# Crear cuentas de inicio de sesión

ONTAP 9

NetApp
April 16, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/authentication/create-svm-user-accounts-task.html on April 16, 2024. Always check docs.netapp.com for the latest.

# Tabla de contenidos

Crear cuentas de inicio de sesión . . . . . 1
Información general de las cuentas de inicio de sesión de . . . . . 1
Habilite el acceso de cuenta local . . . . . 2
Habilite el acceso de cuenta de Active Directory . . . . . 11
Habilite el acceso a cuenta de LDAP o NIS . . . . . 13

# Crear cuentas de inicio de sesión

## Información general de las cuentas de inicio de sesión de

Puede habilitar cuentas de administrador de SVM y de clúster local o remoto. Una cuenta local es aquella en la que reside la información de la cuenta, la clave pública o el certificado de seguridad en el sistema de almacenamiento. La información DE la cuenta DE AD se almacena en un controlador de dominio. Las cuentas LDAP y NIS residen en servidores LDAP y NIS.

### Administradores de clústeres y SVM

Un administrador de *cluster* accede a la SVM de administrador del clúster. La SVM de administrador y un administrador de clúster con el nombre reservado `admin` se crean automáticamente cuando se configura el clúster.

Un administrador de clúster con los valores predeterminados `admin` el rol puede administrar todo el clúster y sus recursos. El administrador de clúster puede crear administradores de clúster adicionales con diferentes roles según sea necesario.

Un administrador de *SVM* accede a una SVM de datos. El administrador de clúster crea SVM de datos y administradores de SVM según sea necesario.

A los administradores de SVM se les asigna el `vsadmin` función predeterminada. El administrador de clúster puede asignar diferentes roles a los administradores de SVM según sea necesario.

#### Convenciones de nomenclatura

Los siguientes nombres genéricos no se pueden utilizar para cuentas de administrador de SVM o de clúster remoto:

- adm
- bandeja
- cli
- demonio
- ftp
- “juegos”
- detener
- lp
- correo
- «hombre»
- «naroot»
- «NetApp»
- «noticias»
- «nadie»

- operador
- «raíz»
- apagado
- sshd
- sincronizar
- sistema
- uucp
- «www»

### Roles fusionados

Si habilita varias cuentas remotas para el mismo usuario, se le asigna la unión de todas las funciones especificadas para las cuentas. Es decir, si se asigna una cuenta LDAP o NIS el `vsadmin` Asimismo, se asigna el rol y la cuenta de grupo AD del mismo usuario `vsadmin-volume` El rol, el usuario de AD inicia sesión con más incluido `vsadmin` funcionalidades. Se dice que los roles son *fusionado*.

# Habilite el acceso de cuenta local

## Habilite la información general de acceso de la cuenta local

Una cuenta local es aquella en la que reside la información de la cuenta, la clave pública o el certificado de seguridad en el sistema de almacenamiento. Puede utilizar el `security login create` Comando para habilitar cuentas locales para acceder a un administrador o una SVM de datos.

## Active el acceso a la cuenta de contraseña

Puede utilizar el `security login create` Comando para habilitar las cuentas de administrador para acceder a una SVM de administrador o de datos con una contraseña. Se le pedirá la contraseña después de introducir el comando.

#### Acerca de esta tarea

Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

#### Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

#### Paso

1. Habilite las cuentas de administrador local para acceder a una SVM mediante una contraseña:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   Para obtener una sintaxis completa del comando, consulte "hoja de trabajo".

