Creare account di accesso

ONTAP 9

NetApp
February 12, 2026

Sommario

Creare account di accesso

Ulteriori informazioni sulla creazione di account di accesso ONTAP

È possibile attivare gli account di amministratore SVM e cluster locali o remoti. Un account locale è un account in cui le informazioni sull'account, la chiave pubblica o il certificato di protezione risiedono nel sistema di storage. Le informazioni sull'account AD vengono memorizzate in un controller di dominio. Gli account LDAP e NIS risiedono sui server LDAP e NIS.

Amministratori di cluster e SVM

Un *amministratore del cluster* accede alla SVM amministrativa per il cluster. La SVM amministrativa e un amministratore del cluster con il nome riservato `admin` vengono creati automaticamente quando viene configurato il cluster.

Un amministratore del cluster con l'impostazione predefinita `admin` il ruolo può amministrare l'intero cluster e le relative risorse. L'amministratore del cluster può creare ulteriori amministratori del cluster con ruoli diversi in base alle esigenze.

Un *amministratore SVM* accede a una SVM di dati. L'amministratore del cluster crea gli amministratori SVM e SVM dei dati in base alle necessità.

Agli amministratori di SVM viene assegnato il `vsadmin` ruolo per impostazione predefinita. L'amministratore del cluster può assegnare ruoli diversi agli amministratori SVM in base alle esigenze.

Convenzioni di naming

I seguenti nomi generici non possono essere utilizzati per gli account di amministratori di cluster remoti e SVM:

- "adm"
- "contenitore"
- "cli"
- "demone"
- "ftp"
- "giochi"
- "arresta"
- "lp"
- "e-mail"
- "uomo"
- "naroot"
- "NetApp"
- "notizie"
- "nessuno"

- "operatore"
- "radice"
- "arresto"
- "sshd"
- "sincronizza"
- "sis"
- "uucp"
- "www"

Ruoli Uniti

Se si abilitano più account remoti per lo stesso utente, all'utente viene assegnata l'Unione di tutti i ruoli specificati per gli account. Ovvero, se viene assegnato un account LDAP o NIS `vsadmin` E all'account di gruppo ad per lo stesso utente viene assegnato il `vsadmin-volume` Ruolo, l'utente ad effettua l'accesso con il più inclusivo `vsadmin` funzionalità. Si dice che i ruoli siano *merged*.

Abilitare l'accesso all'account locale

Ulteriori informazioni sull'attivazione dell'accesso all'account ONTAP locale

Un account locale è un account in cui le informazioni sull'account, la chiave pubblica o il certificato di protezione risiedono nel sistema di storage. Puoi utilizzare `security login create` il comando per abilitare gli account locali per l'accesso a un amministratore o a una SVM dati.

Informazioni correlate

- "creazione dell'accesso di sicurezza"

Attiva l'accesso alla password dell'account ONTAP

Puoi utilizzare `security login create` il comando per abilitare gli account amministratore per l'accesso a una SVM di amministrazione o dati con una password. La password viene richiesta dopo aver immesso il comando.

A proposito di questa attività

Se non si è certi del ruolo di controllo dell'accesso che si desidera assegnare all'account di accesso, è possibile utilizzare il `security login modify` comando per aggiungere il ruolo in un secondo momento.

Ulteriori informazioni su `security login modify` nella "Riferimento al comando ONTAP".

Prima di iniziare

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

Fase

1. Abilitare gli account dell'amministratore locale per accedere a una SVM utilizzando una password:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`*

`-application application -authmethod authentication_method -role role -comment comment`

Il seguente comando attiva l'account amministratore del cluster `admin1` con il predefinito `backup` Ruolo di accesso alla SVM amministrativa`engCluster` utilizzo di una password. La password viene richiesta dopo aver immesso il comando.

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

Ulteriori informazioni su `security login create` nella "Riferimento al comando ONTAP".

Attiva l'accesso a chiave pubblica SSH dell'account ONTAP

Puoi utilizzare `security login create` il comando per abilitare gli account amministratore per l'accesso a una SVM di amministrazione o dati con una chiave pubblica SSH.

A proposito di questa attività

- Prima che l'account possa accedere a SVM, è necessario associare la chiave pubblica all'account.

