



# **Gestire gli account amministratore**

## **ONTAP 9**

NetApp  
April 24, 2024

# Sommario

Gestire gli account amministratore .....	1
Panoramica sulla gestione degli account amministratore .....	1
Associare una chiave pubblica a un account amministratore .....	1
Gestire le chiavi pubbliche SSH e i certificati X.509 per un account amministratore .....	2
Configurare Cisco Duo 2FA per gli accessi SSH .....	4
Generare e installare una panoramica del certificato server firmato dalla CA .....	9
Gestire i certificati con System Manager .....	13
Panoramica sull'accesso al controller di dominio di Active Directory .....	18
Configurare la panoramica dell'accesso al server LDAP o NIS .....	20
Modificare la password dell'amministratore .....	23
Bloccare e sbloccare un account amministratore .....	24
Gestire i tentativi di accesso non riusciti .....	25
Applicare SHA-2 sulle password dell'account amministratore .....	25
Diagnosticare e correggere i problemi di accesso ai file .....	26

# Gestire gli account amministratore

## Panoramica sulla gestione degli account amministratore

A seconda di come è stato attivato l'accesso all'account, potrebbe essere necessario associare una chiave pubblica a un account locale, installare un certificato digitale del server firmato dalla CA o configurare l'accesso ad, LDAP o NIS. È possibile eseguire tutte queste attività prima o dopo aver attivato l'accesso all'account.

## Associare una chiave pubblica a un account amministratore

Per l'autenticazione a chiave pubblica SSH, è necessario associare la chiave pubblica a un account amministratore prima che l'account possa accedere a SVM. È possibile utilizzare `security login publickey create` comando per associare una chiave a un account amministratore.

### A proposito di questa attività

Se si autentica un account su SSH con una password e una chiave pubblica SSH, l'account viene autenticato prima con la chiave pubblica.

### Prima di iniziare

- È necessario aver generato la chiave SSH.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fasi

1. Associare una chiave pubblica a un account amministratore:

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

Per la sintassi completa dei comandi, vedere il riferimento al foglio di lavoro per ["Associazione di una chiave pubblica a un account utente"](#).

2. Verificare la modifica visualizzando la chiave pubblica:

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

### Esempio

Il seguente comando associa una chiave pubblica all'account amministratore di SVM `svmadmin1` Per SVM `engData1`. Alla chiave pubblica viene assegnato il numero di indice 5.

```
cluster1::> security login publickey create -vserver engData1 -username  
svmadmin1 -index 5 -publickey  
"<key text>"
```

# Gestire le chiavi pubbliche SSH e i certificati X.509 per un account amministratore

Per una maggiore sicurezza di autenticazione SSH con gli account amministratore, è possibile utilizzare `security login publickey` Set di comandi per gestire la chiave pubblica SSH e la sua associazione con i certificati X.509.

## Associare una chiave pubblica e un certificato X.509 a un account amministratore

A partire da ONTAP 9.13.1, è possibile associare un certificato X.509 alla chiave pubblica associata all'account amministratore. In questo modo si ottiene la sicurezza aggiuntiva dei controlli di scadenza o revoca del certificato al momento dell'accesso SSH per quell'account.

### A proposito di questa attività

Se si autentica un account su SSH con una chiave pubblica SSH e un certificato X.509, ONTAP verifica la validità del certificato X.509 prima di autenticarsi con la chiave pubblica SSH. L'accesso SSH verrà rifiutato se il certificato è scaduto o revocato e la chiave pubblica verrà disattivata automaticamente.

### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- È necessario aver generato la chiave SSH.
- Se è necessario controllare solo la scadenza del certificato X.509, è possibile utilizzare un certificato autofirmato.
- Se è necessario controllare la scadenza e la revoca del certificato X.509:
  - È necessario aver ricevuto il certificato da un'autorità di certificazione (CA).
  - È necessario installare la catena di certificati (certificati CA intermedi e principali) utilizzando `security certificate install` comandi.
  - Devi attivare OCSP per SSH. Fare riferimento a ["Verificare che i certificati digitali siano validi utilizzando OCSP"](#) per istruzioni.

### Fasi

1. Associare una chiave pubblica e un certificato X.509 a un account amministratore:

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

Per la sintassi completa dei comandi, vedere il riferimento al foglio di lavoro per ["Associazione di una chiave pubblica a un account utente"](#).

