Crear cuentas de inicio de sesión

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Crear cuentas de inicio de sesión

Obtenga más información sobre la creación de cuentas de inicio de sesión de ONTAP

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 clústeres con `admin` el rol predeterminado 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.

```
`vsadmin`De forma predeterminada, a los administradores de SVM se les
asigna el rol. 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 `vsadmin` el rol a una cuenta de LDAP o NIS y se asigna `vsadmin-volume` el rol a la cuenta de grupo de AD para el mismo usuario, el usuario de AD inicia sesión con las `vsadmin` capacidades más inclusivas. Se dice que los roles son *fusionado*.

Habilite el acceso de cuenta local

Obtenga más información sobre cómo habilitar el acceso a la cuenta local de ONTAP

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 usar el `security login create` comando para habilitar las cuentas locales para que accedan a un administrador o a una SVM de datos.

Información relacionada

- "seguridad de inicio de sesión creado"

Active el acceso de contraseña de la cuenta de ONTAP

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

Acerca de esta tarea

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

Obtenga más información sobre `security login modify` en el "Referencia de comandos del ONTAP".

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`*

   El siguiente comando habilita la cuenta de administrador de clúster `admin1` con `backup` el rol predefinido para acceder a la SVM de administrador`engCluster` con 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
   ```

   Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

Habilite el acceso de clave pública SSH para la cuenta de ONTAP

Puede utilizar el `security login create` comando para habilitar las cuentas de administrador para que accedan a una SVM de datos o administrador 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 del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede utilizar `security login modify` el comando para añadir el rol más adelante.

  Obtenga más información sobre `security login modify` en el "Referencia de comandos del ONTAP".

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 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa

9.10.1 y anteriores	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + 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`*

   El siguiente comando habilita la cuenta de administrador de SVM `svmadmin1` con `vsadmin-volume` el rol predefinido para acceder a la SVM`engData1` mediante una clave pública de SSH:

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

   Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

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)

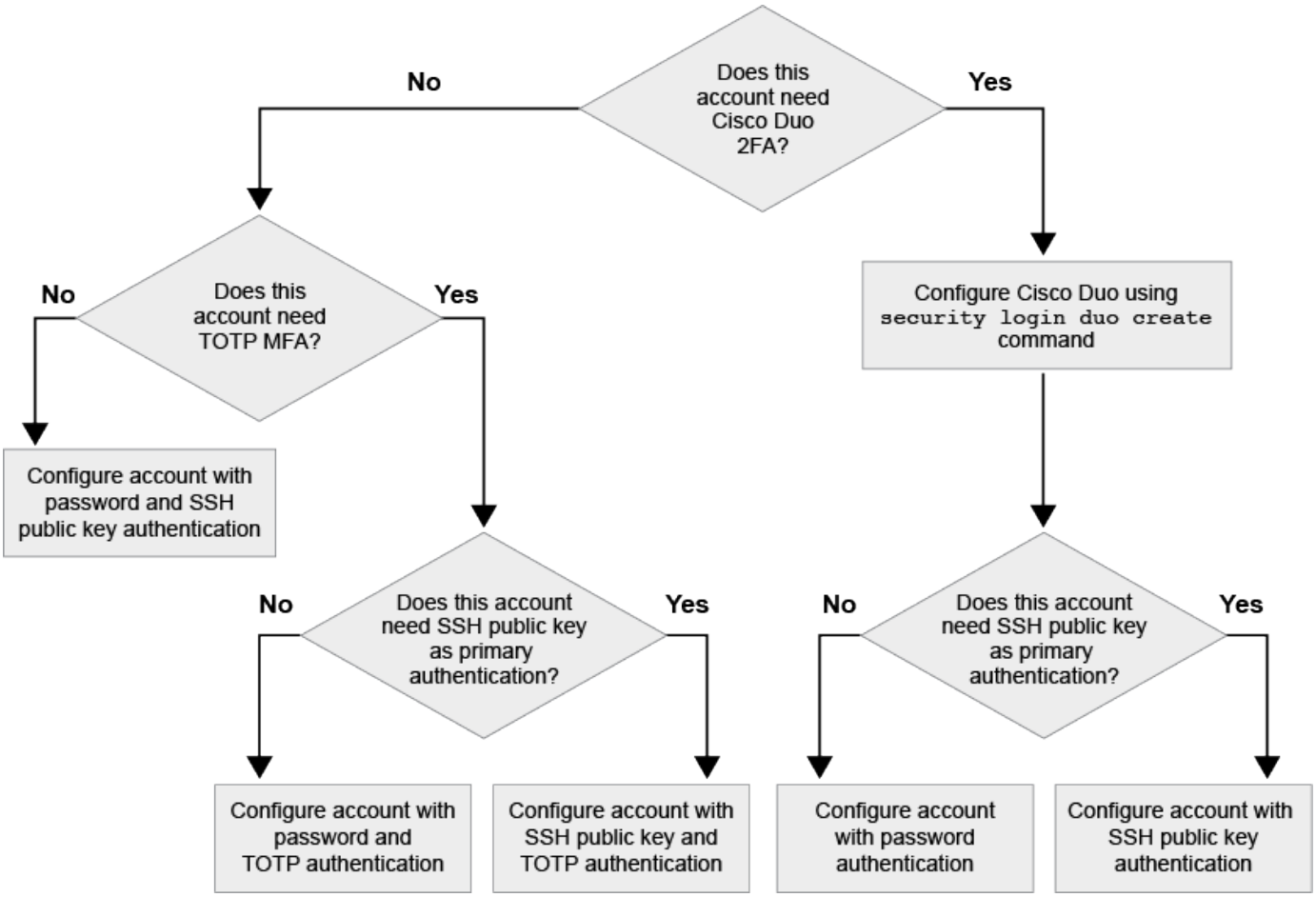
Obtenga más información sobre la autenticación multifactor de ONTAP

