: debe utilizar un usuario de dominio con derechos de administrador local. El usuario del dominio debe ser miembro del grupo de administradores locales en el host de Windows.
- Grupos de trabajo: debe utilizar una cuenta local que tenga derechos de administrador local.

Si bien se admiten las confianzas de dominio, los bosques multidominio y las confianzas entre dominios, no se admiten los dominios entre bosques. La documentación de Microsoft sobre dominios y confianzas de Active Directory contiene más información.



Después de instalar SnapCenter Server, no debe cambiar el dominio en el que se encuentra el host de SnapCenter . Si elimina el host de SnapCenter Server del dominio en el que se encontraba cuando se instaló SnapCenter Server y luego intenta desinstalar SnapCenter Server, la operación de desinstalación falla.

### Requisitos de espacio y tamaño

Debe estar familiarizado con los requisitos de espacio y tamaño.

| Artículo               | Requisitos del host de Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Requisitos del host Linux                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sistemas operativos    | <p>Microsoft Windows</p> <p>Solo se admiten las versiones en inglés, alemán, japonés y chino simplificado de los sistemas operativos.</p> <p>Para obtener la información más reciente sobre las versiones compatibles, consulte <a href="https://imt.netapp.com/matrix/imt.jsp?components=121033;&amp;solution=1258&amp;isHWU&amp;src=IMT">https://imt.netapp.com/matrix/imt.jsp?components=121033;&amp;solution=1258&amp;isHWU&amp;src=IMT</a> [Herramienta de matriz de interoperabilidad de NetApp] .</p> | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux (RHEL) 8 y 9</li><li>• Servidor empresarial SUSE Linux (SLES) 15</li></ul> <p>Para obtener la información más reciente sobre las versiones compatibles, consulte <a href="https://imt.netapp.com/matrix/imt.jsp?components=121032;&amp;solution=1258&amp;isHWU&amp;src=IMT">https://imt.netapp.com/matrix/imt.jsp?components=121032;&amp;solution=1258&amp;isHWU&amp;src=IMT</a> [Herramienta de matriz de interoperabilidad de NetApp] .</p> |
| Cantidad mínima de CPU | 4 núcleos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 4 núcleos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Artículo                                                                              | Requisitos del host de Windows                                                                                                                                                                                                                       | Requisitos del host Linux |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| RAM mínima                                                                            | 8 GB <div>  <p>El grupo de búfer del servidor MySQL utiliza el 20 por ciento de la RAM total.</p> </div>                                                            | 8 GB                      |
| Espacio mínimo en el disco duro para el software y los registros de SnapCenter Server | 7 GB <div>  <p>Si tiene el repositorio de SnapCenter en la misma unidad donde está instalado SnapCenter Server, se recomienda tener 15 GB.</p> </div>               | 15 GB                     |
| Espacio mínimo en el disco duro para el repositorio de SnapCenter                     | 8 GB <div>  <p>NOTA: Si tiene el servidor SnapCenter en la misma unidad donde está instalado el repositorio de SnapCenter , se recomienda tener 15 GB.</p> </div> | No aplicable              |

| Artículo                        | Requisitos del host de Windows                                                                                                                                                                                                                                                                                                                                                                                      | Requisitos del host Linux                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Paquetes de software necesarios | <ul style="list-style-type: none"> <li>• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores)</li> <li>• PowerShell 7.4.2 o posterior</li> </ul> <p>Para obtener información de solución de problemas específicos de .NET, consulte <a href="#">"La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conectividad a Internet"</a> .</p> | <ul style="list-style-type: none"> <li>• .NET Framework 8.0.12 (y todos los parches 8.0.x posteriores)</li> <li>• PowerShell 7.4.2 o posterior</li> <li>• Nginx es un servidor web que se puede utilizar como proxy inverso</li> <li>• Pam-devel</li> </ul> <p>PAM (Módulos de autenticación conectables) es una herramienta de seguridad del sistema que permite a los administradores del sistema establecer políticas de autenticación sin tener que volver a compilar los programas que realizan la autenticación.</p> |



ASP.NET Core necesita IIS\_IUSRS para acceder al sistema de archivos temporal en SnapCenter Server en Windows.