2. Verificare la modifica visualizzando la chiave pubblica:

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

### Esempio

Il seguente comando associa una chiave pubblica e un certificato X.509 all'account amministratore SVM `svmadmin2` Per SVM `engData2`. Alla chiave pubblica viene assegnato il numero di indice 6.

```
cluster1::> security login publickey create -vserver engData2 -username  
svmadmin2 -index 6 -publickey  
"<key text>" -x509-certificate install  
Please enter Certificate: Press <Enter> when done  
<certificate text>
```

## Rimuovere l'associazione del certificato dalla chiave pubblica SSH per un account amministratore

È possibile rimuovere l'associazione del certificato corrente dalla chiave pubblica SSH dell'account, mantenendo la chiave pubblica.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fasi

1. Rimuovere l'associazione del certificato X.509 da un account amministratore e conservare la chiave pubblica SSH esistente:

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

2. Verificare la modifica visualizzando la chiave pubblica:

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

### Esempio

Il comando seguente rimuove l'associazione del certificato X.509 dall'account amministratore SVM svmadmin2 Per SVM engData2 al numero di indice 6.

```
cluster1::> security login publickey modify -vserver engData2 -username  
svmadmin2 -index 6 -x509-certificate delete
```

## Rimuovere la chiave pubblica e l'associazione del certificato da un account amministratore

È possibile rimuovere la chiave pubblica corrente e la configurazione del certificato da un account.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fasi

1. Rimuovere la chiave pubblica e un'associazione di certificati X.509 da un account amministratore:

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

2. Verificare la modifica visualizzando la chiave pubblica:

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

### Esempio

Il comando seguente rimuove una chiave pubblica e un certificato X.509 dall'account amministratore SVM svmadmin3 Per SVM engData3 al numero di indice 7.

```
cluster1::> security login publickey delete -vserver engData3 -username svmadmin3 -index 7
```

## Configurare Cisco Duo 2FA per gli accessi SSH

A partire da ONTAP 9.14.1, è possibile configurare ONTAP in modo che utilizzi Cisco Duo per l'autenticazione a due fattori (2FA) durante gli accessi SSH. Duo viene configurato a livello di cluster e si applica a tutti gli account utente per impostazione predefinita. In alternativa, è possibile configurare Duo al livello della VM di storage (precedentemente denominata vserver), nel qual caso si applica solo agli utenti della VM di storage. Se abiliti e configuri Duo, serve come metodo di autenticazione aggiuntivo, che integra i metodi esistenti per tutti gli utenti.

Se si abilita l'autenticazione Duo per gli accessi SSH, gli utenti dovranno registrare un dispositivo al successivo accesso tramite SSH. Per informazioni sulla registrazione, fare riferimento a Cisco Duo ["documentazione di iscrizione"](#).

È possibile utilizzare l'interfaccia della riga di comando di ONTAP per eseguire le seguenti operazioni con Cisco Duo:

- [Configurare Cisco Duo](#)
- [Modificare la configurazione di Cisco Duo](#)
- [Rimuovere la configurazione di Cisco Duo](#)
- [Visualizzare la configurazione di Cisco Duo](#)
- [Rimuovere un gruppo Duo](#)
- [Visualizza i gruppi Duo](#)
- [Ignora autenticazione Duo per gli utenti](#)

## Configurare Cisco Duo

Puoi creare una configurazione di Cisco Duo per l'intero cluster o per una macchina virtuale storage specifica (denominata vserver nell'interfaccia a riga di comando di ONTAP) utilizzando il `security login duo create` comando. A tale scopo, Cisco Duo è abilitato per gli accessi SSH per il cluster o per la VM di storage.

### Fasi

1. Accedere al pannello di amministrazione di Cisco Duo.

2. Andare a **applicazioni > applicazioni UNIX**.
3. Registrare la chiave di integrazione, la chiave segreta e il nome host API.
4. Accedere al proprio account ONTAP utilizzando SSH.
5. Abilitare l'autenticazione Cisco Duo per questa VM di storage, sostituendo le informazioni dell'ambiente ai valori tra parentesi:

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

Per ulteriori informazioni sui parametri richiesti e facoltativi per questo comando, fare riferimento a ["Fogli di lavoro per l'autenticazione dell'amministratore e la configurazione RBAC"](#).

## Modificare la configurazione di Cisco Duo

È possibile modificare il modo in cui Cisco Duo autentica gli utenti (ad esempio, il numero di richieste di autenticazione o il proxy HTTP utilizzato). Se è necessario modificare la configurazione di Cisco Duo per una macchina virtuale di storage (nota come vserver nell'interfaccia CLI di ONTAP), è possibile utilizzare `security login duo modify` comando.

### Fasi

1. Accedere al pannello di amministrazione di Cisco Duo.
2. Andare a **applicazioni > applicazioni UNIX**.
3. Registrare la chiave di integrazione, la chiave segreta e il nome host API.
4. Accedere al proprio account ONTAP utilizzando SSH.
5. Modificare la configurazione di Cisco Duo per questa VM di archiviazione, sostituendo le informazioni aggiornate dell'ambiente ai valori tra parentesi:

```
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
```

## Rimuovere la configurazione di Cisco Duo

È possibile rimuovere la configurazione di Cisco Duo, che elimina la necessità per gli utenti SSH di eseguire l'autenticazione utilizzando Duo al momento dell'accesso. Per rimuovere la configurazione di Cisco Duo per una VM di storage (nota come server virtuale nell'interfaccia CLI di ONTAP), è possibile utilizzare `security login duo delete` comando.

### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Rimuovere la configurazione Cisco Duo per questa VM di archiviazione, sostituendo il nome della VM di archiviazione con `<STORAGE_VM_NAME>`:

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

In questo modo viene eliminata in modo permanente la configurazione di Cisco Duo per questa VM di storage.