El siguiente comando habilita la cuenta de administrador de clúster `admin1` con los predefinidos `backup` Rol para acceder a la SVM de administrador`engCluster` usar una contraseña. Se le pedirá la contraseña después de introducir el comando.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
admin1 -application ssh -authmethod password -role backup
```

## Habilite cuentas de clave pública de SSH

Puede utilizar el `security login create` Comando para habilitar cuentas de administrador para acceder a una SVM de administrador o de datos con una clave pública SSH.

**Acerca de esta tarea**

- Debe asociar la clave pública a la cuenta para que esta pueda acceder a la SVM.

  Asociación de una clave pública con una cuenta de usuario

  Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

Si desea habilitar el modo FIPS en su clúster, las cuentas de claves públicas SSH existentes sin los algoritmos de clave admitidos deben volver a configurarse con un tipo de clave admitida. Las cuentas se deben volver a configurar antes de habilitar FIPS o se producirá un error en la autenticación del administrador.

La siguiente tabla indica los algoritmos de tipo de clave de host que se admiten para las conexiones SSH de ONTAP. Estos tipos de claves no se aplican a la configuración de la autenticación pública SSH.

| Versión de ONTAP | Tipos de clave compatibles con el modo FIPS | Tipos de clave compatibles con el modo no FIPS |
|---|---|---|
| 9.11.1 y posterior | ecdsa-sha2-nistp256 | ecdsa-sha2-nistp256<br>rsa-sha2-512<br>rsa-sha2-256<br>ssh-ed25519<br>ssh-dss<br>ssh-rsa |
| 9.10.1 y anteriores | ecdsa-sha2-nistp256<br>ssh-ed25519 | ecdsa-sha2-nistp256<br>ssh-ed25519<br>ssh-dss<br>ssh-rsa |

La compatibilidad con el algoritmo de clave de host ssh-ed25519 se elimina a partir de ONTAP 9.11.1.

Para obtener más información, consulte "Configurar la seguridad de red con FIPS".

**Antes de empezar**

Para realizar esta tarea, debe ser un administrador de clústeres.

**Paso**

1. Habilite cuentas de administrador local para acceder a una SVM mediante una clave pública de SSH:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name user_or_group_name -application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   Para obtener una sintaxis completa del comando, consulte "hoja de trabajo".

   El siguiente comando habilita la cuenta de administrador de SVM `svmadmin1` con los predefinidos `vsadmin-volume` Rol para acceder a la SVM`engData1` Mediante una clave pública SSH:

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

**Después de terminar**

Si no ha asociado una clave pública a la cuenta de administrador, debe hacerlo para que la cuenta pueda acceder a la SVM.

Asociación de una clave pública con una cuenta de usuario