## Requisitos del host SAN

SnapCenter no incluye utilidades de host ni un DSM. Si el host de SnapCenter es parte de un entorno SAN (FC/iSCSI), es posible que deba instalar y configurar software adicional en el host del servidor SnapCenter .

- Utilidades de host: las utilidades de host admiten FC e iSCSI y le permiten utilizar MPIO en sus servidores Windows. ["Más información"](#) .
- Microsoft DSM para Windows MPIO: este software funciona con controladores MPIO de Windows para administrar múltiples rutas entre NetApp y computadoras host de Windows. Se requiere un DSM para configuraciones de alta disponibilidad.



Si estaba utilizando ONTAP DSM, debería migrar a Microsoft DSM. Para obtener más información, consulte ["Cómo migrar de ONTAP DSM a Microsoft DSM"](#) .

## Requisitos del navegador

El SnapCenter software es compatible con Chrome 125 y posteriores y Microsoft Edge 110.0.1587.17 y posteriores.

## Requisitos del puerto

El SnapCenter software requiere diferentes puertos para la comunicación entre diferentes componentes.

- Las aplicaciones no pueden compartir un puerto.

- Para puertos personalizables, puede seleccionar un puerto personalizado durante la instalación si no desea utilizar el puerto predeterminado.
- Para puertos fijos, debe aceptar el número de puerto predeterminado.
- Cortafuegos
  - Los firewalls, servidores proxy u otros dispositivos de red no deben interferir con las conexiones.
  - Si especifica un puerto personalizado al instalar SnapCenter , debe agregar una regla de firewall en el host del complemento para ese puerto para el Loader de complementos de SnapCenter .

La siguiente tabla enumera los diferentes puertos y sus valores predeterminados.

| Nombre del puerto                           | Números de puerto | Protocolo | Dirección     | Descripción                                                                                                                                                                                                                                                                                    |
|---------------------------------------------|-------------------|-----------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Puerto web de SnapCenter                    | 8146              | HTTPS     | Bidireccional | <p>Este puerto se utiliza para la comunicación entre el cliente de SnapCenter (el usuario de SnapCenter ) y el servidor de SnapCenter y también se utiliza para la comunicación desde los hosts del complemento al servidor de SnapCenter .</p> <p>Puede personalizar el número de puerto.</p> |
| Puerto de comunicación SMCORE de SnapCenter | 8145              | HTTPS     | Bidireccional | <p>Este puerto se utiliza para la comunicación entre el servidor SnapCenter y los hosts donde están instalados los complementos de SnapCenter .</p> <p>Puede personalizar el número de puerto.</p>                                                                                             |

| Nombre del puerto                  | Números de puerto | Protocolo | Dirección | Descripción                                                                                                                                                                                                                                               |
|------------------------------------|-------------------|-----------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Puerto de servicio del programador | 8154              | HTTPS     |           | <p>Este puerto se utiliza para orquestar los flujos de trabajo del programador de SnapCenter para todos los complementos administrados dentro del host del servidor SnapCenter de manera centralizada.</p> <p>Puede personalizar el número de puerto.</p> |
| Puerto RabbitMQ                    | 5672              | TCP       |           | <p>Este es el puerto predeterminado que RabbitMQ escucha y se utiliza para la comunicación del modelo de publicador-suscriptor entre el servicio Scheduler y SnapCenter.</p>                                                                              |
| Puerto MySQL                       | 3306              | HTTPS     |           | <p>El puerto se utiliza para comunicarse con la base de datos del repositorio de SnapCenter . Puede crear conexiones seguras desde el servidor SnapCenter al servidor MySQL. <a href="#">"Más información"</a></p>                                        |

