



Administrar cuentas de administrador

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

- Administrar cuentas de administrador 1
 - Información general sobre las cuentas de administrador 1
 - Asociar una clave pública a una cuenta de administrador 1
 - Gestione claves públicas SSH y certificados X.509 para una cuenta de administrador 2
 - Configurar Cisco Duo 2FA para inicios de sesión SSH 4
 - Genere e instale una información general de certificados de servidor firmados por CA 9
 - Gestione los certificados con System Manager 13
 - Configurar la información general de acceso al controlador de dominio de Active Directory 18
 - Configure la información general sobre el acceso a servidores LDAP o NIS 20
 - Cambiar una contraseña de administrador 23
 - Bloquear y desbloquear una cuenta de administrador 24
 - Gestionar intentos fallidos de inicio de sesión 25
 - Aplicar SHA-2 en contraseñas de cuenta de administrador 25
 - Diagnosticar y corregir problemas de acceso a archivos 26

Administrar cuentas de administrador

Información general sobre las cuentas de administrador

En función de cómo haya habilitado el acceso a una cuenta, puede que deba asociar una clave pública a una cuenta local, instalar un certificado digital de servidor firmado por CA o configurar AD, LDAP o NIS. Es posible realizar todas estas tareas antes o después de habilitar el acceso a la cuenta.

Asociar una clave pública a una cuenta de administrador

Para la autenticación de clave pública SSH, debe asociar la clave pública a una cuenta de administrador para que la cuenta pueda acceder a la SVM. Puede utilizar el `security login publickey create` comando para asociar una clave a una cuenta de administrador.

Acerca de esta tarea

Si autentica una cuenta a través de SSH tanto con una contraseña como con una clave pública SSH, la cuenta se autentica primero con la clave pública.

Antes de empezar

- Debe haber generado la clave SSH.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Asociar una clave pública a una cuenta de administrador:

```
security login publickey create -vserver SVM_name -username user_name -index  
index -publickey certificate -comment comment
```

Para obtener una sintaxis completa del comando, consulte la referencia de la hoja de datos de ["Asociación de una clave pública con una cuenta de usuario"](#).

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

Ejemplo

El siguiente comando asocia una clave pública con la cuenta de administrador de SVM `svmin1`. Para la SVM `engData1`. A la clave pública se le asigna el número de índice 5.

```
cluster1:> security login publickey create -vserver engData1 -username  
svmin1 -index 5 -publickey  
<key text>
```

Gestione claves públicas SSH y certificados X,509 para una cuenta de administrador

Para una mayor seguridad de autenticación SSH con cuentas de administrador, puede utilizar el `security login publickey` Conjunto de comandos para administrar la clave pública SSH y su asociación con certificados X,509.

Asocie una clave pública y un certificado X,509 a una cuenta de administrador

A partir de ONTAP 9.13.1, puede asociar un certificado X,509 a la clave pública asociada a la cuenta de administrador. Esto le proporciona la seguridad añadida de las comprobaciones de caducidad o revocación de certificados al iniciar sesión SSH para esa cuenta.

Acerca de esta tarea

Si autentica una cuenta a través de SSH con una clave pública SSH y un certificado X,509, ONTAP comprueba la validez del certificado X,509 antes de autenticarse con la clave pública SSH. El inicio de sesión SSH se rechazará si ese certificado caduca o se revoca y la clave pública se deshabilitará automáticamente.

Antes de empezar

- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- Debe haber generado la clave SSH.
- Si solo necesita que el certificado X,509 sea verificado para su vencimiento, puede usar un certificado autofirmado.
- Si necesita que el certificado X,509 sea comprobado para su vencimiento y revocación:
 - Debe haber recibido el certificado de una CA.
 - Debe instalar la cadena de certificados (certificados de CA intermedios y raíz) mediante `security certificate install` comandos.
 - Debe habilitar OCSP para SSH. Consulte ["Verifique que los certificados digitales sean válidos mediante OCSP"](#) si desea obtener instrucciones.

Pasos

1. Asocie una clave pública y un certificado X,509 a una cuenta de administrador:

```
security login publickey create -vserver SVM_name -username user_name -index  
index -publickey certificate -x509-certificate install
```

Para obtener una sintaxis completa del comando, consulte la referencia de la hoja de datos de ["Asociación de una clave pública con una cuenta de usuario"](#).

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

Ejemplo

El siguiente comando asocia una clave pública y un certificado X,509 con la cuenta de administrador de SVM `svmin2` Para la SVM `engData2`. A la clave pública se le asigna el número de índice 6.

```
cluster1::> security login publickey create -vserver engData2 -username  
svmin2 -index 6 -publickey  
"<key text>" -x509-certificate install  
Please enter Certificate: Press <Enter> when done  
<certificate text>
```

Elimine la asociación de certificados de la clave pública SSH para una cuenta de administrador

Puede eliminar la asociación de certificados actual de la clave pública SSH de la cuenta, mientras conserva la clave pública.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Elimine la asociación de certificados X,509 de una cuenta de administrador y conserve la clave pública SSH existente:

```
security login publickey modify -vserver SVM_name -username user_name -index  
index -x509-certificate delete
```

