Preguntas frecuentes

SANtricity software

NetApp
June 16, 2025

This PDF was generated from https://docs.netapp.com/es-es/e-series-santricity/um-certificates/why-cant-i-log-in-unified.html on June 16, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Preguntas frecuentes . . . 1
- ¿Por qué no puedo iniciar sesión? . . . 1
- ¿Qué debo saber antes de añadir un servidor de directorio? . . . 1
- ¿Qué debo saber acerca de la asignación de roles de la cabina de almacenamiento? . . . 1
  - SAML . . . 2
- ¿Qué debo saber antes de configurar y habilitar SAML? . . . 2
  - Requisitos . . . 2
  - Restricciones . . . 2
- ¿De qué se tratan los usuarios locales? . . . 3

Preguntas frecuentes

¿Por qué no puedo iniciar sesión?

Si recibe un error al intentar iniciar sesión, revise estas causas posibles.

Los errores de inicio de sesión pueden ocurrir por uno de estos motivos:

- Introdujo un nombre de usuario o contraseña incorrectos.
- No tiene privilegios suficientes.
- Intentó iniciar sesión reiteradamente sin éxito y se activó el modo de bloqueo. Aguarde 10 minutos y vuelva a intentarlo.
- La autenticación SAML está habilitada. Actualice el explorador para iniciar sesión.

¿Qué debo saber antes de añadir un servidor de directorio?

Antes de añadir un servidor de directorio en Access Management, debe cumplir ciertos requisitos.

- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.
- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

¿Qué debo saber acerca de la asignación de roles de la cabina de almacenamiento?

Antes de asignar grupos a roles, revise las directrices.

Las funcionalidades de RBAC incluyen los siguientes roles:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento de las matrices, pero sin acceso a la configuración de seguridad.
- **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management.
- **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

Si usa un servidor de protocolo ligero de acceso a directorios (LDAP) y servicios de directorio, asegúrese de que:

- Un administrador haya definido grupos de usuarios en el servicio de directorio.
- Conoce los nombres de dominio de los grupos de usuarios LDAP.

SAML

Si usa las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) incorporadas en la cabina de almacenamiento, asegúrese de que:

- Un administrador de proveedor de identidades (IDP) haya configurado atributos de usuario y pertenencia a grupos en el sistema del IDP.
- Conoce los nombres de pertenencia a grupos.
- Conoce el valor de atributo para el grupo que será asignado. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (\) si no forman parte de un patrón de expresión regular:

```
\.[]{}()<>*+-=!?^$|
```

- El rol de supervisión se requiere para todos los usuarios, incluido el administrador. Unified Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

¿Qué debo saber antes de configurar y habilitar SAML?

Antes de configurar y habilitar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) para la autenticación, asegúrese de cumplir con los siguientes requisitos y comprender las restricciones de SAML.

Requisitos

Antes de comenzar, compruebe lo siguiente:

- Se configuró un proveedor de identidades (IDP) en la red. Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. El equipo de seguridad es responsable de mantener el IDP.
- Un administrador IDP configuró los atributos y los grupos del usuario en el sistema IDP.
- Un administrador de IDP comprobó que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.
- Un administrador comprobó que el reloj del servidor de IdP y de la controladora está sincronizado (ya sea mediante un servidor NTP o mediante el ajuste de la configuración del reloj de la controladora).
- Se descargó un archivo de metadatos de IdP del sistema de IdP y ese archivo está disponible en el sistema local que se usa para acceder a Unified Manager.
- Conoce la dirección IP o el nombre de dominio de la controladora de la cabina de almacenamiento.

Restricciones

Además de los requisitos mencionados más arriba, asegúrese de comprender las siguientes restricciones:

- Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede

editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda. Se recomienda que pruebe los inicios de sesión SSO para poder habilitar SAML en el paso final de la configuración. (El sistema también hace una prueba de inicio de sesión SSO antes de habilitar SAML.)

- Si deshabilita SAML en el futuro, el sistema restaura automáticamente la configuración anterior (local User roles o Directory Services).
- Si Directory Services está actualmente configurado para la autenticación de usuario, SAML anula esa configuración.
- Cuando se configura SAML, los siguientes clientes no pueden acceder a los recursos de la cabina de almacenamiento:
  - Enterprise Management Window (EMW)
  - Interfaz de línea de comandos (CLI)
  - Clientes de kits de desarrollo de software (SDK)
  - Clientes en banda
  - Clientes HTTP de la API de REST de autenticación básica
  - Inicio de sesión mediante extremo estándar de la API de REST

¿De qué se tratan los usuarios locales?

Los usuarios locales están predefinidos en el sistema e incluyen permisos específicos.

Entre ellos, se incluyen:

- **Admin** — Super administrador que tiene acceso a todas las funciones del sistema. Este usuario incluye todos los roles. La contraseña se debe establecer en el primer inicio de sesión.
- **Almacenamiento** — el administrador responsable de todo el aprovisionamiento de almacenamiento. Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Security**: El usuario responsable de la configuración de seguridad, incluidos Access Management y Certificate Management. Este usuario incluye los siguientes roles: Administrador de seguridad y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Soporte**: El usuario responsable de recursos de hardware, datos de fallos y actualizaciones de firmware. Este usuario incluye los siguientes roles: Administrador de soporte y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Monitor** — un usuario con acceso de sólo lectura al sistema. Este usuario incluye únicamente el rol Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **rw** (lectura/escritura): Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Ro** (sólo lectura) — este usuario incluye sólo la función Monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.

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.