| Nombre del puerto                                               | Números de puerto | Protocolo | Dirección      | Descripción                                                                                                                                                                                                                      |
|-----------------------------------------------------------------|-------------------|-----------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hosts de complementos de Windows                                | 135, 445          | TCP       |                | Este puerto se utiliza para la comunicación entre el servidor SnapCenter y el host en el que se está instalando el complemento. El rango de puertos dinámicos adicionales especificado por Microsoft también debe estar abierto. |
| Hosts de complementos de Linux o AIX                            | 22                | SSH       | Unidireccional | Este puerto se utiliza para la comunicación entre el servidor SnapCenter y el host, iniciada desde el servidor al host del cliente.                                                                                              |
| Paquete de complementos de SnapCenter para Windows, Linux o AIX | 8145              | HTTPS     | Bidireccional  | Este puerto se utiliza para la comunicación entre SMCORE y los hosts donde está instalado el paquete de complementos. Personalizable.<br><br>Puede personalizar el número de puerto.                                             |
| Complemento de SnapCenter para bases de datos Oracle            | 27216             |           |                | El complemento de Oracle utiliza el puerto JDBC predeterminado para conectarse a la base de datos de Oracle.                                                                                                                     |

| Nombre del puerto                                         | Números de puerto                                                                    | Protocolo                                                                 | Dirección     | Descripción                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Complemento de SnapCenter para bases de datos de Exchange | 909                                                                                  |                                                                           |               | El complemento para Windows utiliza el puerto NET.TCP predeterminado para conectarse a las devoluciones de llamadas VSS de Exchange.                                                                                                                                                                                                    |
| Complementos compatibles con NetApp para SnapCenter       | 9090                                                                                 | HTTPS                                                                     |               | <p>Este es un puerto interno que se utiliza solo en el host del complemento; no se requiere excepción de firewall.</p> <p>La comunicación entre el servidor SnapCenter y los complementos se enruta a través del puerto 8145.</p>                                                                                                       |
| Puerto de comunicación del clúster ONTAP o SVM            | <ul style="list-style-type: none"> <li>• 443 (HTTPS)</li> <li>• 80 (HTTP)</li> </ul> | <ul style="list-style-type: none"> <li>• HTTPS</li> <li>• HTTP</li> </ul> | Bidireccional | <p>El puerto es utilizado por SAL (capa de abstracción de almacenamiento) para la comunicación entre el host que ejecuta SnapCenter Server y SVM.</p> <p>Actualmente, el puerto también lo utiliza el SAL en los hosts del complemento SnapCenter para Windows para la comunicación entre el host del complemento SnapCenter y SVM.</p> |

| Nombre del puerto                                        | Números de puerto                                                                                | Protocolo                                                             | Dirección     | Descripción                                                                                                                                                                                                                                    |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Complemento de SnapCenter para la base de datos SAP HANA | <ul style="list-style-type: none"> <li>3instance_number13</li> <li>3instance_number15</li> </ul> | <ul style="list-style-type: none"> <li>HTTPS</li> <li>HTTP</li> </ul> | Bidireccional | <p>Para un contenedor de base de datos multiinquilino (MDC) de un solo inquilino, el número de puerto termina con 13; para un contenedor que no es MDC, el número de puerto termina con 15.</p> <p>Puede personalizar el número de puerto.</p> |
| Complemento de SnapCenter para PostgreSQL                | 5432                                                                                             |                                                                       |               | <p>Este puerto es el puerto PostgreSQL predeterminado utilizado para la comunicación del complemento PostgreSQL con el clúster PostgreSQL.</p> <p>Puede personalizar el número de puerto.</p>                                                  |

## Regístrese para acceder al SnapCenter software

Debe registrarse para acceder al SnapCenter software si es nuevo en Amazon FSx for NetApp ONTAP o Azure NetApp Files y no tiene una cuenta de NetApp existente.