## Visualizzare la configurazione di Cisco Duo

È possibile visualizzare la configurazione di Cisco Duo esistente di una macchina virtuale di storage (definita vserver nell'interfaccia CLI di ONTAP) utilizzando il `security login duo show` comando.

### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Mostrare la configurazione di Cisco Duo per questa VM di storage. In alternativa, è possibile utilizzare `vserver` Parametro per specificare una VM di storage, sostituendo il nome della VM di storage con `<STORAGE_VM_NAME>`:

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

L'output dovrebbe essere simile a quanto segue:



```
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: -
```

## Creare un gruppo Duo

È possibile richiedere a Cisco Duo di includere solo gli utenti di un determinato Active Directory, LDAP o gruppo di utenti locali nel processo di autenticazione Duo. Se si crea un gruppo Duo, viene richiesta l'autenticazione Duo solo agli utenti del gruppo. È possibile creare un gruppo Duo utilizzando `security login duo group create` comando. Quando si crea un gruppo, è possibile escludere dal processo di autenticazione Duo utenti specifici di tale gruppo.

### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Creare il gruppo Duo, sostituendo le informazioni del proprio ambiente ai valori tra parentesi. Se si omette `-vserver` il gruppo viene creato a livello di cluster:

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

Il nome del gruppo Duo deve corrispondere a un gruppo Active Directory, LDAP o locale. Gli utenti specificati con l'opzione `-exclude-users` Il parametro non verrà incluso nel processo di autenticazione Duo.

## Visualizza i gruppi Duo

È possibile visualizzare le voci di gruppo Cisco Duo esistenti utilizzando `security login duo group show` comando.

### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Mostrare le voci del gruppo Duo, sostituendo le informazioni dell'ambiente con i valori tra parentesi. Se si omette `-vserver` il gruppo viene visualizzato a livello del cluster:

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

Il nome del gruppo Duo deve corrispondere a un gruppo Active Directory, LDAP o locale. Gli utenti specificati con l'opzione `-exclude-users` il parametro non viene visualizzato.

## Rimuovere un gruppo Duo

È possibile rimuovere una voce di gruppo Duo utilizzando `security login duo group delete` comando. Se si rimuove un gruppo, gli utenti del gruppo non saranno più inclusi nel processo di autenticazione Duo.

### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Rimuovere la voce del gruppo Duo, sostituendo le informazioni presenti nell'ambiente in uso con i valori tra parentesi. Se si omette `-vserver` il gruppo viene rimosso a livello di cluster:

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

Il nome del gruppo Duo deve corrispondere a un gruppo Active Directory, LDAP o locale.

## Ignora autenticazione Duo per gli utenti

È possibile escludere tutti gli utenti o utenti specifici dal processo di autenticazione SSH Duo.

### Escludere tutti gli utenti Duo

È possibile disattivare l'autenticazione SSH di Cisco Duo per tutti gli utenti.

### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Disattiva l'autenticazione Cisco Duo per gli utenti SSH, sostituendo il nome del Vserver con `<STORAGE_VM_NAME>`:

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

### Escludere gli utenti del gruppo Duo

È possibile escludere alcuni utenti che fanno parte di un gruppo Duo dal processo di autenticazione SSH Duo.

### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Disattivare l'autenticazione Cisco Duo per utenti specifici di un gruppo. Sostituire il nome del gruppo e l'elenco degli utenti da escludere per i valori tra parentesi:

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

Il nome del gruppo Duo deve corrispondere a un gruppo Active Directory, LDAP o locale. Utenti specificati con `-exclude-users` Il parametro non verrà incluso nel processo di autenticazione Duo.

### Escludere gli utenti Duo locali

È possibile escludere utenti locali specifici dall'uso dell'autenticazione Duo utilizzando il pannello di amministrazione di Cisco Duo. Per istruzioni, fare riferimento a. ["Documentazione di Cisco Duo"](#).

## Generare e installare una panoramica del certificato server firmato dalla CA

Nei sistemi di produzione, è consigliabile installare un certificato digitale con firma CA da utilizzare per l'autenticazione del cluster o SVM come server SSL. È possibile utilizzare `security certificate generate-csr` Per generare una richiesta di firma del certificato (CSR) e il `security certificate install` per installare il certificato ricevuto dall'autorità di certificazione.

### Generare una richiesta di firma del certificato

È possibile utilizzare `security certificate generate-csr` Comando per generare una richiesta di firma del certificato (CSR). Una volta elaborata la richiesta, l'autorità di certificazione (CA) invia il certificato digitale firmato.

#### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

#### Fasi

##### 1. Generare 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
```

Il seguente comando crea una CSR con una chiave privata a 2048 bit generata dalla funzione di hash "SHA256" per l'utilizzo da parte del gruppo "Software" nel reparto "IT" di una società il cui nome comune personalizzato è "server1.companyname.com", con sede a Sunnyvale, California, USA. L'indirizzo e-mail dell'amministratore del contatto della SVM è "[web@example.com](mailto:web@example.com)". Il sistema visualizza la CSR e la chiave privata nell'output.

## Esempio di creazione di 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-----

```
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCVVMx  
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G  
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS  
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi  
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBcWUAA0EA6EagLfso5+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. Copiare la richiesta di certificato dall'output CSR e inviarla in formato elettronico (ad esempio tramite e-mail) a una CA di terze parti attendibile per la firma.