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
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 de ONTAP con SSH y TOTP

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 del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede utilizar `security login modify` el comando para añadir el rol más adelante.

  Obtenga más información sobre `security login modify` en el "Referencia de comandos del ONTAP".

  "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 que la cuenta de administrador de SVM `admin2` con `admin` el rol predefinido inicie 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".
   ```

   Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

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). Una vez que la cuenta se habilita 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>
   ```

   Obtenga más información sobre `security login modify` en el "Referencia de comandos del ONTAP".

2. Compruebe que MFA con TOTP está activado:

```
security login show
```

Obtenga más información sobre `security login show` en el "Referencia de comandos del ONTAP".

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

- "Autenticación multifactor en ONTAP 9 (TR-4647)"
- "Referencia de comandos del ONTAP"

Configure cuentas de usuario locales de ONTAP 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.

  Microsoft Authenticator, Google Authenticator, Authy y cualquier otro autenticador compatible con TOTP son compatibles.

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>"
```

Información relacionada

- "inicio de sesión de seguridad totp create"
- "Inicio de sesión de seguridad totp show"

Restablezca la clave secreta TOTP para una cuenta de usuario de ONTAP

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, póngase en contacto con el administrador de almacenamiento para "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>
```

Información relacionada

- "inicio de sesión de seguridad totp create"
- "inicio de sesión de seguridad totp eliminar"
- "Inicio de sesión de seguridad totp show"

Deshabilite la clave secreta TOTP para una cuenta de usuario de ONTAP

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 modify -vserver <svm_name> -username
<account_username> -enabled false
```

Obtenga más información sobre `security login totp modify` en el "Referencia de comandos del ONTAP".

Active el acceso a la cuenta de ONTAP del certificado SSL

Puede usar el `security login create` comando para habilitar las cuentas de administrador de para acceder a una SVM de datos o administrador 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 `security login modify` el comando.

  Modificar el rol asignado a un administrador

> Para las cuentas de administrador de clúster, se admite la autenticación de certificados con `http` `ontapi` `rest` las aplicaciones , y. En el caso de las cuentas de administrador de SVM, la autenticación de certificados solo es compatible con `ontapi` `rest` las aplicaciones y.

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`

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

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

   Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

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

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Habilite el acceso a la cuenta de Active Directory ONTAP

Puede usar el `security login create` comando para habilitar cuentas de usuario o de grupo de Active Directory (AD) para acceder a un administrador o a una 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 "Utilice el enlace rápido LDAP para la autenticación nsswitch para SVM NFS de ONTAP" si es compatible con el servidor LDAP de AD.
- Si no está seguro del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede utilizar `security login modify` el comando para añadir el rol más adelante.

  Obtenga más información sobre `security login modify` en el "Referencia de comandos del ONTAP".

  Modificar el rol asignado a un administrador

> El acceso a la cuenta de grupo de ANUNCIOS sólo se admite con `SSH` `ontapi` `rest` las aplicaciones , y. 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>`

Versión de ONTAP	Autenticación principal	Autenticación secundaria	Comando

9.13.1 y posterior	Dominio	Clave pública	**Para un nuevo usuario**
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			Para un usuario existente
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

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]`

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

Información relacionada

- "seguridad de inicio de sesión creado"

Active el acceso a la cuenta de ONTAP LDAP o NIS

Puede usar el `security login create` comando para habilitar las cuentas de usuario LDAP o NIS para acceder a una SVM de datos o administrador. 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 del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede utilizar `security login modify` el comando para añadir el rol más adelante.

  Obtenga más información sobre `security login modify` en el "Referencia de comandos del ONTAP".

  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 "Utilice el enlace rápido LDAP para la autenticación nsswitch para SVM NFS de ONTAP" si es compatible con el servidor LDAP.
- Debido a un problema conocido de LDAP, no debe utilizar el `':'` carácter (dos puntos) en ningún campo de información de cuenta de usuario de LDAP (por ejemplo, `gecos` `userPassword` ,, etc.). 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]
   ```

   "Crear o modificar cuentas de inicio de sesión"

El siguiente comando habilita la cuenta de administrador del clúster LDAP o NIS `guest2` con `backup` el rol predefinido 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
```

Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

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 `publickey` como y 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 relacionada

- "inicio de sesión de seguridad"