  Associazione di una chiave pubblica a un account utente

  È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- Se non si è certi del ruolo di controllo dell'accesso che si desidera assegnare all'account di accesso, è possibile utilizzare il `security login modify` comando per aggiungere il ruolo in un secondo momento.

  Ulteriori informazioni su `security login modify` nella "Riferimento al comando ONTAP".

Se si desidera attivare la modalità FIPS sul cluster, gli account a chiave pubblica SSH esistenti senza gli algoritmi a chiave supportati devono essere riconfigurati con un tipo di chiave supportato. Gli account devono essere riconfigurati prima di attivare FIPS, altrimenti l'autenticazione dell'amministratore non avrà esito positivo.

La seguente tabella indica gli algoritmi del tipo di chiave host supportati per le connessioni SSH ONTAP. Questi tipi di chiave non si applicano alla configurazione dell'autenticazione pubblica SSH.

Release di ONTAP	Tipi di chiave supportati in modalità FIPS	Tipi di chiave supportati in modalità non FIPS
9.11.1 e versioni successive	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 e versioni precedenti	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + ssh-rsa

Il supporto per l'algoritmo della chiave host ssh-ed25519 viene rimosso a partire da ONTAP 9.11.1.

Per ulteriori informazioni, vedere "Configurare la sicurezza di rete utilizzando FIPS".

Prima di iniziare

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

Fase

1. Abilitare gli account dell'amministratore locale per accedere a una SVM utilizzando una chiave pubblica SSH:

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

   Il seguente comando attiva l'account amministratore SVM `svmadmin1` con il predefinito `vsadmin-volume` Ruolo per accedere a SVM`engData1` Utilizzando una chiave pubblica SSH:

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

   Ulteriori informazioni su `security login create` nella "Riferimento al comando ONTAP".

Al termine

Se non è stata associata una chiave pubblica all'account amministratore, è necessario farlo prima che l'account possa accedere a SVM.

Associazione di una chiave pubblica a un account utente

Abilitare gli account MFA (Multiple Factor Authentication)

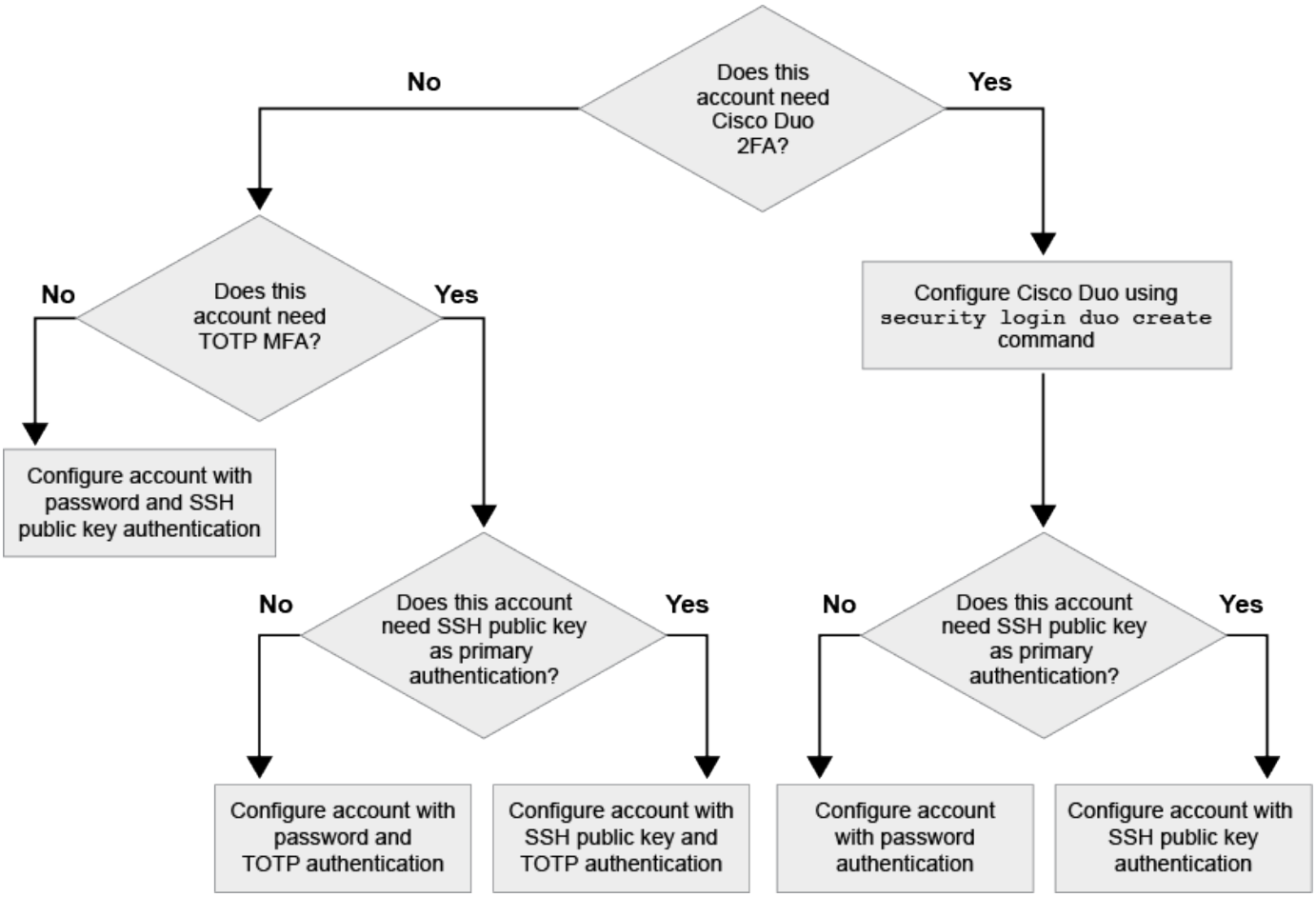
Ulteriori informazioni sull'autenticazione a più fattori ONTAP

