Autenticación multifactor (MFA)

SnapCenter Software 4.9

NetApp
March 20, 2024

Tabla de contenidos

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» } }