## Habilite las cuentas de autenticación multifactor (MFA)

### Información general de la autenticación multifactor

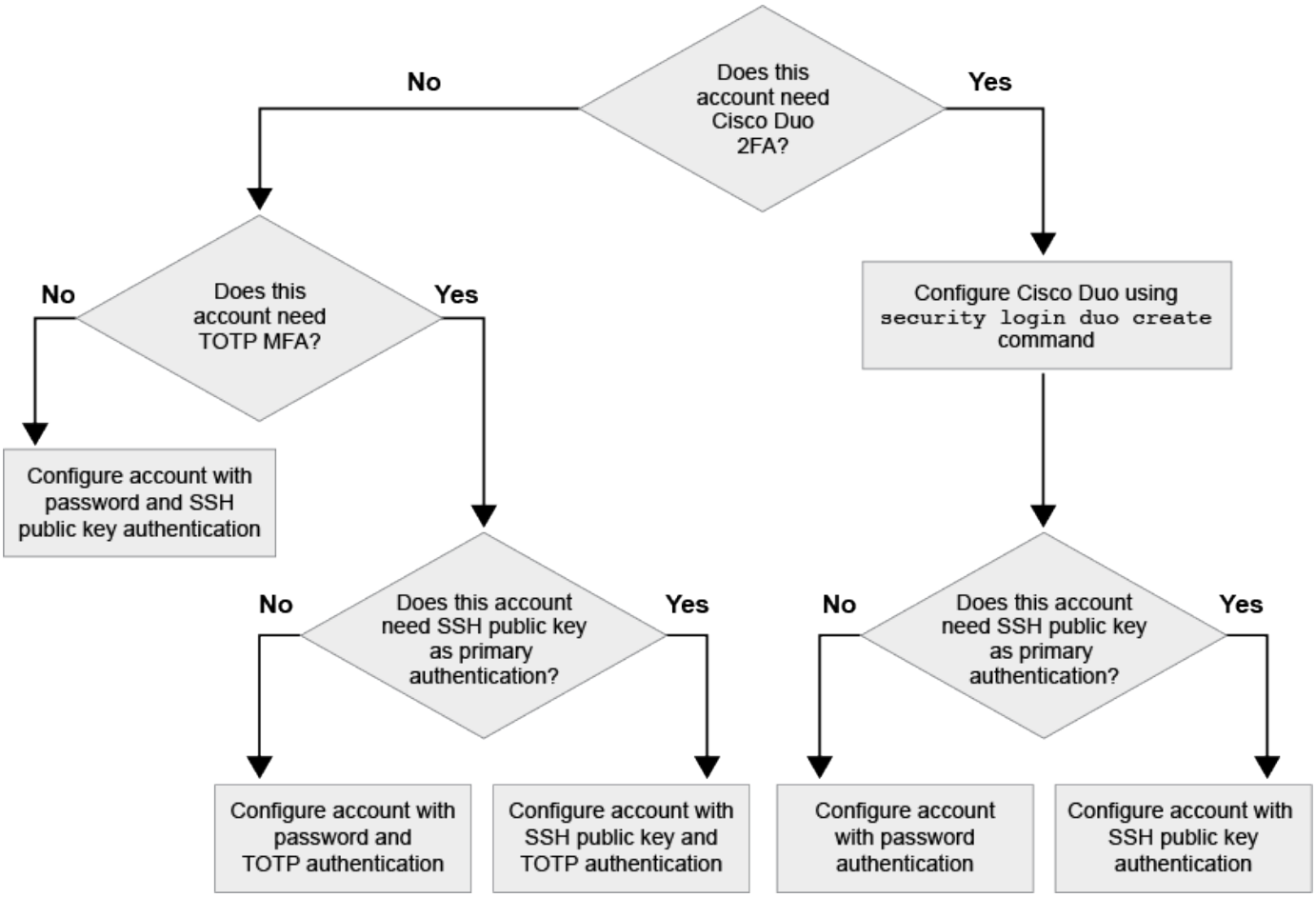
La autenticación multifactor (MFA) permite mejorar la seguridad al requerir que los usuarios proporcionen dos métodos de autenticación para iniciar sesión en un administrador o en un equipo virtual de almacenamiento de datos.

Dependiendo de la versión de ONTAP, puede utilizar una combinación de una clave pública SSH, una contraseña de usuario y una contraseña de un solo uso basada en el tiempo (TOTP) para la autenticación multifactor. Al habilitar y configurar Cisco Duo (ONTAP 9.14.1 y posterior), sirve como un método de autenticación adicional, que complementa los métodos existentes para todos los usuarios.

| Disponible empezando por… | Primer método de autenticación | Segundo método de autenticación |
|---|---|---|
| ONTAP 9.14.1 | Clave pública SSH | TOTP |
| | Contraseña de usuario | TOTP |
| | Clave pública SSH | Cisco Duo |
| | Contraseña de usuario | Cisco Duo |
| ONTAP 9.13.1 | Clave pública SSH | TOTP |
| | Contraseña de usuario | TOTP |

| Disponible empezando por… | Primer método de autenticación | Segundo método de autenticación |
|---|---|---|
| ONTAP 9,3 | Clave pública SSH | Contraseña de usuario |

Si se configura MFA, el administrador del clúster primero debe habilitar la cuenta de usuario local, entonces el usuario local debe configurar la cuenta.




### Habilite la autenticación multifactor

La autenticación multifactor (MFA) permite mejorar la seguridad al requerir que los usuarios proporcionen dos métodos de autenticación para iniciar sesión en un administrador o una SVM de datos.

#### Acerca de esta tarea

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

  "Modificar el rol asignado a un administrador"

- Si utiliza una clave pública para la autenticación, debe asociar la clave pública con la cuenta para que la cuenta pueda acceder a la SVM.

  "Asociar una clave pública a una cuenta de usuario"

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- A partir de ONTAP 9.12.1, puede usar dispositivos de autenticación de hardware Yubikey para la MFA del cliente SSH mediante los estándares de autenticación FIDO2 (Fast Identity Online) o de verificación de identidad personal (PIV).

#### Habilite MFA con clave pública SSH y contraseña de usuario

A partir de ONTAP 9,3, un administrador de clúster puede configurar cuentas de usuario locales para iniciar sesión con MFA mediante una clave pública SSH y una contraseña de usuario.

1. Habilite MFA en cuenta de usuario local con clave pública SSH y contraseña de usuario:

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_name> -application ssh -authentication-method <password|publickey>
   -role admin -second-authentication-method <password|publickey>
   ```