La Multifactor Authentication (MFA) consente di migliorare la sicurezza richiedendo agli utenti di fornire due metodi di autenticazione per l'accesso a una VM di amministrazione o per lo storage dei dati.

A seconda della versione di ONTAP in uso, è possibile utilizzare una combinazione di chiave pubblica SSH, una password utente e una password monouso (TOTP) basata sul tempo per l'autenticazione multifattore. Quando si attiva e si configura Cisco Duo (ONTAP 9.14.1 e versioni successive), questo metodo funge da metodo di autenticazione aggiuntivo, che integra i metodi esistenti per tutti gli utenti.

Disponibile a partire da…	Primo metodo di autenticazione	Secondo metodo di autenticazione
ONTAP 9.14.1	Chiave pubblica SSH	TTP
	User Password (Password utente)	TTP
	Chiave pubblica SSH	Cisco Duo
	Password utente	Cisco Duo
ONTAP 9.13.1	Chiave pubblica SSH	TTP
	Password utente	TTP
ONTAP 9.3	Chiave pubblica SSH	Password utente

Se MFA è configurato, l'amministratore del cluster deve prima abilitare l'account utente locale, quindi l'account deve essere configurato dall'utente locale.



Abilita l'autenticazione a più fattori ONTAP con SSH e TOTP

L'autenticazione a più fattori (MFA) consente di migliorare la sicurezza richiedendo agli utenti di fornire due metodi di autenticazione per accedere a un'SVM amministrativa o di dati.

A proposito di questa attività

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Se non si è certi del ruolo di controllo dell'accesso che si desidera assegnare all'account di accesso, è possibile utilizzare il `security login modify` comando per aggiungere il ruolo in un secondo momento.

  Ulteriori informazioni su `security login modify` nella "Riferimento al comando ONTAP".

  "Modifica del ruolo assegnato a un amministratore"

- Se si utilizza una chiave pubblica per l'autenticazione, è necessario associare la chiave pubblica all'account prima che l'account possa accedere a SVM.

  "Associare una chiave pubblica a un account utente"

  È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- A partire da ONTAP 9.12.1, è possibile utilizzare i dispositivi di autenticazione hardware di Yubikey per l'autenticazione MFA del client SSH utilizzando gli standard di autenticazione FIDO2 (Fast Identity Online) o Personal Identity Verification (PIV).

Abilitare MFA con chiave pubblica SSH e password utente

A partire da ONTAP 9.3, un amministratore del cluster può configurare account utente locali per l'accesso con MFA utilizzando una chiave pubblica SSH e una password utente.