Una volta elaborata la richiesta, la CA invia il certificato digitale firmato. Conservare una copia della chiave privata e del certificato digitale firmato dalla CA.

## Installare un certificato server firmato dalla CA

È possibile utilizzare `security certificate install` Comando per installare un certificato server firmato da CA su una SVM. ONTAP richiede i certificati principali e intermedi dell'autorità di certificazione (CA) che formano la catena di certificati del certificato del server.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

## Fase

1. Installare un certificato server firmato dalla CA:

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

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).



ONTAP richiede i certificati CA principali e intermedi che formano la catena di certificati del certificato del server. La catena inizia con il certificato della CA che ha emesso il certificato del server e può arrivare fino al certificato root della CA. Eventuali certificati intermedi mancanti causano un errore nell'installazione del certificato del server.

Il seguente comando installa il certificato del server firmato dalla CA e i certificati intermedi su SVM `"engData2"`.

## Esempio di installazione di certificati intermedi di un certificato server con firma CA

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTAADEJMAcGA1UECzMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTAADEJMAcGA1UECzM
AMQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAAkEAYXrK2sry
-----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
bGlDZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECzMOR28gRGFkZkhkgQ2xhc3MgMiBDZXJ0
-----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-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACGTG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEzhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDtk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACGTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
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.

## Gestire i certificati con System Manager

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per gestire autorità di certificazione attendibili, certificati client/server e autorità di certificazione locali (integrate).

Con System Manager, è possibile gestire i certificati ricevuti da altre applicazioni in modo da autenticare le comunicazioni da tali applicazioni. È inoltre possibile gestire i propri certificati che identificano il sistema in altre applicazioni.

### Visualizzare le informazioni sul certificato

System Manager consente di visualizzare le autorità di certificazione attendibili, i certificati client/server e le autorità di certificazione locali memorizzati nel cluster.

#### Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Scorrere fino all'area **Security** (sicurezza). Nella sezione **certificati** vengono visualizzati i seguenti dettagli:
  - Il numero di autorità di certificazione attendibili memorizzate.
  - Il numero di certificati client/server memorizzati.
  - Il numero di autorità di certificazione locali memorizzate.
3. Selezionare un numero qualsiasi per visualizzare i dettagli relativi a una categoria di certificati oppure scegliere ➔ Consente di aprire la pagina **certificati**, che contiene informazioni su tutte le categorie. L'elenco visualizza le informazioni relative all'intero cluster. Se si desidera visualizzare le informazioni solo per una specifica macchina virtuale di storage, attenersi alla seguente procedura:
  - a. Selezionare **Storage > Storage VM**.

- b. Selezionare la VM di storage.
- c. Passare alla scheda **Impostazioni**.
- d. Selezionare un numero visualizzato nella sezione **certificato**.

#### Cosa fare in seguito

- Dalla pagina **certificati**, è possibile [Generare una richiesta di firma del certificato](#).
- Le informazioni sul certificato sono suddivise in tre schede, una per ciascuna categoria. È possibile eseguire le seguenti attività da ciascuna scheda:

In questa scheda...	È possibile eseguire queste procedure...
<b>Autorità di certificazione attendibili</b>	<ul style="list-style-type: none"> <li>• <a href="#">[install-trusted-cert]</a></li> <li>• <a href="#">Eliminare un'autorità di certificazione attendibile</a></li> <li>• <a href="#">Rinnovare un'autorità di certificazione attendibile</a></li> </ul>
<b>Certificati client/server</b>	<ul style="list-style-type: none"> <li>• <a href="#">[install-cs-cert]</a></li> <li>• <a href="#">[gen-cs-cert]</a></li> <li>• <a href="#">[delete-cs-cert]</a></li> <li>• <a href="#">[renew-cs-cert]</a></li> </ul>
<b>Autorità locali di certificazione</b>	<ul style="list-style-type: none"> <li>• <a href="#">Creare una nuova autorità di certificazione locale</a></li> <li>• <a href="#">Firmare un certificato utilizzando un'autorità di certificazione locale</a></li> <li>• <a href="#">Eliminare un'autorità di certificazione locale</a></li> <li>• <a href="#">Rinnovare un'autorità di certificazione locale</a></li> </ul>

## Generare una richiesta di firma del certificato

È possibile generare una richiesta di firma del certificato (CSR) con System Manager da qualsiasi scheda della pagina **certificati**. Vengono generate una chiave privata e una CSR corrispondente, che possono essere firmate utilizzando un'autorità di certificazione per generare un certificato pubblico.

#### Fasi

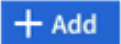
1. Visualizzare la pagina **certificati**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare **+genera CSR**.
3. Inserire le informazioni relative al nome del soggetto:
  - a. Immettere un **nome comune**.
  - b. Selezionare un **paese**.
  - c. Inserire un'organizzazione \*.
  - d. Inserire un'unità organizzativa\*.
4. Se si desidera ignorare le impostazioni predefinite, selezionare **altre opzioni** e fornire ulteriori informazioni.