   El siguiente comando requiere la cuenta de administrador de SVM `admin2` con los predefinidos `admin` Rol que desea iniciar sesión en la SVM`engData1` Con una clave pública SSH y una contraseña de usuario:

   ```
   cluster-1::> security login create -vserver engData1 -user-or-group-name
   admin2 -application ssh -authentication-method publickey -role admin
   -second-authentication-method password

   Please enter a password for user 'admin2':
   Please enter it again:
   Warning: To use public-key authentication, you must create a public key
   for user "admin2".
   ```

#### Habilite MFA con TOTP

A partir de ONTAP 9.13.1, puede mejorar la seguridad al requerir que los usuarios locales inicien sesión en un administrador o una SVM de datos con una clave pública SSH o una contraseña de usuario y una contraseña de un solo uso basada en un tiempo (TOTP). Después de habilitar la cuenta para MFA con TOTP, el usuario local debe iniciar sesión en "complete la configuración".

TOTP es un algoritmo informático que utiliza la hora actual para generar una contraseña de un solo uso. Si se utiliza TOTP, siempre es la segunda forma de autenticación después de la clave pública SSH o la contraseña de usuario.

**Antes de empezar**

Debe ser un administrador de almacenamiento para realizar estas tareas.

**Pasos**

Puede configurar MFA con una contraseña de usuario o una clave pública SSH como primer método de autenticación y TOTP como segundo método de autenticación.

**Habilite MFA con contraseña de usuario y TOTP**

1. Habilite una cuenta de usuario para la autenticación multifactor con una contraseña de usuario y TOTP.

   **Para nuevas cuentas de usuario**

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   **Para cuentas de usuario existentes**

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Compruebe que MFA con TOTP está activado:

   ```
   security login show
   ```

**Habilite MFA con clave pública SSH y TOTP**

1. Habilite una cuenta de usuario para la autenticación multifactor con una clave pública SSH y TOTP.

   **Para nuevas cuentas de usuario**

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   **Para cuentas de usuario existentes**

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Compruebe que MFA con TOTP está activado:

```
security login show
```

**Después de terminar**

- Si no ha asociado una clave pública a la cuenta de administrador, debe hacerlo para que la cuenta pueda acceder a la SVM.

  "Asociación de una clave pública con una cuenta de usuario"

- El usuario local debe iniciar sesión para completar la configuración MFA con TOTP.

  "Configure la cuenta de usuario local para MFA con TOTP"

**Información relacionada**

Más información acerca de "Autenticación multifactor en ONTAP 9 (TR-4647)".

### Configure la cuenta de usuario local para MFA con TOTP

A partir de ONTAP 9.13.1, las cuentas de usuario se pueden configurar con autenticación multifactor (MFA) con una contraseña de un solo uso basada en tiempo (TOTP).

**Antes de empezar**

- El administrador de almacenamiento debe "Habilite MFA con TOTP" como segundo método de autenticación para su cuenta de usuario.
- El método de autenticación de la cuenta de usuario principal debe ser una contraseña de usuario o una clave SSH pública.
- Debes configurar tu aplicación TOTP para que funcione con tu smartphone y crear tu clave secreta TOTP.

  TOTP es compatible con varias aplicaciones de autenticación como Google Authenticator.

**Pasos**

1. Inicie sesión en su cuenta de usuario con el método de autenticación actual.

   Su método de autenticación actual debe ser una contraseña de usuario o una clave pública SSH.

2. Cree la configuración de TOTP en su cuenta:

   ```
   security login totp create -vserver "<svm_name>" -username
   "<account_username >"
   ```

3. Compruebe que la configuración de TOTP está activada en su cuenta:

   ```
   security login totp show -vserver "<svm_name>" -username
   "<account_username>"
   ```

### Restablezca la clave secreta TOTP

Para proteger la seguridad de su cuenta, si su clave secreta TOTP se ve comprometida o se pierde, debe deshabilitarla y crear una nueva.

#### Restablezca TOTP si su clave está comprometida

Si tu clave secreta TOTP está comprometida, pero aún tienes acceso a ella, puedes quitar la clave comprometida y crear una nueva.