1. Abilitare MFA sull'account utente locale con chiave pubblica SSH e password utente:

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

   Il seguente comando richiede l'account amministratore SVM `admin2` con il predefinito `admin` Ruolo di accesso a SVM`engData1` Con una chiave pubblica SSH e una password utente:

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

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

   Ulteriori informazioni su `security login create` nella "Riferimento al comando ONTAP".

Abilitare MFA con TOTP

A partire da ONTAP 9.13.1, è possibile migliorare la sicurezza richiedendo agli utenti locali di accedere a un server di amministrazione o a una SVM di dati con una chiave pubblica SSH o una password utente e una

password monouso (TOTP) basata sul tempo. Una volta abilitato l'account MFA con TOTP, l'utente locale deve effettuare l'accesso a. "completare la configurazione".

TOTP è un algoritmo per computer che utilizza l'ora corrente per generare una password monouso. Se si utilizza il protocollo TOTP, si tratta sempre della seconda forma di autenticazione dopo la chiave pubblica SSH o la password dell'utente.

Prima di iniziare

Per eseguire queste attività, è necessario essere un amministratore dello storage.

Fasi

È possibile impostare MFA su con una password utente o una chiave pubblica SSH come primo metodo di autenticazione e TOTP come secondo metodo di autenticazione.

Abilitare MFA con password utente e TOTP

1. Abilitare un account utente per l'autenticazione a più fattori con una password utente e TOTP.

   Per nuovi account utente

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

   Per gli account utente esistenti

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

2. Verificare che MFA con TOTP sia attivato:

   ```
   security login show
   ```

Abilitare MFA con chiave pubblica SSH e TOTP

1. Abilitare un account utente per l'autenticazione a più fattori con una chiave pubblica SSH e TOTP.

   Per nuovi account utente

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

   Per gli account utente esistenti

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

   Ulteriori informazioni su `security login modify` nella "Riferimento al comando ONTAP".

2. Verificare che MFA con TOTP sia attivato:

```
security login show
```

Ulteriori informazioni su `security login show` nella "Riferimento al comando ONTAP".

Al termine

- Se non è stata associata una chiave pubblica all'account amministratore, è necessario farlo prima che l'account possa accedere a SVM.

  "Associazione di una chiave pubblica a un account utente"

- L'utente locale deve effettuare l'accesso per completare la configurazione MFA con TOTP.

  "Configurare l'account utente locale per MFA con TOTP"

Informazioni correlate

- "Autenticazione multifattore in ONTAP 9 (TR-4647)"
- "Riferimento al comando ONTAP"

Configurare gli account utente ONTAP locali per MFA con TOTP

A partire da ONTAP 9.13.1, gli account utente possono essere configurati con Multifactor Authentication (MFA) utilizzando una password monouso basata sul tempo (TOTP).

Prima di iniziare

- L'amministratore dello storage deve "Abilitare MFA con TOTP" come secondo metodo di autenticazione per l'account utente.
- Il metodo di autenticazione dell'account utente principale deve essere una password utente o una chiave SSH pubblica.
- È necessario configurare l'applicazione TOTP per il funzionamento con lo smartphone e creare la chiave segreta TOTP.

  Sono supportati Microsoft Authenticator, Google Authenticator, Authy e qualsiasi altro autenticatore compatibile con TOTP.

Fasi

1. Accedere all'account utente con il metodo di autenticazione corrente.

   Il metodo di autenticazione corrente deve essere una password utente o una chiave pubblica SSH.

2. Creare la configurazione TOTP sull'account:

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

3. Verificare che la configurazione TOTP sia attivata sull'account:

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

Informazioni correlate

- "creazione di accesso di sicurezza tottop"
- "accesso di sicurezza tottop show"

Reimpostare la chiave segreta TOTP per un account utente ONTAP

Per proteggere la sicurezza del tuo account, se la tua chiave segreta TOTP viene compromessa o persa, devi disattivarla e crearne una nuova.

Reimpostare il TOTP se la chiave viene compromessa

Se la chiave segreta TOTP è compromessa, ma si dispone ancora dell'accesso, è possibile rimuovere la chiave compromessa e crearne una nuova.