## Installare (aggiungere) un'autorità di certificazione attendibile

È possibile installare altre autorità di certificazione attendibili in System Manager.

### Fasi

1. Visualizzare la scheda **autorità di certificazione attendibili**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare  **Add**.
3. Nella finestra **Aggiungi autorità di certificazione attendibile**, eseguire le seguenti operazioni:
  - Immettere un **nome**.
  - Per il campo **scope**, selezionare una VM di storage.
  - Immettere un **nome comune**.
  - Selezionare un **tipo**.
  - Immettere o importare **dati del certificato**.


## Eliminare un'autorità di certificazione attendibile

System Manager consente di eliminare un'autorità di certificazione attendibile.



Non è possibile eliminare le autorità di certificazione attendibili preinstallate con ONTAP.


### Fasi

1. Visualizzare la scheda **autorità di certificazione attendibili**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome dell'autorità di certificazione attendibile.
3. Selezionare  Accanto al nome, selezionare **Elimina**.

## Rinnovare un'autorità di certificazione attendibile

System Manager consente di rinnovare un'autorità di certificazione attendibile scaduta o in scadenza.

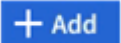
### Fasi

1. Visualizzare la scheda **autorità di certificazione attendibili**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome dell'autorità di certificazione attendibile.
3. Selezionare  Accanto al nome del certificato, quindi **Rinnova**.

## Installare (aggiungere) un certificato client/server

Con System Manager, è possibile installare certificati client/server aggiuntivi.

### Fasi

1. Visualizzare la scheda **certificati client/server**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare  **Add**.
3. Nel pannello **Aggiungi certificato client/server**, eseguire le seguenti operazioni:

- Immettere un **nome del certificato**.
- Per il campo **scope**, selezionare una VM di storage.
- Immettere un **nome comune**.
- Selezionare un **tipo**.
- Immettere o importare **dati del certificato**. È possibile scrivere o copiare e incollare i dettagli del certificato da un file di testo oppure importare il testo da un file di certificato facendo clic su **Importa**.
- Immettere la **chiave privata**.  
È possibile scrivere o copiare e incollare la chiave privata da un file di testo oppure importare il testo da un file di chiave privata facendo clic su **Importa**.

## Generare (aggiungere) un certificato client/server autofirmato

Con System Manager, è possibile generare certificati client/server autofirmati aggiuntivi.


### Fasi

1. Visualizzare la scheda **certificati client/server**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare **+genera certificato autofirmato**.
3. Nel pannello **genera certificato autofirmato**, eseguire le seguenti operazioni:
  - Immettere un **nome del certificato**.
  - Per il campo **scope**, selezionare una VM di storage.
  - Immettere un **nome comune**.
  - Selezionare un **tipo**.
  - Selezionare una funzione **hash**.
  - Selezionare una **dimensione chiave**.
  - Selezionare una **VM di storage**.

## Eliminare un certificato client/server

Con System Manager, è possibile eliminare i certificati client/server.


### Fasi

1. Visualizzare la scheda **certificati client/server**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome del certificato client/server.
3. Selezionare  Accanto al nome, quindi fare clic su **Delete** (Elimina).

## Rinnovare un certificato client/server

System Manager consente di rinnovare un certificato client/server scaduto o in scadenza.

### Fasi

1. Visualizzare la scheda **certificati client/server**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome del certificato client/server.
3. Selezionare  Accanto al nome, quindi fare clic su **Rinnova**.

## Creare una nuova autorità di certificazione locale

Con System Manager, è possibile creare una nuova autorità di certificazione locale.


### Fasi

1. Visualizzare la scheda **autorità locali dei certificati**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare  **Add**.
3. Nel pannello **Add Local Certificate Authority** (Aggiungi autorità di certificazione locale), eseguire le seguenti operazioni:
  - Immettere un **nome**.
  - Per il campo **scope**, selezionare una VM di storage.
  - Immettere un **nome comune**.
4. Se si desidera ignorare le impostazioni predefinite, selezionare **altre opzioni** e fornire ulteriori informazioni.

## Firmare un certificato utilizzando un'autorità di certificazione locale

In System Manager, è possibile utilizzare un'autorità di certificazione locale per firmare un certificato.


### Fasi

1. Visualizzare la scheda **autorità locali dei certificati**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome dell'autorità di certificazione locale.
3. Selezionare  Accanto al nome, quindi **Firma un certificato**.
4. Compilare il modulo **Sign a Certificate Signing Request** (Firma una richiesta di firma certificato).
  - È possibile incollare il contenuto della firma del certificato o importare un file di richiesta della firma del certificato facendo clic su **Importa**.
  - Specificare il numero di giorni per i quali il certificato sarà valido.

## Eliminare un'autorità di certificazione locale

Con System Manager, è possibile eliminare un'autorità di certificazione locale.