1. Inicie sesión en su cuenta de usuario con su contraseña de usuario o clave pública SSH y su clave secreta TOTP comprometida.
2. Elimine la clave secreta TOTP comprometida:

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. Cree una nueva clave secreta de TOTP:

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

#### Restablezca TOTP si se pierde la clave

Si se pierde la clave secreta de TOTP, comuníquese con el administrador de almacenamiento de "tener la clave desactivada". Una vez desactivada la clave, puede utilizar el primer método de autenticación para iniciar sesión y configurar un nuevo TOTP.

**Antes de empezar**

La clave secreta de TOTP debe ser deshabilitada por un administrador de almacenamiento. Si no tiene una cuenta de administrador de almacenamiento, póngase en contacto con su administrador de almacenamiento para deshabilitar la clave.

**Pasos**

1. Una vez que un administrador de almacenamiento haya desactivado el secreto TOTP, utilice el método de autenticación principal para iniciar sesión en su cuenta local.
2. Cree una nueva clave secreta de TOTP:

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

#### Desactive la clave secreta TOTP para la cuenta local

Si se pierde la clave secreta de una sola vez basada en el tiempo (TOTP) de un usuario local, el administrador de almacenamiento debe desactivar la clave perdida antes de que el usuario pueda crear una nueva clave secreta TOTP.

**Acerca de esta tarea**

Esta tarea solo se puede realizar desde una cuenta de administrador de clúster.

**Paso**

1. Desactive la clave secreta TOTP:

```
security login totp delete -vserver "<svm_name>" -username
"<account_username>"
```

### Habilite cuentas de certificado SSL

Puede utilizar el `security login create` Comando para habilitar las cuentas de administrador para acceder a una SVM de administrador o de datos con un certificado SSL.

**Acerca de esta tarea**

- Para que la cuenta pueda acceder a la SVM, debe instalar un certificado digital de servidor firmado por CA.

  Generar e instalar un certificado de servidor firmado por CA

  Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- Si no está seguro del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede añadir el rol más adelante con la `security login modify` comando.

  Modificar el rol asignado a un administrador

> Para las cuentas de administrador de clúster, se admite la autenticación de certificados con el `http`, `ontapi`, y. `rest` más grandes. Para las cuentas de administrador de SVM, la autenticación de certificados solo se admite con el `ontapi` y.. `rest` más grandes.

**Paso**

1. Habilite las cuentas de administrador local para acceder a una SVM mediante un certificado SSL:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

Para obtener una sintaxis completa del comando, consulte "Páginas manuales de ONTAP por versión".

El siguiente comando habilita la cuenta de administrador de SVM `svmadmin2` con el valor predeterminado `vsadmin` Rol para acceder a la SVM`engData2` Mediante un certificado digital SSL.

```
cluster1::>security login create -vserver engData2 -user-or-group-name
svmadmin2 -application ontapi -authmethod cert
```

**Después de terminar**

Si no instaló un certificado digital de servidor firmado por CA, debe hacerlo para que la cuenta pueda acceder a la SVM.

Generar e instalar un certificado de servidor firmado por CA

# Habilite el acceso de cuenta de Active Directory

Puede utilizar el `security login create` Comando para habilitar cuentas de usuarios o grupos de Active Directory (AD) para acceder a un administrador o a la SVM de datos. Cualquier usuario del grupo de AD puede acceder a la SVM con el rol asignado al grupo.

**Acerca de esta tarea**

- Para poder acceder a la SVM, es necesario configurar el acceso de la controladora de dominio de AD al clúster o a la SVM.

  Configuración del acceso al controlador de dominio de Active Directory

  Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- A partir de ONTAP 9.13.1, puede usar una clave pública SSH como método de autenticación principal o secundario con una contraseña de usuario de AD.

  Si elige usar una clave pública SSH como autenticación principal, no se realiza ninguna autenticación de AD.

- A partir de ONTAP 9.11.1, se puede utilizar "Enlace rápido LDAP para la autenticación nsswitch" Si es compatible con el servidor LDAP de AD.
- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

  Modificar el rol asignado a un administrador

El acceso a la cuenta DE grupo DE AD solo se admite con `SSH`, `ontapi`, y. `rest` más grandes. Los grupos de AD no se admiten con la autenticación de clave pública SSH, que se utiliza comúnmente para la autenticación multifactor.