### Antes de empezar

- Debe tener acceso a la ID de correo electrónico corporativa.
- Si usa Azure NetApp Files, debe tener el identificador de suscripción de Azure.
- Si está utilizando Amazon FSx for NetApp ONTAP, debe tener el ID del sistema de archivos de su sistema de archivos FSx para ONTAP .

### Acerca de esta tarea

Su registro está sujeto a validaciones de información y puede demorar hasta un día para confirmar y actualizar la nueva cuenta del Sitio de soporte de NetApp (NSS) a acceso **completo** desde acceso **de invitado**.

### Pasos

1. Hacer clic <https://mysupport.netapp.com/site/user/registration> para registro.
2. Ingrese su ID de correo electrónico corporativo, complete el captcha, acepte la política de privacidad de NetApp y haga clic en **Enviar**.
3. Autentica el registro ingresando el OTP enviado a tu ID de correo electrónico y haz clic en **Continuar**.
4. En la página de finalización del registro, ingrese los siguientes detalles para completar el registro.

- a. Seleccione **Cliente de NetApp /Usuario final**.
- b. En el campo NÚMERO DE SERIE, ingrese el ID de suscripción de Azure si usa Azure NetApp Files o el ID del sistema de archivos si usa Amazon FSx for NetApp ONTAP.



Puedes generar un ticket en <https://mysupport.netapp.com/site/help> Si enfrenta algún problema durante el registro o para conocer el estado.

## Autenticación multifactor (MFA)

### Administrar 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 en el servidor de SnapCenter .

### Habilitar la autenticación multifactor (MFA)

Puede habilitar la funcionalidad MFA para SnapCenter Server mediante 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 ciertas configuraciones de AD FS, SnapCenter podría requerir autenticación de usuario por razones 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` . Alternativamente, también puedes ver "[Guía de referencia de cmdlets del software SnapCenter](#)" .

#### Antes de empezar

- El Servicio de federación de Active Directory (AD FS) de Windows debe estar en funcionamiento en el dominio respectivo.
- Debe tener un servicio de autenticación multifactor compatible con AD FS, como Azure MFA, Cisco Duo, etc.
- La marca de tiempo de SnapCenter y del servidor AD FS deben ser las mismas independientemente de la zona horaria.
- Obtenga y configure el certificado CA autorizado para SnapCenter Server.

El certificado CA es obligatorio por las siguientes razones:

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

Para obtener información sobre el certificado CA, consulte "[Generar archivo CSR de certificado de CA](#)" .

## Pasos

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

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

6. Copie el archivo generado en el host de AD FS para configurar SnapCenter como entidad cliente.
7. Habilite MFA para SnapCenter Server mediante el *Set-SmMultiFactorAuthentication* cmdlet.
8. (Opcional) Verifique el estado y la configuración de MFA mediante *Get-SmMultiFactorAuthentication* cmdlet.
9. Vaya a la consola de administración de Microsoft (MMC) y realice los siguientes pasos:
  - a. Haga clic en **Archivo > Agregar o quitar complemento**.
  - b. En la ventana Agregar o quitar complementos, seleccione **Certificados** y luego haga clic en **Agregar**.
  - c. En la ventana del complemento Certificados, seleccione la opción **Cuenta de equipo** y haga clic en **Finalizar**.
  - d. Haga clic en **Raíz de consola > Certificados – Equipo local > Personal > Certificados**.
  - e. Haga clic con el botón derecho en el certificado de CA vinculado a SnapCenter y luego 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 del objeto, ingrese 'IIS\_IUSRS' y haga clic en **Verificar nombres** y haga clic en **Aceptar**.

Si la comprobación es exitosa, haga clic en **Aceptar**.

10. En el host de AD FS, abra el asistente de administración de AD FS y realice los siguientes pasos:
  - a. Haga clic derecho en **Confianzas de usuario autenticado > Agregar confianza de usuario autenticado > Iniciar**.
  - b. Seleccione la segunda opción y busque el archivo de metadatos MFA de SnapCenter y haga clic en **Siguiente**.
  - c. Especifique un nombre para mostrar y haga clic en **Siguiente**.
  - d. Seleccione una política de control de acceso según sea necesario y haga clic en **Siguiente**.
  - e. Seleccione la configuración en la siguiente pestaña para establecerla como predeterminada.
  - f. Haga clic en **Finalizar**.