### Fasi

1. Visualizzare la scheda **autorità di certificazione locale**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome dell'autorità di certificazione locale.
3. Selezionare  Accanto al nome, quindi **Elimina**.

## Rinnovare un'autorità di certificazione locale

Con System Manager, è possibile rinnovare un'autorità di certificazione locale scaduta o in scadenza.

### Fasi

1. Visualizzare la scheda **autorità di certificazione locale**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome dell'autorità di certificazione locale.
3. Selezionare  Accanto al nome, quindi fare clic su **Rinnova**.

# Panoramica sull'accesso al controller di dominio di Active Directory

È necessario configurare l'accesso del controller di dominio ad al cluster o alla SVM prima che un account ad possa accedere alla SVM. Se è già stato configurato un server SMB per una SVM di dati, è possibile configurare la SVM come gateway, o *tunnel*, per l'accesso ad al cluster. Se non è stato configurato un server SMB, è possibile creare un account di computer per SVM nel dominio ad.

ONTAP supporta i seguenti servizi di autenticazione dei controller di dominio:

- Kerberos
- LDAP
- Netlogon
- Autorità di sicurezza locale (LSA)

ONTAP supporta i seguenti algoritmi delle chiavi di sessione per connessioni di accesso alla rete sicure:

Algoritmo della chiave di sessione	Disponibile a partire da...
HMAC-SHA256, basato su Advanced Encryption Standard (AES)  Se il cluster esegue ONTAP 9.9.1 o versione precedente e il controller di dominio applica AES per i servizi di Netlogon protetti, la connessione non riesce. In questo caso, è necessario riconfigurare il controller di dominio per accettare connessioni con chiave forte con ONTAP.	ONTAP 9.10.1
DES e HMAC-MD5 (quando è impostato il tasto forte)	Tutte le release di ONTAP 9

Se si desidera utilizzare le chiavi di sessione AES durante la creazione del canale protetto Netlogon, è necessario verificare che AES sia attivato nella SVM.

- A partire da ONTAP 9.14.1, l'AES viene attivato per impostazione predefinita quando si crea una SVM e non è necessario modificare le impostazioni di sicurezza della SVM per utilizzare le chiavi di sessione AES durante la creazione del canale protetto Netlogon.
- Negli ONTAP da 9.10.1 a 9.13.1, quando si crea una SVM, il sistema AES è disattivato per impostazione predefinita. È necessario attivare AES utilizzando il seguente comando:

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



L'upgrade a ONTAP 9.14.1 o versione successiva non cambia automaticamente le impostazioni AES per le SVM esistenti create con le release precedenti di ONTAP. È comunque necessario aggiornare il valore di questa impostazione per attivare AES su queste SVM.

## Configurare un tunnel di autenticazione

Se è già stato configurato un server SMB per una SVM dati, è possibile utilizzare `security login domain-tunnel create` Comando per configurare la SVM come gateway, o *tunnel*, per l'accesso ad al cluster.

### Prima di iniziare

- È necessario aver configurato un server SMB per una SVM dati.
- Per accedere alla SVM amministrativa per il cluster, è necessario aver attivato un account utente di dominio ad.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

A partire da ONTAP 9.10.1, se si dispone di un gateway SVM (tunnel di dominio) per l'accesso ad, è possibile utilizzare Kerberos per l'autenticazione dell'amministratore se NTLM è stato disattivato nel dominio ad. Nelle versioni precedenti, Kerberos non era supportato con l'autenticazione admin per i gateway SVM. Questa funzionalità è disponibile per impostazione predefinita; non è richiesta alcuna configurazione.



L'autenticazione Kerberos viene sempre tentata per prima. In caso di errore, viene quindi tentata l'autenticazione NTLM.

### Fase

1. Configurare una SVM di dati abilitata per SMB come tunnel di autenticazione per l'accesso del controller di dominio ad al cluster:

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

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).



Affinché l'utente possa essere autenticato, SVM deve essere in esecuzione.

Il seguente comando configura la SVM dei dati con abilitazione SMB `engData` come tunnel di autenticazione.

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

## Creare un account di computer SVM sul dominio

Se non è stato configurato un server SMB per una SVM dati, è possibile utilizzare `vserver active-directory create` Per creare un account di computer per la SVM nel dominio.

### A proposito di questa attività

Dopo aver inserito `vserver active-directory create` Viene richiesto di fornire le credenziali per un account utente ad con privilegi sufficienti per aggiungere computer all'unità organizzativa specificata nel dominio. La password dell'account non può essere vuota.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fase