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

Ejemplo

El siguiente comando quita la asociación de certificados X,509 de la cuenta de administrador de SVM svmin2 Para la SVM engData2 en el índice número 6.

```
cluster1::> security login publickey modify -vserver engData2 -username  
svmin2 -index 6 -x509-certificate delete
```

Elimine la asociación de clave pública y certificado de una cuenta de administrador

Puede eliminar la configuración de clave pública y certificado actual de una cuenta.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Elimine la clave pública y una asociación de certificados X,509 de una cuenta de administrador:

```
security login publickey delete -vserver SVM_name -username user_name -index  
index
```

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Ejemplo

El siguiente comando quita una clave pública y un certificado X,509 de la cuenta de administrador de SVM svmin3 Para la SVM engData3 en el índice número 7.

```
cluster1::> security login publickey delete -vserver engData3 -username svmin3 -index 7
```

Configurar Cisco Duo 2FA para inicios de sesión SSH

A partir de ONTAP 9.14.1, puede configurar ONTAP para que use Cisco Duo para la autenticación de dos factores (2FA) durante los inicios de sesión SSH. Se configura Duo a nivel de clúster y se aplica a todas las cuentas de usuario de forma predeterminada. También puede configurar Duo a nivel del equipo virtual de almacenamiento (anteriormente denominado Vserver), en cuyo caso sólo se aplica a los usuarios para dicho equipo virtual de almacenamiento. Si habilita y configura DUO, sirve como un método de autenticación adicional, que complementa los métodos existentes para todos los usuarios.

Si habilita la autenticación Duo para los inicios de sesión SSH, los usuarios tendrán que inscribir un dispositivo la próxima vez que inicien sesión con SSH. Para obtener información sobre la inscripción, consulte el Cisco Duo ["documentación de inscripción"](#).

Puede utilizar la interfaz de línea de comandos de ONTAP para realizar las siguientes tareas con Cisco Duo:

- [Configurar Cisco Duo](#)
- [Cambie la configuración de Cisco Duo](#)
- [Elimine la configuración de Cisco Duo](#)
- [Vea la configuración de Cisco Duo](#)
- [Eliminar un grupo Duo](#)
- [Ver grupos Duo](#)
- [Omitir autenticación Duo para usuarios](#)

Configurar Cisco Duo

Puede crear una configuración de Cisco Duo para todo el clúster o para un equipo virtual de almacenamiento específico (denominado Vserver en la CLI de ONTAP) mediante el `security login duo create` comando. Cuando hace esto, Cisco Duo se habilita para inicios de sesión SSH para este clúster o máquina virtual de almacenamiento.

Pasos

1. Inicie sesión en el panel de administración de Cisco Duo.

2. Vaya a **Aplicaciones > Aplicación UNIX**.
3. Registre la clave de integración, la clave secreta y el nombre de host de la API.
4. Inicie sesión en su cuenta de ONTAP con SSH.
5. Habilite la autenticación de Cisco Duo para esta VM de almacenamiento, sustituyendo la información de su entorno por los valores entre paréntesis:

```
security login duo create \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME>
```

Para obtener más información sobre los parámetros necesarios y opcionales para este comando, consulte ["Hojas de cálculo para la autenticación del administrador y la configuración de RBAC"](#).

Cambie la configuración de Cisco Duo

Puede cambiar la forma en que Cisco Duo autentica a los usuarios (por ejemplo, cuántas peticiones de datos de autenticación se dan o qué proxy HTTP se utiliza). Si necesita cambiar la configuración de Cisco Duo para un equipo virtual de almacenamiento (conocido como Vserver en la CLI de ONTAP), puede utilizar el `security login duo modify` comando.

Pasos

1. Inicie sesión en el panel de administración de Cisco Duo.
2. Vaya a **Aplicaciones > Aplicación UNIX**.
3. Registre la clave de integración, la clave secreta y el nombre de host de la API.
4. Inicie sesión en su cuenta de ONTAP con SSH.
5. Cambie la configuración de Cisco Duo para esta máquina virtual de almacenamiento, sustituyendo la información actualizada de su entorno por los valores entre paréntesis:

```
security login duo modify \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME> \  
-pushinfo true|false \  
-http-proxy <HTTP_PROXY_URL> \  
-autopush true|false \  
-prompts 1|2|3 \  
-max-unenrolled-logins <NUM_LOGINS> \  
-is-enabled true|false \  
-fail-mode safe|secure
```

Elimine la configuración de Cisco Duo

Puede eliminar la configuración de Cisco Duo, que eliminará la necesidad de que los usuarios de SSH se autenticuen mediante Duo al iniciar sesión. Para eliminar la configuración de Cisco Duo para un equipo virtual de almacenamiento (denominado Vserver en la CLI de ONTAP), puede utilizar el `security login duo delete` comando.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Elimine la configuración de Cisco Duo para esta máquina virtual de almacenamiento y sustituya el nombre de máquina virtual de almacenamiento para `<STORAGE_VM_NAME>`:

```
security login duo delete -vserver <STORAGE_VM_NAME>
```

De este modo se elimina de forma permanente la configuración de Cisco Duo para este equipo virtual de almacenamiento.