SnapCenter ahora se refleja como una parte confiable con el nombre para mostrar proporcionado.

11. Seleccione el nombre y realice los siguientes pasos:
  - a. Haga clic en **Editar política 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 **User-Principal-Name** y el tipo de reclamo saliente como **Name-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 importaron correctamente.
  - a. Haga clic con el botón derecho en la cuenta de confianza del usuario confiante y seleccione **Propiedades**.
  - b. Asegúrese de que los campos Puntos finales, Identificadores y Firma estén completos.
14. Cierre todas las pestañas del navegador y vuelva a abrirlo para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

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

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

### Actualizar metadatos de MFA de AD FS

Debe actualizar los metadatos de MFA de AD FS en SnapCenter siempre que haya alguna modificación en el servidor de AD FS, como una actualización, una renovación del certificado de CA, una recuperación ante desastres, etc.

#### Pasos

1. Descargar el archivo de metadatos de federación de AD FS desde "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>"
2. Copie el archivo descargado en SnapCenter Server 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 abrirlo para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

### Actualizar metadatos de MFA de SnapCenter

Debe actualizar los metadatos de MFA de SnapCenter en AD FS siempre que haya alguna modificación en el servidor ADFS, como reparación, renovación de certificado de CA, DR, etc.

## Pasos

1. En el host de AD FS, abra el asistente de administración de AD FS y realice los siguientes pasos:
  - a. Seleccione **Fideicomisos de terceros que confían**.
  - b. Haga clic con el botón derecho en la relación de confianza creada para SnapCenter y seleccione **Eliminar**.

Se mostrará el nombre definido por el usuario de la parte confiable.

- c. Habilitar la autenticación multifactor (MFA).

Ver "[Habilitar la autenticación multifactor](#)".

2. Cierre todas las pestañas del navegador y vuelva a abrirlo para borrar las cookies de sesión existentes o activas y vuelva a iniciar sesión.

## Deshabilitar la autenticación multifactor (MFA)

### Pasos

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

## Administrar la autenticación multifactor (MFA) mediante Rest API, PowerShell y SCCLI

El inicio de sesión MFA es compatible con el navegador, la API REST, PowerShell y SCCLI. MFA se admite a través de un administrador de identidad AD FS. Puede habilitar MFA, deshabilitar MFA y configurar MFA desde GUI, API REST, PowerShell y SCCLI.

## Configurar AD FS como OAuth/OIDC

### Configurar AD FS mediante el asistente de GUI de Windows

1. Vaya a **Panel del administrador del servidor > Herramientas > Administración de ADFS**.
2. Vaya a **ADFS > Grupos de aplicaciones**.
  - a. Haga clic derecho en **Grupos de aplicaciones**.
  - b. Seleccione **Agregar grupo de aplicaciones** e ingrese **Nombre de la aplicación**.
  - c. Seleccione **Aplicación de servidor**.
  - d. Haga clic en **Siguiente**.
3. Copiar **Identificador de cliente**.

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

4. Seleccione **Generar secreto compartido**.

Copiar el valor secreto. Éste es el secreto del cliente. .. Haga clic en **Siguiente**.

5. En la página **Resumen**, haga clic en **Siguiente**.
  - a. En la página **Completa**, haga clic en **Cerrar**.
6. Haga clic derecho en el **Grupo de aplicaciones** recién agregado y seleccione **Propiedades**.
7. Seleccione **Agregar aplicación** en Propiedades de la aplicación.
8. Haga clic en **Agregar aplicación**.