**Antes de empezar**

- La hora del clúster debe sincronizarse con un plazo de cinco minutos desde la hora del controlador de dominio de AD.
- Para realizar esta tarea, debe ser un administrador de clústeres.

**Paso**

1. Habilite las cuentas de administrador de usuario o de grupo de AD para acceder a una SVM:

   **Para usuarios de AD:**

| Versión de ONTAP | Autenticación principal | Autenticación secundaria | Comando |
|---|---|---|---|
| 9.13.1 y posterior | Clave pública | Ninguno | `security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>` |
| 9.13.1 y posterior | Dominio | Clave pública | **Para un nuevo usuario**<br>`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`<br>**Para un usuario existente**<br>`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>` |

| Versión de ONTAP | Autenticación principal | Autenticación secundaria | Comando |
|---|---|---|---|
| 9,0 y posterior | Dominio | Ninguno | `security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]` |

**Para grupos AD:**

| Versión de ONTAP | Autenticación principal | Autenticación secundaria | Comando |
|---|---|---|---|
| 9,0 y posterior | Dominio | Ninguno | `security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]` |

Para obtener una sintaxis completa del comando, consulte "Hojas de trabajo para la autenticación de administrador y la configuración de RBAC"

#### Después de terminar

Si no configuró el acceso de la controladora de dominio de AD al clúster o a la SVM, debe hacerlo antes de que la cuenta pueda acceder a la SVM.

Configuración del acceso al controlador de dominio de Active Directory

## Habilite el acceso a cuenta de LDAP o NIS

Puede utilizar el `security login create` Comando para habilitar cuentas de usuario LDAP o NIS para acceder a un administrador o una SVM de datos. Si no ha configurado el acceso del servidor LDAP o NIS a la SVM, debe hacerlo antes de que la cuenta pueda acceder a la SVM.

#### Acerca de esta tarea

- Las cuentas de grupo no son compatibles.
- Para que la cuenta pueda acceder a la SVM, debe configurar el acceso del servidor LDAP o NIS con la SVM.

  Configurar el acceso a servidores LDAP o NIS

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

  Modificar el rol asignado a un administrador

- A partir de ONTAP 9.4, la autenticación multifactor (MFA) es compatible para usuarios remotos a través de servidores LDAP o NIS.
- A partir de ONTAP 9.11.1, se puede utilizar "Enlace rápido LDAP para la autenticación nsswitch" Si es compatible con el servidor LDAP.
- Debido a un problema LDAP conocido, no debe utilizar el `':'` (Dos puntos) carácter en cualquier campo de la información de la cuenta de usuario LDAP (por ejemplo, `gecos`, `userPassword`, y así sucesivamente). De lo contrario, la operación de búsqueda fallará para ese usuario.

**Antes de empezar**

Para realizar esta tarea, debe ser un administrador de clústeres.

**Pasos**

1. Habilite las cuentas de usuario o grupo de LDAP o NIS para acceder a una SVM:

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

   Para obtener una sintaxis completa del comando, consulte "hoja de trabajo".

   "Crear o modificar cuentas de inicio de sesión"

   El siguiente comando habilita la cuenta de administrador de clúster LDAP o NIS `guest2` con los predefinidos `backup` Rol para acceder a la SVM de administrador`engCluster`.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   guest2 -application ssh -authmethod nsswitch -role backup
   ```

2. Habilitar el inicio de sesión MFA para usuarios de LDAP o NIS:

   ```
   security login modify -user-or-group-name rem_usr1 -application ssh
   -authentication-method nsswitch -role admin -is-ns-switch-group no -second
   -authentication-method publickey
   ```

   El método de autenticación se puede especificar como `publickey` y el segundo método de autenticación como `nsswitch`.

   En el siguiente ejemplo, se muestra la autenticación MFA que está habilitada:

   ```
   cluster-1::*> security login modify -user-or-group-name rem_usr2
   -application ssh -authentication-method nsswitch -vserver
   cluster-1 -second-authentication-method publickey"
   ```

**Después de terminar**

Si no ha configurado el acceso del servidor LDAP o NIS a la SVM, debe hacerlo antes de que la cuenta pueda acceder a la SVM.

Configurar el acceso a servidores LDAP o NIS

**Información de copyright**

Copyright © 2024 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.