Vea la configuración de Cisco Duo

Puede ver la configuración existente de Cisco Duo para un equipo virtual de almacenamiento (denominado Vserver en la CLI de ONTAP) mediante el `security login duo show` comando.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Muestre la configuración de Cisco Duo para esta máquina virtual de almacenamiento. Opcionalmente, puede utilizar la `vserver` Parámetro para especificar una máquina virtual de almacenamiento, en lugar del nombre de la máquina virtual de almacenamiento para `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

Debería ver una salida similar a la siguiente:


```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Cree un grupo Duo

Puede indicar a Cisco Duo que incluya solo los usuarios de un determinado Active Directory, LDAP o grupo de usuarios local en el proceso de autenticación Duo. Si crea un grupo Duo, sólo se solicita la autenticación Duo a los usuarios de ese grupo. Puede crear un grupo Duo mediante `security login duo group create` comando. Al crear un grupo, opcionalmente puede excluir usuarios específicos de ese grupo del proceso de autenticación Duo.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Cree el grupo DUO, sustituyendo la información del entorno por los valores entre paréntesis. Si omite `-vserver` parámetro, el grupo se crea en el nivel de clúster:

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local. Usuarios que especifique con el opcional `-exclude-users` El parámetro no se incluirá en el proceso de autenticación Duo.

Ver grupos Duo

Puede ver las entradas de grupo Cisco Duo existentes mediante el `security login duo group show` comando.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Muestra las entradas del grupo Duo, sustituyendo la información del entorno por los valores entre paréntesis. Si omite `-vserver` parámetro, el grupo se muestra en el nivel de clúster:

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -exclude-users <USER1, USER2>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local. Usuarios que especifique con el opcional `-exclude-users` no se mostrará el parámetro.

Eliminar un grupo Duo

Puede eliminar una entrada de grupo Duo mediante `security login duo group delete` comando. Si elimina un grupo, los usuarios de ese grupo ya no se incluirán en el proceso de autenticación Duo.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Elimine la entrada de grupo Duo, sustituyendo la información de su entorno por los valores entre paréntesis. Si omite `-vserver` parámetro, el grupo se elimina en el nivel de clúster:

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local.

Omitir autenticación Duo para usuarios

Puede excluir a todos los usuarios o usuarios específicos del proceso de autenticación Duo SSH.

Excluir todos los usuarios de DUO

Puede deshabilitar la autenticación SSH de Cisco Duo para todos los usuarios.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Desactive la autenticación de Cisco Duo para usuarios SSH, sustituyendo el nombre de Vserver por `<STORAGE_VM_NAME>`:

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled=false
```

Excluir usuarios del grupo DUO

Puede excluir ciertos usuarios que forman parte de un grupo Duo del proceso de autenticación Duo SSH.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Desactive la autenticación de Cisco Duo para usuarios específicos de un grupo. Sustituya el nombre de grupo y la lista de usuarios para excluir los valores entre paréntesis:

```
security login group modify -group-name <GROUP_NAME> -exclude-users  
<USER1, USER2>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local. Usuarios que especifique con `-exclude-users` El parámetro no se incluirá en el proceso de autenticación Duo.

Excluir usuarios locales de DUO

Puede excluir a usuarios locales específicos del uso de la autenticación Duo mediante el panel de administración de Cisco Duo. Para obtener instrucciones, consulte "[Documentación de Cisco Duo](#)".

Genere e instale una información general de certificados de servidor firmados por CA

En los sistemas de producción, se recomienda instalar un certificado digital firmado por CA para usarlo en la autenticación del clúster o SVM como servidor SSL. Puede utilizar el `security certificate generate-csr` Para generar una solicitud de firma de certificación (CSR) y la `security certificate install` comando para instalar el certificado que recibe de la autoridad de certificación.

Genere una solicitud de firma de certificación

Puede utilizar el `security certificate generate-csr` Comando para generar una solicitud de firma de certificación (CSR). Después de procesar la solicitud, la entidad de certificación (CA) envía el certificado digital firmado.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Genere una CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size  
512|1024|1536|2048 -country country -state state -locality locality  
-organization organization -unit unit -email-addr email_of_contact -hash  
-function SHA1|SHA256|MD5
```

El siguiente comando crea un CSR con una clave privada de 2048 bits generada por la función de hash «SHA256» para su uso por el grupo «Software» en el departamento «IT» de una empresa cuyo nombre común personalizado es «`server1.companyname.com``», ubicada en Sunnyvale, California, EE.UU. La dirección de correo electrónico del administrador de contacto de SVM es «``web@example.com``». El sistema muestra la CSR y la clave privada en la salida.