## 1. Creare un account di computer per una SVM nel dominio ad:

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

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

Il seguente comando crea un account di computer denominato "ADSERVER1" nel dominio "example.com" per SVM "engData". Dopo aver immesso il comando, viene richiesto di immettere le credenziali dell'account utente ad.

```
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:

## Configurare la panoramica dell'accesso al server LDAP o NIS

È necessario configurare l'accesso al server LDAP o NIS a una SVM prima che gli account LDAP o NIS possano accedere alla SVM. La funzione di switch consente di utilizzare LDAP o NIS come origini alternative del servizio di nomi.

### Configurare l'accesso al server LDAP

È necessario configurare l'accesso del server LDAP a una SVM prima che gli account LDAP possano accedere alla SVM. È possibile utilizzare `vserver services name-service ldap client create` Per creare una configurazione del client LDAP su SVM. È quindi possibile utilizzare `vserver services name-service ldap create` Comando per associare la configurazione del client LDAP a SVM.

#### A proposito di questa attività

La maggior parte dei server LDAP può utilizzare gli schemi predefiniti forniti da ONTAP:

- MS-ad-BIS (lo schema preferito per la maggior parte dei server ad Windows 2012 e successivi)
- AD-IDMU (server AD Windows 2008, Windows 2016 e versioni successive)
- AD-SFU (server ad Windows 2003 e precedenti)
- RFC-2307 (SERVER LDAP UNIX)

Si consiglia di utilizzare gli schemi predefiniti, a meno che non vi sia un requisito diverso. In tal caso, è possibile creare uno schema personalizzato copiando uno schema predefinito e modificando la copia. Per

ulteriori informazioni, consulta:

- ["Configurazione NFS"](#)
- ["Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"](#)

### Prima di iniziare

- È necessario aver installato un ["Certificato digitale del server firmato CA"](#) Su SVM.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fasi

1. Creare una configurazione del client LDAP su 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 è supportato solo per l'accesso ai dati SVM. Non è supportato per l'accesso alle SVM amministrative.

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

Il seguente comando crea una configurazione del client LDAP denominata "corp" su SVM "engData". Il client crea un'associazione anonima ai server LDAP con gli indirizzi IP 172.160.0.100 e 172.16.0.101. Il client utilizza lo schema RFC-2307 per eseguire query LDAP. La comunicazione tra il client e il server viene crittografata 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 partire da ONTAP 9.2, il campo `-ldap-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server LDAP.

2. Associare la configurazione del client LDAP a SVM: 

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

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

Il seguente comando associa la configurazione del client LDAP corp Con SVM `engData` E attiva il client LDAP su SVM.

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



A partire da ONTAP 9.2, la `vserver services name-service ldap create` il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non è in grado di contattare il server dei nomi.

3. Convalidare lo stato dei server dei nomi utilizzando il comando di controllo `ldap name-service` dei servizi `vserver`.

Il seguente comando convalida i server LDAP su 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". |
```

Il comando `name service check` è disponibile a partire da ONTAP 9.2.

## Configurare l'accesso al server NIS

È necessario configurare l'accesso del server NIS a una SVM prima che gli account NIS possano accedere alla SVM. È possibile utilizzare `vserver services name-service nis-domain create` Per creare una configurazione di dominio NIS su una SVM.

### A proposito di questa attività

È possibile creare più domini NIS. È possibile impostare un solo dominio NIS su `active` alla volta.

### Prima di iniziare

- Tutti i server configurati devono essere disponibili e accessibili prima di configurare il dominio NIS sulla SVM.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fase

1. Creare una configurazione di dominio NIS su una SVM:

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

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).



A partire da ONTAP 9.2, il campo `-nis-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server NIS.