1. Accedere all'account utente con la password utente o la chiave pubblica SSH e la chiave segreta TOTP compromessa.
2. Rimuovere la chiave segreta TOTP compromessa:

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

3. Creare una nuova chiave segreta TOTP:

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

4. Verificare che la configurazione TOTP sia attivata sull'account:

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

Ripristinare il TOTP se la chiave viene persa

Se la chiave segreta TOTP viene persa, contattare l'amministratore dello storage per "disattivare la chiave". Una volta disattivata la chiave, è possibile utilizzare il primo metodo di autenticazione per accedere e configurare un nuovo TOTP.

Prima di iniziare

La chiave segreta TOTP deve essere disattivata da un amministratore dello storage. Se non si dispone di un account amministratore dello storage, contattare l'amministratore dello storage per disattivare la chiave.

Fasi

1. Una volta disattivato il segreto TOTP da un amministratore dello storage, utilizzare il metodo di autenticazione principale per accedere all'account locale.
2. Creare una nuova chiave segreta TOTP:

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

3. Verificare che la configurazione TOTP sia attivata sull'account:

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

Informazioni correlate

- "creazione di accesso di sicurezza tottop"
- "accesso di sicurezza tottop elimina"
- "accesso di sicurezza tottop show"

Disattivare la chiave segreta TOTP per un account utente ONTAP

Se la chiave segreta TOTP (Time-Based One-Time Password) di un utente locale viene persa, la chiave persa deve essere disattivata da un amministratore dello storage prima che l'utente possa creare una nuova chiave segreta TOTP.

A proposito di questa attività

Questa attività può essere eseguita solo da un account amministratore del cluster.

Fase

1. Disattivare la chiave segreta TOTP:

```
security login totp modify -vserver <svm_name> -username
<account_username> -enabled false
```

Ulteriori informazioni su `security login totp modify` nella "Riferimento al comando ONTAP".

Attiva l'accesso all'account ONTAP del certificato SSL

Puoi utilizzare `security login create` il comando per abilitare gli account amministratore ad accedere a una SVM di amministrazione o dati con un certificato SSL.

A proposito di questa attività

- È necessario installare un certificato digitale del server firmato dalla CA prima che l'account possa accedere alla SVM.

Creazione e installazione di un certificato server firmato dalla CA

È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- Se non si è sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile aggiungerlo successivamente con `security login modify` comando.

  Modifica del ruolo assegnato a un amministratore

> Per gli account degli amministratori del cluster, l'autenticazione del certificato è supportata con `http`, `ontapi`, e. `rest` applicazioni. Per gli account amministratore SVM, l'autenticazione del certificato è supportata solo con `ontapi` e. `rest` applicazioni.

Fase

1. Abilitare gli account dell'amministratore locale per accedere a una SVM utilizzando un certificato SSL:

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

   Il seguente comando attiva l'account amministratore SVM `svmadmin2` con l'impostazione predefinita `vsadmin` Ruolo per accedere a SVM`engData2` Utilizzando un certificato digitale SSL.

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

   Ulteriori informazioni su `security login create` nella "Riferimento al comando ONTAP".

Al termine

Se non è stato installato un certificato digitale del server firmato dalla CA, è necessario farlo prima che l'account possa accedere alla SVM.

Creazione e installazione di un certificato server firmato dalla CA

Per ulteriori informazioni sui comandi descritti in questa procedura, consultare la "Riferimento al comando ONTAP".

Abilitare l'accesso all'account ONTAP di Active Directory

Puoi utilizzare `security login create` il comando per abilitare account di utenti o gruppi di Active Directory (ad) per l'accesso a un'SVM di amministrazione o dati. Qualsiasi utente del gruppo ad può accedere a SVM con il ruolo assegnato al gruppo.

A proposito di questa attività

- È necessario configurare l'accesso del controller di dominio ad al cluster o alla SVM prima che l'account possa accedere alla SVM.

  Configurazione dell'accesso al controller di dominio Active Directory

È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- A partire da ONTAP 9.13.1, è possibile utilizzare una chiave pubblica SSH come metodo di autenticazione primario o secondario con una password utente ad.

  Se si sceglie di utilizzare una chiave pubblica SSH come autenticazione principale, non viene eseguita alcuna autenticazione ad.

- A partire da ONTAP 9.11.1, è possibile utilizzare "Utilizzare il fast bind LDAP per l'autenticazione nsswitch per le SVM ONTAP NFS" se è supportato dal server LDAP ad.
- Se non si è certi del ruolo di controllo dell'accesso che si desidera assegnare all'account di accesso, è possibile utilizzare il `security login modify` comando per aggiungere il ruolo in un secondo momento.