Ejemplo de creación de una CSR

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
```

Certificate Signing Request :

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCMVVMx
CTAHBgNVBAgtADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBChUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

-----BEGIN RSA PRIVATE KEY-----

```
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+jlhrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
```

Note: Please keep a copy of your certificate request and private key for future reference.

2. Copie la solicitud de certificado de la salida CSR y envíela en formato electrónico (por ejemplo, correo electrónico) a una CA de terceros de confianza para su firma.

Después de procesar la solicitud, la CA envía el certificado digital firmado. Debe conservar una copia de la clave privada y el certificado digital firmado por la CA.

Instale un certificado de servidor firmado por CA

Puede utilizar el `security certificate install` Comando para instalar un certificado de servidor firmado por CA en una SVM. ONTAP solicita los certificados raíz y intermedios de la entidad de certificación (CA) que forman la cadena de certificados del certificado de servidor.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Paso

1. Instale un certificado de servidor firmado por CA:

```
security certificate install -vserver SVM_name -type certificate_type
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).



ONTAP solicita los certificados intermedios y de raíz de CA que forman la cadena de certificados del certificado de servidor. La cadena comienza con el certificado de la CA que emitió el certificado de servidor y puede llegar hasta el certificado raíz de la CA. Cualquier certificado intermedio que falte provocará el error en la instalación del certificado de servidor.

El siguiente comando instala el certificado de servidor firmado por CA y los certificados intermedios en SVM 'engData2'.