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

9. En la página Configurar API web, ingrese la URL del servidor SnapCenter y el identificador de cliente creado 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**, seleccione la política de control según sus requisitos (por ejemplo, Permitir a todos y requerir MFA) y haga clic en **Siguiente**.
11. En la página **Configurar permiso de aplicación**, de manera predeterminada se selecciona openid como alcance; haga clic en **Siguiente**.
12. En la página **Resumen**, haga clic en **Siguiente**.

En la página **Completa**, haga clic en **Cerrar**.

13. En la página **Propiedades de la aplicación de muestra**, haga clic en **Aceptar**.
14. Token JWT emitido por un servidor de autorización (AD FS) y destinado a ser consumido por el recurso.

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

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

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

16. Abra la herramienta **Administración de AD FS** ubicada en el menú **Herramientas** 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. Ir a la pestaña Reglas de transformación de emisión

17. Haga clic en **Agregar regla**.
  - a. Seleccione **Enviar atributos LDAP como reclamos** en el menú desplegable Plantilla de regla de reclamo.
  - b. Haga clic en **Siguiente**.

18. Introduzca el nombre de la **regla de reclamación**.
  - a. Seleccione **Active Directory** en el menú desplegable Almacén de atributos.
  - b. Seleccione **Nombre principal del usuario** en el menú desplegable **Atributo LDAP** y **UPN** en el menú desplegable **Tipo de reclamación saliente**.
  - c. Haga clic en **Finalizar**.

## Crear un grupo de aplicaciones mediante comandos de PowerShell

Puede crear el grupo de aplicaciones, la API web y agregar el alcance y las notificaciones mediante comandos de PowerShell. Estos comandos están disponibles en formato de script automatizado. Para obtener más información, consulte el <enlace al artículo de Knowledge Base>.

1. Cree el nuevo grupo de aplicaciones en AD FS utilizando el siguiente comando.

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

`ClientRoleIdentifier`nombre de su grupo de aplicaciones

`redirectURL`URL válida para redirección después de la autorización

2. Cree la aplicación de servidor 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 del cliente y el secreto del cliente de la salida de los siguientes comandos porque solo se muestran 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. Nombre la aplicación de API web y defina sus reglas de transformación de emisión utilizando un archivo externo.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"  
-TargetIdentifier  
  