  Ulteriori informazioni su `security login modify` nella "Riferimento al comando ONTAP".

  Modifica del ruolo assegnato a un amministratore

> L'accesso all'account DEL GRUPPO DI ANNUNCI è supportato solo con `SSH`, `ontapi`, e. `rest` applicazioni. I gruppi DI ANNUNCI NON sono supportati con l'autenticazione a chiave pubblica SSH, comunemente utilizzata per l'autenticazione a più fattori.

Prima di iniziare

- Il tempo del cluster deve essere sincronizzato entro cinque minuti dal tempo sul controller di dominio ad.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fase

1. Abilitare gli account amministratore di gruppo o utente ad per accedere a una SVM:

   Per utenti ad:

Versione di ONTAP	Autenticazione primaria	Autenticazione secondaria	Comando
9.13.1 e versioni successive	Chiave pubblica	Nessuno	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

Versione di ONTAP	Autenticazione primaria	Autenticazione secondaria	Comando

9.13.1 e versioni successive	Dominio	Chiave pubblica	**Per un nuovo utente**
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			Per un utente esistente
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0 e versioni successive	Dominio	Nessuno	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

Per gruppi ad:

Versione di ONTAP	Autenticazione primaria	Autenticazione secondaria	Comando
9.0 e versioni successive	Dominio	Nessuno	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

Al termine

Se non è stato configurato l'accesso del controller di dominio ad al cluster o alla SVM, è necessario farlo prima che l'account possa accedere alla SVM.

Configurazione dell'accesso al controller di dominio Active Directory

Informazioni correlate

- "creazione dell'accesso di sicurezza"

Attiva l'accesso all'account LDAP o NIS ONTAP

Puoi utilizzare `security login create` il comando per abilitare gli account utente LDAP o NIS per l'accesso a un amministratore o a una SVM dati. Se non è stato configurato l'accesso al server LDAP o NIS alla SVM, è necessario farlo prima che l'account possa accedere alla SVM.

A proposito di questa attività

- Gli account di gruppo non sono supportati.
- È necessario configurare l'accesso al server LDAP o NIS alla SVM prima che l'account possa accedere alla SVM.

  Configurazione dell'accesso al server LDAP o NIS

  È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- Se non si è certi del ruolo di controllo dell'accesso che si desidera assegnare all'account di accesso, è possibile utilizzare il `security login modify` comando per aggiungere il ruolo in un secondo momento.

  Ulteriori informazioni su `security login modify` nella "Riferimento al comando ONTAP".

  Modifica del ruolo assegnato a un amministratore

- A partire da ONTAP 9.4, l'autenticazione multifattore (MFA) è supportata per gli utenti remoti su server LDAP o NIS.
- A partire da ONTAP 9.11.1, è possibile utilizzare "Utilizzare il fast bind LDAP per l'autenticazione nsswitch per le SVM ONTAP NFS" se è supportato dal server LDAP.
- A causa di un problema LDAP noto, non utilizzare `':'` (Due punti) carattere in qualsiasi campo delle informazioni dell'account utente LDAP (ad esempio, `gecos`, `userPassword`e così via). In caso contrario, l'operazione di ricerca non riuscirà per quell'utente.

Prima di iniziare

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

Fasi

1. Abilitare gli account utente o gruppo LDAP o NIS per accedere a una SVM:

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

"Creazione o modifica degli account di accesso"

Il seguente comando attiva l'account amministratore del cluster LDAP o NIS `guest2` con il predefinito `backup` Ruolo di accesso alla SVM amministrativa`engCluster`.

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

Ulteriori informazioni su `security login create` nella "Riferimento al comando ONTAP".

2. Abilitare l'accesso MFA per gli utenti LDAP o NIS:

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

Il metodo di autenticazione può essere specificato come `publickey` e secondo metodo di autenticazione as `nsswitch`.

L'esempio seguente mostra l'attivazione dell'autenticazione MFA:

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

Al termine

Se non è stato configurato l'accesso al server LDAP o NIS alla SVM, è necessario farlo prima che l'account possa accedere alla SVM.

Configurazione dell'accesso al server LDAP o NIS

Informazioni correlate

- "accesso di sicurezza"

Informazioni sul copyright

Informazioni sul marchio commerciale