Ejemplo de instalación de certificados intermedios de certificado de servidor firmados por CA

```
cluster1:>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCA ZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADAJMAcGA1UECXMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADAJMAcGA1UECXMAM
Q8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C6lX2G32Sx8VEalth94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG7lUyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAZt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSGAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bG1dZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbG1dZXJ0IENsYXNzIDIGUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDEwExd3d3LnZhbG1jZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECXMOR28gRGFkZkhkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACzG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEzhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTE5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACzG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENs
YXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEzhodHRw
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.

Gestione los certificados con System Manager

A partir de ONTAP 9.10.1, se puede utilizar System Manager para gestionar autoridades de certificados de confianza, certificados de cliente/servidor y autoridades de certificados locales (integradas).

Con System Manager, puede gestionar los certificados recibidos de otras aplicaciones para que pueda autenticar las comunicaciones de dichas aplicaciones. También puede administrar sus propios certificados que identifican su sistema a otras aplicaciones.

Ver información del certificado

Con System Manager, es posible ver las autoridades de certificados de confianza, los certificados de cliente/servidor y las autoridades de certificados locales almacenadas en el clúster.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Desplácese hasta el área **Seguridad**.
En la sección **certificados**, se muestran los siguientes detalles:
 - El número de autoridades de certificados de confianza almacenadas.
 - El número de certificados de cliente/servidor almacenados.
 - El número de autoridades de certificados locales almacenadas.
3. Seleccione cualquier número para ver los detalles de una categoría de certificados o seleccione → Para abrir la página **Certificados**, que contiene información sobre todas las categorías.
La lista muestra la información del clúster completo. Si desea mostrar información solo de una máquina virtual de almacenamiento específica, realice los pasos siguientes:
 - a. Seleccione **Almacenamiento > Storage VMs**.

- b. Seleccione la máquina virtual de almacenamiento.
- c. Cambie a la pestaña **Settings**.
- d. Seleccione un número que se muestra en la sección **Certificado**.

Qué hacer a continuación

- Desde la página **certificados**, puede [Genere una solicitud de firma de certificación](#).
- La información del certificado se divide en tres fichas, una para cada categoría. Es posible realizar las siguientes tareas desde cada pestaña:

En esta pestaña...	Puede ejecutar estos procedimientos...
Autoridades de certificados de confianza	<ul style="list-style-type: none"> • [install-trusted-cert] • Elimine una entidad de certificación de confianza • Renueve una entidad de certificación de confianza
Certificados cliente/servidor	<ul style="list-style-type: none"> • [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
Autoridades de certificados locales	<ul style="list-style-type: none"> • Cree una nueva entidad de certificación local • Firme un certificado mediante una entidad de certificación local • Elimine una entidad de certificación local • Renueve una autoridad de certificación local

Genere una solicitud de firma de certificación

Puede generar una solicitud de firma de certificación (CSR) con System Manager desde cualquier pestaña de la página **certificados**. Se genera una clave privada y una CSR correspondiente, que se pueden firmar mediante una autoridad de certificación para generar un certificado público.


Pasos

1. Abra la página **certificados**. Consulte [Ver información del certificado](#).
2. Seleccione **+Generar CSR**.
3. Complete la información del nombre del asunto:
 - a. Introduzca un **nombre común**.
 - b. Seleccione un **país**.
 - c. Introduzca una **organización**.
 - d. Introduzca una **unidad organizativa**.
4. Si desea anular los valores predeterminados, seleccione **más opciones** y proporcione información adicional.

Instale (añada) una entidad de certificación de confianza

Puede instalar autoridades de certificado de confianza adicionales en System Manager.

Pasos

1. Abra la pestaña **autoridades de certificados de confianza**. Consulte [Ver información del certificado](#).
2. Seleccione .
3. En el panel **Agregar autoridad de certificado de confianza**, realice lo siguiente:
 - Introduzca un **nombre**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
 - Seleccione un **tipo**.
 - Introduzca o importe **detalles del certificado**.


Elimine una entidad de certificación de confianza

Con System Manager, es posible eliminar una entidad de certificación de confianza.



No puede eliminar las autoridades de certificación de confianza preinstaladas con ONTAP.


Pasos

1. Abra la pestaña **autoridades de certificados de confianza**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la entidad de certificación de confianza.
3. Seleccione  Junto al nombre, luego selecciona **Eliminar**.

Renueve una entidad de certificación de confianza

Con System Manager, puede renovar una entidad de certificación de confianza que ha caducado o está a punto de expirar.

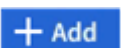
Pasos

1. Abra la pestaña **autoridades de certificados de confianza**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la entidad de certificación de confianza.
3. Seleccione  Junto al nombre del certificado, luego **Renew**.

Instale (agregue) un certificado de cliente/servidor

Con System Manager, puede instalar certificados de cliente/servidor adicionales.

Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione .
3. En el panel **Agregar certificado de cliente/servidor**, realice lo siguiente:
 - Introduzca un **nombre de certificado**.

- Para **Scope**, seleccione un equipo virtual de almacenamiento.
- Introduzca un **nombre común**.
- Seleccione un **tipo**.
- Introduzca o importe **detalles del certificado**.
Puede escribir o copiar y pegar los detalles del certificado desde un archivo de texto o puede importar el texto desde un archivo de certificado haciendo clic en **Importar**.
- Introduzca la **clave privada**.
Puede escribir o copiar y pegar en la clave privada desde un archivo de texto o puede importar el texto desde un archivo de claves privadas haciendo clic en **Importar**.

Genere (agregue) un certificado de cliente/servidor autofirmado

Con System Manager, puede generar otros certificados de cliente/servidor autofirmados.


Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione **+Generar certificado autofirmado**.
3. En el panel **generar certificado autofirmado**, realice lo siguiente:
 - Introduzca un **nombre de certificado**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
 - Seleccione un **tipo**.
 - Seleccione una función **hash**.
 - Seleccione un **tamaño de clave**.
 - Seleccione una **VM de almacenamiento**.

Eliminar un certificado de cliente/servidor

Con System Manager, puede eliminar certificados de cliente/servidor.


Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre del certificado de cliente/servidor.
3. Seleccione  Junto al nombre, haga clic en **Eliminar**.

Renueve un certificado de cliente/servidor

Con System Manager, puede renovar un certificado de cliente/servidor que ha caducado o está a punto de expirar.


Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre del certificado de cliente/servidor.
3. Seleccione  Junto al nombre, haga clic en **renovar**.

Cree una nueva entidad de certificación local

Con System Manager, es posible crear una nueva entidad de certificación local.

Pasos

1. Abra la ficha **autoridades de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione  **Add**.
3. En el panel **Agregar autoridad de certificación local**, realice lo siguiente:
 - Introduzca un **nombre**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
4. Si desea anular los valores predeterminados, seleccione **más opciones** y proporcione información adicional.

Firme un certificado mediante una entidad de certificación local

En System Manager, es posible usar una entidad de certificación local para firmar un certificado.


Pasos

1. Abra la ficha **autoridades de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la autoridad de certificación local.
3. Seleccione  Junto al nombre luego **Firma un certificado**.
4. Complete el formulario **firmar una solicitud de firma de certificado**.
 - Puede pegar el contenido de firma de certificados o importar un archivo de solicitud de firma de certificados haciendo clic en **Importar**.
 - Especifique el número de días para los que será válido el certificado.

Elimine una entidad de certificación local

Con System Manager, es posible eliminar una entidad de certificación local.


Pasos

1. Abra la ficha **Autoridad de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la autoridad de certificación local.
3. Seleccione  Junto al nombre luego **Eliminar**.

Renueve una autoridad de certificación local

Con System Manager, puede renovar una autoridad de certificado local que ha caducado o está a punto de expirar.

Pasos

1. Abra la ficha **Autoridad de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la autoridad de certificación local.
3. Seleccione  Junto al nombre, haga clic en **renovar**.

Configurar la información general de acceso al controlador de dominio de Active Directory

Para poder acceder a la SVM, es necesario configurar el acceso de la controladora de dominio de AD al clúster o a la SVM. Si ya ha configurado un servidor SMB para una SVM de datos, puede configurar la SVM como puerta de enlace, o *tunnel*, para el acceso de AD al clúster. Si no configuró un servidor SMB, puede crear una cuenta de equipo para la SVM en el dominio de AD.

ONTAP admite los siguientes servicios de autenticación de controladores de dominio:

- Kerberos
- LDAP
- Netlogon
- Autoridad de seguridad local (LSA)

ONTAP admite los siguientes algoritmos de clave de sesión para conexiones seguras de Netlogon:

Algoritmo de clave de sesión	Disponible empezando por...
HMAC-SHA256, basado en el estándar de cifrado avanzado (AES) Si el clúster ejecuta ONTAP 9.9.1 o una versión anterior y el controlador de dominio aplica AES para los servicios seguros de Netlogon, la conexión falla. En este caso, debe reconfigurar el controlador de dominio para aceptar conexiones de clave fuerte con ONTAP.	ONTAP 9.10.1
DES y HMAC-MD5 (cuando se establece la clave fuerte)	Todas las versiones de ONTAP 9

Si desea utilizar claves de sesión AES durante la creación de canal seguro Netlogon, debe verificar que AES esté habilitado en su SVM.

- A partir de ONTAP 9.14.1, AES se habilita de forma predeterminada cuando crea una SVM y no necesita modificar la configuración de seguridad de su SVM para utilizar las claves de sesión AES durante la establecimiento de canal seguro Netlogon.
- En ONTAP 9.10.1 a 9.13.1, AES se deshabilita de forma predeterminada al crear una SVM. Debe habilitar AES mediante el siguiente comando:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```



Cuando se actualice a ONTAP 9.14.1 o una versión posterior, la configuración de AES para las SVM existentes creadas con versiones de ONTAP anteriores no cambiará automáticamente. Aún debe actualizar el valor de esta configuración para habilitar AES en esas SVM.

Configure un túnel de autenticación

Si ya ha configurado un servidor SMB para una SVM de datos, puede usar el `security login domain-tunnel create` Comando para configurar la SVM como puerta de enlace, o *tunnel*, para obtener acceso AD al clúster.

Antes de empezar

- Debe haber configurado un servidor SMB para una SVM de datos.
- Debe haber habilitado una cuenta de usuario de dominio de AD para acceder a la SVM de administrador para el clúster.
- Para realizar esta tarea, debe ser un administrador de clústeres.

A partir de ONTAP 9.10.1, si tiene una puerta de enlace SVM (túnel de dominio) para acceso AD, puede usar Kerberos para autenticación de administrador si ha deshabilitado NTLM en el dominio de AD. En versiones anteriores, Kerberos no era compatible con la autenticación de administrador para puertas de enlace de SVM. Esta funcionalidad está disponible de forma predeterminada; no se requiere configuración.



La autenticación Kerberos siempre se intenta primero. En caso de error, se intenta la autenticación NTLM.

Paso

1. Configure una SVM de datos habilitada para SMB como túnel de autenticación para el acceso de la controladora de dominio AD al clúster:

```
security login domain-tunnel create -vserver svm_name
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).



La SVM debe estar en ejecución para que el usuario se autentique.

El siguiente comando configura la SVM de datos habilitada para SMB como túnel de autenticación.

```
cluster1::>security login domain-tunnel create -vserver engData
```

Cree una cuenta de equipo SVM en el dominio

Si no ha configurado un servidor SMB para una SVM de datos, puede usar el `vserver active-directory create` Comando para crear una cuenta de equipo para la SVM en el dominio.

Acerca de esta tarea

Después de introducir el `vserver active-directory create` Se le pedirá que proporcione las credenciales de una cuenta de usuario de AD con privilegios suficientes para agregar equipos a la unidad organizativa especificada en el dominio. La contraseña de la cuenta no puede estar vacía.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Paso

1. Cree una cuenta de equipo para una SVM en el dominio de AD:

```
vserver active-directory create -vserver SVM_name -account-name  
NetBIOS_account_name -domain domain -ou organizational_unit
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

El siguiente comando crea una cuenta de computadora llamada 'ADSERVER1' en el dominio 'example.com' para SVM 'engData'. Se le pedirá que introduzca las credenciales de cuenta de usuario de AD después de introducir el comando.

```
cluster1::>vserver active-directory create -vserver engData -account  
-name ADSERVER1 -domain example.com
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: Administrator

Enter the password:

Configure la información general sobre el acceso a servidores LDAP o NIS

Debe configurar el acceso del servidor LDAP o NIS a una SVM para que las cuentas LDAP o NIS puedan acceder a la SVM. La función de conmutador le permite utilizar LDAP o NIS como fuentes alternativas de servicio de nombres.

Configure el acceso al servidor LDAP

Para que las cuentas LDAP puedan acceder a la SVM, debe configurar el acceso del servidor LDAP a una SVM. Puede utilizar el `vserver services name-service ldap client create` Comando para crear una configuración de cliente LDAP en la SVM. A continuación, puede utilizar la `vserver services name-service ldap create` Comando para asociar la configuración del cliente LDAP con la SVM.

Acerca de esta tarea

La mayoría de los servidores LDAP pueden utilizar los esquemas predeterminados proporcionados por ONTAP:

- MS-AD-BIS (el esquema preferido para la mayoría de los servidores AD de Windows 2012 y posteriores)
- AD-IDMU (Windows 2008, Windows 2016 y servidores AD posteriores)
- AD-SFU (servidores Windows 2003 y anteriores de AD)
- RFC-2307 (SERVIDORES UNIX LDAP)

Es mejor utilizar los esquemas predeterminados a menos que haya un requisito para hacer lo contrario. Si es

así, puede crear su propio esquema copiando un esquema predeterminado y modificando la copia. Para obtener más información, consulte:

- ["Configuración de NFS"](#)
- ["Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP"](#)

Antes de empezar

- Debe haber instalado un ["Certificado digital de servidor firmado por CA"](#) En la SVM.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Cree una configuración de cliente LDAP en una SVM:

```
vserver services name-service ldap client create -vserver SVM_name -client
-config client_configuration -servers LDAP_server_IPs -schema schema -use
-start-tls true|false
```



Start TLS es compatible únicamente para acceder a las SVM de datos. No admite el acceso a las SVM de administración.