$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile  
  
$relativePath
```

### Actualizar el tiempo de expiración del token de acceso

Puede actualizar el tiempo de expiración del token de acceso mediante el comando de 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 expiración de un token de acceso es de 60 minutos. Este tiempo mínimo de expiración es suficiente y escalable. Debe proporcionar valor suficiente para evitar que se realicen trabajos críticos para el negocio.

#### Paso

Para actualizar el tiempo de vencimiento del token de acceso para un grupo de aplicaciones WebApi, use el siguiente comando en el servidor AD FS.

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

### Obtener el token portador de AD FS

Debe completar los parámetros mencionados a continuación en cualquier cliente REST (como Postman) y le solicitará que complete las credenciales del usuario. Además, debes ingresar la autenticación de segundo factor (algo que tienes y algo que eres) para obtener el token de portador.

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

| Campo              | Valor                  |
|--------------------|------------------------|
| Tipo de subvención | Código de autorización |

|                              |                                                                                                                                                                           |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL de devolución de llamada | Ingrese la URL base de su aplicación si no tiene una URL de devolución de llamada.                                                                                        |
| URL de autorización          | [nombre-de-dominio-adfs]/adfs/oauth2/authorize                                                                                                                            |
| URL del token de acceso      | [nombre-de-dominio-adfs]/adfs/oauth2/token                                                                                                                                |
| ID de cliente                | Introduzca el ID del cliente de AD FS                                                                                                                                     |
| Secreto del cliente          | Ingrese el secreto del cliente de AD FS                                                                                                                                   |
| Alcance                      | OpenID                                                                                                                                                                    |
| Autenticación del cliente    | Enviar como encabezado de autenticación básico                                                                                                                            |
| Recurso                      | En la pestaña <b>Opciones avanzadas</b> , 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. |

## Configurar MFA en SnapCenter Server mediante PowerShell, SCCLI y API REST

Puede configurar MFA en SnapCenter Server mediante PowerShell, SCCLI y API REST.

### Autenticación CLI de MFA de SnapCenter

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

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

Después de ejecutar el cmdlet anterior, se crea una sesión para que el usuario respectivo ejecute otros cmdlets de SnapCenter .

### Autenticación de API Rest de MFA de SnapCenter

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

### Flujo de trabajo de la API Rest de MFA

Cuando MFA está configurado con AD FS, debe autenticarse usando un token de acceso (portador) para acceder a la aplicación SnapCenter mediante cualquier API Rest.

### Acerca de esta tarea

- Puede utilizar cualquier cliente REST como Postman, Swagger UI o FireCamp.

- Obtenga un token de acceso y utilícelo para autenticar solicitudes posteriores (API Rest de SnapCenter ) para realizar cualquier operación.

## Pasos

### Para autenticarse a través de AD FS MFA

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

Cuando presione el botón para obtener un token de acceso para una aplicación, será redirigido a la página SSO de AD FS donde deberá 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 tener el formato usuario@dominio o dominio\usuario.

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

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

6. En la API Rest, debes pasar el token de acceso y el nombre del 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. Utilizando el nombre de usuario y el nombre del rol, SnapCenter autentica al usuario para una ejecución de API.

Si la autenticación tiene éxito, SnapCenter devuelve el resultado; de lo contrario, se muestra un mensaje de error.

### Habilitar o deshabilitar la funcionalidad MFA de SnapCenter para API Rest, CLI y GUI

## GUI

### Pasos

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

## Interfaz de PowerShell

### Pasos

1. Ejecute los comandos de PowerShell o CLI para habilitar MFA para GUI, API Rest, PowerShell y SCCLI.

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

El parámetro de ruta especifica la ubicación del archivo XML de metadatos de AD FS MFA.

Habilita MFA para la GUI de SnapCenter , la API Rest, PowerShell y SCCLI configurados con la ruta de archivo de metadatos de AD FS especificada.

2. Verifique el estado y la configuración de MFA mediante el `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 de publicación para habilitar MFA para GUI, API Rest, PowerShell y SCCLI.

| Parámetro              | Valor                                                                                                                                                                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL solicitada         | /api/4.9/configuraciones/autenticación multifactor                                                                                                                                                                                                                                 |
| Método HTTP            | Correo                                                                                                                                                                                                                                                                             |
| Cuerpo de la solicitud | { "IsGuiMFAEnabled": falso,<br>"IsRestApiMFAEnabled": verdadero,<br>"IsCliMFAEnabled": falso, "ADFSConfigFilePath":<br>"C:\ADFS_metadata\abc.xml" }                                                                                                                                |
| Cuerpo de respuesta    | { "Configuración MFAC": { "IsGuiMFAEnabled":<br>falso, "RutaDeArchivoDeConfigADFS":<br>"C:\ADFS_metadata\abc.xml",<br>"RutaDeArchivoDeConfigSC": nulo,<br>"IsRestApiMFAEnabled": verdadero,<br>"IsCliMFAEnabled": falso, "NombreDeHostADFS":<br>"win-adfs-sc49.winscedom2.com" } } |

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

| Parámetro | Valor |
|-----------|-------|
|-----------|-------|

|                     |                                                                                                                                                                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL solicitada      | /api/4.9/configuraciones/autenticación multifactor                                                                                                                                                                                                                 |
| Método HTTP         | Conseguir                                                                                                                                                                                                                                                          |
| Cuerpo de respuesta | { "Configuración MFAC": { "IsGuiMFAEnabled": falso, "RutaDeArchivoDeConfigADFS": "C:\\ADFS_metadata\\abc.xml", "RutaDeArchivoDeConfigSC": nulo, "IsRestApiMFAEnabled": verdadero, "IsCliMFAEnabled": falso, "NombreDeHostADFS": "win-adfs-sc49.winscedom2.com" } } |

## Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.