Il seguente comando crea una configurazione di dominio NIS su SVM `"engData"`. Il dominio NIS `nisdomain` È attivo alla creazione e comunica con un server NIS con l'indirizzo 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
```

## Creare un name service switch

La funzione di switch del name service consente di utilizzare LDAP o NIS come origini alternative del name service. È possibile utilizzare `vserver services name-service ns-switch modify` per specificare l'ordine di ricerca delle origini del servizio nome.

### Prima di iniziare

- È necessario aver configurato l'accesso al server LDAP e NIS.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fase

1. Specificare l'ordine di ricerca per le origini del servizio nome:

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

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

Il seguente comando specifica l'ordine di ricerca delle origini del servizio nomi LDAP e NIS per il database "passwd" su SVM "engData".

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

## Modificare la password dell'amministratore

È necessario modificare la password iniziale subito dopo aver effettuato l'accesso al sistema per la prima volta. Gli amministratori di SVM possono utilizzare `security login password` per modificare la password. Gli amministratori del cluster possono utilizzare `security login password` per modificare la password dell'amministratore.

### A proposito di questa attività

La nuova password deve rispettare le seguenti regole:

- Non può contenere il nome utente
- La lunghezza deve essere di almeno otto caratteri
- Deve contenere almeno una lettera e un numero
- Non può essere uguale alle ultime sei password



È possibile utilizzare `security login role config modify` comando per modificare le regole delle password per gli account associati a un determinato ruolo. Per ulteriori informazioni, consultare "[riferimento al comando](#)".

#### Prima di iniziare

- Per modificare la password, è necessario essere un amministratore del cluster o di SVM.
- Per modificare la password di un altro amministratore, è necessario essere un amministratore del cluster.

#### Fase

1. Modifica della password di amministratore: `security login password -vserver svm_name -username user_name`

Il seguente comando modifica la password dell'amministratore `admin1` Per SVM `vs1.example.com`. Viene richiesto di inserire la password corrente, quindi di inserire e immettere nuovamente la nuova password.

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

## Bloccare e sbloccare un account amministratore

È possibile utilizzare `security login lock` per bloccare un account amministratore e il `security login unlock` per sbloccare l'account.

#### Prima di iniziare

Per eseguire queste attività, è necessario essere un amministratore del cluster.

#### Fasi

1. Blocco di un account amministratore:

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

Il seguente comando blocca l'account amministratore `admin1` Per SVM `vs1.example.com`:

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

2. Sbloccare un account amministratore:

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

Il seguente comando sblocca l'account amministratore `admin1` Per SVM `vs1.example.com`:

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

## Gestire i tentativi di accesso non riusciti

Tentativi ripetuti di accesso non riusciti indicano talvolta che un intruso sta tentando di accedere al sistema di storage. È possibile eseguire una serie di operazioni per evitare l'intrusione.

### Come saprai che i tentativi di accesso non sono riusciti

Il sistema di gestione degli eventi (EMS) notifica ogni ora i tentativi di accesso non riusciti. È possibile trovare un record dei tentativi di accesso non riusciti in `audit.log` file.

### Cosa fare se i tentativi di accesso ripetuti non riescono

A breve termine, è possibile adottare una serie di misure per prevenire un'intrusione:

- Richiedere che le password siano composte da un numero minimo di caratteri maiuscoli, minuscoli, caratteri speciali e/o cifre
- Imporre un ritardo dopo un tentativo di accesso non riuscito
- Limitare il numero di tentativi di accesso non riusciti consentiti e bloccare gli utenti dopo il numero specificato di tentativi non riusciti
- Scade e blocca gli account inattivi per un determinato numero di giorni

È possibile utilizzare `security login role config modify` per eseguire queste attività.

A lungo termine, è possibile eseguire le seguenti operazioni aggiuntive:

- Utilizzare `security ssh modify` Comando per limitare il numero di tentativi di accesso non riusciti per tutte le SVM appena create.
- Migrare gli account dell'algoritmo MD5 esistenti sull'algoritmo SHA-512 più sicuro richiedendo agli utenti di modificare le password.

## Applicare SHA-2 sulle password dell'account amministratore

Gli account amministratore creati prima di ONTAP 9.0 continuano a utilizzare le password MD5 dopo l'aggiornamento, fino a quando le password non vengono modificate manualmente. MD5 è meno sicuro di SHA-2. Pertanto, dopo l'aggiornamento, è necessario richiedere agli utenti degli account MD5 di modificare le password per utilizzare la funzione hash SHA-512 predefinita.

### A proposito di questa attività

La funzionalità di hash delle password consente di effettuare le seguenti operazioni:

- Visualizza gli account utente che corrispondono alla funzione hash specificata.

- Gli account con scadenza che utilizzano una funzione hash specificata (ad esempio MD5), costringendo gli utenti a modificare le password nel successivo accesso.
- Bloccare gli account le cui password utilizzano la funzione hash specificata.
- Quando si torna a una release precedente a ONTAP 9, reimpostare la password dell'amministratore del cluster affinché sia compatibile con la funzione hash (MD5) supportata dalla release precedente.

ONTAP accetta password SHA-2 pre-hash solo utilizzando l'SDK di gestione NetApp (`security-login-create` e `security-login-modify-password`).

## Fasi

### 1. Migrare gli account amministratore MD5 alla funzione hash della password SHA-512:

- a. Scadenza di tutti gli account amministratore MD5: `security login expire-password -vserver * -username * -hash-function md5`

In questo modo, gli utenti degli account MD5 devono modificare le password al successivo accesso.

- b. Chiedere agli utenti degli account MD5 di effettuare l'accesso tramite una console o una sessione SSH.

Il sistema rileva che gli account sono scaduti e richiede agli utenti di modificare le password. SHA-512 viene utilizzato per impostazione predefinita per le password modificate.

### 2. Per gli account MD5 i cui utenti non effettuano l'accesso per modificare le password entro un determinato periodo di tempo, forzare la migrazione dell'account:


- a. Bloccare gli account che utilizzano ancora la funzione hash MD5 (livello di privilegio avanzato):  
`security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

Dopo il numero di giorni specificato da `-lock-after`, Gli utenti non possono accedere ai propri account MD5.

- b. Sbloccare gli account quando gli utenti sono pronti a modificare le proprie password: `security login unlock -vserver svm_name -username user_name`
- c. Chiedere agli utenti di accedere ai propri account tramite una console o una sessione SSH e modificare le password quando richiesto dal sistema.

## Diagnosticare e correggere i problemi di accesso ai file

## Fasi

1. In System Manager, selezionare **Storage > Storage VM**.
2. Selezionare la VM di storage su cui si desidera eseguire una traccia.
3. Fare clic su  **Altro**.
4. Fare clic su **accesso al file di traccia**.
5. Fornire il nome utente e l'indirizzo IP del client, quindi fare clic su **Avvia traccia**.

I risultati della traccia vengono visualizzati in una tabella. La colonna **motivi** indica il motivo per cui non è stato possibile accedere a un file.

6. Fare clic su  nella colonna sinistra della tabella dei risultati per visualizzare le autorizzazioni di accesso

al file.

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.