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

El siguiente comando crea una configuración de cliente LDAP llamada «corp» en SVM «engData». El cliente hace enlaces anónimos a los servidores LDAP con las direcciones IP 172.160.0.100 y 172.16.0.101. El cliente utiliza el esquema RFC-2307 para realizar consultas LDAP. La comunicación entre el cliente y el servidor se cifra mediante Start TLS.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```



A partir de ONTAP 9.2, el campo `-ldap-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor LDAP.

2. Asocie la configuración del cliente LDAP con la SVM:

```
vserver services name-service ldap
create -vserver SVM_name -client-config client_configuration -client-enabled
true|false
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

El siguiente comando asocia la configuración del cliente LDAP corp Con la SVM engData, Y habilita el cliente LDAP en la SVM.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```



A partir de ONTAP 9.2, el `vserver services name-service ldap create` El comando realiza una validación automática de la configuración e informa de un mensaje de error si ONTAP no puede comunicarse con el servidor de nombres.

3. Validar el estado de los servidores de nombres mediante el comando `vserver Services NAME-service ldap check`.

El siguiente comando valida los servidores LDAP en la SVM vs0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13". |
```

El comando `name service check` está disponible a partir de ONTAP 9.2.

Configurar el acceso al servidor NIS

Debe configurar el acceso del servidor NIS a una SVM antes de que las cuentas NIS puedan acceder a la SVM. Puede utilizar el `vserver services name-service nis-domain create` Comando para crear una configuración de dominio NIS en una SVM.

Acerca de esta tarea

Puede crear varios dominios NIS. Sólo se puede establecer un dominio NIS en `active` a la vez.

Antes de empezar

- Todos los servidores configurados deben estar disponibles y accesibles antes de configurar el dominio NIS en la SVM.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Paso

1. Cree una configuración de dominio NIS en una SVM:

```
vserver services name-service nis-domain create -vserver SVM_name -domain
client_configuration -active true|false -nis-servers NIS_server_IPs
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).



A partir de ONTAP 9.2, el campo `-nis-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor NIS.

El siguiente comando crea una configuración de dominio NIS en 'engData' de SVM. El dominio NIS `nisdomain` Está activo durante la creación y se comunica con un servidor NIS con la dirección IP `192.0.2.180`.


```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

Crear un conmutador de servicio de nombres

La función de conmutador de servicio de nombres le permite utilizar LDAP o NIS como fuentes alternativas de servicio de nombres. Puede utilizar el `vserver services name-service ns-switch modify` para especificar el orden de búsqueda de fuentes de servicio de nombres.

Antes de empezar

- Debe haber configurado el acceso a los servidores LDAP y NIS.
- Debe ser un administrador de clúster o un administrador de SVM para ejecutar esta tarea.

Paso

1. Especifique el orden de búsqueda para los orígenes de servicios de nombres:

```
vserver services name-service ns-switch modify -vserver SVM_name -database
name_service_switch_database -sources name_service_source_order
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

El siguiente comando especifica el orden de búsqueda de los orígenes de servicios de nombres LDAP y NIS para la base de datos «passwd» en SVM «engData».

```
cluster1::>vserver services name-service ns-switch
modify -vserver engData -database passwd -source files ldap,nis
```

Cambiar una contraseña de administrador

Debe cambiar la contraseña inicial inmediatamente después de iniciar sesión en el sistema por primera vez. Si es un administrador de SVM, puede usar el `security login password` para cambiar su propia contraseña. Si es un administrador de clúster, puede utilizar el `security login password` para cambiar la contraseña de cualquier administrador.

Acerca de esta tarea

La nueva contraseña debe respetar las siguientes reglas:

- No puede contener el nombre de usuario
- Debe tener al menos 8 caracteres
- Debe contener al menos una letra y un número
- No puede ser igual que las últimas seis contraseñas



Puede utilizar el `security login role config modify` comando para modificar las reglas de contraseña de las cuentas de asociadas con un rol determinado. Para obtener más información, consulte ["referencia de comandos"](#).

Antes de empezar

- Debe ser un administrador de clústeres o SVM para cambiar su propia contraseña.
- Para cambiar la contraseña de otro administrador, debe ser un administrador de clústeres.

Paso

1. Cambiar una contraseña de administrador: `security login password -vserver svm_name -username user_name`

El siguiente comando cambia la contraseña del administrador `admin1` Para la SVM `vs1.example.com`. Se le pedirá que introduzca la contraseña actual, a continuación, introduzca y vuelva a introducir la nueva contraseña.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

Bloquear y desbloquear una cuenta de administrador

Puede utilizar el `security login lock` para bloquear una cuenta de administrador y la `security login unlock` comando para desbloquear la cuenta.

Antes de empezar

Para poder realizar estas tareas, debe ser un administrador de clústeres.

Pasos

1. Bloquear una cuenta de administrador:

```
security login lock -vserver SVM_name -username user_name
```

El siguiente comando bloquea la cuenta de administrador `admin1` Para la SVM `vs1.example.com`:

```
cluster1::>security login lock -vserver engData -username admin1
```

2. Desbloquear una cuenta de administrador:

```
security login unlock -vserver SVM_name -username user_name
```

El siguiente comando desbloquea la cuenta de administrador `admin1` Para la SVM `vs1.example.com`:

```
cluster1::>security login unlock -vserver engData -username admin1
```

Gestionar intentos fallidos de inicio de sesión

Los intentos repetidos de inicio de sesión fallidos a veces indican que un intruso está intentando acceder al sistema de almacenamiento. Puede tomar una serie de pasos para asegurarse de que no se produzca una intrusión.

Cómo sabrá que los intentos de inicio de sesión han fallado

El sistema de gestión de eventos (EMS) notifica los intentos de inicio de sesión con errores cada hora. Puede encontrar un registro de intentos fallidos de inicio de sesión en `audit.log` archivo.

Qué hacer si fallan los intentos repetidos de inicio de sesión

A corto plazo, puede tomar una serie de pasos para evitar una intrusión:

- Requerir que las contraseñas estén compuestas por un número mínimo de caracteres en mayúscula, caracteres en minúscula, caracteres especiales y/o dígitos
- Imponer un retraso tras un intento de inicio de sesión fallido
- Limite el número de intentos fallidos permitidos y bloquee los usuarios después del número especificado de intentos fallidos
- Caducar y bloquee cuentas que estén inactivas durante un número determinado de días

Puede utilizar el `security login role config modify` comando para ejecutar estas tareas.

A largo plazo, puede realizar estos pasos adicionales:

- Utilice la `security ssh modify` Comando para limitar el número de intentos de inicio de sesión con errores de todas las SVM recién creadas.
- Migre las cuentas de algoritmo MD5 existentes al algoritmo SHA-512 más seguro al requerir que los usuarios cambien sus contraseñas.

Aplicar SHA-2 en contraseñas de cuenta de administrador

Las cuentas de administrador creadas antes de ONTAP 9.0 siguen utilizando contraseñas MD5 después de la actualización, hasta que las contraseñas se modifican manualmente. MD5 es menos seguro que SHA-2. Por lo tanto, después de la actualización, debería pedir a los usuarios de cuentas MD5 que cambien sus contraseñas para utilizar la función hash SHA-512 predeterminada.

Acerca de esta tarea

La funcionalidad hash de contraseña le permite hacer lo siguiente:

- Muestra las cuentas de usuario que coinciden con la función hash especificada.
- Caducar cuentas que utilizan una función hash especificada (por ejemplo, MD5), obligando a los usuarios

a cambiar sus contraseñas en su siguiente inicio de sesión.

- Bloquear cuentas cuyas contraseñas utilizan la función hash especificada.
- Al volver a una versión anterior a ONTAP 9, restablezca la contraseña propia del administrador del clúster para que sea compatible con la función hash (MD5) admitida por la versión anterior.

ONTAP solo acepta contraseñas SHA-2 predefinidas mediante el SDK de capacidad de gestión de NetApp (`security-login-create` y `security-login-modify-password`).

Pasos

1. Migrar las cuentas de administrador MD5 a la función hash de contraseña SHA-512:

- a. Caducar todas las cuentas de administrador de MD5: `security login expire-password -vserver * -username * -hash-function md5`

Al hacerlo, se obliga a los usuarios de cuentas MD5 a cambiar sus contraseñas al siguiente inicio de sesión.

- b. Pida a los usuarios de cuentas MD5 que inicien sesión a través de una consola o una sesión SSH.

El sistema detecta que las cuentas han caducado y solicita a los usuarios que cambien sus contraseñas. SHA-512 se utiliza de forma predeterminada para las contraseñas modificadas.

2. Para las cuentas MD5 cuyos usuarios no inician sesión para cambiar sus contraseñas en un período de tiempo, fuerce la migración de la cuenta:

- a. Cuentas de bloqueo que todavía utilizan la función hash MD5 (nivel de privilegio avanzado):
`security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

Después del número de días especificado por `-lock-after`, Los usuarios no pueden acceder a sus cuentas MD5.

- b. Desbloquee las cuentas cuando los usuarios estén preparados para cambiar sus contraseñas:
`security login unlock -vserver svm_name -username user_name`

- c. Hacer que los usuarios inicien sesión en sus cuentas mediante una sesión SSH o de consola y cambien sus contraseñas cuando el sistema les solicite que lo hagan.

Diagnosticar y corregir problemas de acceso a archivos

Pasos

1. En System Manager, seleccione **almacenamiento > Storage VMs**.
2. Seleccione la máquina virtual de almacenamiento a la que desee realizar un seguimiento.
3. Haga clic en **Más**.
4. Haga clic en **acceso a archivos de rastreo**.
5. Proporcione el nombre de usuario y la dirección IP del cliente y, a continuación, haga clic en **Iniciar rastreo**.

Los resultados del seguimiento se muestran en una tabla. La columna **razones** proporciona la razón por la que no se pudo acceder a un archivo.

6. Haga clic en  en la columna izquierda de la tabla de resultados para ver los permisos de acceso a

archivos.

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.